G-3000 Series

802.11b/g Wireless Access Point

User's Guide

Version 3.60
10/2006
Edition 1

ZyXEL
www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. A basic knowledge of TCP/IP networking concepts and topology will be helpful but is not necessary.

This User’s Guide covers configuration of the G-3000 and G-3000H. Screens and menus for the G-3000 are shown. Screens and menus in the G-3000 may differ slightly. See your device’s Quick Start Guide for instructions on how to make hardware connections.

Related Documentation

- Quick Start Guide

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

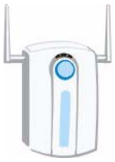
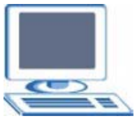
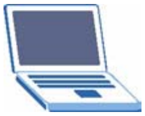
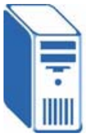
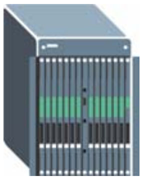
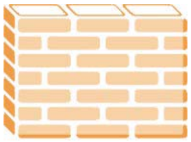
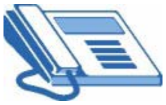
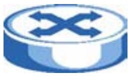
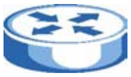
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The G-3000 or G-3000H may be referred to as the "ZyXEL Device", the "device", the "product" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance** > **Log** > **Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

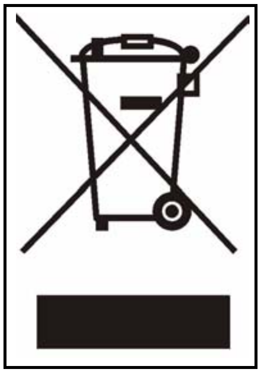
ZyXEL Device 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Safety Warnings

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.
- ONLY qualified service personnel should service or disassemble this device.
- 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 it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

This product is recyclable. Dispose of it properly.



Contents Overview

Table of Contents

List of Figures

List of Tables

PART I
Introduction

1

Introducing the ZyXEL Device

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

1.1 Introducing the ZyXEL Device

Your ZyXEL Device extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

It is highly versatile, supporting up to eight ESSIDs simultaneously. The Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

Multiple security profiles allow you to easily assign different types of security to groups of users. The ZyXEL Device controls network access with MAC address filtering and layer 2 isolation. It also provides a high level of network traffic security, supporting IEEE 802.1x, Wi-Fi Protected Access (WPA), WPA2 and WEP data encryption.

Your ZyXEL Device is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance.

1.2 Applications for the ZyXEL Device

The ZyXEL Device can be configured to use the following WLAN operating modes

1. AP
2. AP+Bridge
3. Bridge/Repeater
4. MESSID

Applications for each operating mode are shown below.

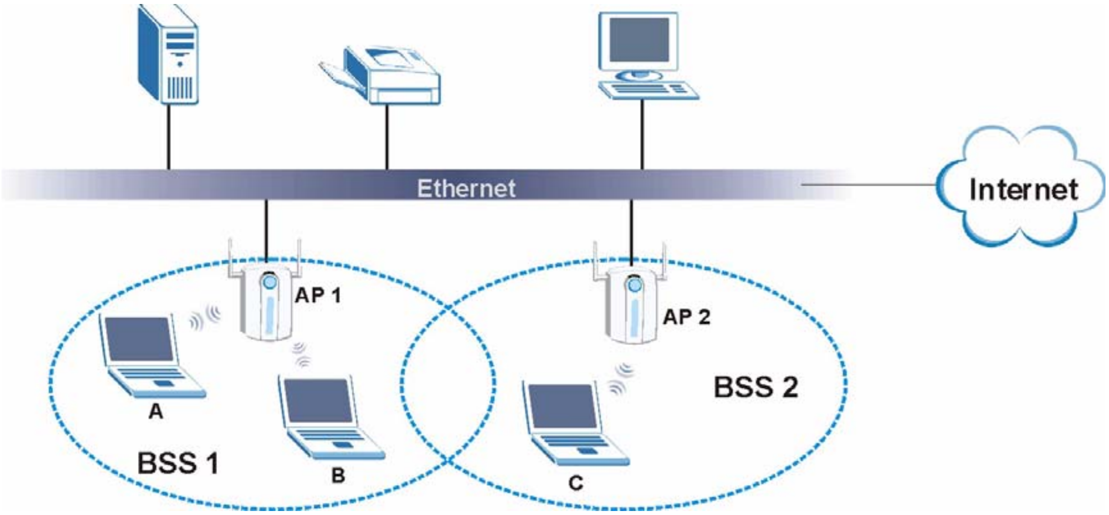
The G-3000 also has an extension slot where you can add a second WLAN card. With two WLAN cards, the G-3000 can be set up with two different wireless configurations. For example, one card could function as a bridge/repeater and the other card could be in MESSID mode to support up to eight ESSIDs.

A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

1.2.1 Access Point

The ZyXEL Device is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyXEL Device is shown as follows. Stations A, B and C can access the wired network through the ZyXEL Devices.

Figure 1 Access Point Application



1.2.2 Bridge / Repeater

The ZyXEL Device can act as a wireless network bridge and establish wireless links with other APs. In the figure below, the two ZyXEL Devices (**A** and **B**) are connected to independent wired networks and have a bridge connection (**A** can communicate with **B**) at the same time. A ZyXEL Device in repeater mode (**C**) has no Ethernet connection. When the ZyXEL Device is in bridge mode, you should enable STP to prevent bridge loops.

When the ZyXEL Device is in **Bridge / Repeater** mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. When WDS security is enabled, both APs must use the same pre-shared key. See Section 6.6.2 on page 81 for more details.

Once the security settings of the two APs match one another, the WDS connection is made.

If you do not enable WDS security in **Bridge / Repeater** mode, traffic between APs is not encrypted.

Figure 2 Bridge Application

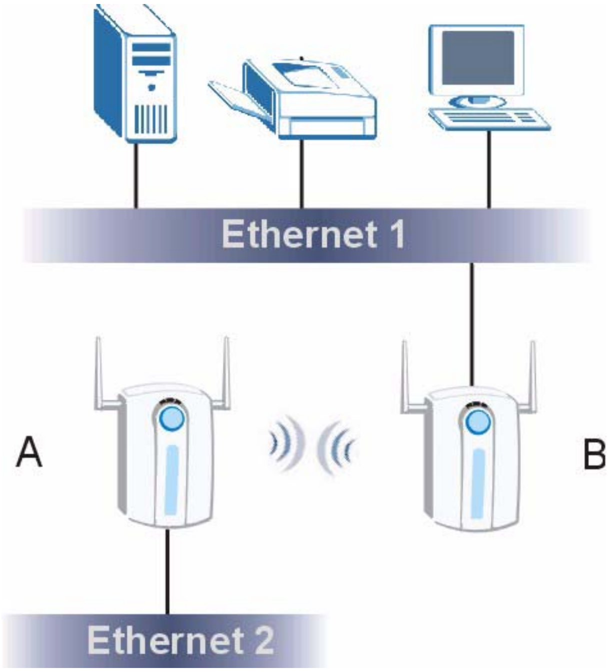
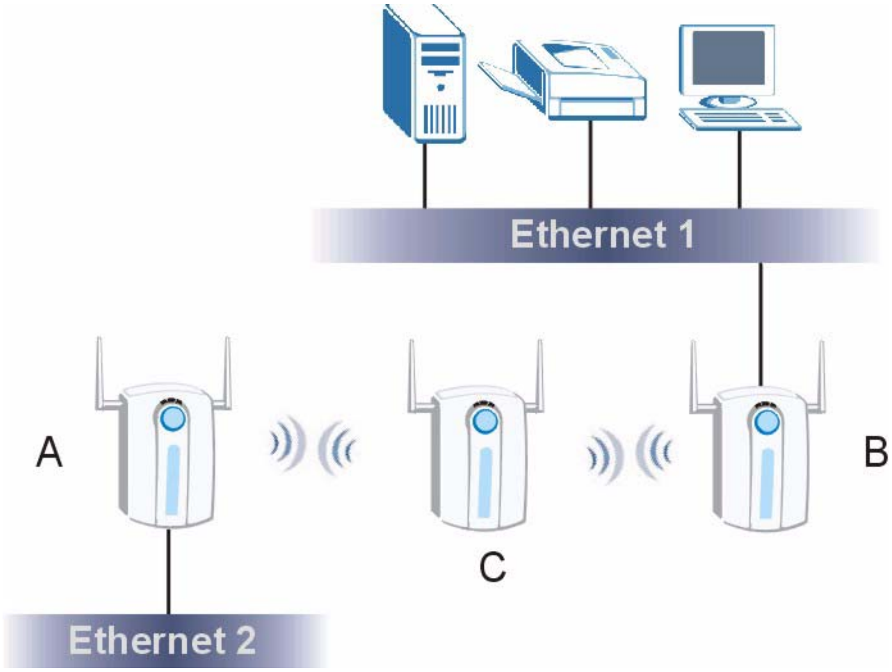


Figure 3 Repeater Application



1.2.3 AP + Bridge

In **AP+Bridge** mode, the ZyXEL Device supports both AP and bridge connection at the same time.

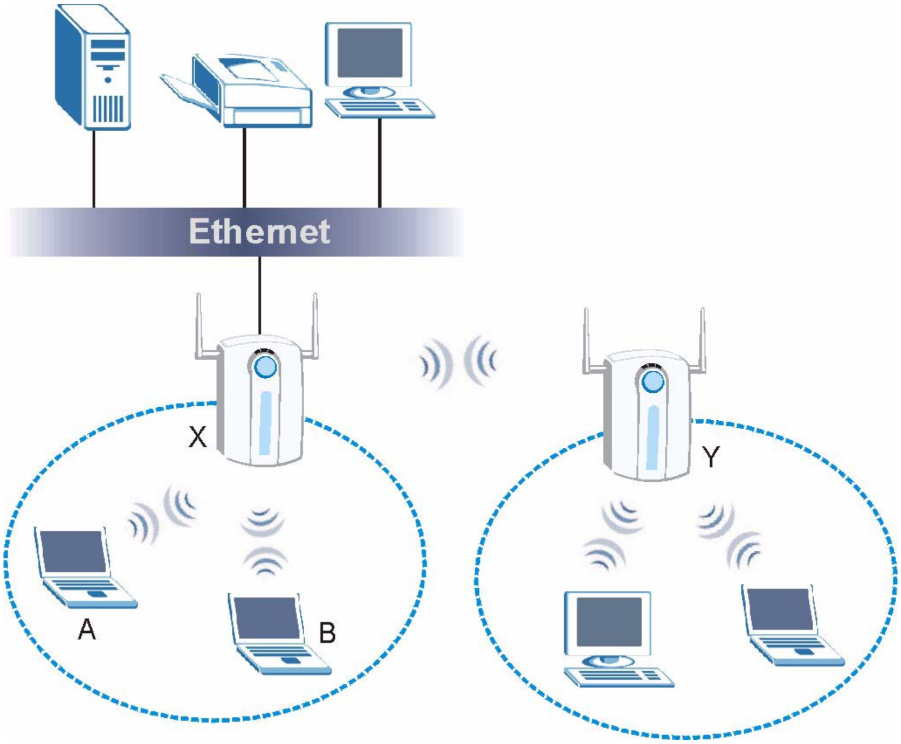
In the figure below, **A** and **B** use **X** as an **AP** to access the wired network, while **X** and **Y** communicate in bridge mode.

When the ZyXEL Device is in **AP+Bridge** mode, you must use security for both the AP and bridge functions, or for neither. However, the security the ZyXEL Device uses between APs (the Wireless Distribution System or WDS) is different from the security between the wireless stations and the AP. See Chapter 6 on page 73 and Chapter 7 on page 87 for more details.

Unless specified, the term "security settings" refers to the traffic between the wireless stations and the ZyXEL Device.

If you do not configure security in **AP+Bridge** mode, traffic between the wireless stations and the APs and traffic between the APs is not encrypted.

Figure 4 AP+Bridge Application

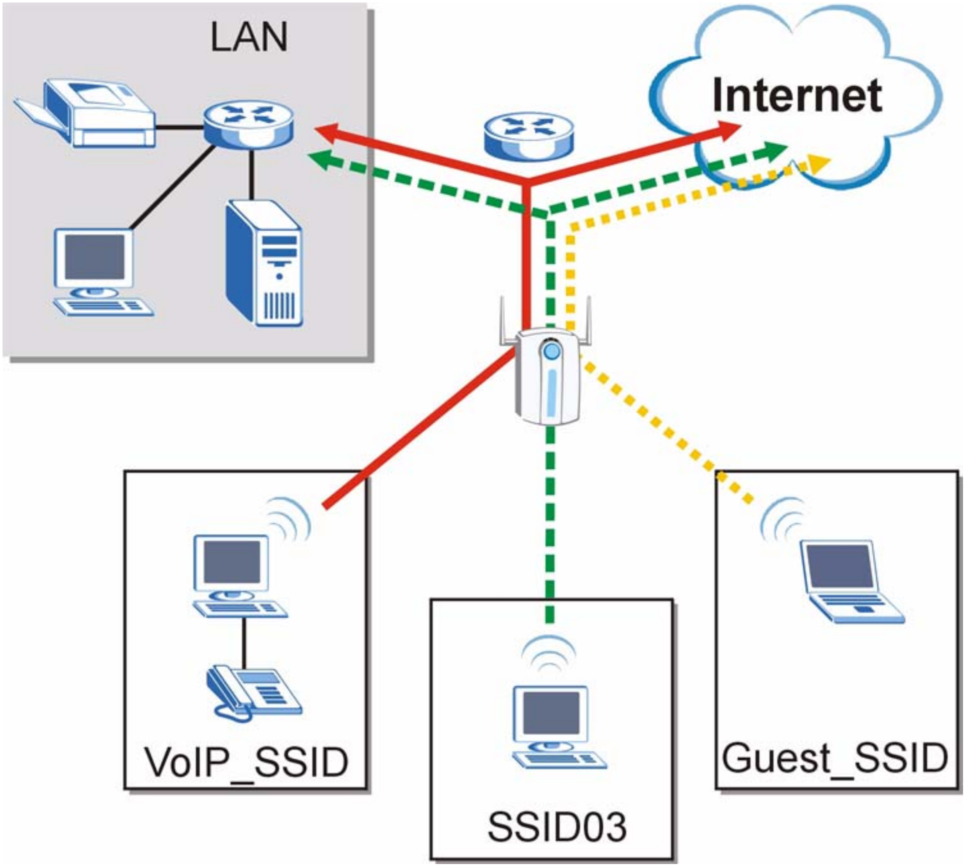


1.2.4 MESSID (Multiple Extended Service Set IDentifier)

MESSID allows one access point to provide several ESSs simultaneously. It basically allows the ZyXEL Device to provide several wireless networks with different wireless and security settings. You can then assign varying levels of privilege to different wireless clients based on the SSIDs they use.

For example, you might want to set up a wireless network in your office where Internet telephony (Voice over IP, or VoIP) users have priority. You also want a regular wireless network for standard users, as well as a ‘guest’ wireless network for visitors. In the following figure, **VoIP_SSID** users have Quality of Service (QoS) priority, **SSID03** is the wireless network for standard users, and **Guest_SSID** is the wireless network for guest users. In this example, the guest user is forbidden access to the wired LAN behind the AP and can access only the Internet.

Figure 5   Multiple BSSs



1.3 Ways to Manage the ZyXEL Device

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

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device. Use Telnet to access the SMT.
- FTP for firmware upgrades and configuration backup and restore.

- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.4 Good Habits for Managing the ZyXEL Device

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

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

2

Introducing the Web Configurator

This chapter describes how to access the ZyXEL Device’s web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyXEL Device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

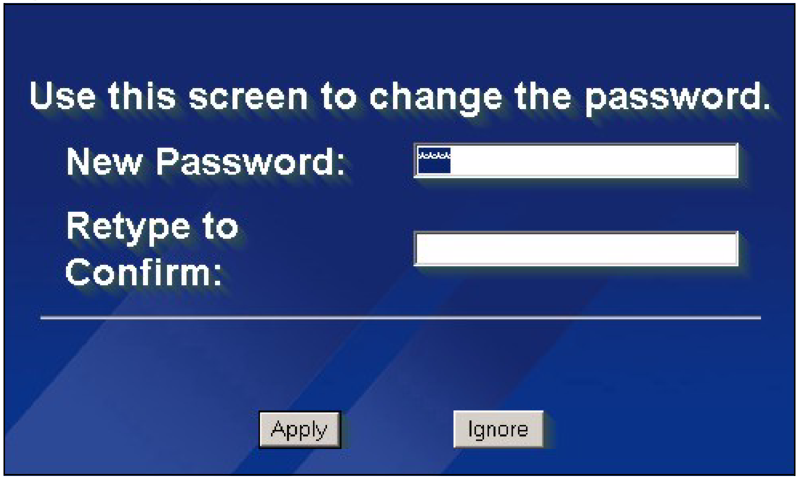
See Appendix F on page 309 if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

2.2 Accessing the Web Configurator

1. Make sure your hardware is properly connected and prepare your computer or computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.2" as the URL (default).
4. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
5. You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) then click **Apply**. Alternatively, click **Ignore**.

If you do not change the password, the following screen appears every time you login.

Figure 6 Change Password Screen



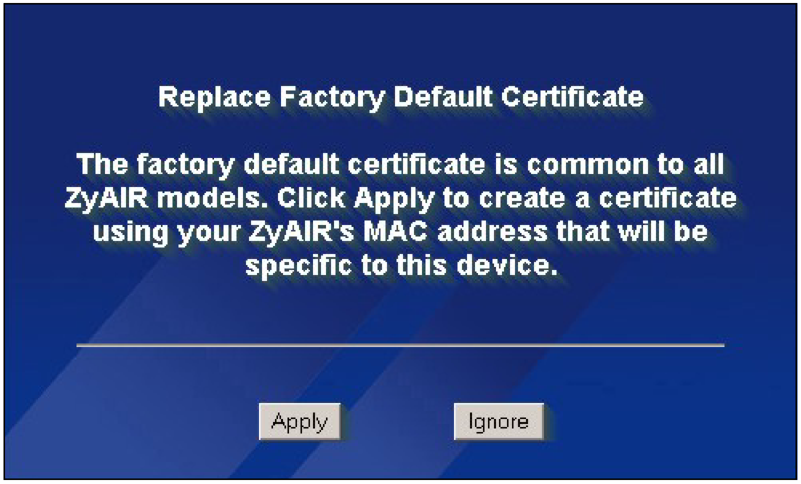
Use this screen to change the password.

New Password:

Retype to Confirm:

6 Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device.

Figure 7 Replace Certificate Screen



Replace Factory Default Certificate

The factory default certificate is common to all ZyAIR models. Click Apply to create a certificate using your ZyAIR's MAC address that will be specific to this device.

You should now see the **MAIN MENU** screen.

The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the ZyXEL Device if this happens.

2.3 Resetting the ZyXEL Device

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button. This replaces the current configuration file with the factory-default configuration file. This means that you will lose all the settings you previously configured. The password will be reset to 1234.

2.3.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in three ways:

Use the **RESET** button to upload the default configuration file. Hold this button in for about 10 seconds (the lights will begin to blink). Use this method for cases when the password or IP address of the ZyXEL Device is not known.

Use the web configurator to restore defaults (refer to Chapter 16 on page 189).

Transfer the configuration file to your ZyXEL Device using FTP. See the section on SMT configuration for more information.

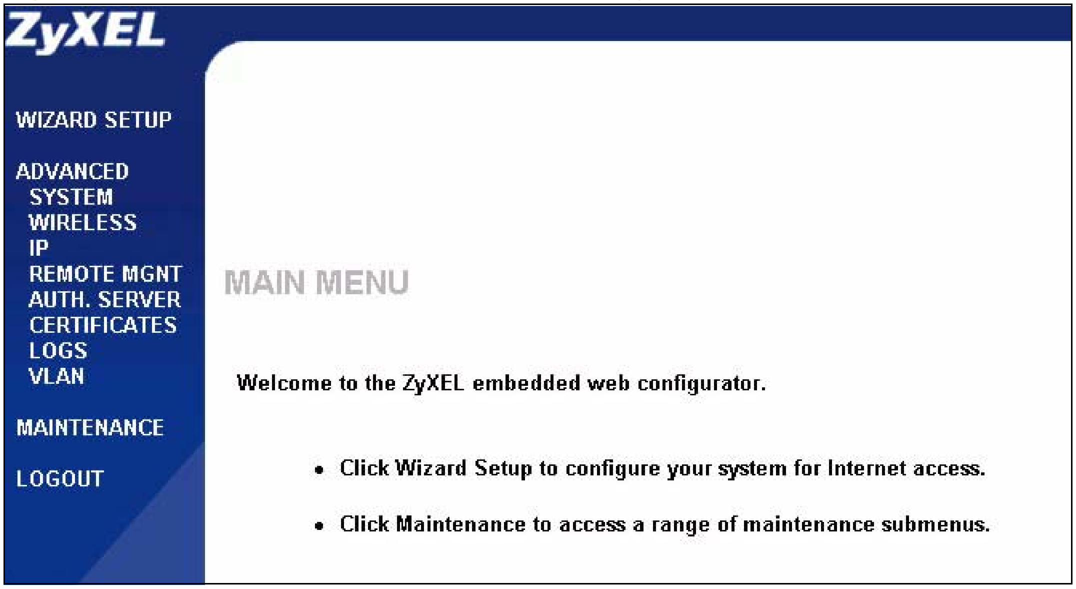
2.4 Navigating the Web Configurator

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

Click **LOGOUT** at any time to exit the web configurator.

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

Figure 8 The MAIN MENU Screen of the Web Configurator



MAIN MENU

Welcome to the ZyXEL embedded web configurator.

- Click Wizard Setup to configure your system for Internet access.
- Click Maintenance to access a range of maintenance submenus.

Click **WIZARD SETUP** for initial configuration including general setup, Wireless LAN setup and IP address assignment.

Click the links under **ADVANCED** to configure advanced features such as **SYSTEM** (**General Setup**, **Password** and **Time Zone**), **WIRELESS** (**Wireless**, **SSID, Security**, **RADIUS**, **Layer-2 Isolation**, **MAC Filter**, **Roaming** and **Local User Database**), **IP**, **REMOTE MGNT** (**Telnet**, **FTP**, **WWW** and **SNMP**), **AUTH SERVER** (not available on all models) (**Settings**, **Trusted AP** and **Trusted User)**, **CERTIFICATES** (**My Certificates**, **Trusted CAs**), **LOGS** (**View Log** and **Log Settings**) and **VLAN**.

Click **MAINTENANCE** to view information about your ZyXEL Device or upgrade configuration/firmware files. Maintenance includes **Status** (Statistics), **Association List**, **Channel Usage**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore and Default) and **Restart**.

Click **LOGOUT** at any time to exit the web configurator

3

Wizard Setup

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

3.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your ZyXEL Device for wireless stations to access your wired LAN. The wizard applies configuration settings to the ZyXEL Device's built-in wireless card by default, even if you have installed another card.

3.1.1 Channel

A channel is the radio frequency(ies) used by IEEE 802.11b and IEEE 802.11g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

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

The ZyXEL Device's "Scan" function is especially designed to automatically scan for a channel with the least interference.

3.1.2 ESS ID

An Extended Service Set (ESS) is a group of access points connected to a wired LAN on the same subnet. An SS ID uniquely identifies each set. All access points and their associated wireless stations in the same set must have the same SSID.

3.1.3 WEP Encryption

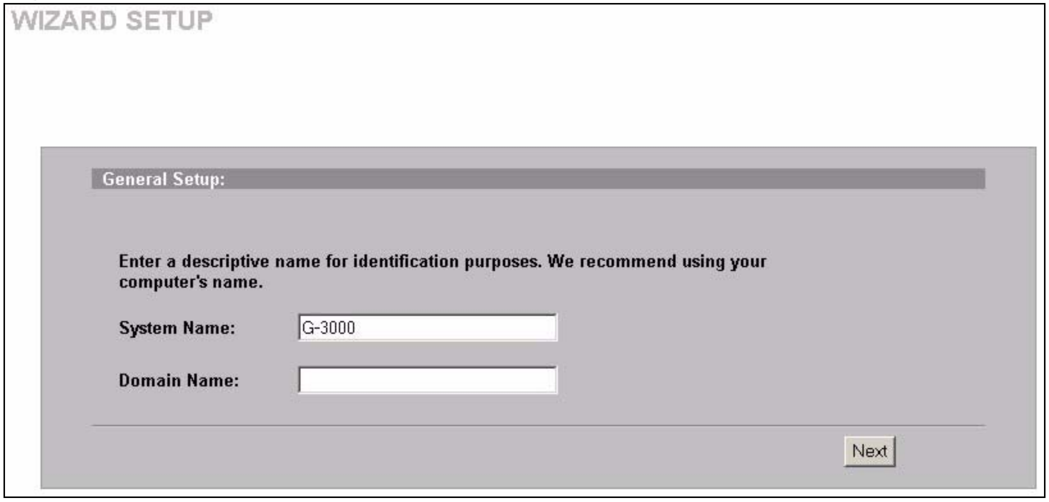
WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

3.2 Wizard Setup: General Setup

General Setup contains administrative and system-related information.

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

Figure 9 Wizard 1 : General Setup



Enter a descriptive name for identification purposes. We recommend using your computer's name.

System Name: G-3000

Domain Name:

The following table describes the labels in this screen.

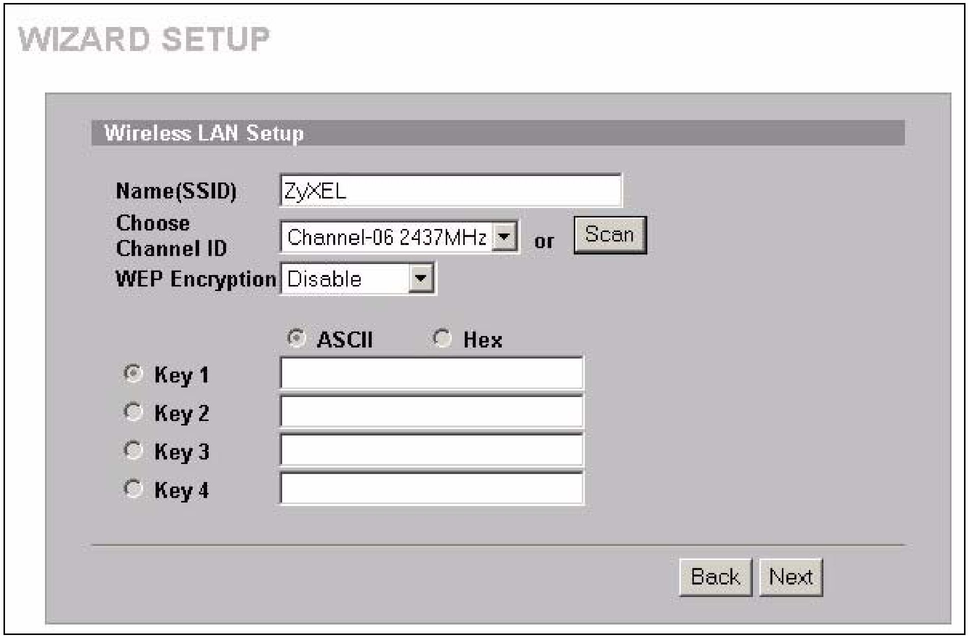
Table 1 Wizard 1 : General Setup

LABEL	DESCRIPTION
System Name	It is recommended you type your computer's "Computer name". In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**. In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**. In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.
Next	Click **Next** to proceed to the next screen.

3.3 Wizard Setup: Wireless LAN

Use the second wizard screen to set up the wireless LAN.

Figure 10 Wizard 2 : Wireless LAN Setup



WIZARD SETUP

Wireless LAN Setup

Name(SSID): ZyXEL

Choose Channel ID: Channel-06 2437MHz or Scan

WEP Encryption: Disable

● ASCII ○ Hex

● Key 1

○ Key 2

○ Key 3

○ Key 4

The following table describes the labels in this screen.

Table 2 Wizard 2 : Wireless LAN Setup

LABEL	DESCRIPTION
Wireless LAN Setup	
Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyXEL Device, make sure all wireless stations use the same Name (SSID) in order to access the network.
Choose Channel ID	To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyXEL Device automatically select a channel, click **Scan** instead.
Scan	Click this button to have the ZyXEL Device automatically scan for and select a channel with the least interference.
WEP Encryption	Select **Disable** allows all wireless computers to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding 0x is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the 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"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.

Table 2 Wizard 2 : Wireless LAN Setup

LABEL	DESCRIPTION
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.4 Wizard Setup: IP Address

The third wizard screen allows you to configure IP address assignment.

3.4.1 IP Address Assignment

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

Table 3 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

3.4.2 IP Address and Subnet Mask

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

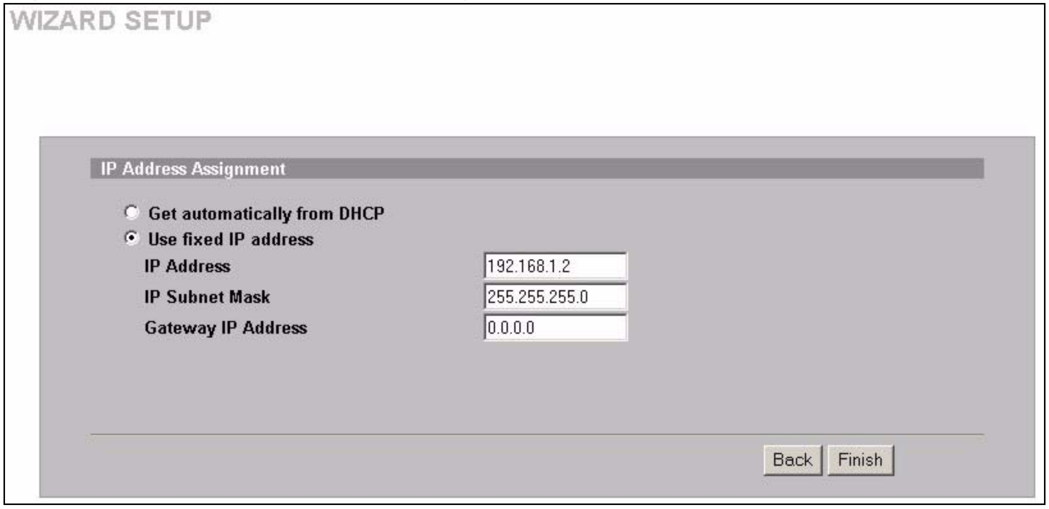
Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

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

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

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

Figure 11 Wizard 3 : IP Address Assignment



WIZARD SETUP

IP Address Assignment

○ Get automatically from DHCP
● Use fixed IP address

IP Address: 192.168.1.2
IP Subnet Mask: 255.255.255.0
Gateway IP Address: 0.0.0.0

The following table describes the labels in this screen.

Table 4 Wizard 3 : IP Address Assignment

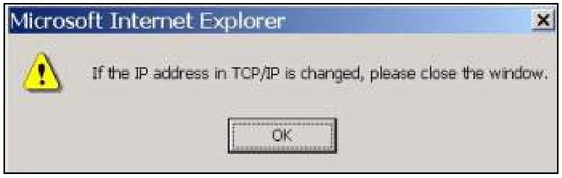
LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option if your ZyXEL Device is using a dynamically assigned IP address from a DHCP server each time. Note: You must know the IP address assigned to the ZyXEL Device (by the DHCP server) to access the ZyXEL Device again.
Use fixed IP address	Select this option if your ZyXEL Device is using a static IP address. When you select this option, fill in the fields below.

Table 4 Wizard 3 : IP Address Assignment

LABEL	DESCRIPTION
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Note: If you changed the ZyXEL Device's IP address, you must use the new IP address if you want to access the web configurator again.
IP Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. The gateway must be a router on the same segment as your ZyXEL Device's LAN or WAN port.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to proceed to complete the Wizard setup.

3.5 Basic Setup Complete

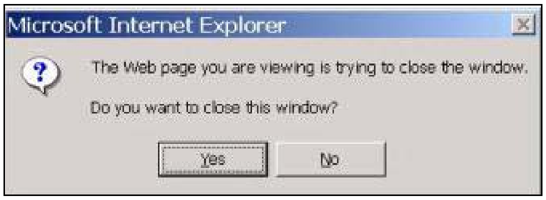
When you click **Finish** in the **Wizard 3 IP Address Assignment** screen, a warning window display as shown. Click **OK** to close the window and log in to the web configurator again using the new IP address if you change the default IP address (192.168.1.2).



Microsoft Internet Explorer

If the IP address in TCP/IP is changed, please close the window.

You have successfully set up the ZyXEL Device. A screen displays prompting you to close the web browser.



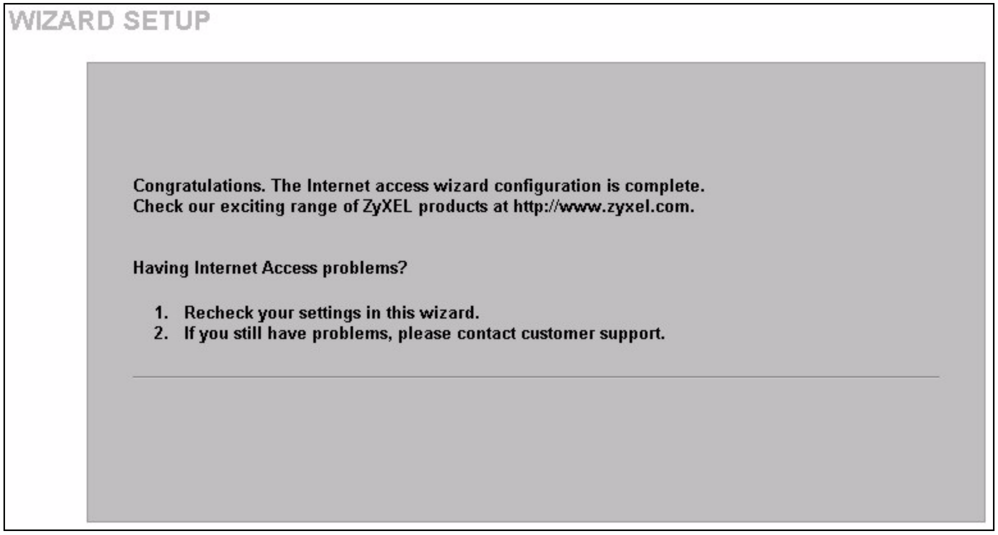
Microsoft Internet Explorer

The Web page you are viewing is trying to close the window.

Do you want to close this window?

Click **Yes**. Otherwise, click **No** and the congratulations screen shows next.

Figure 12 Wizard 4 : Setup Complete



Congratulations. The Internet access wizard configuration is complete.
Check our exciting range of ZyXEL products at http://www.zyxel.com.

Having Internet Access problems?

1. Recheck your settings in this wizard.
2. If you still have problems, please contact customer support.

Well done! You have successfully set up your ZyXEL Device to operate on your network and access the Internet.

4

Tutorial

This chapter first provides step-by-step guidelines showing how to configure your ZyXEL Device for an example scenario with multiple wireless networks.

4.1 How to Configure the Wireless LAN

This section shows how to choose which wireless operating mode you should use on the ZyXEL Device.

4.1.1 Choosing the Wireless Mode

- Use **Access Point** operating mode if you want to allow wireless clients to access your wired network, all using the same security and Quality of Service (QoS) settings. See Section 1.2.1 on page 36 for details.
- Use **Bridge/Repeater** operating mode if you want to use the ZyXEL Device to communicate with other access points. See Section 1.2.2 on page 36 for details.

  The ZyXEL Device is a bridge when other APs access your wired Ethernet network through the ZyXEL Device.

  The ZyXEL Device is a repeater when it has no Ethernet connection and allows other APs to communicate with one another through the ZyXEL Device.
- Use **AP+Bridge** operating mode if you want to use the ZyXEL Device as an access point (see above) while also communicating with other access points. See Section 1.2.3 on page 37 for details.
- Use **MBSSID** operating mode if you want to use the ZyXEL Device as an access point with some groups of users having different security or QoS settings from other groups of users. See Section 1.2.4 on page 38 for details.

4.1.1.1 Configuring Dual WLAN Adapters

The G-3000 is equipped with dual wireless adapters. This means you can configure two different wireless networks to operate simultaneously.

You can configure each wireless adapter separately in the **WIRELESS > Wireless** screen. First select one wireless adapter and configure your settings. Then select the other wireless adapter and follow the same procedure to configure the second network.

4.2 How to Configure Multiple Wireless Networks

In this example, you have been using your ZyXEL Device as an access point for your office network (See your Quick Start Guide for information on how to set up your ZyXEL Device in Access Point mode). Now your network is expanding and you want to make use of the MESSID feature (see Chapter 8 on page 105) to provide multiple wireless networks. Each wireless network will cater for a different type of user.

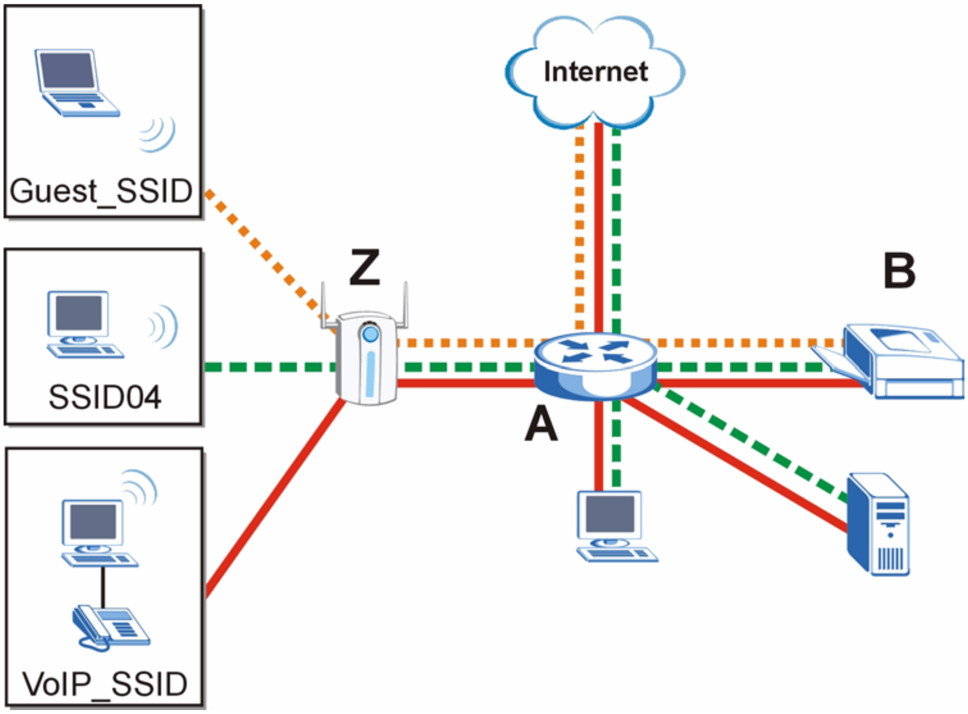
You want to make three wireless networks: one standard office wireless network with all the same settings you already have, another wireless network with high Quality of Service (QoS) settings for Voice over IP users, and a guest network that allows visitors to your office to access only the Internet and the network printer.

To do this, you will take the following steps:

1. Change the operating mode from Access Point to MESSID and reactivate the standard network.
2. Configure a wireless network for Voice over IP users.
3. Configure a wireless network for guests to your office.

The following figure shows the multiple networks you want to set up. Your ZyXEL Device is marked **Z**, the main network router is marked **A**, and your network printer is marked **B**.

Figure 13 Tutorial: Example MESSID Setup



The standard network (**SSID04**) has access to all resources. The VoIP network (**VoIP_SSID**) has access to all resources and a high Quality of Service (QoS) setting (see Section 6.3 on page 75 for information on QoS). The guest network (**Guest_SSID**) has access to the Internet and the network printer only, and a low QoS setting.

To configure these settings, you need to know the MAC (Media Access Control) addresses of the devices you want to allow users of the guest network to access. The following table shows the addresses used in this example.

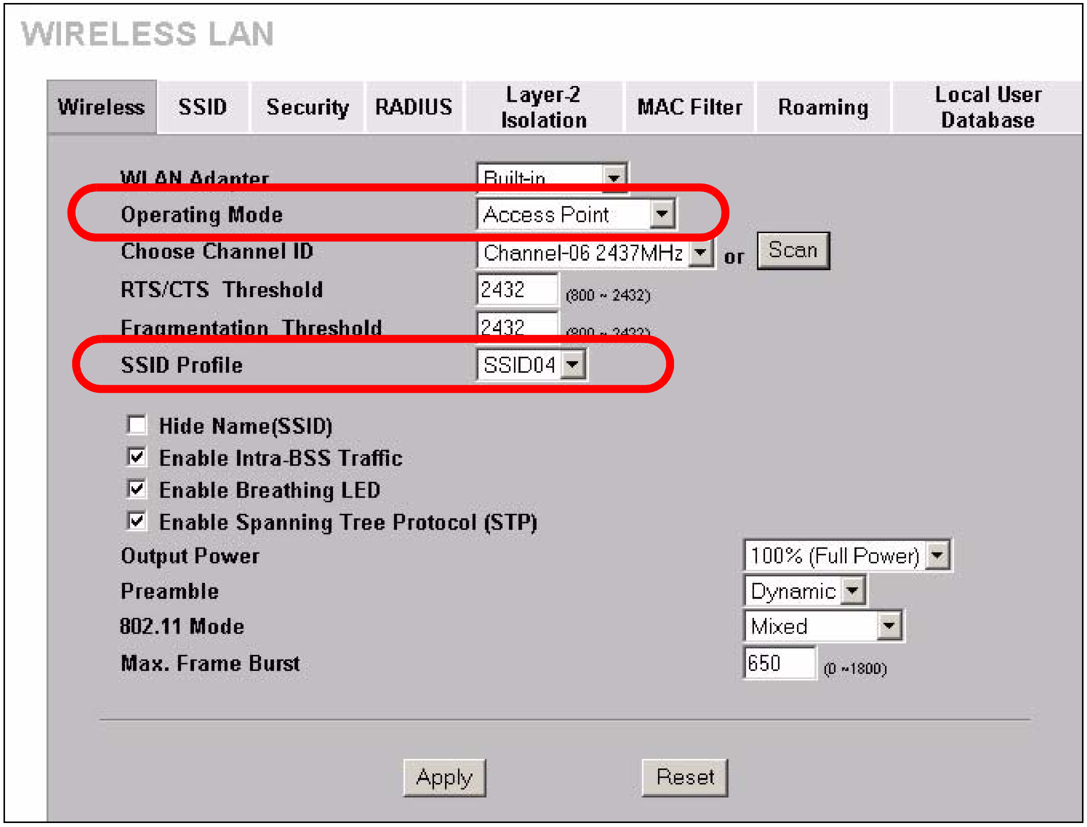
Table 5 Tutorial: Example Information

Network router (**A**) MAC address	00:AA:00:AA:00:AA
Network printer (**B**) MAC address	AA:00:AA:00:AA:00

4.2.1 Change the Operating Mode

Log in to the ZyXEL Device (see Section 2.2 on page 41). Click **WIRELESS** > **Wireless**. The **Wireless** screen appears. In this example, the ZyXEL Device is set to **Access Point** operating mode, and is currently using the **SSID04** profile.

Figure 14 Tutorial: Wireless LAN: Before



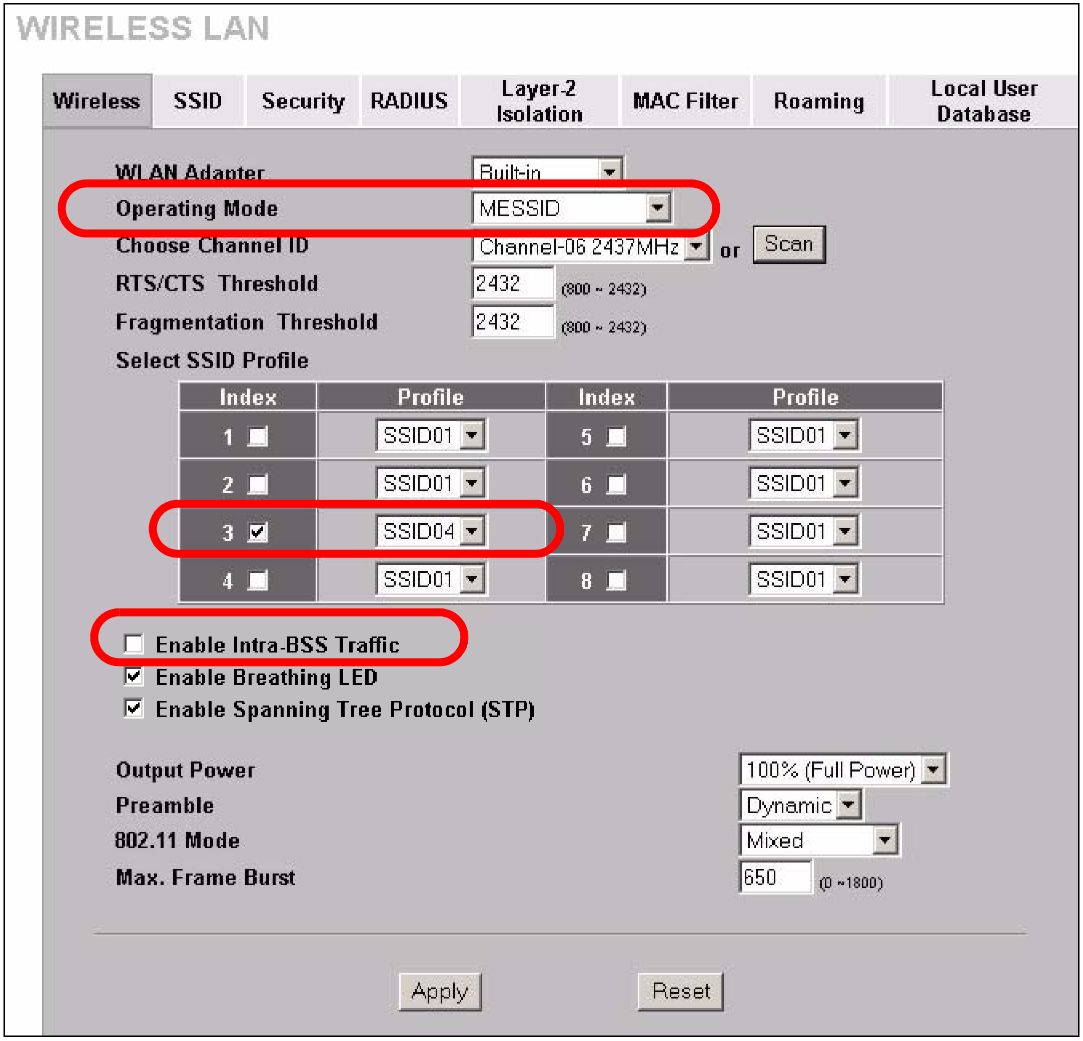
WLAN Adapter: Built-in
Operating Mode: Access Point
Choose Channel ID: Channel-06 2437MHz or Scan
RTS/CTS Threshold: 2432 (800 ~ 2432)
Fragmentation Threshold: 2432 (800 ~ 2432)
SSID Profile: SSID04

☐ Hide Name(SSID)
☑ Enable Intra-BSS Traffic
☑ Enable Breathing LED
☑ Enable Spanning Tree Protocol (STP)

Output Power: 100% (Full Power)
Preamble: Dynamic
802.11 Mode: Mixed
Max. Frame Burst: 650 (0 ~1800)

Select **MESSID** from the **Operating Mode** drop-down list box. The screen displays as follows.

Figure 15 Tutorial: Wireless LAN: Change Mode



WLAN Adapter: Built-in

Operating Mode: MESSID

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (800 ~ 2432)

Fragmentation Threshold: 2432 (800 ~ 2432)

Select SSID Profile

Index	Profile	Index	Profile
1 □	SSID01	5 □	SSID01
2 □	SSID01	6 □	SSID01
3 ☑	SSID04	7 □	SSID01
4 □	SSID01	8 □	SSID01

□ Enable Intra-BSS Traffic

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power: 100% (Full Power)

Preamble: Dynamic

802.11 Mode: Mixed

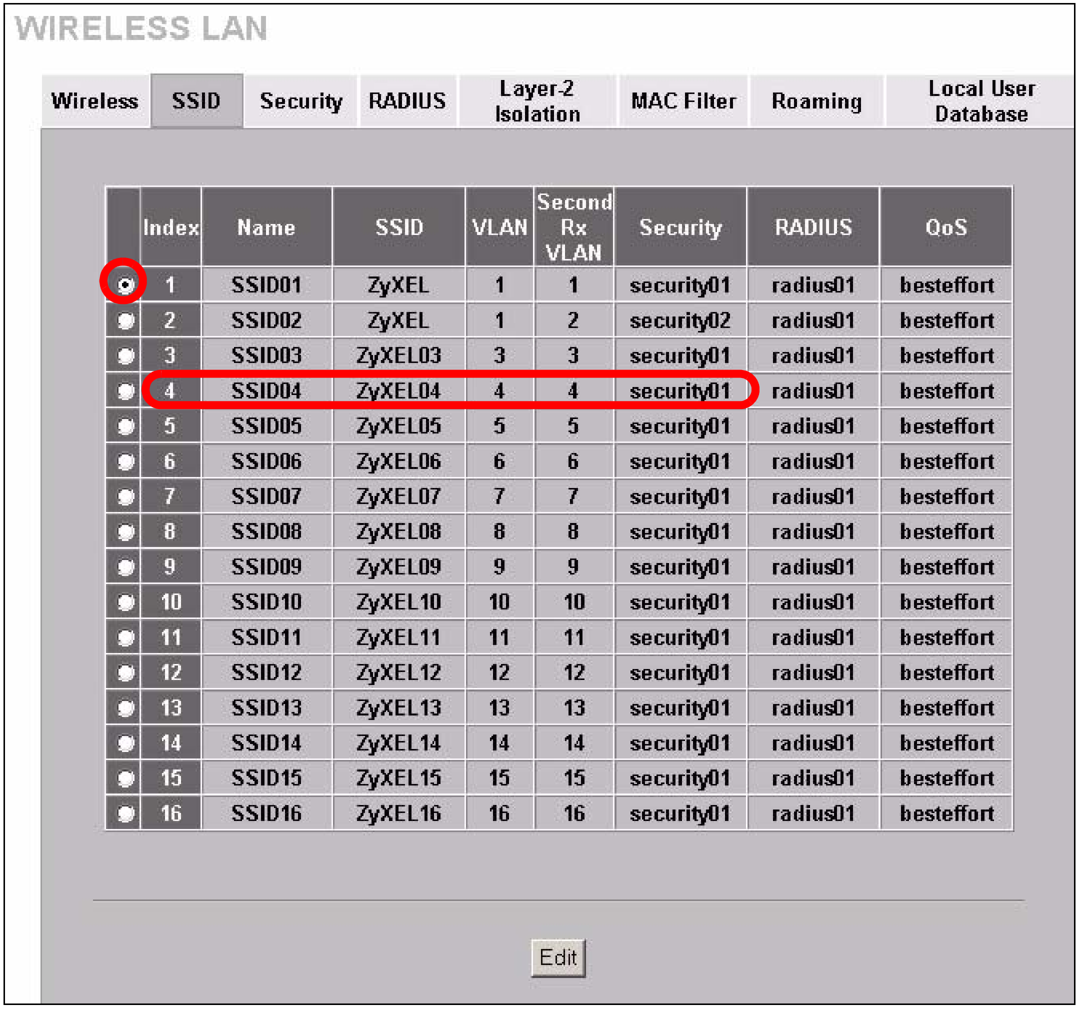
Max. Frame Burst: 650 (0 ~1800)

- This **Select SSID Profile** table allows you to activate or deactivate SSID profiles. Your wireless network was previously using the **SSID04** profile, so select **SSID04** in one of the **Profile** list boxes (number **3** in this example).
- Select the **Index** box for the entry and click **Apply** to activate the profile. Your standard wireless network (**SSID04**) is now accessible to your wireless clients as before. You do not need to configure anything else for your standard network.
- Clear the **Enable Intra BSS Traffic** check box so clients cannot access other clients on the same wireless network (see Section 6.1.1 on page 73).

4.2.2 Configure the VoIP Network

Next, click **WIRELESS** > **SSID**. The following screen displays. Note that all of the SSID profiles are using the **security01** security profile. You cannot change this security profile without changing the security parameters for every SSID (including SSID4, the standard network), so you will use different security profiles for the different SSIDs.

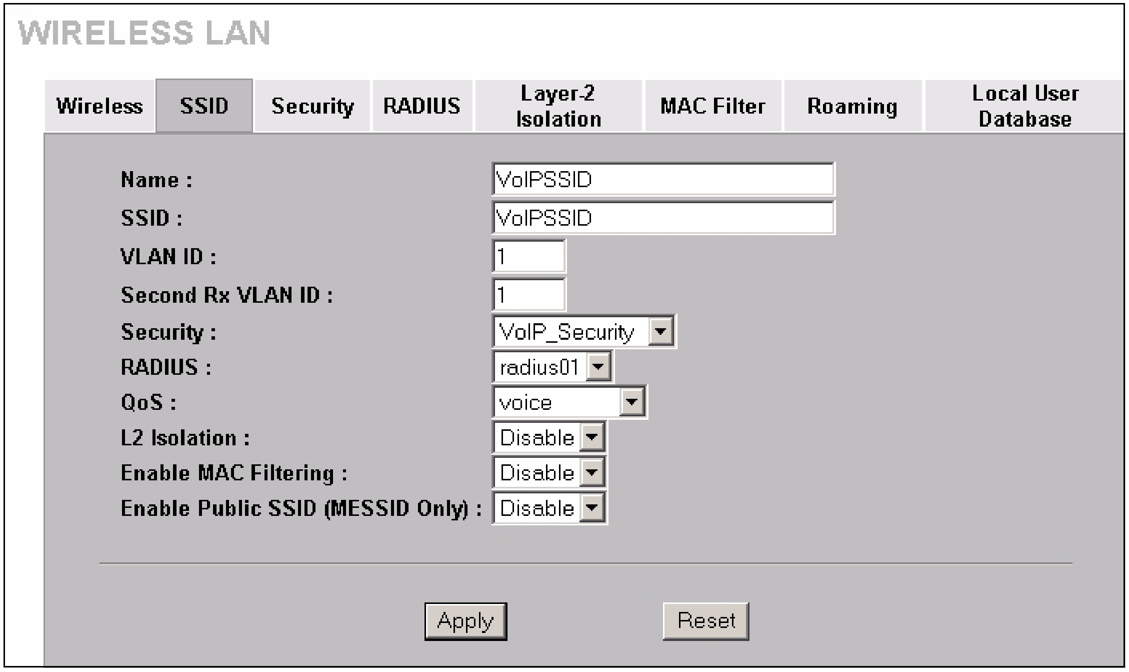
Figure 16 Tutorial: WIRELESS > SSID



	Index	Name	SSID	VLAN	Second Rx VLAN	Security	RADIUS	QoS
●	1	SSID01	ZyXEL	1	1	security01	radius01	besteffort
○	2	SSID02	ZyXEL	1	2	security02	radius01	besteffort
○	3	SSID03	ZyXEL03	3	3	security01	radius01	besteffort
○	4	SSID04	ZyXEL04	4	4	security01	radius01	besteffort
○	5	SSID05	ZyXEL05	5	5	security01	radius01	besteffort
○	6	SSID06	ZyXEL06	6	6	security01	radius01	besteffort
○	7	SSID07	ZyXEL07	7	7	security01	radius01	besteffort
○	8	SSID08	ZyXEL08	8	8	security01	radius01	besteffort
○	9	SSID09	ZyXEL09	9	9	security01	radius01	besteffort
○	10	SSID10	ZyXEL10	10	10	security01	radius01	besteffort
○	11	SSID11	ZyXEL11	11	11	security01	radius01	besteffort
○	12	SSID12	ZyXEL12	12	12	security01	radius01	besteffort
○	13	SSID13	ZyXEL13	13	13	security01	radius01	besteffort
○	14	SSID14	ZyXEL14	14	14	security01	radius01	besteffort
○	15	SSID15	ZyXEL15	15	15	security01	radius01	besteffort
○	16	SSID16	ZyXEL16	16	16	security01	radius01	besteffort

You will use the first SSID for the Voice over IP (VoIP) network, so select SSID1's radio button and click **Edit**. The following screen displays.

Figure 17 Tutorial: VoIP SSID Profile Edit



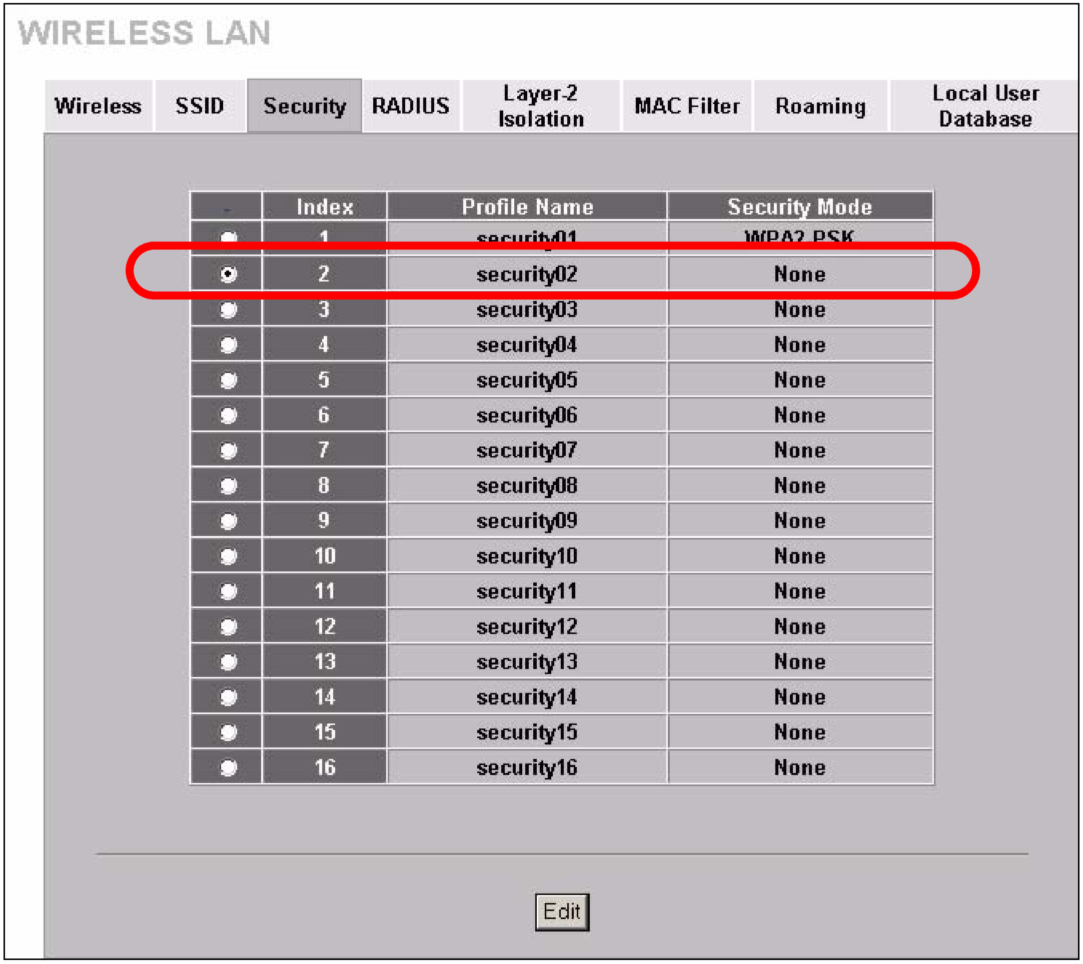
Name :	VoIPSSID
SSID :	VoIPSSID
VLAN ID :	1
Second Rx VLAN ID :	1
Security :	VoIP_Security
RADIUS :	radius01
QoS :	voice
L2 Isolation :	Disable
Enable MAC Filtering :	Disable
Enable Public SSID (MESSID Only) :	Disable

- Choose a new profile name and SSID for the VoIP network. In this example, enter **VOIP_SSID**.
- Select **Disable** from the **Enable Public SSID** list box. You want only authorized company employees to use this network, so there is no need to broadcast the SSID to wireless clients scanning the area.
- The standard network (SSID04) is currently using the **security01** profile, so use a different profile for the VoIP network. If you used the **security01** profile, anyone who could access the standard network could access the VoIP wireless network. Select **security02** from the **Security** field.
- Select **Voice** in the **QoS** field to give the traffic high priority.
- Leave all the other fields at their defaults and click **Apply**.

4.2.2.1 Set Up Security for the VoIP Profile

Now you need to configure the security settings to use on the VoIP wireless network. Click the **Security** tab.

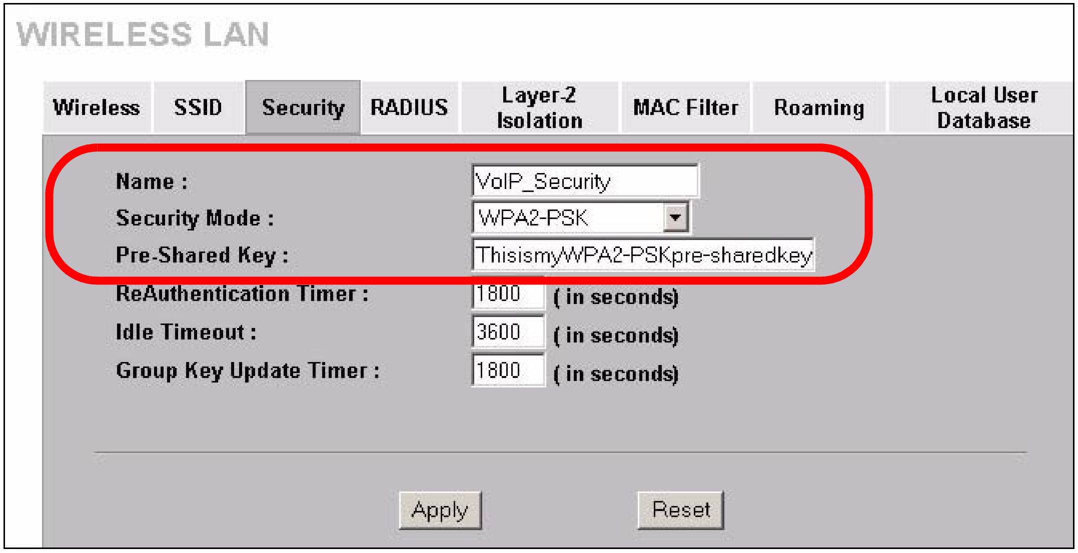
Figure 18 Tutorial: VoIP Security



	Index	Profile Name	Security Mode
○	1	security01	WPA2-PSK
●	2	security02	None
○	3	security03	None
○	4	security04	None
○	5	security05	None
○	6	security06	None
○	7	security07	None
○	8	security08	None
○	9	security09	None
○	10	security10	None
○	11	security11	None
○	12	security12	None
○	13	security13	None
○	14	security14	None
○	15	security15	None
○	16	security16	None

You already chose to use the **security02** profile for this network, so select the radio button for **security02** and click **Edit**. The following screen appears.

Figure 19 Tutorial: VoIP Security Profile Edit

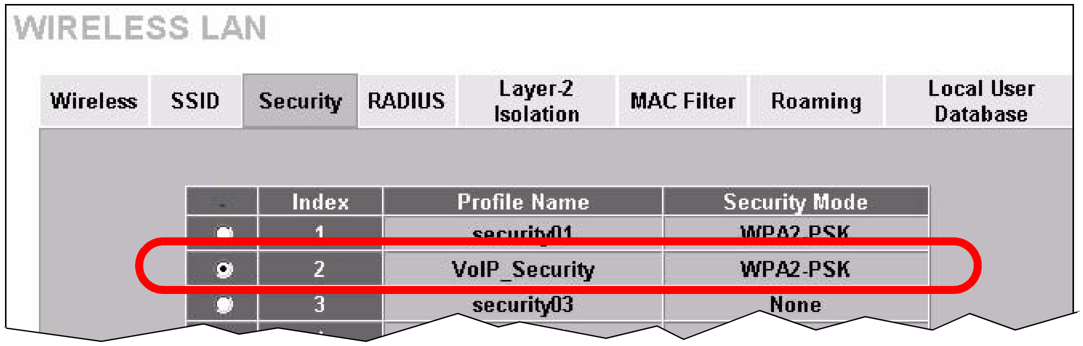


Name :	VoIP_Security
Security Mode :	WPA2-PSK
Pre-Shared Key :	ThisismyWPA2-PSKpre-sharedkey
ReAuthentication Timer :	1800 (in seconds)
Idle Timeout :	3600 (in seconds)
Group Key Update Timer :	1800 (in seconds)

- Change the **Name** field to "VoIP_Security" to make it easier to remember and identify.

- In this example, you do not have a RADIUS server for authentication, so select **WPA2-PSK** in the **Security Mode** field. WPA2-PSK provides strong security that anyone with a compatible wireless client can use, once they know the pre-shared key (PSK). Enter the PSK you want to use in your network in the **Pre Shared Key** field. In this example, the PSK is “ThisismyWPA2-PSKpre-sharedkey”.
- Click **Apply**. The **WIRELESS > Security** screen displays. Ensure that the **Profile Name** for entry 2 displays “**VoIP_Security**” and that the **Security Mode** is **WPA2-PSK**.

Figure 20 Tutorial: VoIP Security: Updated

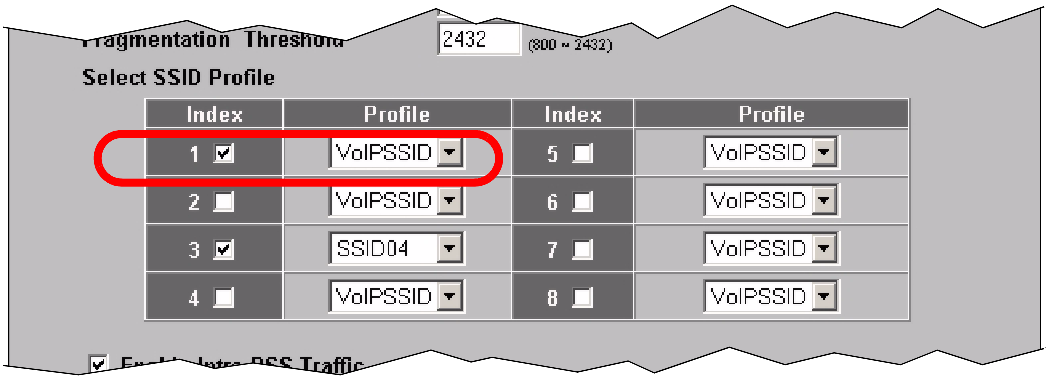


	Index	Profile Name	Security Mode
○	1	security01	WPA2-PSK
●	2	VoIP_Security	WPA2-PSK
○	3	security03	None

4.2.2.2 Activate the VoIP Profile

You need to activate the **VoIP_SSID** profile before it can be used. Click the **Wireless** tab. In the **Select SSID Profile** table, select the **VoIP_SSID** profile and click **Apply**.

Figure 21 Tutorial: Activate VoIP Profile



ragmentation Threshold 2432 (800 ~ 2432)

Select SSID Profile

Index	Profile	Index	Profile
1 ☑	VoIPSSID	5 ☐	VoIPSSID
2 ☐	VoIPSSID	6 ☐	VoIPSSID
3 ☑	SSID04	7 ☐	VoIPSSID
4 ☐	VoIPSSID	8 ☐	VoIPSSID

☑ Enable Intra-BSS Traffic

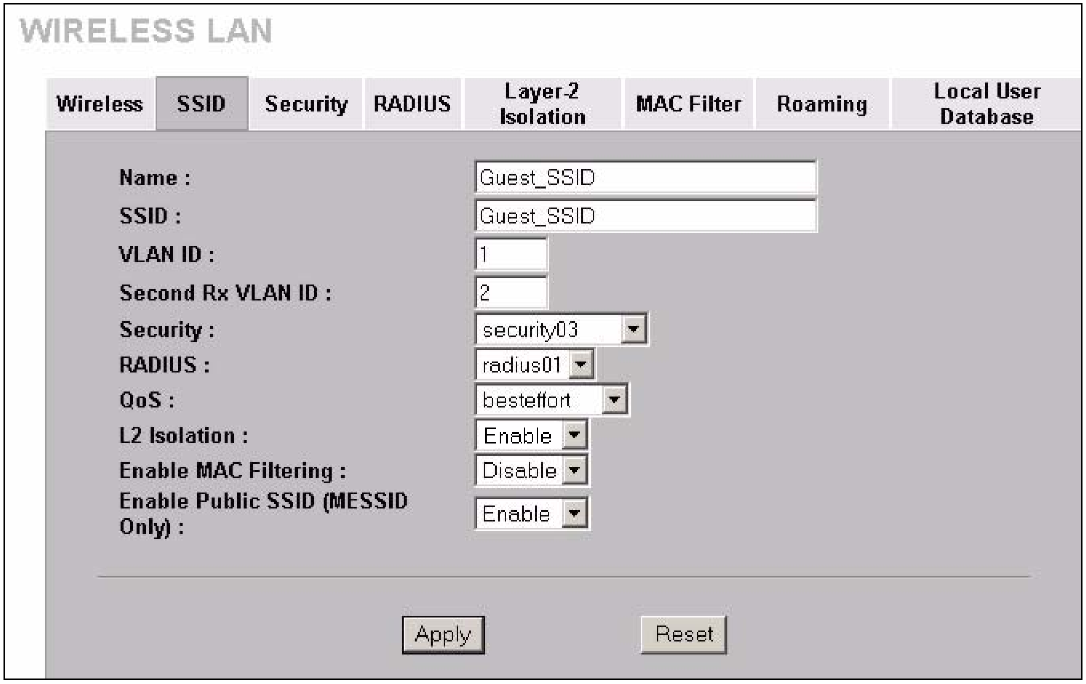
Your VoIP wireless network is now ready to use. Any traffic using the **VoIP_SSID** profile will be given the highest priority across the wireless network.

4.2.3 Configure the Guest Network

When you are setting up the wireless network for guests to your office, your primary concern is to keep your network secure while allowing access to certain resources (such as a network printer, or the Internet). For this reason, you will enable layer-2 isolation for the **Guest_SSID** profile. “Layer-2 isolation” means that a client accessing the network via the **Guest_SSID** profile can access only certain pre-defined devices on the network (see Section 9.1 on page 115).

Click **WIRELESS** > **SSID**. Select **SSID02**'s entry in the list and click **Edit**. The following screen appears.

Figure 22 Tutorial: Guest Edit



Name : Guest_SSID
SSID : Guest_SSID
VLAN ID : 1
Second Rx VLAN ID : 2
Security : security03
RADIUS : radius01
QoS : besteffort
L2 Isolation : Enable
Enable MAC Filtering : Disable
Enable Public SSID (MESSID Only) : Enable

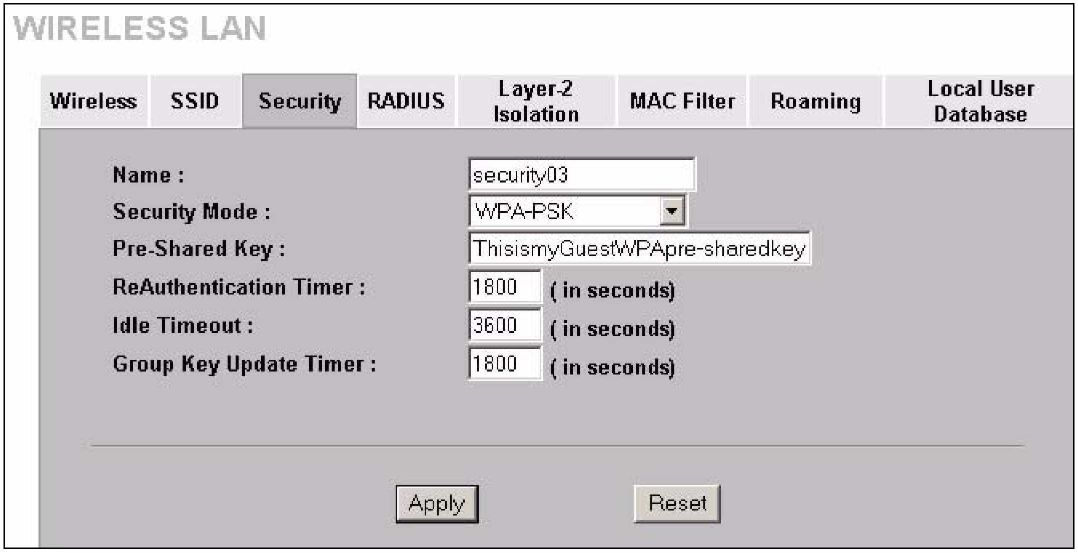
- Choose a new SSID for the guest network. In this example, enter **Guest_SSID**. You can also change the SSID profile name to **Guest_SSID** (although it is not required).
- The standard network (SSID04) is already using the **security01** profile, and the VoIP network is using the **security02** profile (renamed **VoIP_Security**) so select the **security03** profile from the **Security** field.
- Select **Enable** in the **L2 Isolation** field so clients accessing the network via the **Guest_SSID** profile can access only certain pre-defined devices on the network
- Select **Enable** in the **Enable Public SSID (MESSID Only)** list box. This makes it easier for guests to configure their computers' wireless clients to your network's settings.
- Leave all the other fields at their defaults and click **Apply**.

4.2.3.1 Set Up Security for the Guest Profile

Now you need to configure the security settings to use on the guest wireless network. Click the **Security** tab.

You already chose to use the **security03** profile for this network, so select **security03**'s entry in the list and click **Edit**. The following screen appears.

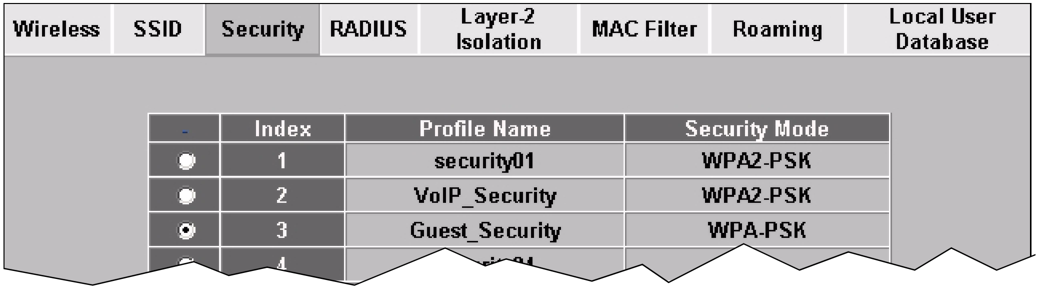
Figure 23 Tutorial: Guest Security Profile Edit



Name :	security03
Security Mode :	WPA-PSK
Pre-Shared Key :	ThisismyGuestWPApre-sharedkey
ReAuthentication Timer :	1800 (in seconds)
Idle Timeout :	3600 (in seconds)
Group Key Update Timer :	1800 (in seconds)

- Change the **Name** field to “Guest_Security” to make it easier to remember and identify.
- Select **WPA-PSK** in the **Security Mode** field. WPA-PSK provides strong security that is supported by most wireless clients. Even though your Guest_SSID clients do not have access to sensitive information on the network, you should not leave the network without security. An attacker could still cause damage to the network or intercept unsecured communications.
- Enter the PSK you want to use in your network in the **Pre Shared Key** field. In this example, the PSK is “ThisismyGuestWPApre-sharedkey”.
- Click **Apply**. The **WIRELESS > Security** screen displays. Ensure that the **Profile Name** for entry 3 displays “**Guest_Security**” and that the **Security Mode** is **WPA-PSK**.

Figure 24 Tutorial: Guest Security: Updated

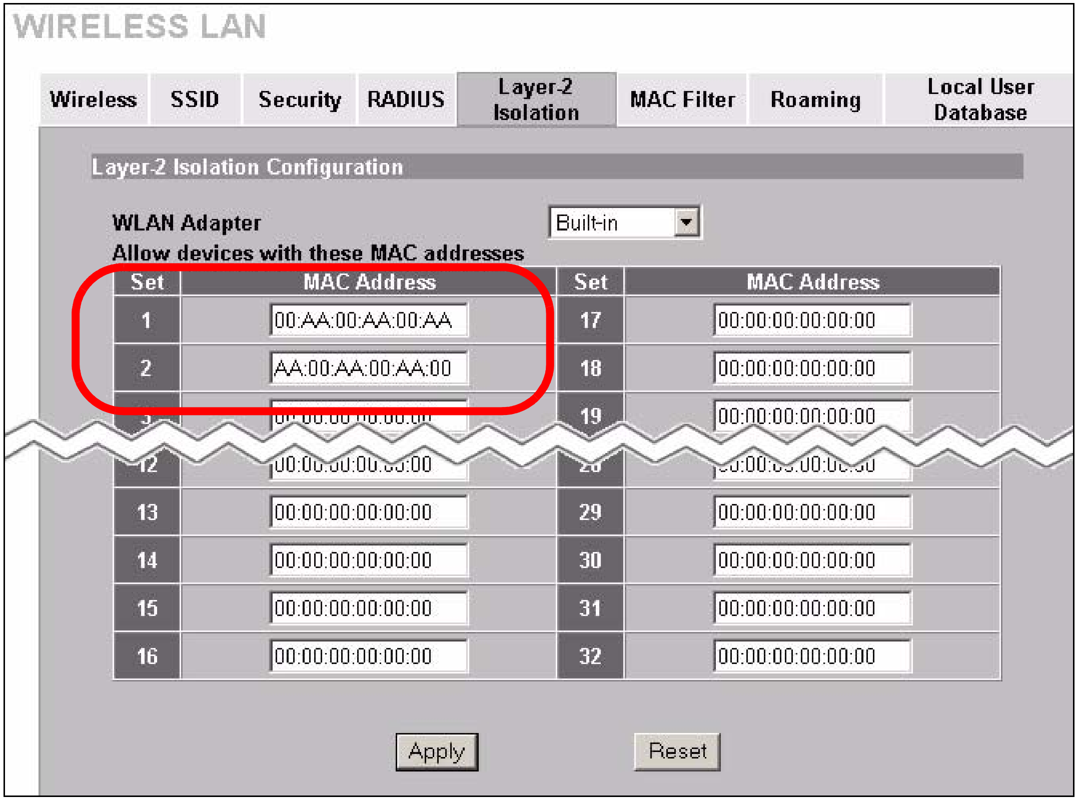


-	Index	Profile Name	Security Mode
○	1	security01	WPA2-PSK
○	2	VoIP_Security	WPA2-PSK
●	3	Guest_Security	WPA-PSK
○	4		

4.2.3.2 Set up Layer-2 Isolation

Configure layer-2 isolation to control the specific devices you want the users on your guest network to access. Click **WIRELESS** > **Layer-2 Isolation**. The following screen appears.

Figure 25 Tutorial: Layer 2 Isolation



Layer-2 Isolation Configuration

WLAN Adapter: Built-in

Allow devices with these MAC addresses

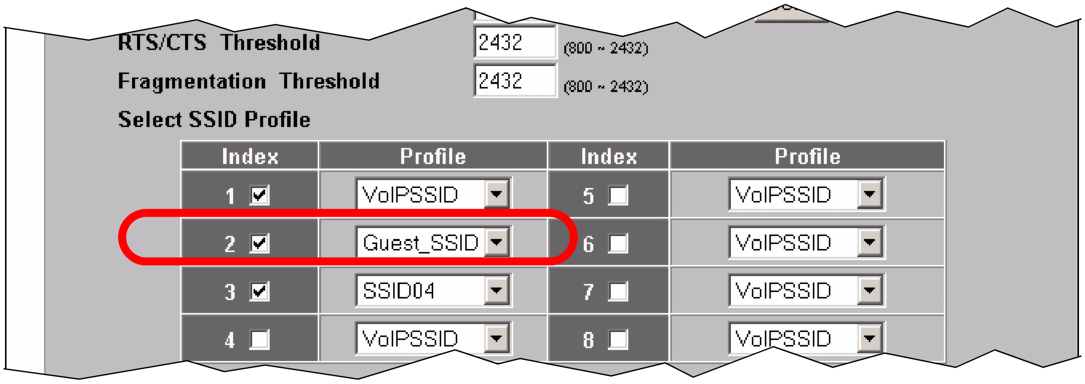
Set	MAC Address	Set	MAC Address
1	00:AA:00:AA:00:AA	17	00:00:00:00:00:00
2	AA:00:AA:00:AA:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

Enter the MAC addresses of the two network devices you want users on the guest network to be able to access; the main network router (00:AA:00:AA:00:AA) and the network printer (AA:00:AA:00:AA:00). Click **Apply**.

4.2.3.3 Activate the Guest Profile

You need to activate the **Guest_SSID** profile before it can be used. Click the **Wireless** tab. In the **Select SSID Profile** table, select the check box for the second index entry and select the **Guest_SSID** profile. Click **Apply**.

Figure 26 Tutorial: Activate Guest Profile



RTS/CTS Threshold: 2432 (800 ~ 2432)

Fragmentation Threshold: 2432 (800 ~ 2432)

Select SSID Profile

Index	Profile	Index	Profile
1 ☑	VoIPSSID	5 □	VoIPSSID
2 ☑	Guest_SSID	6 □	VoIPSSID
3 ☑	SSID04	7 □	VoIPSSID
4 □	VoIPSSID	8 □	VoIPSSID

Your Guest wireless network is now ready to use.

4.2.4 Testing the Wireless Networks

To make sure that the three networks are correctly configured, do the following.

- On a computer with a wireless client, scan for access points. You should see the **Guest_SSID** network, but not the **VoIP_SSID** network. If you can see the VoIP_SSID network, go to its **SSID Edit** screen and make sure **Enable Public SSID (MESSID Only)** is set to **Disable**.

  Whether or not you see the standard network's SSID (**SSID04**) depends on whether "hide SSID" is enabled.
- Try to access each network using the correct security settings, and then using incorrect security settings, such as the WPA-PSK for another active network. If the behavior is different from expected (for example, if you can access the VoIP wireless network using the security settings for the Guest_SSID wireless network) check that the SSID profile is set to use the correct security profile, and that the settings of the security profile are correct.
- Access the Guest_SSID network and try to access other resources than those specified in the Layer-2 Isolation screen.

  You can use the ping utility to do this. Click **Start** > **Run...** and enter "cmd" in the **Open:** field. Click **OK**. At the **c:\>** prompt, enter "ping 192.168.1.10" (substitute the IP address of a real device on your network that is not on the layer 2 isolation list). If you receive a reply, check the settings in the **WIRELESS** > **Layer-2 Isolation** screen, and ensure that layer 2 isolation is enabled in the Guest_SSID profile screen.

PART II
The Web Configurator

5

System Screens

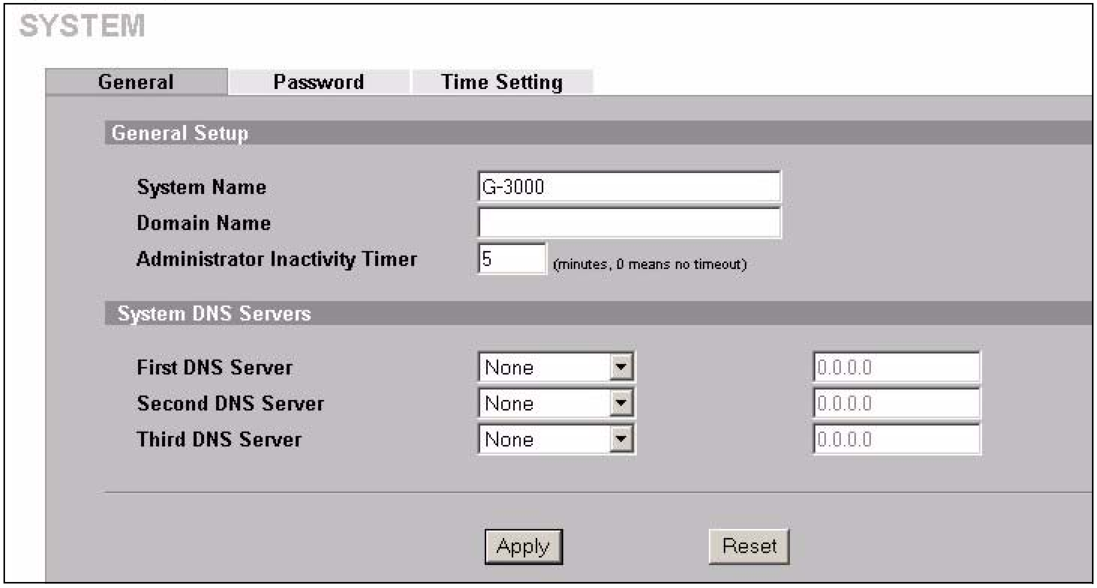
5.1 System Overview

This section provides information on general system setup.

5.2 Configuring General Setup

Click **SYSTEM** > **General**.

Figure 27 System General Setup



System Name: G-3000
Domain Name:
Administrator Inactivity Timer: 5 (minutes, 0 means no timeout)

First DNS Server: None 0.0.0.0
Second DNS Server: None 0.0.0.0
Third DNS Server: None 0.0.0.0

The following table describes the labels in this screen.

Table 6 System General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Type a descriptive name to identify the ZyXEL Device in the Ethernet network. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.

Table 6 System General Setup

LABEL	DESCRIPTION
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) 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).
System DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From DHCP** if your DHCP server dynamically assigns DNS server information (and the ZyXEL Device's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. The default setting is **None**.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.3 Administrator Authentication on RADIUS

The administrator authentication on RADIUS feature lets a (external or internal) RADIUS server authenticate management logins to the ZyXEL Device. This is useful if you need to regularly change a password that you use to manage several ZyXEL Devices.

Activate administrator authentication on RADIUS in the **SYSTEM > Password** screen and configure the same user name, password and RADIUS server information on each ZyXEL Device. Then, whenever you want to change the password, just change it on the RADIUS server.

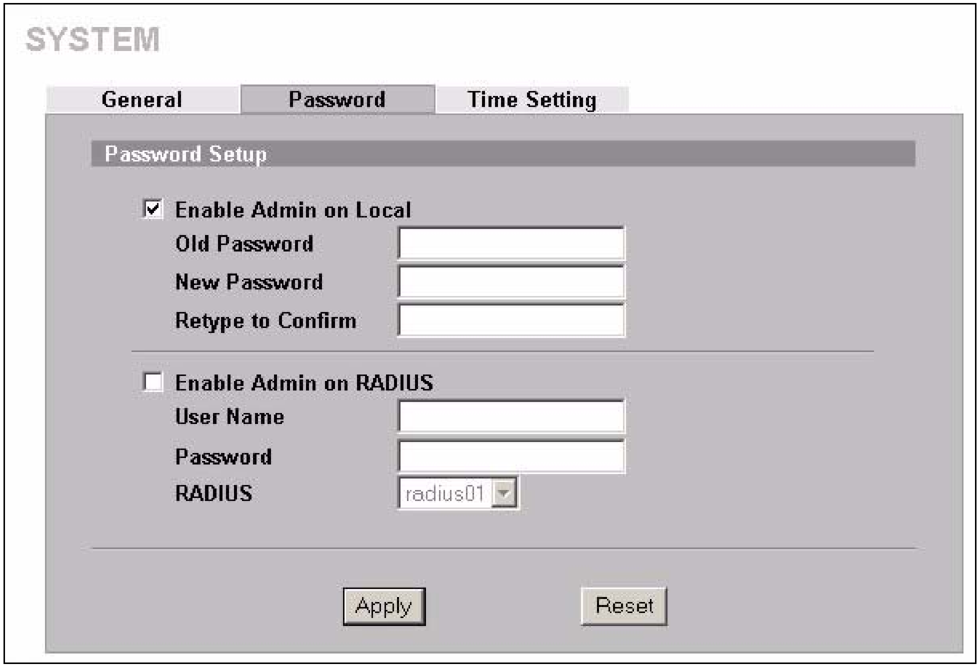
5.4 Configuring Password

It is strongly recommended that you change your ZyXEL Device's password. Click **SYSTEM > Password**. The screen appears as shown.

If you forget your ZyXEL Device's password, you will need to reset the device. See Section 2.3 on page 43 for details on resetting the ZyXEL Device.

Regardless of how you configure this screen, you still use the local system password to log in via the console port (not available on all models).

Figure 28 Password.



☑ Enable Admin on Local

Old Password

New Password

Retype to Confirm

☐ Enable Admin on RADIUS

User Name

Password

RADIUS radius01

The following table describes the labels in this screen.

Table 7 Password

LABEL	DESCRIPTIONS
Enable Admin on Local	Select this check box to have the device authenticate management logins to the device.
Old Password	Type in your existing system password (1234 is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Enable Admin on RADIUS	Select this (and configure the other fields in this section) to have a RADIUS server authenticate management logins to the ZyXEL Device. Configuring the administrator authentication on RADIUS option automatically configures the last wireless LAN security profile and sets it to **8021x-Only**.
User Name	Enter the username for this user account. This name can be up to 31 ASCII characters long, including spaces.
Password	Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type. Spaces are allowed. Note: If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length.
RADIUS	Select the RADIUS server profile of the RADIUS server that is to authenticate management logins to the ZyXEL Device. The ZyXEL Device tests the user name and password against the RADIUS server when you apply your settings. • The user name and password must already be configured in the RADIUS server. • You must already have a RADIUS profile configured for the RADIUS server (see Section 7.12 on page 102). • The server must be set to **Active** in the profile.

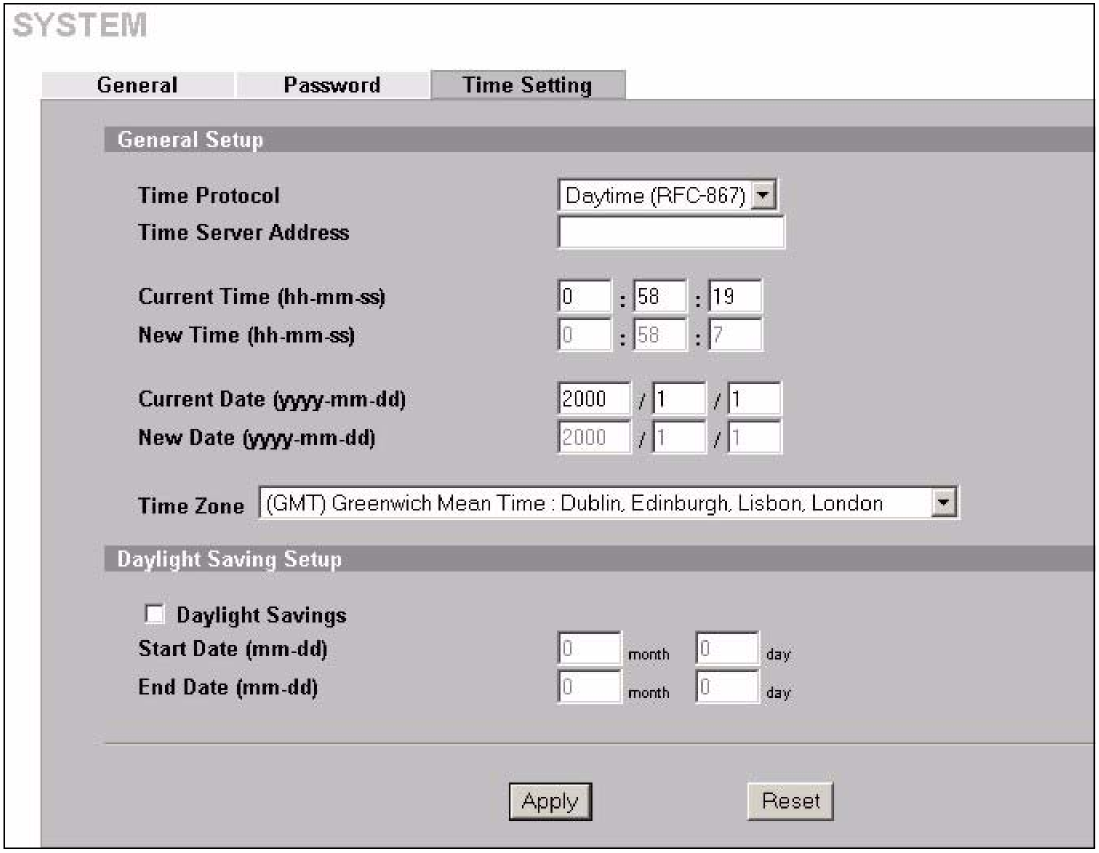
Table 7 Password

LABEL	DESCRIPTIONS
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.5 Configuring Time Setting

To change your ZyXEL Device's time and date, click **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 29 Time Setting



General Setup

Time Protocol	Daytime (RFC-867)
Time Server Address	
Current Time (hh-mm-ss)	0 : 58 : 19
New Time (hh-mm-ss)	0 : 58 : 7
Current Date (yyyy-mm-dd)	2000 / 1 / 1
New Date (yyyy-mm-dd)	2000 / 1 / 1
Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Daylight Saving Setup

☐ Daylight Savings

Start Date (mm-dd)	0 month 0 day
End Date (mm-dd)	0 month 0 day

The following table describes the labels in this screen.

Table 8 Time Setting

LABEL	DESCRIPTION
Time Protocol	Select the time service protocol that your time server sends when you turn on the ZyXEL Device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. When you select the **Daytime (RFC 867)** format, the ZyXEL Device displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305),** is similar to Time (RFC 868). Select **None** to enter the time and date manually.
Time Server Address	Enter the IP address or the URL of your time server. Check with your ISP/ network administrator if you are unsure of this information.
Current Time (hh:mm:ss)	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.
New Time (hh:mm:ss)	This field displays the last updated time from the time server. When you select **None** in the **Time Protocol** field, enter the new time in this field and then click **Apply**.
Current Date (yyyy/ mm/dd)	This field displays the date of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.
New Date (yyyy/mm/ dd)	This field displays the last updated date from the time server. When you select **None** in the **Time Protocol** field, enter the new date in this field and then click **Apply**.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings 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.
Start Date (mm-dd)	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date (mm-dd)	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.5.1 Resetting the Time

The ZyXEL Device resets the time in the following instances:

- On saving your changes.
- When the ZyXEL Device starts up.
- 24-hour intervals after starting.

6

Wireless Configuration

This chapter discusses how to configure the Wireless screens on the ZyXEL Device.

6.1 Wireless LAN Overview

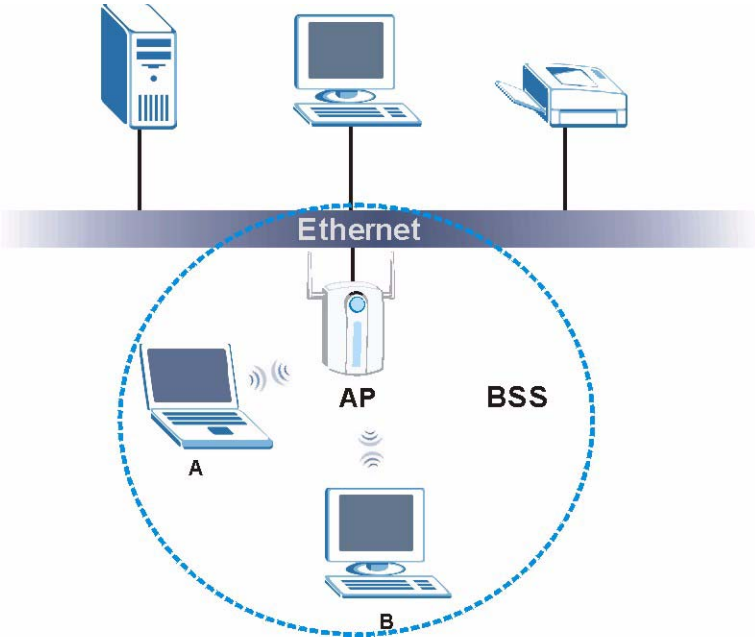
This section introduces the wireless LAN (WLAN) and some basic scenarios.

6.1.1 BSS

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

Intra-BSS traffic is traffic between wireless stations in the BSS. When intra-BSS traffic is allowed, wireless station A and B can access the wired network and communicate with each other. When intra-BSS traffic is blocked, wireless station A and B can still access the wired network but cannot communicate with each other.

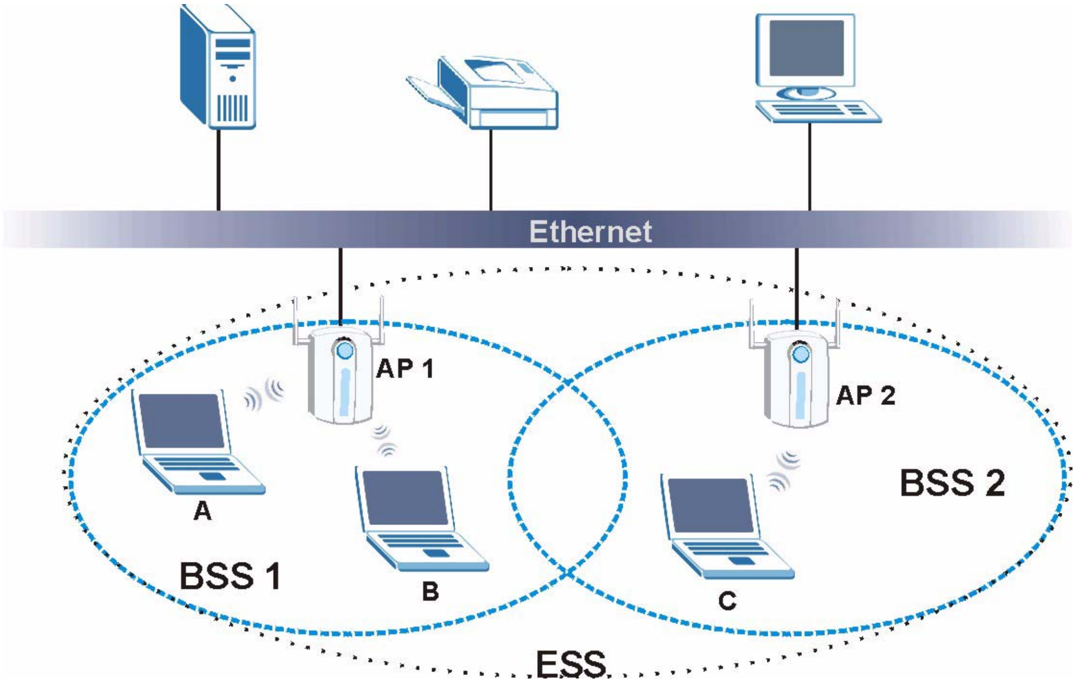
Figure 30 Basic Service set



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

Figure 31 Extended Service Set



6.2 Wireless LAN Basics

See the Wireless LANs Appendix for information on the following:

- Wireless LAN Topologies
- Channel
- RTS/CTS
- Fragmentation Threshold
- Preamble Type
- IEEE 802.1x
- RADIUS
- Types of Authentication
- WPA
- Security Parameters Summary

6.3 Quality of Service

This section discusses the Quality of Service (QoS) features available on the ZyXEL Device.

6.3.1 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be sent over the wireless network.

WMM QoS prioritizes wireless traffic according to the delivery requirements of the individual and applications. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The ZyXEL Device uses WMM QoS to prioritize traffic streams according to the VLAN or DSCP information in each packet's header. The ZyXEL Device automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency (delay) and jitter (variations in delay).

6.3.1.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the uses.

6.3.2 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the ZyXEL Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

6.3.2.1 DiffServ

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

6.3.2.2 DSCP and Per-Hop Behavior

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

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

Figure 32 DiffServ: Differentiated Service Field

DSCP	Unused
(6-bit)	(2-bit)

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

6.3.3 ToS (Type of Service) and WMM QoS

The DSCP value of outgoing packets is between 0 and 255. 0 is the default priority. WMM QoS checks the DSCP value in the header of data packets. It gives the traffic a priority according to this number.

In order to control which priority level is given to traffic, the device sending the traffic must set the DSCP value in the header. If the DSCP value is not specified, then the traffic is treated as best-effort. This means the wireless clients and the devices with which they are communicating must both set the DSCP value in order to make the best use of WMM QoS. A Voice over IP (VoIP) device for example may allow you to define the DSCP value.

The following table lists which WMM QoS priority level the ZyXEL Device uses for specific DSCP values.

6.4 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

6.4.1 Rapid STP

The ZyXEL Device uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

6.4.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the following table.

Table 11 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

6.4.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

6.4.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 12 STP Port States

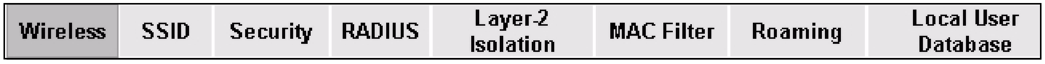
PORT STATES	DESCRIPTIONS
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.

Table 12 STP Port States

PORT STATES	DESCRIPTIONS
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

6.5 Wireless Screen Overview

The following is a list of the screens you can configure on the ZyXEL Device.



1. Configure the ZyXEL Device to operate in AP, AP+Bridge, Bridge/Repeater or MESSID mode in the **Wireless** screen (see Chapter 8 on page 105 for MESSID). You can also select SSID profiles in the **Wireless** screen.
2. Use the **SSID** screens to view and edit SSID profiles.
3. Use the **Security** screen to configure wireless profiles.
4. Use the **RADIUS** screen to configure RADIUS authentication and accounting settings.
5. Use the **Layer-2 Isolation** screen to prevent wireless clients associated with your ZyXEL Device from communicating with other wireless clients, APs, computers or routers in a network.
6. Use the **MAC Filter** screen to allow or restrict access to your wireless network based on a client's MAC address.
7. Use the **Roaming** screen to allow wireless stations to switch from one access point to another as they move between the coverage areas of multiple access points in a network.
8. Use the **Local User Database** screen to configure a list of trusted user names and passwords.

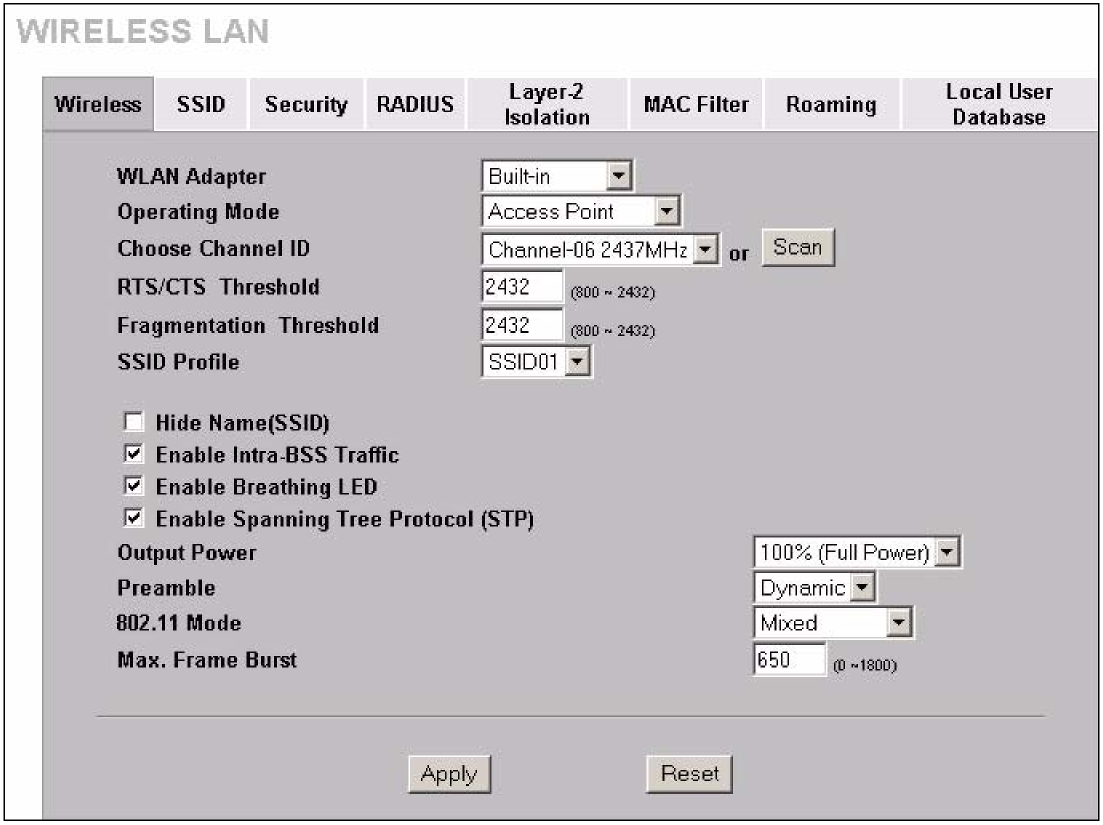
6.6 Configuring Wireless Settings

Click **WIRELESS** > **Wireless**. The screen varies depending upon the operating mode you select.

6.6.1 Access Point Mode

Select **Access Point** as the **Operating Mode** to display the screen as shown next.

Figure 33 Wireless: Access Point



WLAN Adapter: Built-in

Operating Mode: Access Point

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (800 ~ 2432)

Fragmentation Threshold: 2432 (800 ~ 2432)

SSID Profile: SSID01

☐ Hide Name(SSID)

☑ Enable Intra-BSS Traffic

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power: 100% (Full Power)

Preamble: Dynamic

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

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

Table 13 Wireless: Access Point

LABEL	DESCRIPTION
WLAN Adapter	This field only appears when you have a compatible WLAN card in the ZyXEL Device's extension card slot. Note: Contact your distributor for information on compatible WLAN cards. Select **Built-in** to configure settings for the ZyXEL Device's the internal WLAN card. Select **Removable** to configure settings for the ZyXEL Device's WLAN card in the extension card slot.
Operating Mode	Select **Access Point** from the drop-down list.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyXEL Device automatically select a channel, click **Scan** instead.
Scan	Click this button to have the ZyXEL Device automatically scan for and select the channel with the least interference.

Table 13 Wireless: Access Point

LABEL	DESCRIPTION
RTS/CTS Threshold	(Request To Send/Clear To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **800** and **2346**.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **800** and **2346**.
SSID Profile	The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Select an **SSID Profile** from the drop-down list box. Configure SSID profiles in the **SSID** screen (see Section 8.2 on page 109 for information on configuring SSID). Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or 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.
Hide Name (SSID)	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Enable Breathing LED	Select this check box to enable the "breathing" LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyXEL Device is receiving power and blinks (or breathes) when data is being transmitted to and from its wireless stations. Clear the check box to turn this LED off even when the ZyXEL Device is on and data is being transmitted and received.
Enable Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the same BSS. Enable Intra-BSS traffic to allow wireless stations connected to the ZyXEL Device to communicate with each other. Disable Intra-BSS traffic to only allow wireless stations to communicate with the wired network, not with each other. Note: This check box is automatically cleared (intra-BSS traffic is blocked) if you configure an SSID to use layer-2 isolation. Re-select this check box if you want to allow intra-BSS traffic.
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select from **100% (Full Power)**, **50%**, **25%** and **12.5%**. See Appendix A on page 261 for more information on your ZyXEL Device's output power.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** and **Dynamic**. See the section on preamble for more information.

Table 13 Wireless: Access Point

LABEL	DESCRIPTION
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **Mixed** to allow both IEEE 802.11b and IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Max. Frame Burst	Enable maximum frame burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum frame burst sets the maximum time, in microseconds, that the ZyXEL Device transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

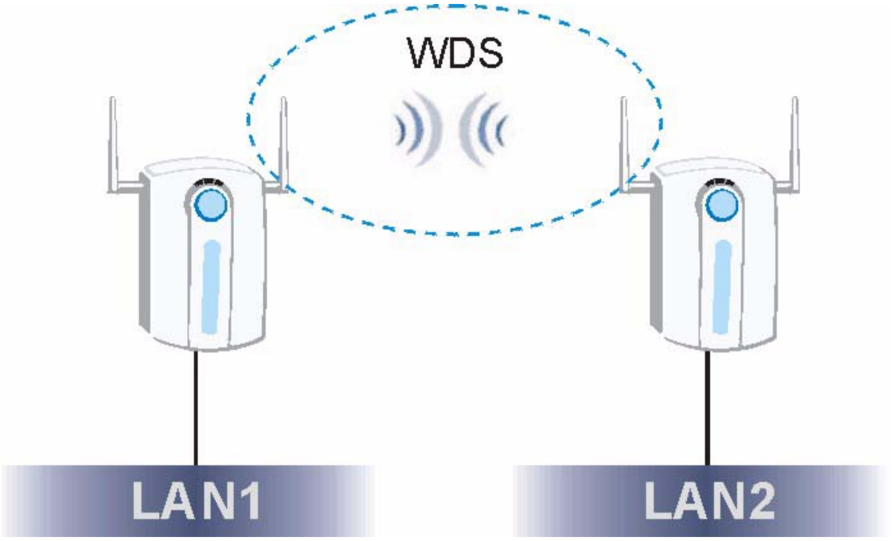
6.6.2 Bridge/Repeater Mode

The ZyXEL Device can act as a wireless network bridge and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

The ZyXEL Device can establish up to five wireless links with other APs.

In the example below, when both ZyXEL Devices are in Bridge/Repeater mode, they form a WDS (Wireless Distribution System) allowing the computers in LAN 1 to connect to the computers in LAN 2.

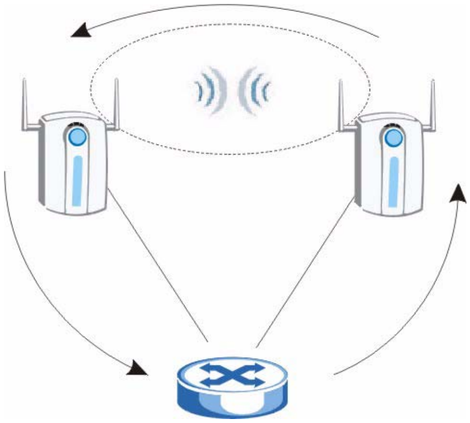
Figure 34 Bridging Example



Be careful to avoid bridge loops when you enable bridging in the ZyXEL Device. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show two network topologies that can lead to this problem:

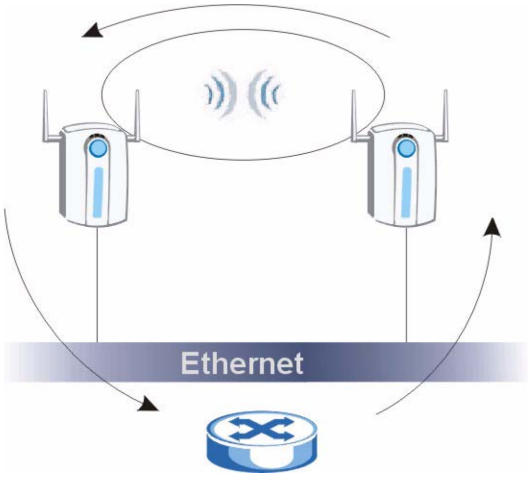
- If two or more ZyXEL Devices (in bridge mode) are connected to the same switch (as shown next).

Figure 35 Bridge Loop: Two Bridges Connected to Switch



- If your ZyXEL Device (in bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN (as shown next).

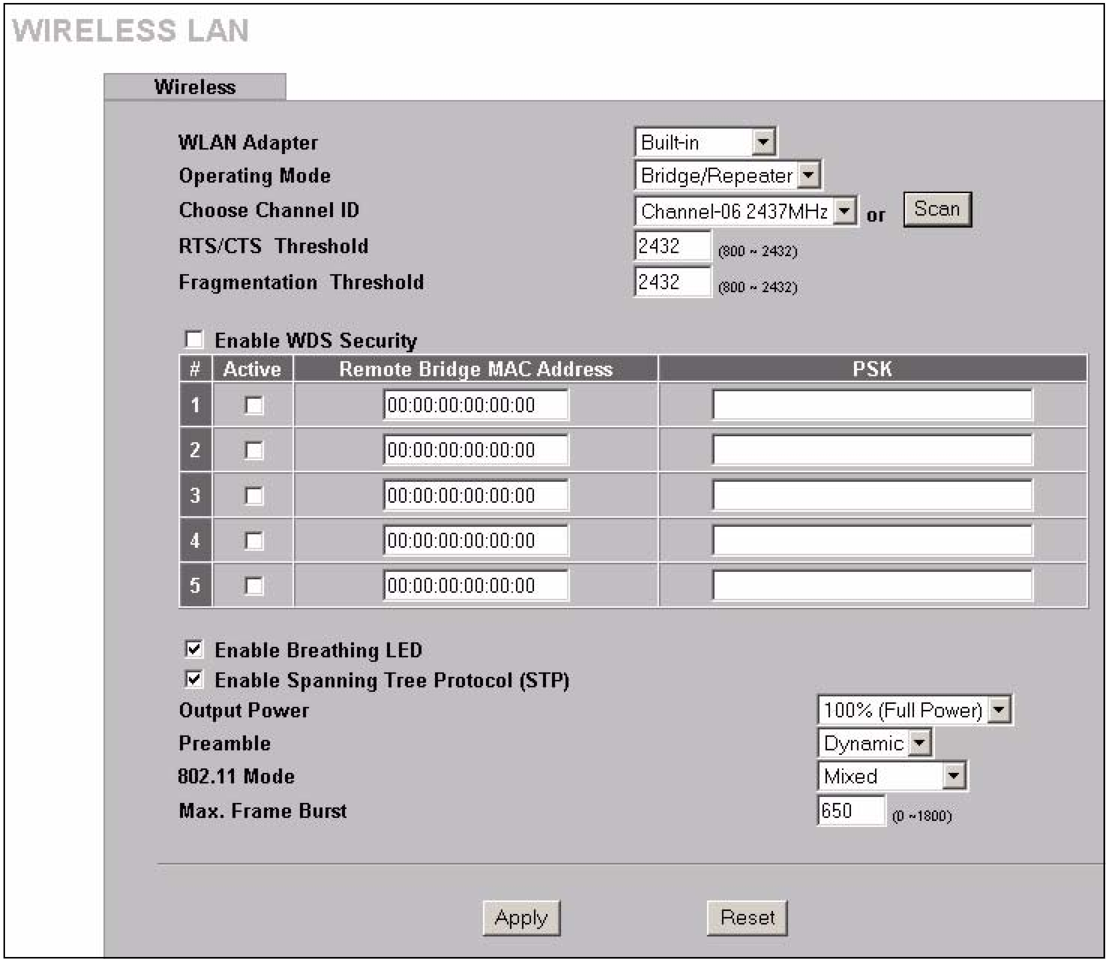
Figure 36 Bridge Loop: Bridge Connected to Wired LAN



To prevent bridge loops, ensure that you enable STP in the **Wireless** screen or your ZyXEL Device is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

To have the ZyXEL Device act as a wireless bridge only, click **WIRELESS** > **Wireless** and select **Bridge/Repeater** as the **Operating Mode**.

Figure 37 Wireless: Bridge/Repeater



WIRELESS LAN

Wireless

WLAN Adapter	Built-in
Operating Mode	Bridge/Repeater
Choose Channel ID	Channel-06 2437MHz or Scan
RTS/CTS Threshold	2432 (800 ~ 2432)
Fragmentation Threshold	2432 (800 ~ 2432)

□ Enable WDS Security

#	Active	Remote Bridge MAC Address	PSK
1	□	00:00:00:00:00:00	
2	□	00:00:00:00:00:00	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power	100% (Full Power)
Preamble	Dynamic
802.11 Mode	Mixed
Max. Frame Burst	650 (0 ~1800)

The following table describes the labels specific to the bridge/repeater mode. See Table 13 on page 79 for descriptions of the other fields.

Table 14 Wireless: Bridge/Repeater

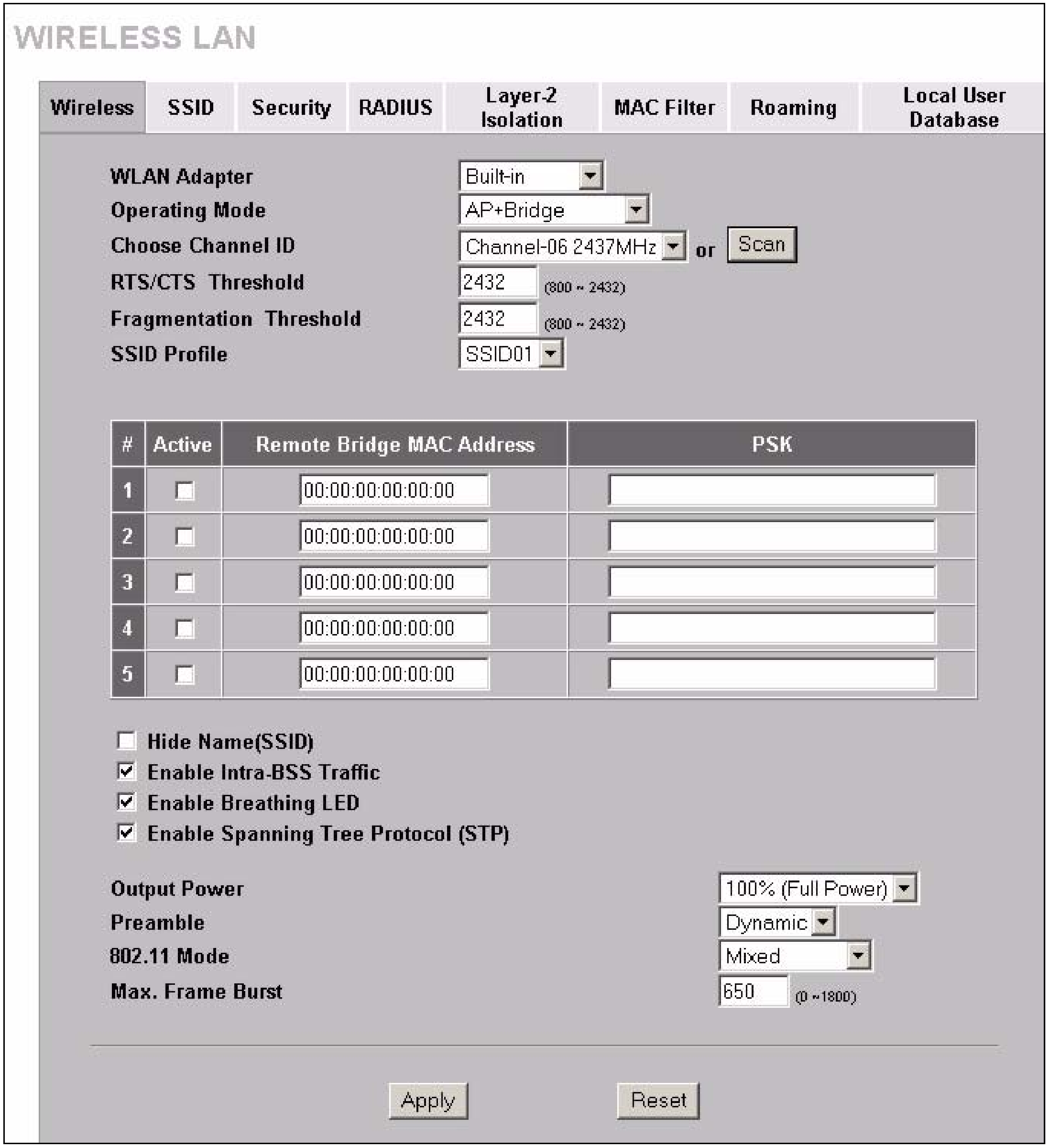
LABEL	DESCRIPTIONS
Operating Mode	Select **Bridge/Repeater** in this field.
Enable WDS Security	A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Select the check box to encrypt the traffic between the APs. When you select the check box, need to configure a Pre-Shared Key (PSK) for each peer device. The ZyXEL Device uses TKIP to encrypt traffic on the WDS between APs. Note: Other APs must use the same encryption method to enable WDS security.
#	This is the index number of the bridge connection.
Active	Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it.
Remote Bridge MAC Address	Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

See Table 13 on page 79 for information on the other labels in this screen.

6.6.3 AP+Bridge Mode

Select **AP+Bridge** as the **Operating Mode** in the **WIRELESS** > **Wireless** screen to have the ZyXEL Device function as a bridge and access point simultaneously. See the section on applications for more information.

Figure 38 Wireless: AP+Bridge



WLAN Adapter	Built-in
Operating Mode	AP+Bridge
Choose Channel ID	Channel-06 2437MHz or Scan
RTS/CTS Threshold	2432 (800 ~ 2432)
Fragmentation Threshold	2432 (800 ~ 2432)
SSID Profile	SSID01

#	Active	Remote Bridge MAC Address	PSK
1	□	00:00:00:00:00:00	
2	□	00:00:00:00:00:00	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	

□ Hide Name(SSID)
☑ Enable Intra-BSS Traffic
☑ Enable Breathing LED
☑ Enable Spanning Tree Protocol (STP)

Output Power	100% (Full Power)
Preamble	Dynamic
802.11 Mode	Mixed
Max. Frame Burst	650 (0 ~1800)

See the tables describing the fields in the **Access Point** and **Bridge/Repeater** operating modes for descriptions of the fields in this screen.

In **AP+Bridge** mode, you must use security for both the AP and bridge functions, or for neither. If the security profile (for the traffic between the AP and the wireless clients) is not set to use security, there is also no security for the bridge traffic between APs. If the security profile is set to use security, you must also configure security for the bridge connections.

6.6.4 MESSID Mode

Select **MESSID** as the **Operating Mode** to display the screen. Refer to Chapter 8 on page 105 for configuration and detailed information. See Chapter 7 on page 87 for details on the security settings.

7

Wireless Security Configuration

This chapter describes how to use the **Security**, **RADIUS** and **Local User Database** screens to configure wireless security on your ZyXEL Device.

7.1 Wireless Security Overview

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

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

7.1.1 Encryption

- Use WPA(2) security if you have WPA(2)-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.
- If you don't have WPA(2)-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off. You can manually enter 64-bit or 128-bit WEP keys.

7.1.2 Authentication

WPA has user authentication and you can also configure IEEE 802.1x to use the built-in database (Local User Database) or a RADIUS server to authenticate wireless clients before joining your network.

- Use RADIUS authentication if you have a RADIUS server. See the appendices for information on protocols used when a client authenticates with a RADIUS server via the ZyXEL Device.
- Use the Local User Database if you have less than 32 wireless clients in your network. The ZyXEL Device uses MD5 encryption when a client authenticates with the Local User Database

7.1.3 Restricted Access

The **MAC Filter** screen allows you to configure the AP to give exclusive access to devices (**Allow Association**) or exclude them from accessing the AP (**Deny Association**).

7.1.4 Hide Identity

If you hide the SSID, then the ZyXEL Device cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the ZyXEL Device may be inconvenience for some valid WLAN clients.

7.1.5 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.

7.2 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

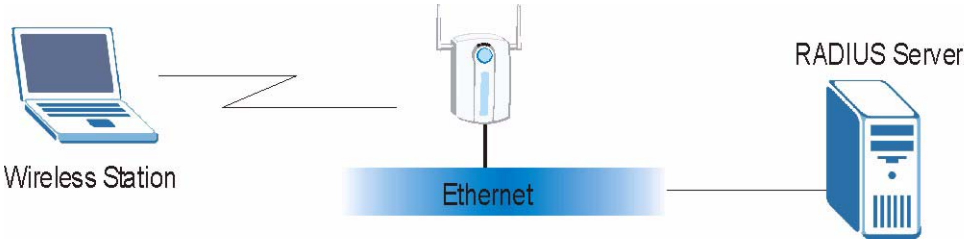
7.3 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP. The ZyXEL Device supports EAP-TLS, EAP-TTLS, EAP-MD5 and PEAP with RADIUS. Refer to the Types of EAP Authentication appendix for descriptions on the common types.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

Figure 39 EAP Authentication



The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

1 The wireless station sends a "start" message to the ZyXEL Device.

2 The ZyXEL Device sends a “request identity” message to the wireless station for identity information.

3 The wireless station replies with identity information, including username and password.

4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

7.4 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption.

7.4.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS, EAP and PEAP.

If you don’t have an external RADIUS server you should use WPA-PSK (WPA -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 client will be granted access to a WLAN.

7.4.2 Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

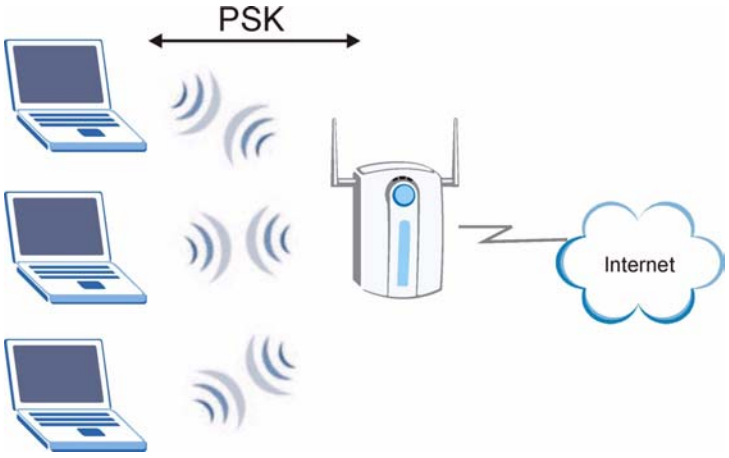
The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

7.4.3 WPA(2)-PSK Application Example

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

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
2. The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 40 WPA(2)-PSK Authentication

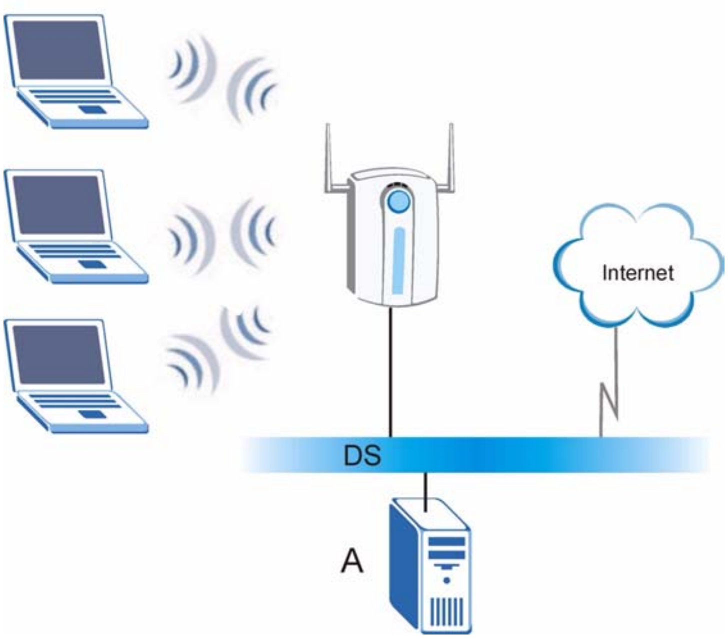


7.5 WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. “A” is the RADIUS server. “DS” is the distribution system.

1. The AP passes the wireless client’s authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 41   WPA(2) with RADIUS Application Example



7.6 Security Modes

The following table describes the security modes you can configure.

Table 15   Security Modes

SECURITY MODE	DESCRIPTION
None	Select this to have no data encryption.
WEP	Select this to use WEP encryption.
802.1x-Only	Select this to use 802.1x authentication with no data encryption.
802.1x-Static64	Select this to use 802.1x authentication with a static 64bit WEP key and an authentication server.
802.1x-Static128	Select this to use 802.1x authentication with a static 128bit WEP key and an authentication server.
802.1x-Dynamic64	Select this to use 802.1x authentication with a dynamic 64bit WEP key and an authentication server.
802.1x-Dynamic128	Select this to use 802.1x authentication with a dynamic 128bit WEP key and an authentication server.
WPA	Select this to use WPA.
WPA-MIX	Select this to use either WPA, 802.1x authentication with a dynamic 64bit WEP key or 802.1x authentication with a dynamic 128bit WEP key depending on which security mode the wireless client uses.
WPA-PSK	Select this to use WPA with a pre-shared key.
WPA2	Select this to use WPA2.
WPA2-MIX	Select this to use either WPA2 or WPA depending on which security mode the wireless client uses.
WPA2-PSK	Select this to use WPA2 with a pre-shared key.

Table 15 Security Modes

SECURITY MODE	DESCRIPTION
WPA2-PSK-MIX	Select this to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
No-Access	Select this to stop wireless clients from accessing the ZyXEL Device.

7.7 Security Modes and Wireless Client Compatibility

Different security modes can be configured for each SSID. However, not all security modes are compatible with the security mode of the wireless client. The following table shows combinations of security modes between a Windows XP wireless client and the ZyXEL Device. Combinations of security modes not marked with a "**O**" or not listed may not be able to make a connection using the SSID. Other wireless clients such as Funk Odyssey may connect using a security combination not listed on the table.

Table 16 Security Modes for ZyXEL Device and Windows XP Wireless Client

	WEP	8021X-ONLY	8021X-DYNAMIC	8021X-STATIC	WPA	WPA-PSK	WPA-MIX	WPA2	WPA2-PSK	WPA2-MIX	WPA2-PSK-MIX	NONE	NO ACCESS
WEP	O	O	O	O									O
8021X-ONLY	O	O	O	O									O
8021X-DYNAMIC	O	O	O	O									O
8021X-STATIC	O	O	O	O									O
WPA					O			O	O				
WPA-PSK						O		O	O				
WPA-MIX							O	O	O				
WPA2					O	O	O	O					
WPA2-PSK					O	O	O		O				
WPA2-MIX										O			
WPA2-PSK-MIX											O		
NONE												O	
NO ACCESS	O	O	O	O									O

7.8 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, and Meetinghouse Data Communications' AEGIS 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.

The Funk Software's Odyssey client is bundled free (at the time of writing) with the client wireless adaptor(s).

7.9 Wireless Security Effectiveness

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device. EAP (Extensible Authentication Protocol) is used for authentication and utilizes static WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

Table 17 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

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

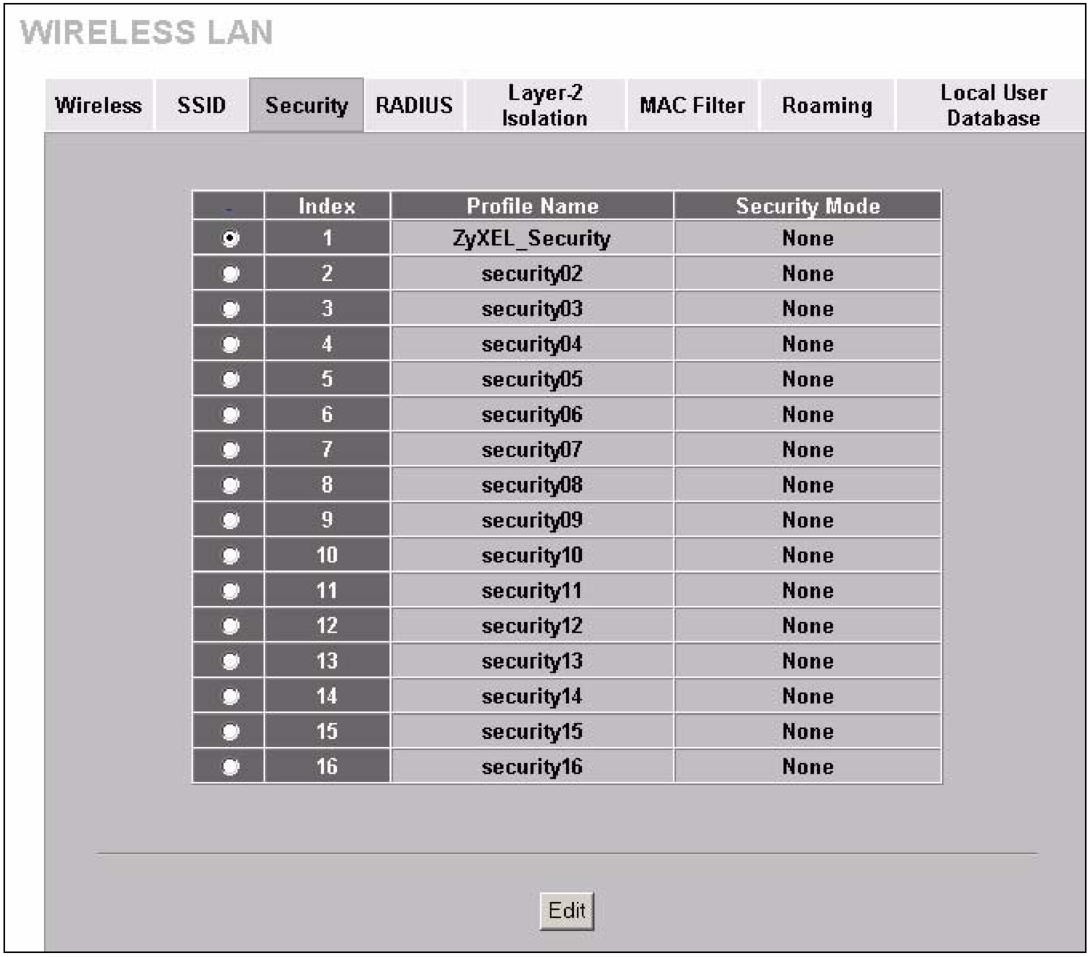
7.10 Configuring Security

The following screens are configurable only in **Access Point, AP+Bridge and MESSID** operating modes only.

Use the wireless security screens to create secure profiles. A security profile is a group of configuration settings which can be assigned to an SSID profile in the **SSID** configuration screen.

To change your ZyXEL Device’s wireless security settings, click **WIRELESS** > **Security**.

Figure 42 Security



-	Index	Profile Name	Security Mode
●	1	ZyXEL_Security	None
○	2	security02	None
○	3	security03	None
○	4	security04	None
○	5	security05	None
○	6	security06	None
○	7	security07	None
○	8	security08	None
○	9	security09	None
○	10	security10	None
○	11	security11	None
○	12	security12	None
○	13	security13	None
○	14	security14	None
○	15	security15	None
○	16	security16	None

The following table describes the labels in this screen.

Table 18 Security

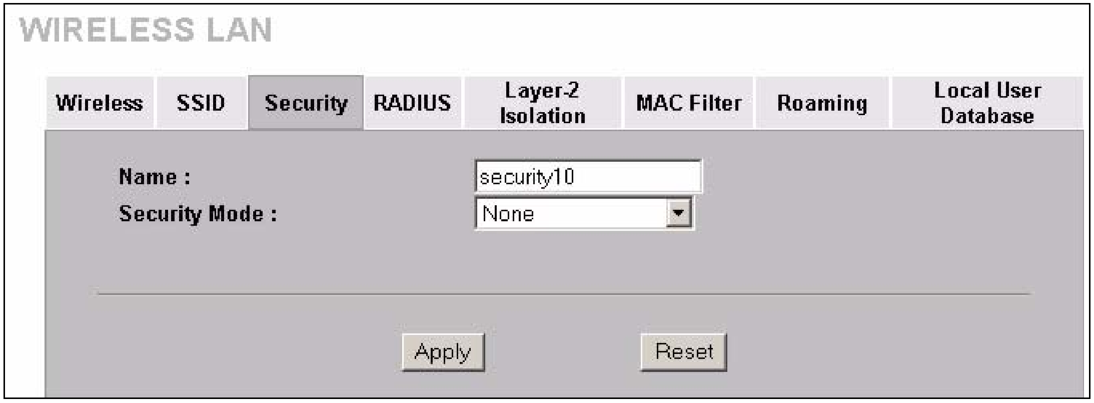
LABEL	DESCRIPTION
Index	This is the number of the security profile.
Profile Name	This field displays a name given to a security profile in the **Security** configuration screen.
Security Mode	This field displays the security mode this security profile uses. The last profile is automatically set to **8021x-Only** if configure the **Password** screen's administrator authentication on RADIUS option.
Edit	Select an entry from the list and click **Edit** to configure security settings for that profile.

The next screen varies according to the **Security Mode** you select.

7.10.1 Security: None

Select **None** in the **Security Mode** field to allow all wireless clients access to the ZyXEL Device.

Figure 43 Security: None



Name : security10

Security Mode : None

The following table describes the labels in this screen.

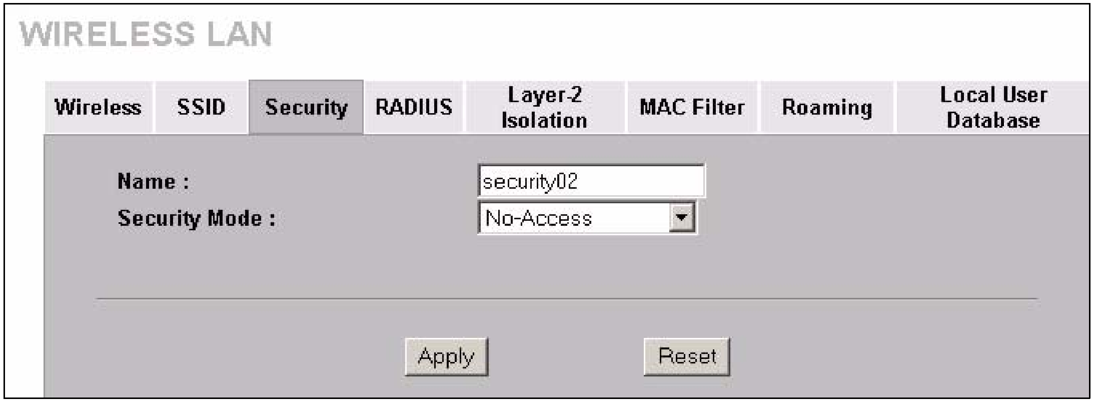
Table 19 Security: No-Access

LABEL	DESCRIPTION
Name	Type a name to identify this security profile. Use up to 20 ASCII characters. Spaces are allowed.
Security Mode	Choose **None** in this field.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.10.2 Security: No-Access

Select **No-Access** in the **Security Mode** field to block all wireless access to the ZyXEL Device.

Figure 44 Security: No-Access



Name : security02

Security Mode : No-Access

The following table describes the labels in this screen.

Table 20 Security: No-Access

LABEL	DESCRIPTION
Name	Type a name to identify this security profile. Use up to 20 ASCII characters. Spaces are allowed.
Security Mode	Choose **No-Access** in this field.

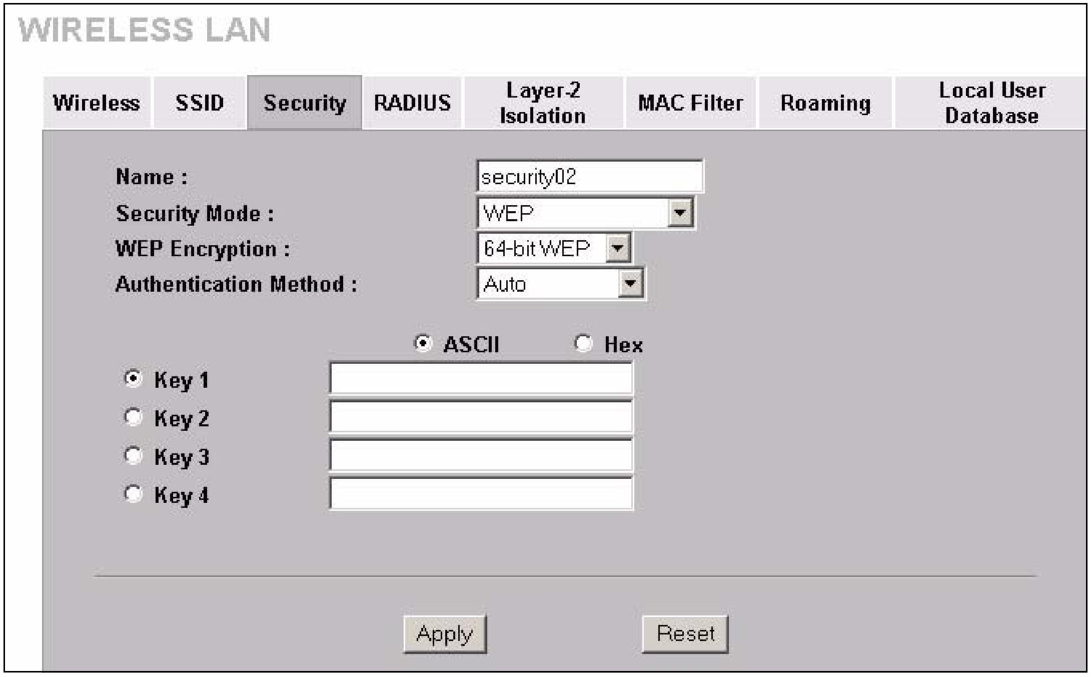
Table 20 Security: No-Access

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.10.3 Security: WEP

Select **WEP** in the **Security Mode** field to display the following screen.

Figure 45 Security: WEP



Name : security02
Security Mode : WEP
WEP Encryption : 64-bit WEP
Authentication Method : Auto

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

The following table describes the labels in this screen.

Table 21 Security: WEP

LABEL	DESCRIPTION
Name	Type a name to identify this security profile. Use up to 20 ASCII characters. Spaces are allowed.
Security Mode	Choose **WEP** in this field.
WEP Encryption	Select **Disable** to allow wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	Select **Auto**, **Open System** or **Shared Key** from the drop-down list box. The default setting is **Auto**.
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding “0x” is entered automatically.

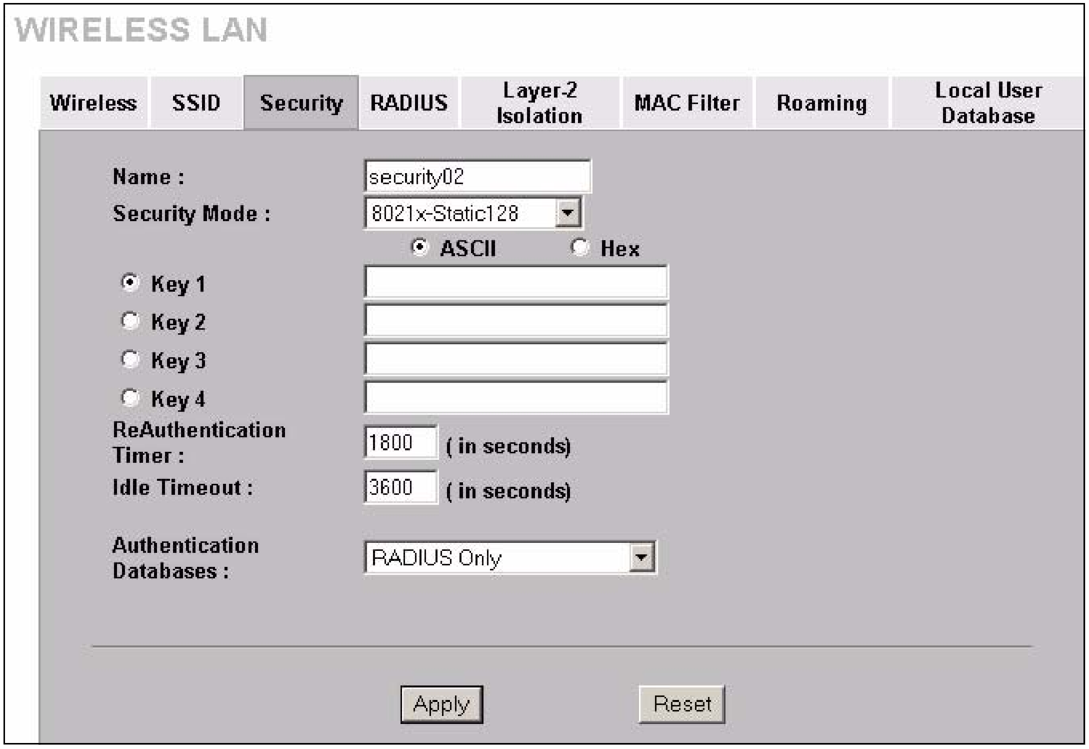
Table 21 Security: WEP

LABEL	DESCRIPTION
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"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.10.4 Security: 802.1x Only, 802.1x Static 64-bit, 802.1x Static 128-bit

Select **802.1x Only, 802.1x Static 64** or **802.1x Static 128** in the **Security Mode** field to display the following screen.

Figure 46 Security: 802.1x Static 64-bit, 802.1x Static 128-bit



Name : security02
Security Mode : 8021x-Static128
● ASCII ○ Hex
● Key 1
○ Key 2
○ Key 3
○ Key 4
ReAuthentication Timer : 1800 (in seconds)
Idle Timeout : 3600 (in seconds)
Authentication Databases : RADIUS Only

The following table describes the labels in this screen.

Table 22 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

LABEL	DESCRIPTION
Name	Type a name to identify this security profile. Use up to 20 ASCII characters. Spaces are allowed.
Security Mode	Choose **802.1x Static 64 or 802.1x Static 128** in this field.
ASCII	Select this option to enter ASCII characters as the WEP keys.

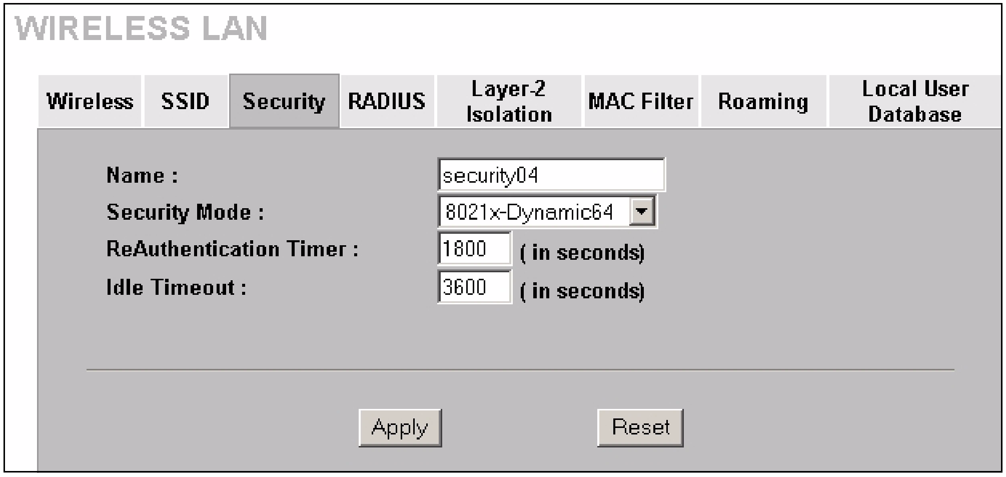
Table 22 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

LABEL	DESCRIPTION
Hex	Select this option to enter hexadecimal characters as the WEP keys.The preceding “0x” is entered automatically.
Key 1 to Key 4	If you chose **802.1x Static 64**, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **802.1x Static 128-bit**, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations. The preceding “0x” is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. The default time interval is **3600** seconds (or 1 hour).
Authentication Databases	Select **Local User Database Only** to have the system use the internal user account database. Select **RADIUS Only** to have the system use an external RADIUS server. Select **Local first then RADIUS** to have the system check the internal user account database first, and then the external RADIUS server if there is no match. Select **RADIUS first then Local** to have the system check the external RADIUS server first, and then the internal user account database if there is no match.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.10.5 Security: 802.1x Dynamic 64-bit or 802.1x Dynamic 128-bit

Select **8021x-Dynamic64** or **8021x-Dynamic128** in the **Security Mode** field to display the following screen.

Figure 47 Security: WPA, 802.1x Dynamic 64-bit, 802.1x Dynamic 128-bit or WPA-MIX



Name : security04

Security Mode : 8021x-Dynamic64

ReAuthentication Timer : 1800 (in seconds)

Idle Timeout : 3600 (in seconds)

The following table describes the labels in this screen.

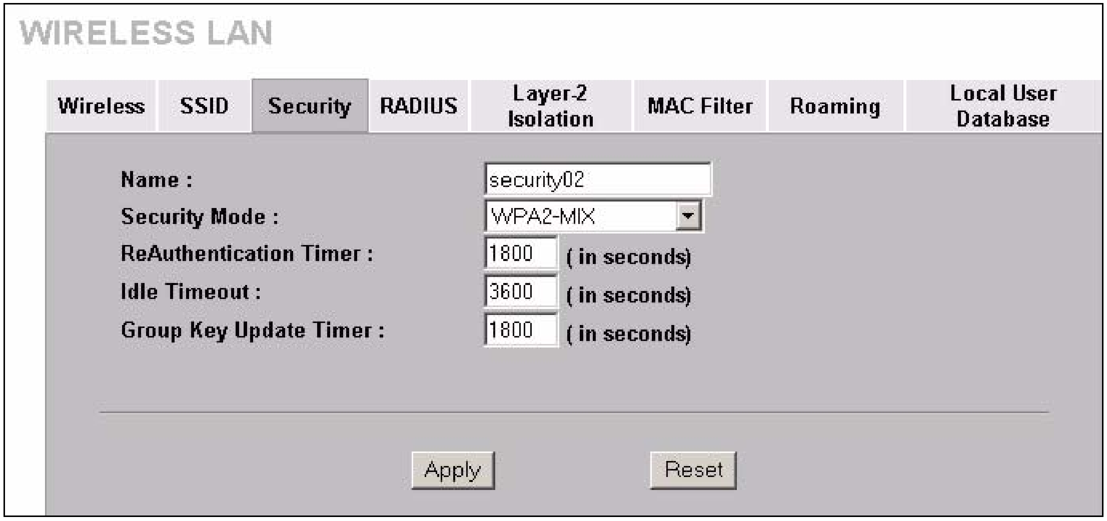
Table 23 Security: 802.1x Dynamic 64-bit or 802.1x Dynamic 128-bit

LABEL	DESCRIPTION
Name	Type a name to identify this security profile. Use up to 20 ASCII characters. Spaces are allowed.
Security Mode	Choose **8021x-Dynamic64** or **8021x-Dynamic128** in this field.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device default is 1800 seconds (30 minutes).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.10.6 Security: WPA, WPA2, WPA-MIX or WPA2-MIX

Select **WPA, WPA2, WPA-MIX** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

Figure 48 Security:WPA2 or WPA2-MIX



Name : security02

Security Mode : WPA2-MIX

ReAuthentication Timer : 1800 (in seconds)

Idle Timeout : 3600 (in seconds)

Group Key Update Timer : 1800 (in seconds)

The following table describes the labels not previously discussed

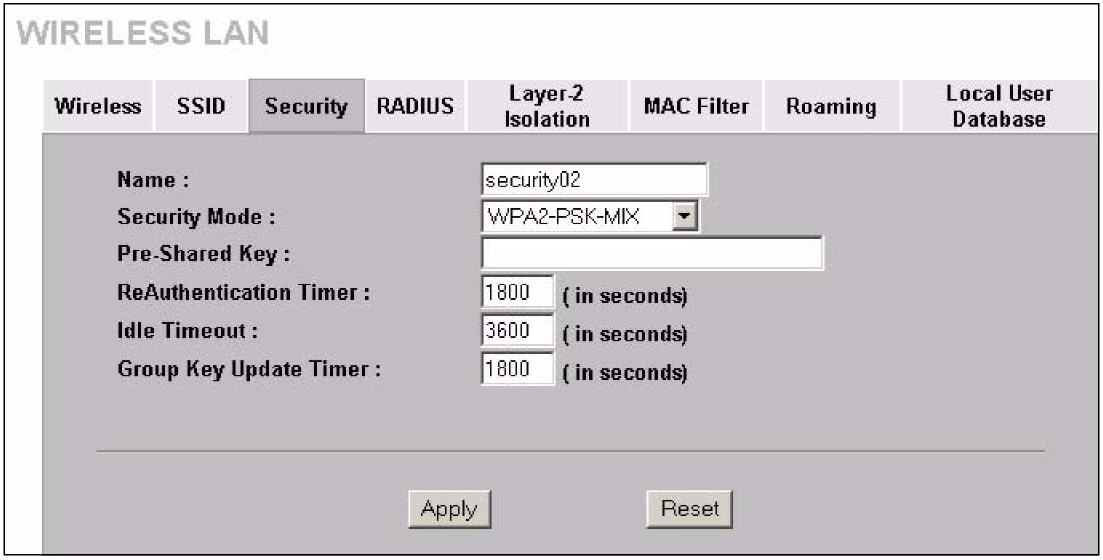
Table 24 Security: WPA2 or WPA2-MIX

LABEL	DESCRIPTIONS
Name	Type a name to identify this security profile. Use up to 20 ASCII characters. Spaces are allowed.
Security Mode	Choose **WPA, WPA2, WPA-MIX** or **WPA2-MIX** in this field.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device‘s default is 1800 seconds (30 minutes).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.10.7 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in the **Security Mode** field to display the following screen.

Figure 49 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX



Name : security02
Security Mode : WPA2-PSK-MIX
Pre-Shared Key :
ReAuthentication Timer : 1800 (in seconds)
Idle Timeout : 3600 (in seconds)
Group Key Update Timer : 1800 (in seconds)

The following table describes the labels not previously discussed

Table 25 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Name	Type a name to identify this security profile. Use up to 20 ASCII characters. Spaces are allowed.
Security Mode	Choose **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in this field.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device's default is 1800 seconds (30 minutes).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.11 Introduction to RADIUS

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

- Authentication
  Determines the identity of the users.
- Accounting
  Keeps track of the client's network activity.

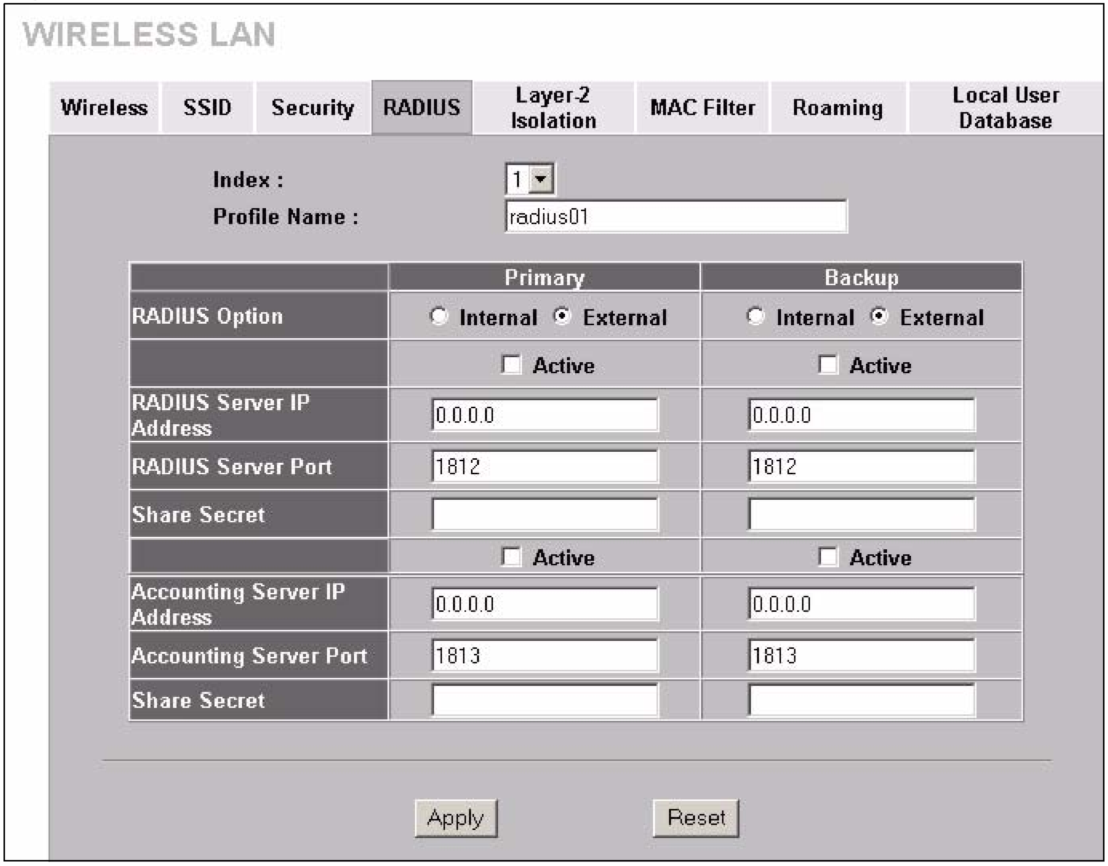
7.12 Configuring RADIUS

Use RADIUS if you want to authenticate wireless users using a RADIUS server.

You can configure up to four RADIUS server profiles. Each profile also has one backup authentication server and a backup accounting server. These profiles can be assigned to an SSID profile in the **SSID** configuration screen

To set up your ZyXEL Device's RADIUS server settings, click **WIRELESS** > **RADIUS**. The screen appears as shown.

Figure 50 RADIUS



Index : 1

Profile Name : radius01

	Primary	Backup
RADIUS Option	○ Internal ● External	○ Internal ● External
	□ Active	□ Active
RADIUS Server IP Address	0.0.0.0	0.0.0.0
RADIUS Server Port	1812	1812
Share Secret		
	□ Active	□ Active
Accounting Server IP Address	0.0.0.0	0.0.0.0
Accounting Server Port	1813	1813
Share Secret		

The following table describes the labels in this screen.

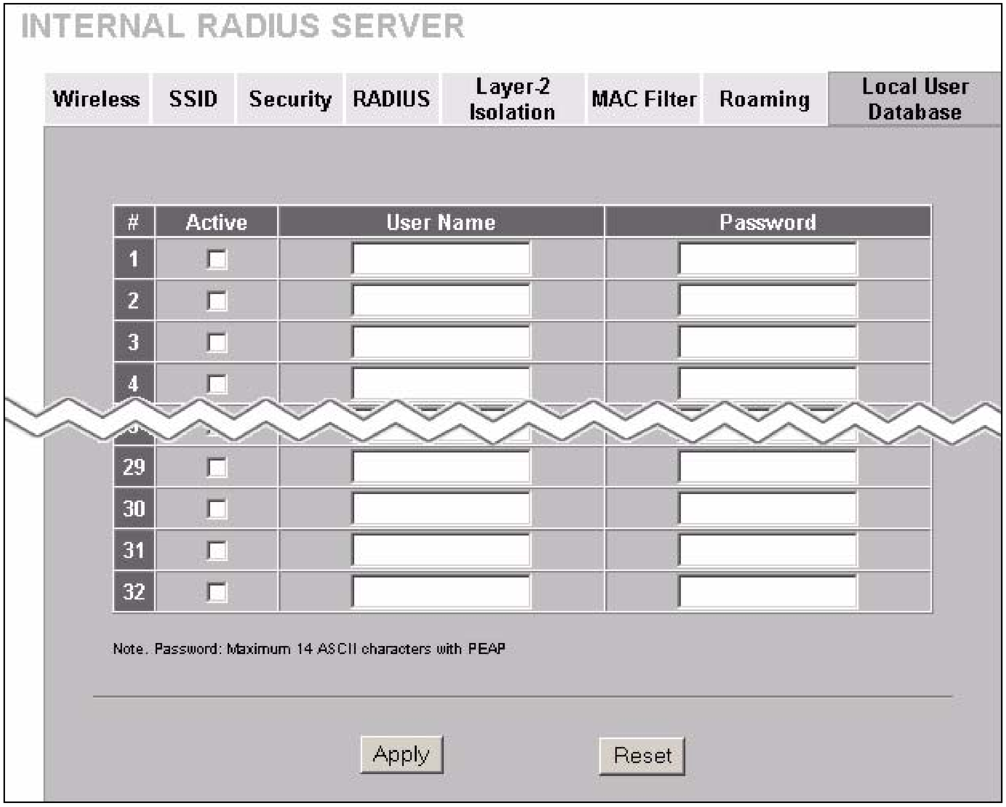
Table 26 RADIUS

LABEL	DESCRIPTION
Index	Select the RADIUS profile you want to configure from the drop-down list box.
Profile Name	Type a name for the RADIUS profile associated with the **Index** number above. Use up to 32 ASCII characters. Spaces are allowed.
Primary	Configure the fields below to have user authentication and accounting through RADIUS servers.
Backup	If the ZyXEL Device cannot communicate with the **Primary** RADIUS server, it can use a **Backup** RADIUS server. Make sure both **Active** check boxes are selected if you want to use backup servers. The ZyXEL Device will attempt to communicate three times before using **Backup** servers. Requests can be issued from the client interface to use the backup server. The length of time for each authentication is decided by the wireless client or based on the configuration of the **ReAuthentication Timer** field in the **Security** screen.
RADIUS Option	This option is not available on all models. Select **Internal** to use the ZyXEL Device's internal RADIUS server. Select **External** to use an external RADIUS server.
Active	Select the check box to enable user authentication using the RADIUS server specified in this column.
RADIUS Server IP Address	Enter the IP address of the authentication server in dotted decimal notation. You do not need to configure this field when using the ZyXEL Device's internal RADIUS server (not available on all models).
RADIUS Server Port	Enter the port number of the authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so. You do not need to configure this field when using the ZyXEL Device's internal RADIUS server (not available on all models).
Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the authentication server and the ZyXEL Device. The key must be the same on the authentication server and your ZyXEL Device. The key is not sent over the network. You do not need to configure this field when using the ZyXEL Device's internal RADIUS server (not available on all models).
Active	Select the check box to enable user accounting through the RADIUS server specified in this column. You cannot use an accounting server when using a ZyXEL Device's internal RADIUS server.
Accounting Server IP Address	Enter the IP address of the accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the 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.
Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the accounting server and the ZyXEL Device. The key must be the same on the accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.13 Configuring Local User Database

To change your ZyXEL Device's trusted users, click **WIRELESS > Local User Database**. The screen appears as shown.

Figure 51 Local User Database



#	Active	User Name	Password
1	□		
2	□		
3	□		
4	□		
29	□		
30	□		
31	□		
32	□		

Note. Password: Maximum 14 ASCII characters with PEAP

The following table describes the labels in this screen.

Table 27 Local User Database

LABEL	DESCRIPTION
#	This field displays the trusted user index number.
Active	Select this check box to have the ZyXEL Device authenticate wireless clients with the same user name and password activated on their wireless utility.
User Name	Enter the username for this user account. This name can be up to 31 alphanumeric characters long, including spaces. The login name on the wireless client's utility must be the same as this user name on so it can authenticate the RADIUS server using the certificate information.
Password	Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type. The password on the wireless client's utility must be the same as this password on so it can authenticate the RADIUS server using the certificate information. If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to begin configuring this screen afresh.

8

MESSID and SSID

This chapter describes how to configure and use your ZyXEL Device's MESSID mode and configure SSID profiles.

8.1 Wireless LAN Infrastructures

See the Wireless LAN chapter for some basic WLAN scenarios and terminology.

8.1.1 MESSID

Traditionally, you needed to use different APs to configure different Extended Service Sets (ESSs). As well as the cost of buying extra APs, there was also the possibility of channel interference. The ZyXEL Device's MESSID (Multiple Extended Service Set IDentifier) function allows you to use one access point to provide several ESSs simultaneously. You can then assign varying levels of privilege to different SSIDs.

Wireless stations can use different ESSIDs to associate with the same AP.

You can assign different wireless and security settings to each SSID profile. This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain ESSs.

To the wireless clients in the network, each SSID appears to be a different access point. As in any wireless network, clients can associate only with the SSIDs for which they have the correct security settings.

8.1.2 Notes on Multiple ESS

- Configure up to 16 ESSs on the ZyXEL Device.
- A maximum of eight ESSs can operate simultaneously on the ZyXEL Device.
- Use different security settings for different ESSs. For example, if two stations connect to different ESSIDs (they are in different ESSs), but have the same WEP keys, they may hear each other's communications (but not communicate with each other).
- You can hide or broadcast ESS IDs (so site survey tools can or cannot find them by scanning).
- Multi-ESS should not replace but rather be used in conjunction with 802.1x security.

8.1.3 Multiple ESS Example

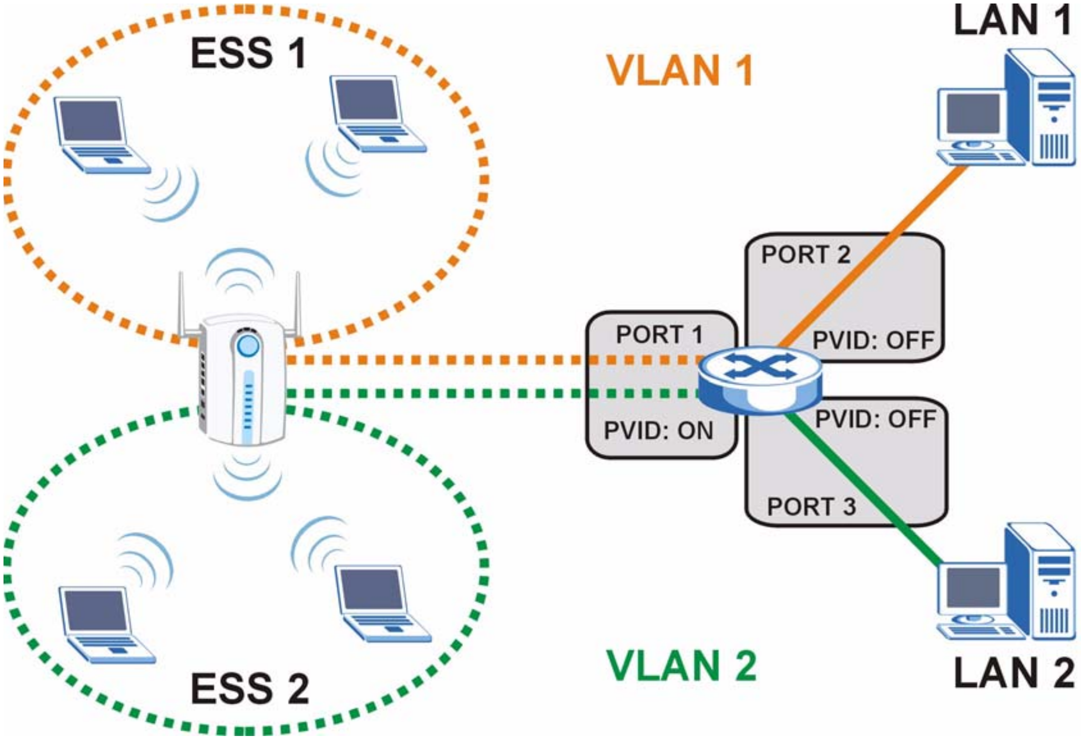
Refer to the applications section for more information.

8.1.4 Multiple ESS with VLAN Example

In this example, VLAN 2 includes the computers in ESS1 and LAN 1. Computers in ESS2 and LAN 2 belong to VLAN 2. Users in ESS1 are limited to accessing the resources on LAN 1 and similarly users in ESS2 may only access resources on LAN 2. VLAN 2 is the management VLAN.

The switch adds PVID (Port VLAN IDentity) tags to incoming frames that don’t already have tags (on switch ports where PVID is enabled).

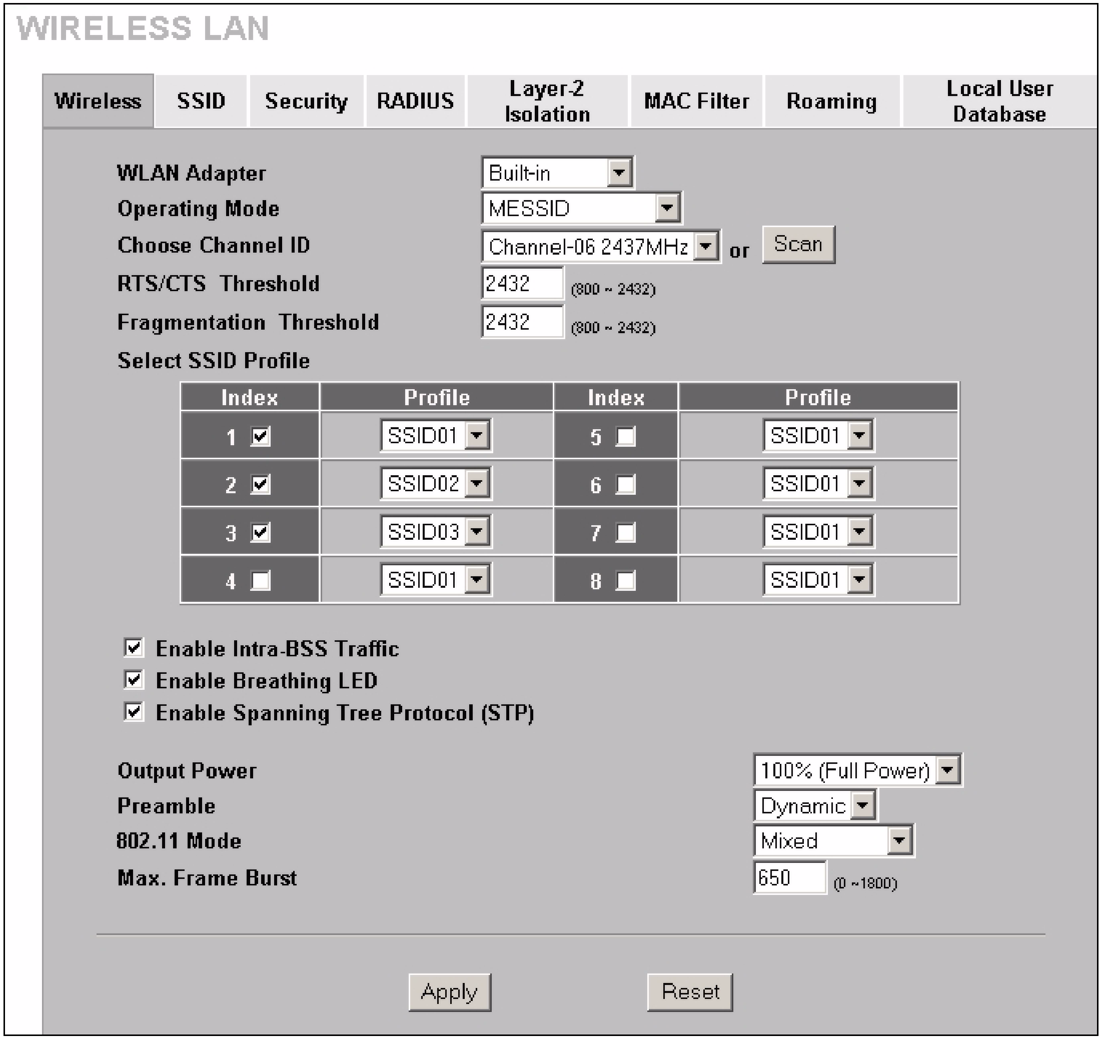
Figure 52   Multiple ESS with VLAN Example



8.1.5 Configuring Multiple ESSs

Click **WIRELESS** > **Wireless** and select **MESSID** in the **Operating Mode** drop-down list box to display the screen as shown.

Figure 53 Wireless: Multiple ESS



WLAN Adapter: Built-in

Operating Mode: MESSID

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (800 ~ 2432)

Fragmentation Threshold: 2432 (800 ~ 2432)

Select SSID Profile

Index	Profile	Index	Profile
1 ☑	SSID01	5 □	SSID01
2 ☑	SSID02	6 □	SSID01
3 ☑	SSID03	7 □	SSID01
4 □	SSID01	8 □	SSID01

☑ Enable Intra-BSS Traffic

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power: 100% (Full Power)

Preamble: Dynamic

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

The following table describes the labels in this screen.

Table 28 Wireless: Multiple ESS

LABEL	DESCRIPTION
WLAN Adapter	This field only appears when you have a compatible WLAN card in the ZyXEL Device's extension card slot. Note: Contact your distributor for information on compatible WLAN cards. Select **Built-in** to configure settings for the ZyXEL Device's the internal WLAN card. Select **Removable** to configure settings for the ZyXEL Device's WLAN card in the extension card slot.
Operating Mode	Select **MESSID** in this field to display the screen as shown

Table 28 Wireless: Multiple ESS

LABEL	DESCRIPTION
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyXEL Device automatically select a channel, click **Scan** instead.
Scan	Click this button to have the ZyXEL Device automatically select the wireless channel with the lowest interference.
RTS/CTS Threshold	The threshold (number of bytes) for enabling RTS/CTS handshake. Data with a frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **800** and **2346**.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **800** and **2346**.
Select SSID Profile	An SSID profile is the set of parameters relating to one of the ZyXEL Device's ESSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating with the access point (AP) must have the same SSID. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or 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.
Index	Select the check box to activate an SSID profile.
Profile	Select the profile(s) of the SSIDs you want to use in your wireless network. You can have up to eight ESSs running on the ZyXEL Device simultaneously. Configure SSID profiles in the **SSID** screen.
Enable Breathing LED	Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyXEL Device is on and blinks (or breathes) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyXEL Device is on and data is being transmitted/received.
Enable Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the same BSS. Enable intra-BSS traffic to allow wireless stations connected to one of the ZyXEL Device's BSSs to communicate with each other. Disable intra-BSS traffic to only allow wireless stations in a BSS to communicate with the wired network, not with each other. Wireless stations can still communicate with wireless stations in other BSSs. Use layer-2 isolation to also block wireless stations from communicating with wireless stations in other BSSs. Note: This check box is automatically cleared (intra-BSS traffic is blocked) if you configure an SSID to use layer-2 isolation. Re-select this check box if you want to allow intra-BSS traffic.

Table 28 Wireless: Multiple ESS

LABEL	DESCRIPTION
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select from **100% (Full Power)**, **50%**, **25%** and **12.5%**. See the product specifications for more information on your ZyXEL Device's output power.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** and **Dynamic**. See the section on preamble for more information.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **Mixed** to allow both IEEE 802.11b and IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Max. Frame Burst	Enable maximum frame burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum frame burst sets the maximum time, in microseconds, that the ZyXEL Device transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.2 SSID

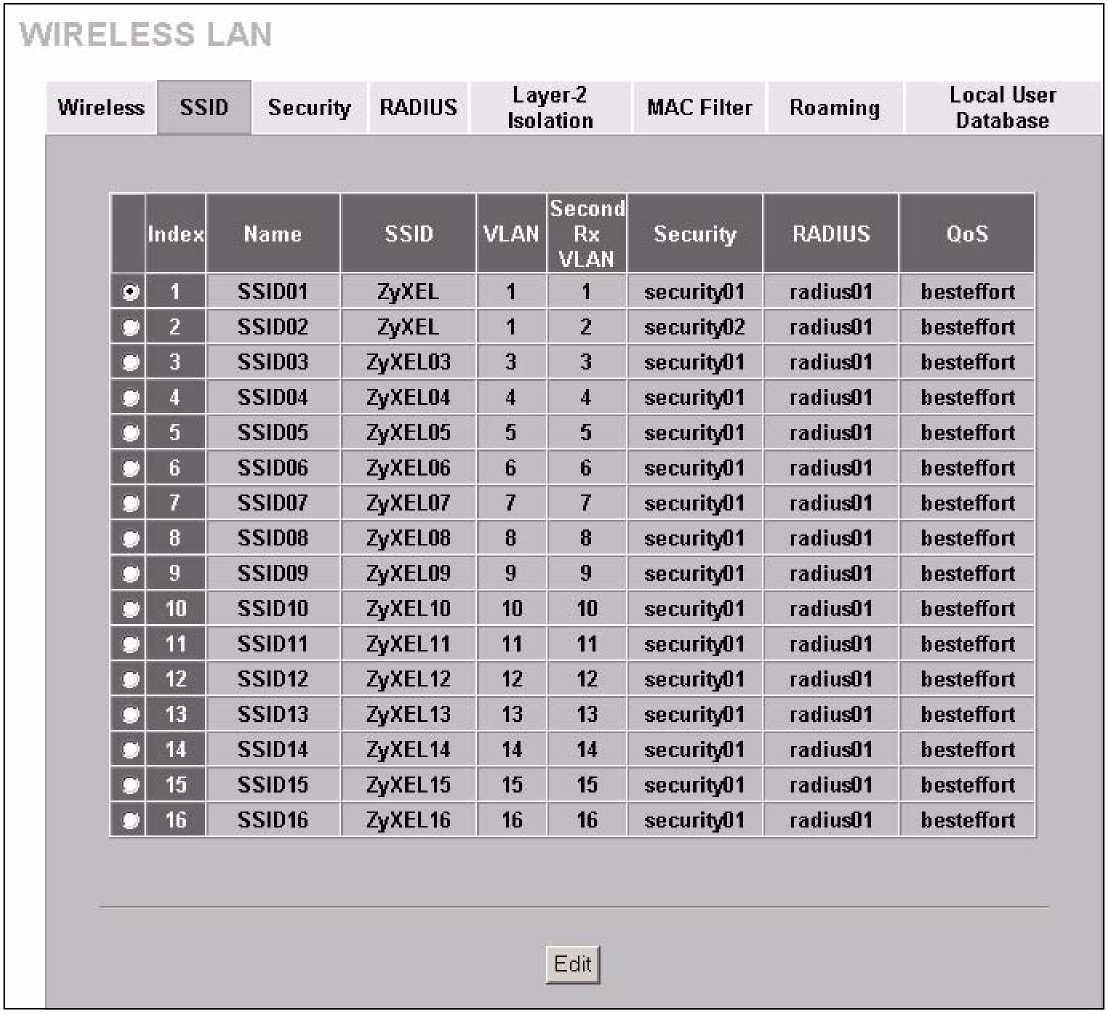
When the ZyXEL Device is set to Access Point, AP+Bridge or MESSID mode, you need to choose the SSID profile(s) you want to use in your wireless network (see Section 6.5 on page 78 for more information on operating modes).

Use the **WIRELESS** > **SSID** screen to see information about the SSID profiles on the ZyXEL Device, and use the **WIRELESS** > **SSID** > **Edit** screen to configure the SSID profiles.

8.2.1 The SSID Screen

Click **WIRELESS** > **SSID** to display the screen as shown.

Figure 54 SSID



	Index	Name	SSID	VLAN	Second Rx VLAN	Security	RADIUS	QoS
◉	1	SSID01	ZyXEL	1	1	security01	radius01	besteffort
○	2	SSID02	ZyXEL	1	2	security02	radius01	besteffort
○	3	SSID03	ZyXEL03	3	3	security01	radius01	besteffort
○	4	SSID04	ZyXEL04	4	4	security01	radius01	besteffort
○	5	SSID05	ZyXEL05	5	5	security01	radius01	besteffort
○	6	SSID06	ZyXEL06	6	6	security01	radius01	besteffort
○	7	SSID07	ZyXEL07	7	7	security01	radius01	besteffort
○	8	SSID08	ZyXEL08	8	8	security01	radius01	besteffort
○	9	SSID09	ZyXEL09	9	9	security01	radius01	besteffort
○	10	SSID10	ZyXEL10	10	10	security01	radius01	besteffort
○	11	SSID11	ZyXEL11	11	11	security01	radius01	besteffort
○	12	SSID12	ZyXEL12	12	12	security01	radius01	besteffort
○	13	SSID13	ZyXEL13	13	13	security01	radius01	besteffort
○	14	SSID14	ZyXEL14	14	14	security01	radius01	besteffort
○	15	SSID15	ZyXEL15	15	15	security01	radius01	besteffort
○	16	SSID16	ZyXEL16	16	16	security01	radius01	besteffort

The following table describes the labels in this screen.

Table 29 SSID

LABEL	DESCRIPTION
Index	This field displays the index number of each SSID profile.
Name	This field displays the identification name of each SSID profile on the ZyXEL Device.
SSID	This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
VLAN	This field displays the number of the VLAN to which the wireless clients using this SSID belong.
Second RX VLAN	This field displays the number of a second VLAN to which the wireless clients using this SSID belong.
Security	This field indicates which security profile is currently associated with each SSID profile. See Section 7.10 on page 93 for more information.
RADIUS	This field displays which RADIUS profile is currently associated with each SSID profile, if you have a RADIUS server configured.

Table 29 SSID

LABEL	DESCRIPTION
QoS	This field displays the Quality of Service setting for this profile.
Edit	Click the radio button next to the profile you want to configure and click **Edit** to go to the SSID configuration screen.

8.2.2 Configuring SSID

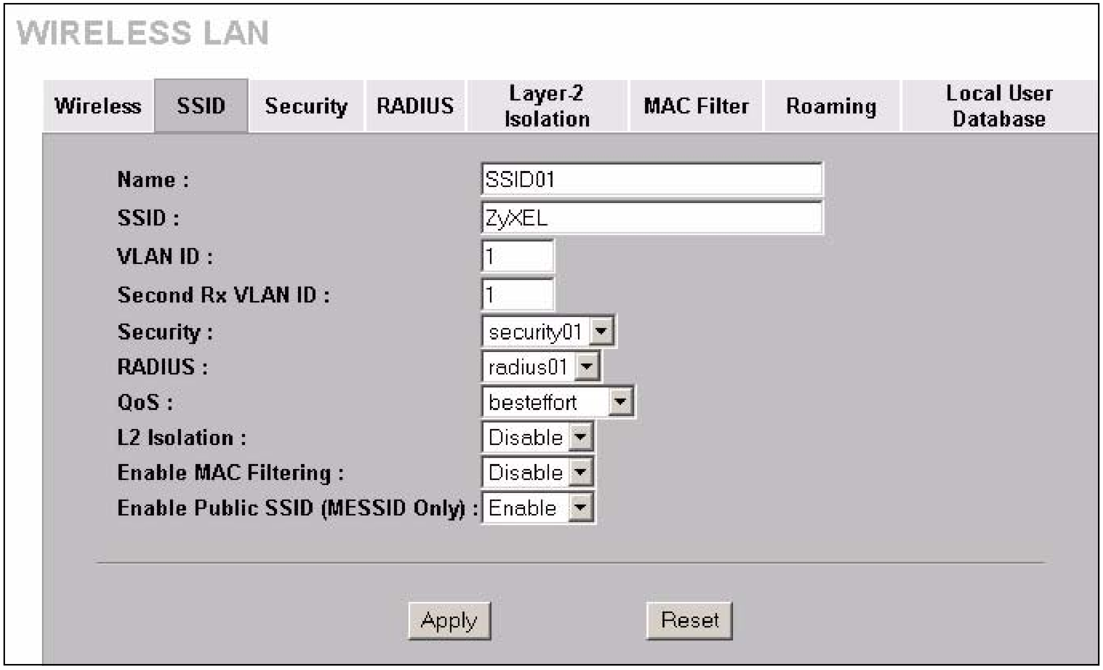
Each SSID profile references the settings configured in the following screens:

- **WIRELESS** > **Security** (one of the security profiles).
- **WIRELESS** > **RADIUS** (one of the RADIUS profiles).
- **WIRELESS** > **MAC Filter** (the MAC filter list, if activated in the SSID profile).
- **WIRELESS** > **Layer 2 Isolation** (the layer 2 isolation list, if activated in the SSID profile).
- Also, use the **VLAN** screen to set up wireless VLANs based on SSID.

Configure the fields in the above screens to use the settings in an SSID profile.

Select an SSID profile in the **WIRELESS** > **SSID** screen and click **Edit** to display the following screen.

Figure 55 Configuring SSID



Name : SSID01
SSID : ZyXEL
VLAN ID : 1
Second Rx VLAN ID : 1
Security : security01
RADIUS : radius01
QoS : besteffort
L2 Isolation : Disable
Enable MAC Filtering : Disable
Enable Public SSID (MESSID Only) : Enable

The following table describes the labels in this screen.

Table 30 Configuring SSID

LABEL	DESCRIPTION
Name	Enter a name (up to 32 ASCII characters) to identify this profile. Spaces are allowed.
SSID	When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.

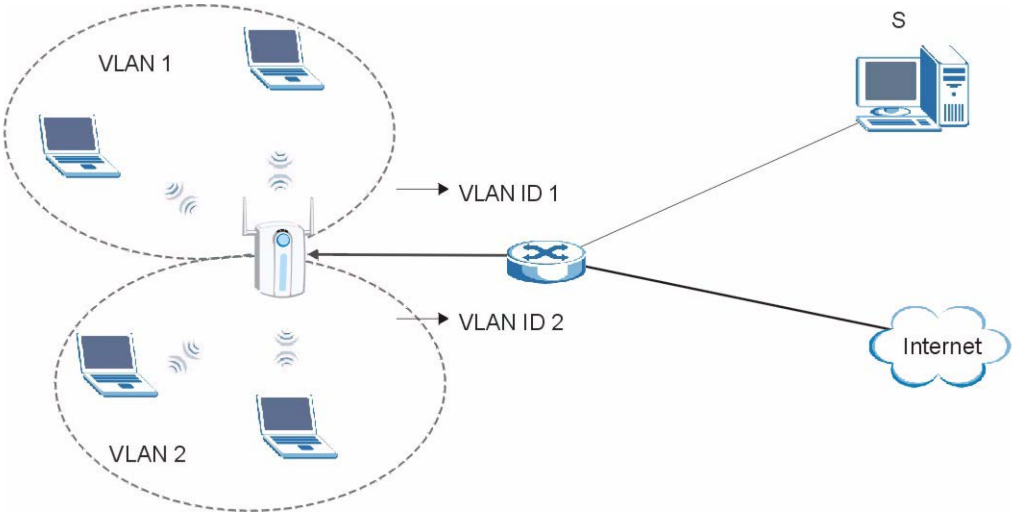
Table 30 Configuring SSID

LABEL	DESCRIPTION
VLAN ID	Enter a VLAN ID number from 1 to 4094. Packets coming from the WLAN using this SSID profile are tagged with this VLAN ID number by the ZyXEL Device. Different SSID profiles can use the same or different VLAN IDs. This allows you to split wireless stations into groups using similar VLAN IDs.
Second RX VLAN ID	Enter a number from 1 to 4094, but different from the **VLAN ID**. Traffic received from the LAN that is tagged with this VLAN ID is sent to all SSIDs with this VLAN ID configured in the **VLAN ID** or **Second Rx VLAN ID** fields. See Chapter 15 on page 173 for more information.
Security	Select a security profile to use with this SSID profile. See Section 7.10 on page 93 for more information.
RADIUS	Select a RADIUS profile from the drop-down list box, if you have a RADIUS server configured. If you do not need to use RADIUS authentication, ignore this field. See Section 7.12 on page 102 for more information.
QoS	Select the Quality of Service priority for this ESS's traffic. • Select **voice** for traffic that is especially sensitive to jitter. Use this priority to reduce latency for improved voice quality. • Select **video** for traffic which has some tolerance for jitter but needs to be prioritized over other data traffic. • Select **best effort** for traffic from applications or devices that lack QoS capabilities. Use best effort priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing. • Select **background** for non-critical traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use background priority for applications that do not have strict latency and throughput requirements. Note: When you configure an SSID profile's QoS settings, the ZyXEL Device applies the same QoS setting to all of the profile's traffic.
L2 Isolation	Turn on layer-2 isolation to block wireless clients associated with this SSID from communicating with other wireless clients, APs, computers or routers in the network except for the ones with MAC addresses that you list in the layer-2 isolation table. When you Note: When you enable layer-2 isolation, the **Enable Intra-BSS Traffic** check box in the **WIRELESS > Wireless** screen is automatically cleared (intra-BSS traffic is blocked). Go to the **WIRELESS > Wireless** screen and re-select the **Enable Intra-BSS Traffic** check box if you want to allow intra-BSS traffic.
Enable MAC Filtering	Select **Enable** from the drop down list box to activate MAC address filtering.
Enable Public SSID (MESSID Only)	Select **Enable** from the drop down list box to have the ZyXEL Device broadcast this SSID in a response that it transmits after receiving a probe. This means a wireless client scanning for an AP can find this SSID. Select **Disable** to have the ZyXEL Device hide this SSID in the responses that it transmits after receiving probes. This means a wireless client scanning for an AP cannot find this SSID.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.2.3 Second Rx VLAN ID

The ZyAIR tags Ethernet frames in VLAN 1 with VLAN ID 1 and tags Ethernet frames in VLAN 2 with VLAN ID 2. Both VLAN 1 and VLAN 2 have Internet access. VLAN 1 and VLAN 2 have access to a server. Ethernet frames forwarded from the server back to the switch are tagged. Ethernet frames are tagged with a second Rx VLAN ID (incoming VLAN ID). These incoming VLAN packets are forwarded to the ZyAIR. The ZyAIR matches the Second Rx VLAN ID with VLAN ID.

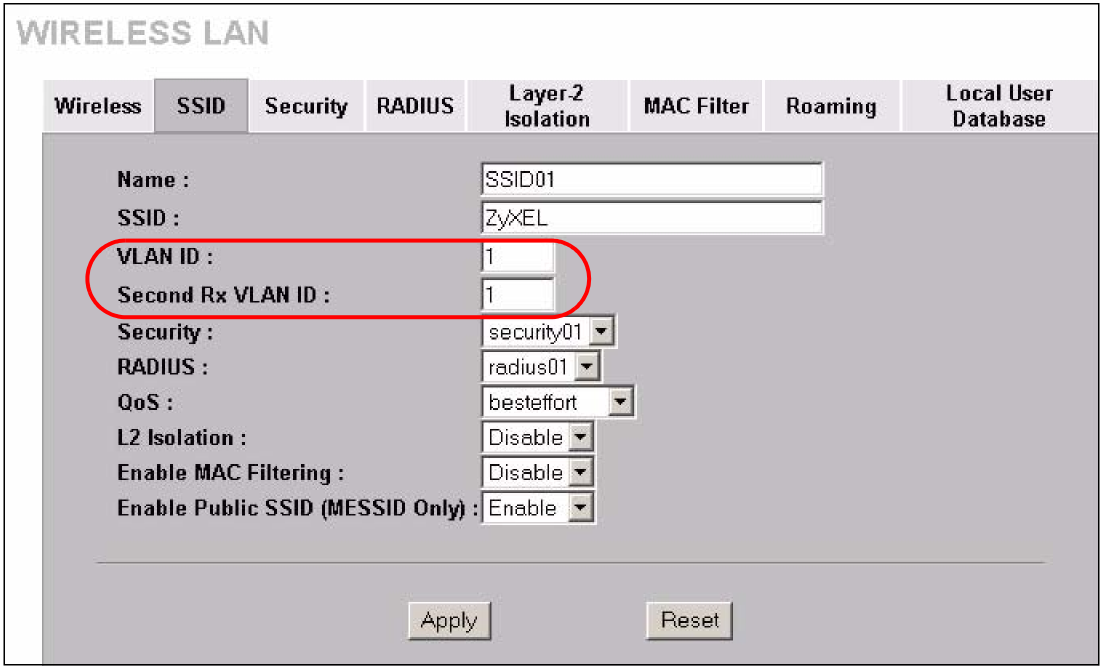
Figure 56 Second Rx VLAN ID Example



The following steps show you where to setup a Second Rx VLAN ID on the ZyAIR.

1. Click **WIRELESS** under **ADVANCED** in your web configurator and the SSID tab.
2. Click **Edit** in the **SSID** screen.
3. You can enter a **Second Rx VLAN ID** in the following screen. The following screen shows VLAN 1 tagged with VLAN ID 1. Incoming packets (Second Rx VLAN ID) with a VLAN ID 3 are matched to VLAN 1.

Figure 57 Configuring SSID: Second Rx VLAN ID Example



Name : SSID01
SSID : ZyXEL
VLAN ID : 1
Second Rx VLAN ID : 1
Security : security01
RADIUS : radius01
QoS : besteffort
L2 Isolation : Disable
Enable MAC Filtering : Disable
Enable Public SSID (MESSID Only) : Enable

4 Click **Apply** to save these settings to the ZyAIR.

9

Other Wireless Configuration

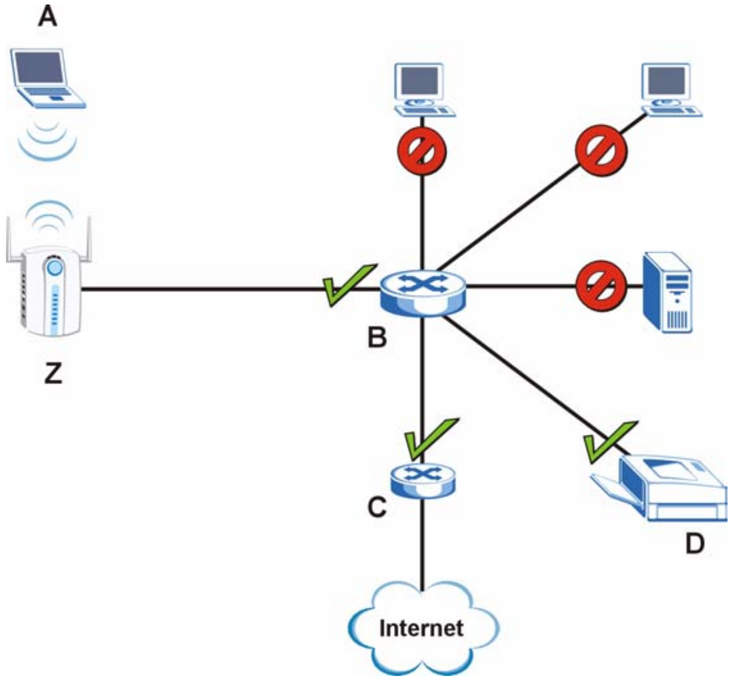
This chapter describes how to configure the **Wireless Layer-2 Isolation**, **MAC Filter** and **Roaming** screens on your ZyXEL Device.

9.1 Layer-2 Isolation Introduction

Layer-2 isolation prevents wireless clients associated with one of your ZyXEL Device's SSIDs from communicating with other wireless clients, APs, computers or routers in the network except for the ones with MAC addresses that you list in the layer-2 isolation table.

In the following example, layer-2 isolation is enabled on the ZyXEL Device (**Z**, in the figure) to allow a guest wireless client (**A**) to access the main network router (**B**), the router providing Internet access (**C**), and the network printer (**D**) while preventing the client from accessing other computers and servers on the network. The client can communicate with other wireless clients only if **Enable Intra-BSS Traffic** is selected.

Figure 58 Layer-2 Isolation Application



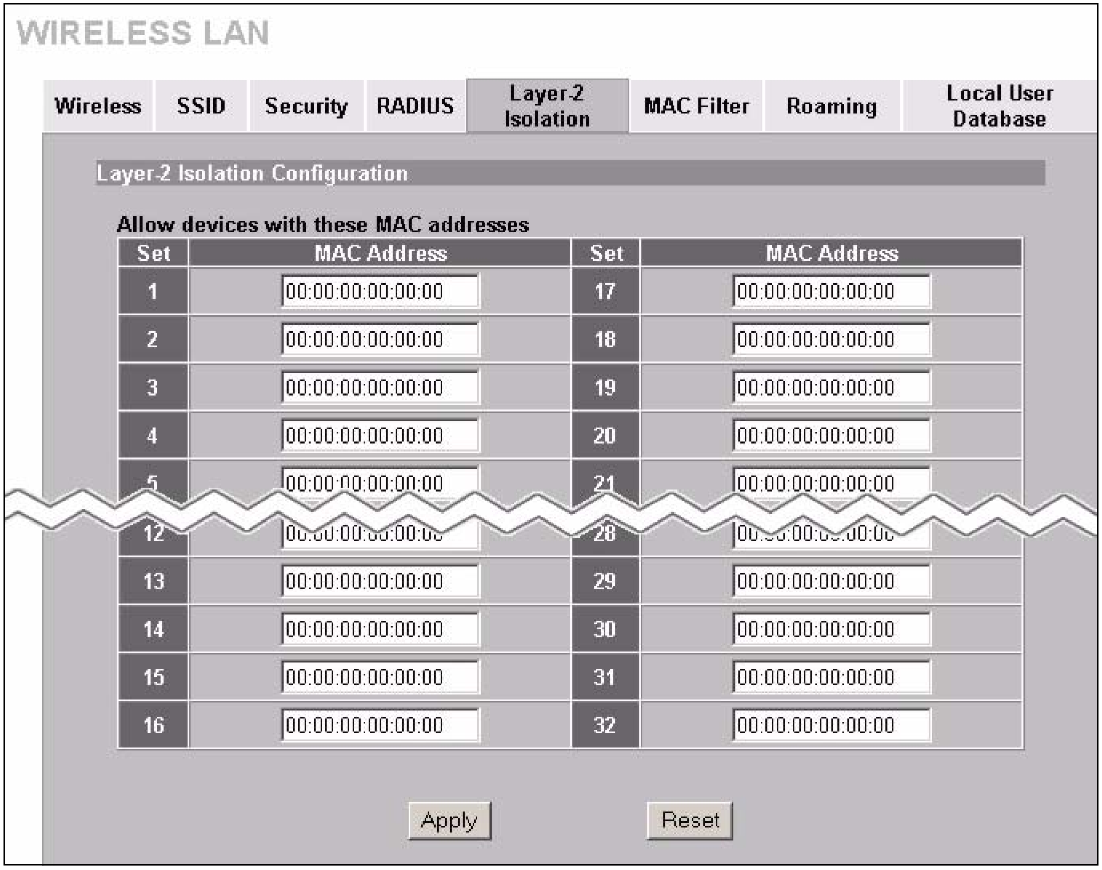
MAC addresses that are not listed in the Allow devices with these MAC addresses table are blocked from communicating with the ZyXEL Device’s wireless clients except for broadcast packets. Layer-2 isolation does not check the traffic between wireless clients that are associated with the same AP. Intra-BSS Traffic allows wireless clients associated with the same AP to communicate with each other.

9.2 Configuring Layer-2 Isolation

If layer-2 isolation is enabled, you need to know the MAC addresses of the wireless clients, APs, computers or routers that you want to allow to communicate with the ZyXEL Device's wireless clients.

To configure layer-2 isolation, click **WIRELESS** > **Layer-2 Isolation**. The screen appears as shown next.

Figure 59 Layer-2 Isolation Configuration Screen



Layer-2 Isolation Configuration

Allow devices with these MAC addresses

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this screen.

Table 31 Layer-2 Isolation Configuration

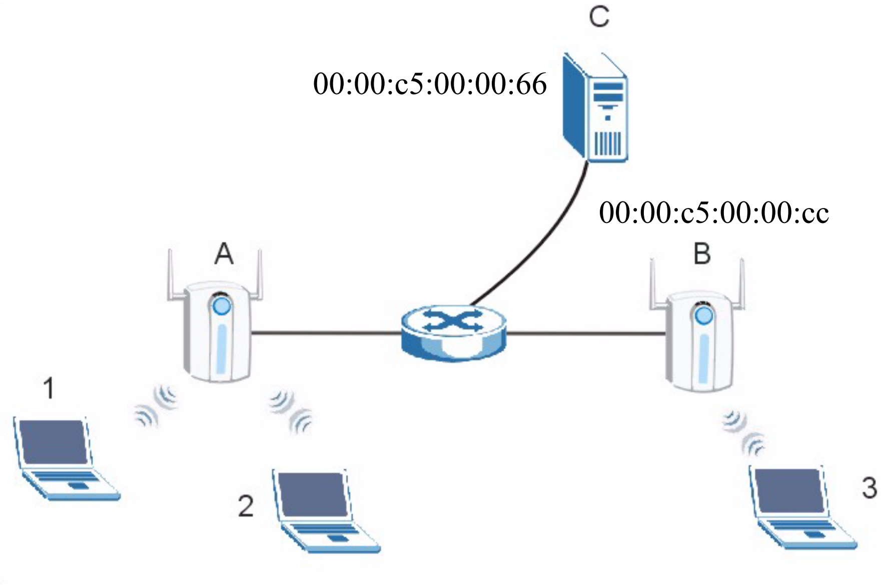
LABEL	DESCRIPTION
Allow devices with these MAC addresses	These are the MAC address of a wireless client, AP, computer or router. A wireless client associated with the ZyXEL Device can communicate with another wireless client, AP, computer or router only if the MAC addresses of those devices are listed in this table.
Set	This is the index number of the MAC address.
MAC Address	Type the MAC addresses of the wireless client, AP, computer or router that you want to allow the associated wireless clients to have access to in these address fields. Type the MAC address in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

9.2.1 Layer-2 Isolation Examples

The following section shows you example layer-2 isolation configurations on the ZyXEL Device (**A**).

When configuring, remember to enable layer-2 isolation in the **WIRELESS > SSID > Edit** screen of the relevant SSID profile.

Figure 60 Layer-2 Isolation Example

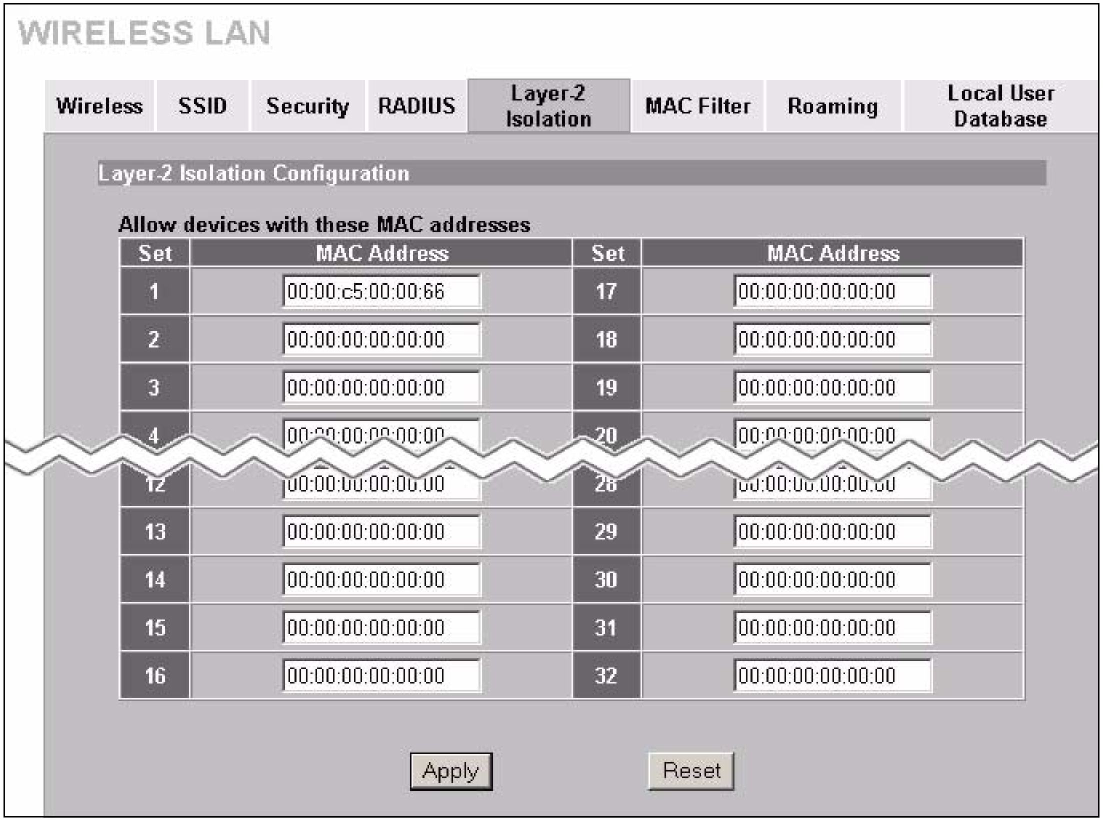


9.2.1.1 Layer-2 Isolation Example 1

In the following example wireless clients **1** and **2** can communicate with **C**, but not **B** or **3**.

- Enter C’s MAC address in the **Allow devices with these MAC addresses** field.

Figure 61 Layer-2 Isolation Example 1



Layer-2 Isolation Configuration

Allow devices with these MAC addresses

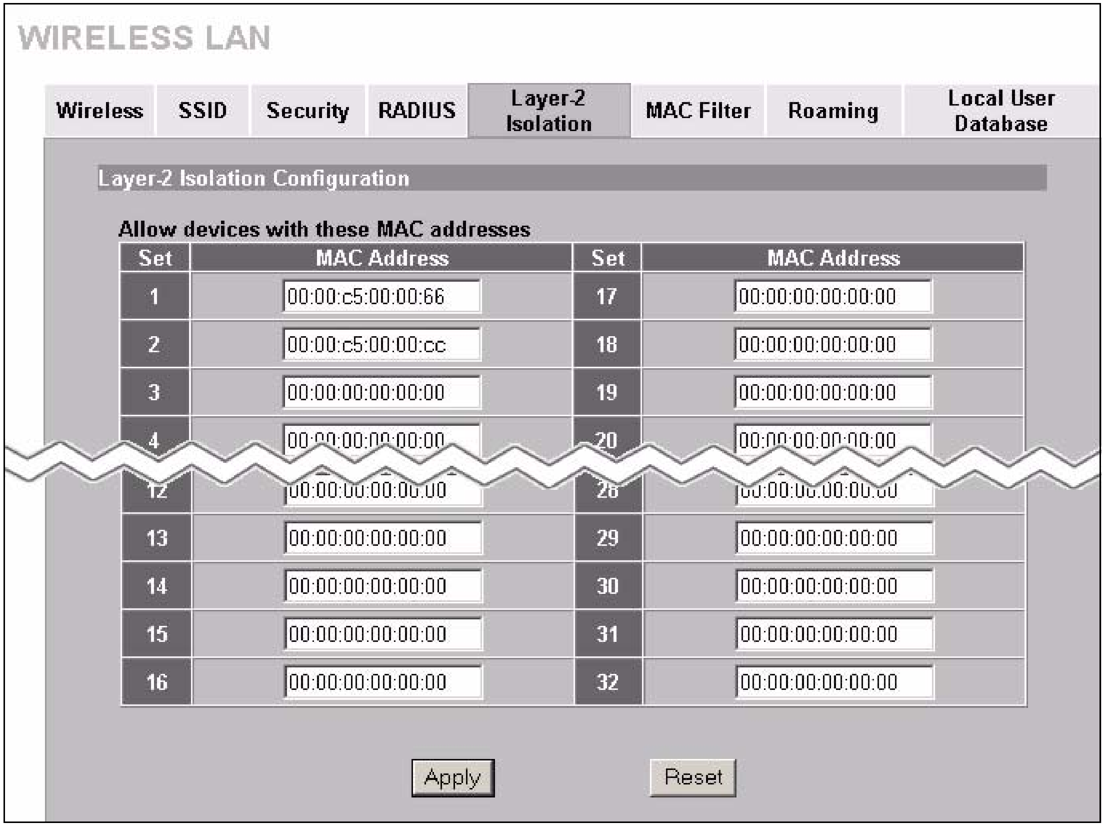
Set	MAC Address	Set	MAC Address
1	00:00:c5:00:00:66	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

9.2.1.2 Layer-2 Isolation Example 2

In the following example wireless clients **1** and **2** can communicate with **B** and **C** but not **3**.

- Configure more than one MAC address. Enter the server's and your ZyXEL Device's MAC addresses in the **Allow devices with these MAC addresses** fields.

Figure 62 Layer-2 Isolation Example 2



Layer-2 Isolation Configuration

Allow devices with these MAC addresses

Set	MAC Address	Set	MAC Address
1	00:00:c5:00:00:66	17	00:00:00:00:00:00
2	00:00:c5:00:00:cc	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

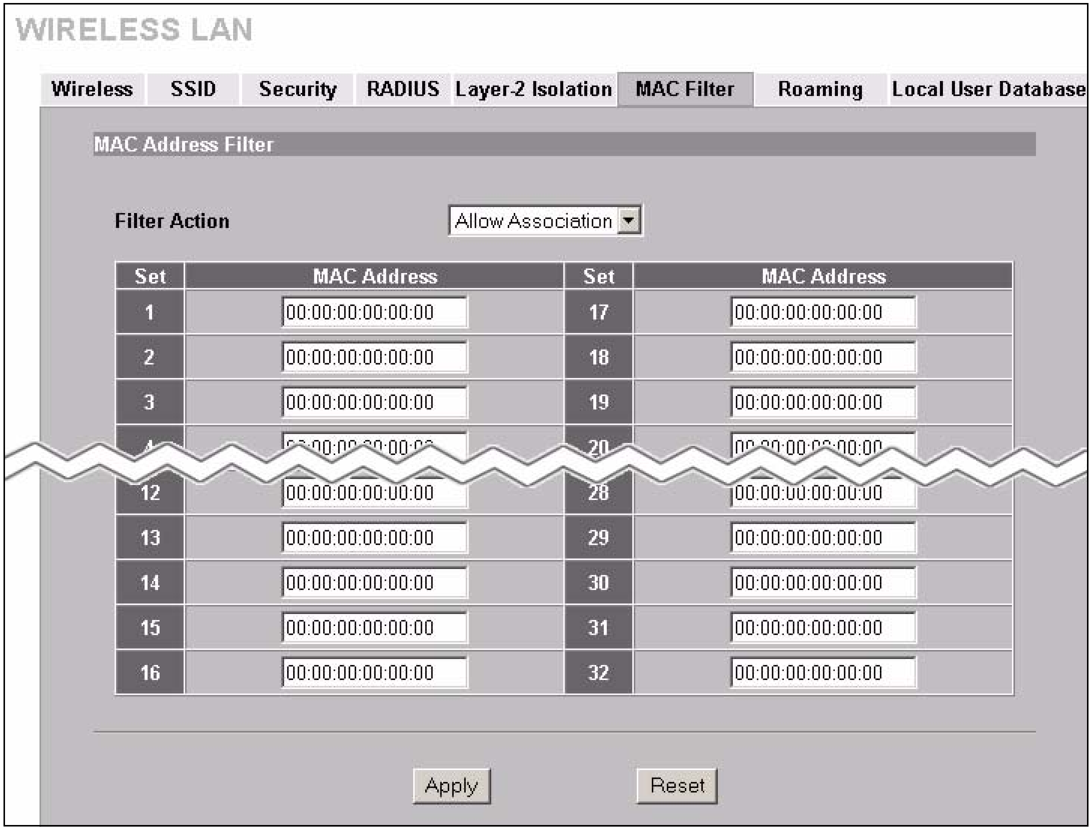
9.3 Configuring MAC Filter

The MAC filter screen allows you to configure the ZyXEL Device to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the ZyXEL Device (Deny Association).

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

To change your ZyXEL Device's MAC filter settings, click **WIRELESS** > **MAC Filter**. The screen appears as shown.

Figure 63 MAC Address Filter



MAC Address Filter

Filter Action: Allow Association

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this screen.

Table 32 MAC Address Filter

LABEL	DESCRIPTION
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny Association** to block access to the router. MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router. MAC addresses not listed will be denied access to the router.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station to be allowed or denied access to the ZyXEL Device.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

To activate MAC filtering on a profile, select **Enable** from the **Enable MAC Filtering** drop-down list box in the **WIRELESS** > **SSID** > **Edit** screen and click **Apply**.

9.4 Configuring Roaming

An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

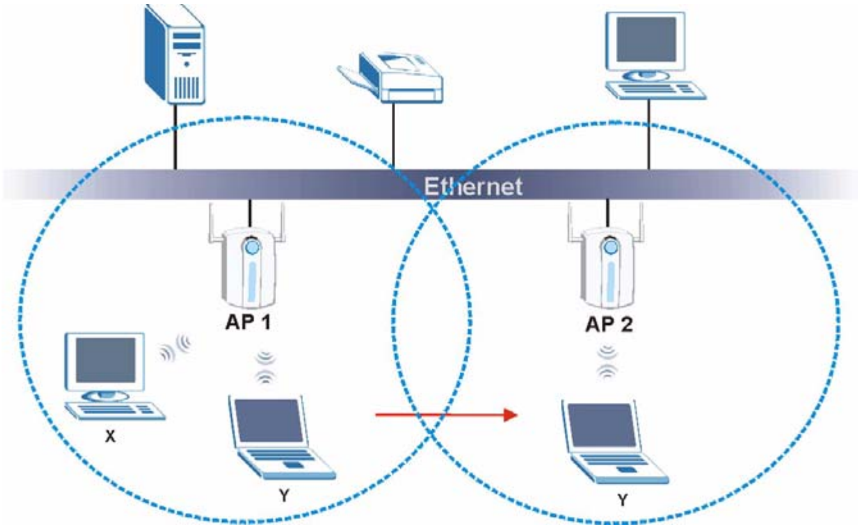
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is known as roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the other access points on the LAN about the change. An example is shown in Figure 64 on page 121.

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

Enable roaming to exchange the latest bridge information of all wireless stations between APs when a wireless station moves between coverage areas. Wireless stations can still associate with other APs even if you disable roaming. Enabling roaming ensures correct traffic forwarding (bridge tables are updated) and maximum AP efficiency. The AP deletes records of wireless stations that associate with other APs (Non-ZyXEL APs may not be able to perform this). 802.1x authentication information is not exchanged (at the time of writing).

Figure 64 Roaming Example



The steps below describe the roaming process.

1 Wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point **AP 2**.

2 Wireless station **Y** scans and detects the signal of access point **AP 2**.

3 Wireless station **Y** sends an association request to access point **AP 2**.

4 Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.

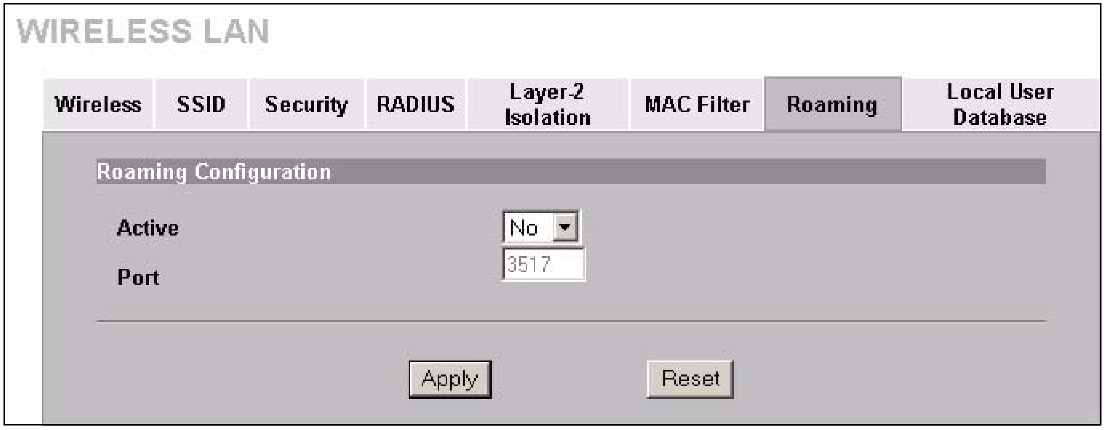
9.4.1 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1 All the access points must be on the same subnet and configured with the same ESSID.
2 If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
3 The adjacent access points should use different radio channels when their coverage areas overlap.
4 All access points must use the same port number to relay roaming information.
5 The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

To enable roaming on your ZyXEL Device, click **WIRELESS** > **Roaming**. The screen appears as shown.

Figure 65 Roaming



WIRELESS LAN

Roaming Configuration

Active: No

Port: 3517

The following table describes the labels in this screen.

Table 33 Roaming

LABEL	DESCRIPTION
Active	Select **Yes** from the drop-down list box to enable roaming on the ZyXEL Device. This is useful if you have two or more APs on the same subnet. Note: All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.
Port #	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is 3517. Make sure this port is not used by other services.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to begin configuring this screen afresh.

10

IP Screen

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

10.1 Factory Ethernet Defaults

The Ethernet parameters of the ZyXEL Device are preset in the factory with the following values:

1 IP address of 192.168.1.2

2 Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

10.2 TCP/IP Parameters

10.2.1 WAN IP Address Assignment

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

Table 34 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

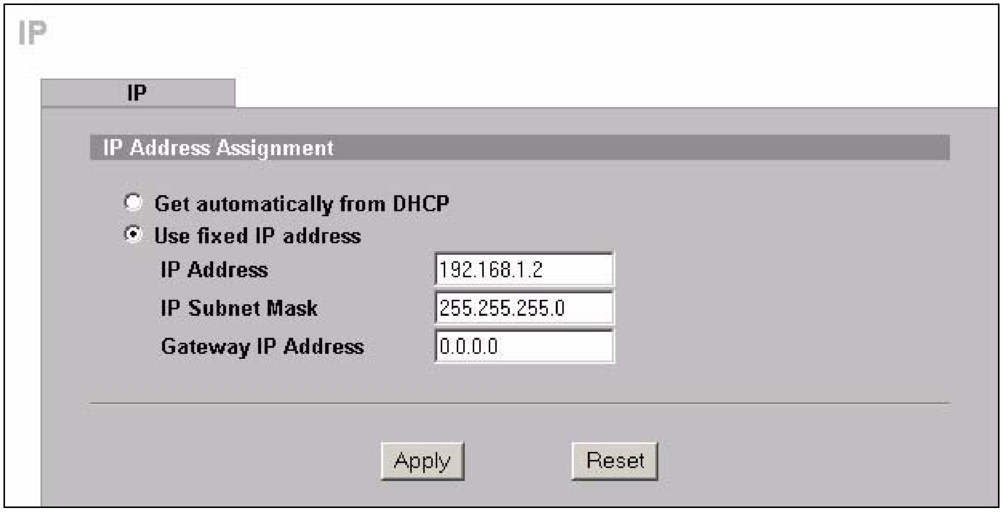
You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much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

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

10.3 Configuring IP

Click **IP** to display the screen shown next.

Figure 66 IP Setup



IP

IP Address Assignment

○ Get automatically from DHCP
● Use fixed IP address

IP Address: 192.168.1.2
IP Subnet Mask: 255.255.255.0
Gateway IP Address: 0.0.0.0

The following table describes the labels in this screen.

Table 35 IP Setup

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option if your ZyXEL Device is using a dynamically assigned IP address from a DHCP server each time. Note: You must know the IP address assigned to the ZyXEL Device (by the DHCP server) to access the ZyXEL Device again.
Use fixed IP address	Select this option if your ZyXEL Device is using a static IP address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Note: If you change the ZyXEL Device's IP address, you must use the new IP address if you want to access the web configurator again.
IP Subnet Mask	Type the subnet mask.

Table 35 IP Setup

LABEL	DESCRIPTION
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over the WAN, the gateway must be the IP address of one of the remote nodes.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

11

Remote Management Screens

This chapter provides information on the Remote Management screens.

11.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which of the ZyXEL Device's interfaces (if any) from which computers.

You may manage your ZyXEL Device from a remote location via:

Table 36 Remote Management Overview

• WLAN	• ALL (LAN and WLAN)
• LAN only	• Neither (Disable).

You can disable a service on the ZyXEL Device by not allowing access for the service/ protocol through any of the ZyXEL Device interfaces.

You may only have one management session running at a time. The ZyXEL Device automatically disconnects a management session of lower priority when another management session of higher priority starts. The priorities for the different types of management sessions are as follows.

1 Console

1 Telnet

2 Web (HTTP or HTTPS)

11.1.1 Remote Management Limitations

Remote management over LAN or WLAN will not work when:

1. You have disabled that service in one of the remote management screens.
2. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

11.1.2 System Timeout

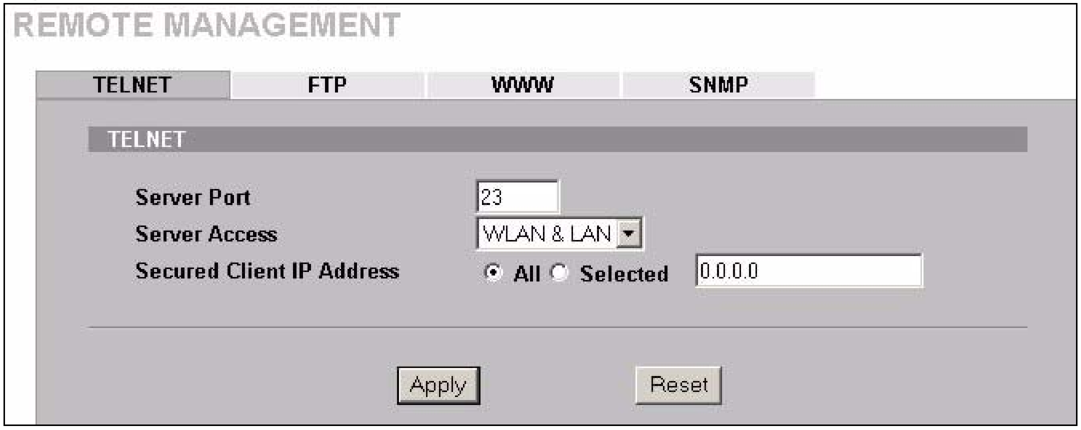
There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System > General** screen (see Section 5.2 on page 67).

11.2 Configuring Telnet

You can configure your ZyXEL Device for remote Telnet access. Use this screen to specify which interfaces allow Telnet access and from which IP address the access can come.

Click **REMOTE MGNT** and the **TELNET** tab to display the screen as shown.

Figure 67 Remote Management: Telnet



Server Port: 23
Server Access: WLAN & LAN
Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 37 Remote Management: Telnet

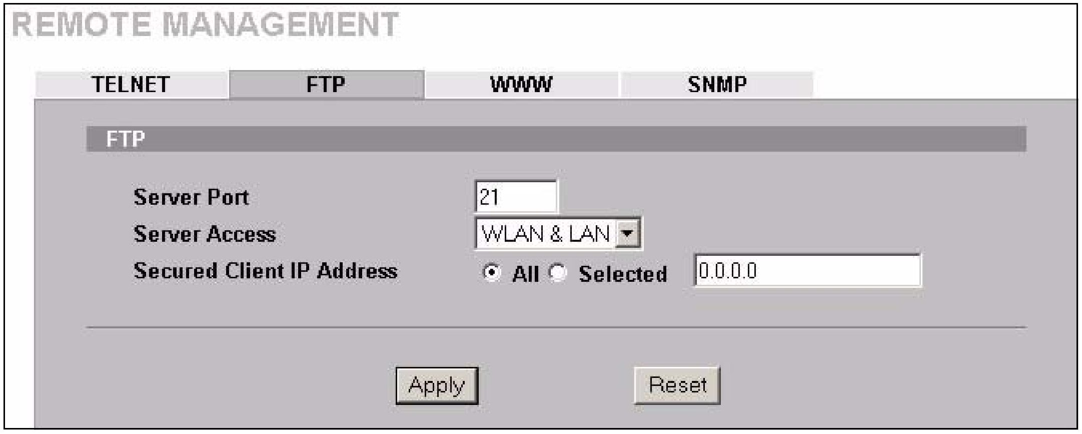
LABEL	DESCRIPTION
TELNET	
Server Port	You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using Telnet.
Secured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

11.3 Configuring FTP

You can use FTP (File Transfer Protocol) to upload and download the ZyXEL Device's firmware and configuration files, please see Chapter 23 on page 365 for details. To use this feature, your computer must have an FTP client.

To change your ZyXEL Device's FTP settings, click **REMOTE MGMT** > **FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

Figure 68 Remote Management: FTP



Server Port: 21
Server Access: WLAN & LAN
Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 38 Remote Management: FTP

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

11.4 WWW (HTTP and HTTPS)

You can set the ZyXEL Device to use HTTP or HTTPS (HTTPS adds security) for web configurator sessions. Specify which interfaces allow web configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

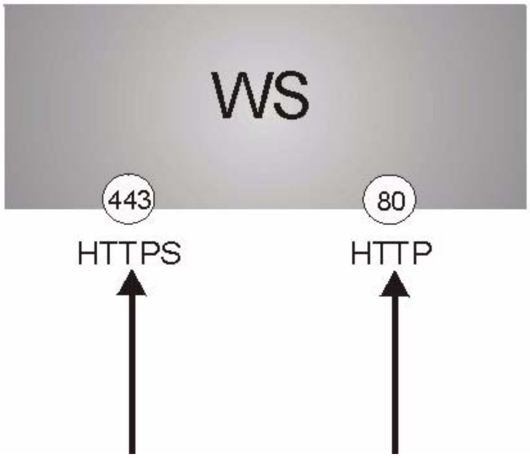
It relies upon certificates, public keys, and private keys (see Chapter 14 on page 239 for more information).

HTTPS on the ZyXEL Device is used so that you may securely access the ZyXEL Device using the web configurator. The SSL protocol specifies that the SSL server (the ZyXEL Device) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT** > **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyXEL Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyXEL Device.

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyXEL Device's WS (web server).
2. HTTP connection requests from a web browser go to port 80 (by default) on the ZyXEL Device's WS (web server).

Figure 69 HTTPS Implementation

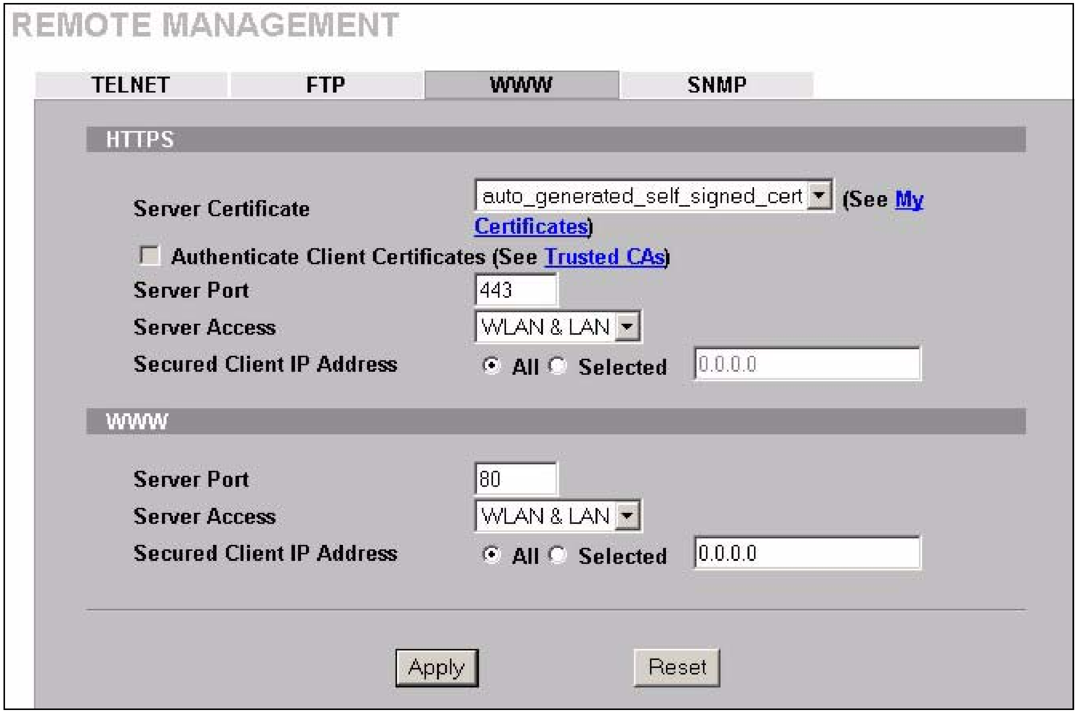


If you disable the HTTP service in the **REMOTE MGMT > WWW** screen, then the ZyXEL Device blocks all HTTP connection attempts.

11.5 Configuring WWW

To change your ZyXEL Device's World Wide Web settings, click **REMOTE MGNT** to display the **WWW** screen.

Figure 70 Remote Management: WWW



REMOTE MANAGEMENT

HTTPS

Server Certificate: auto_generated_self_signed_cert (See My Certificates)

□ Authenticate Client Certificates (See Trusted CAs)

Server Port: 443

Server Access: WLAN & LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

WWW

Server Port: 80

Server Access: WLAN & LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 39 Remote Management: WWW

LABEL	DESCRIPTION
HTTPS	
Server Certificate	Select the **Server Certificate** that the ZyXEL Device will use to identify itself. The ZyXEL Device is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device).
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself with the ZyXEL Device by sending the ZyXEL Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyXEL Device (see the appendix on importing certificates for details).
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyXEL Device, for example 8443, then you must notify people who need to access the ZyXEL Device web configurator to use "https://ZyXEL Device IP Address:**8443**" as the URL.
Server Access	Select a ZyXEL Device interface from **Server Access** on which incoming HTTPS access is allowed. You can allow only secure web configurator access by setting the **HTTP Server Access** field to **Disable** and setting the **HTTPS Server Access** field to an interface(s).
Secured Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
WWW	

Table 39 Remote Management: WWW

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

11.6 HTTPS Example

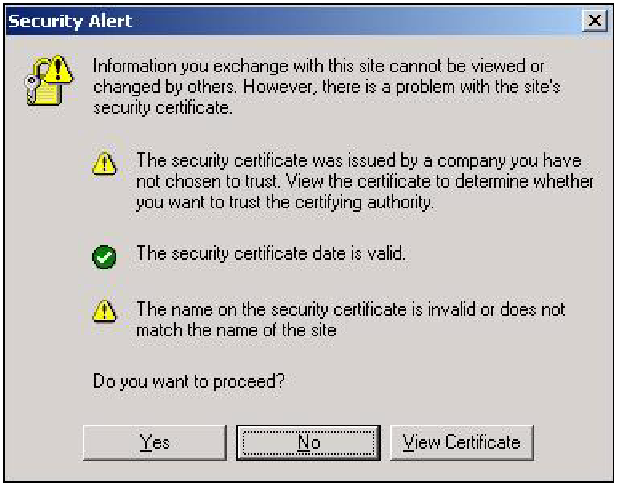
If you have not changed the default HTTPS port on the ZyXEL Device, then in your browser enter "https://ZyXEL Device IP Address/" as the web site address where "ZyXEL Device IP Address" is the IP address or domain name of the ZyXEL Device you wish to access.

11.6.1 Internet Explorer Warning Messages

When you attempt to access the ZyXEL Device HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ZyXEL Device.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 71 Security Alert Dialog Box (Internet Explorer)



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?

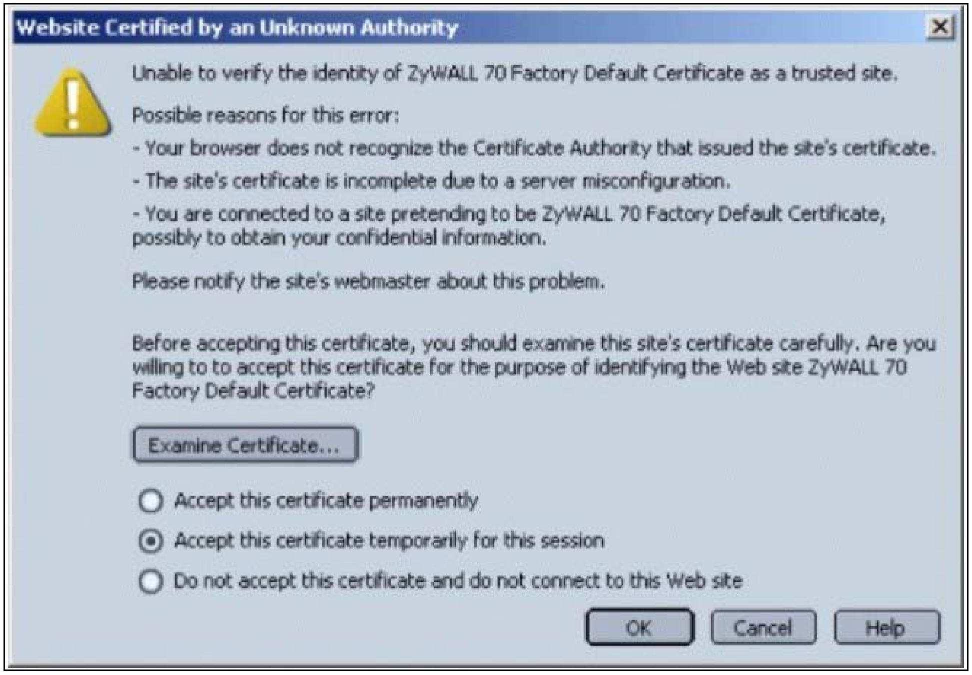
11.6.2 Netscape Navigator Warning Messages

When you attempt to access the ZyXEL Device HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the ZyXEL Device.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the ZyXEL Device's certificate into the SSL client.

Figure 72 Security Certificate 1 (Netscape)



Website Certified by an Unknown Authority

Unable to verify the identity of ZyWALL 70 Factory Default Certificate as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be ZyWALL 70 Factory Default Certificate, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

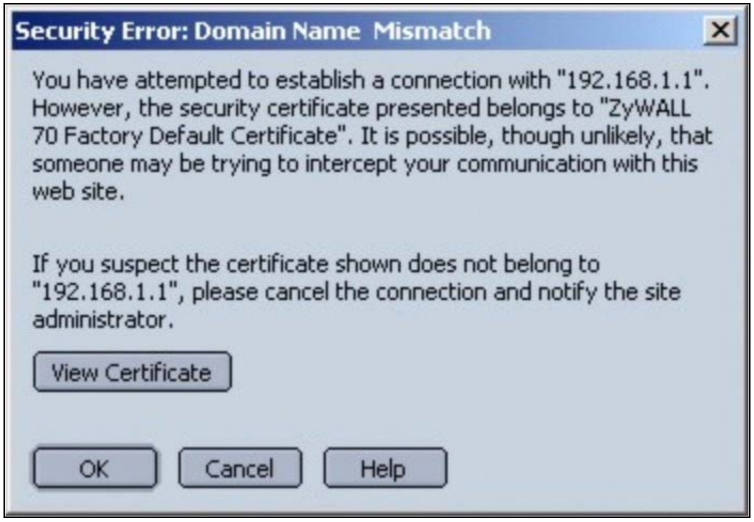
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site ZyWALL 70 Factory Default Certificate?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this Web site

Figure 73 Security Certificate 2 (Netscape)



Security Error: Domain Name Mismatch

You have attempted to establish a connection with "192.168.1.1". However, the security certificate presented belongs to "ZyWALL 70 Factory Default Certificate". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "192.168.1.1", please cancel the connection and notify the site administrator.

11.6.3 Avoiding the Browser Warning Messages

The following describes the main reasons that your browser displays warnings about the ZyXEL Device's HTTPS server certificate and what you can do to avoid seeing the warnings.

- The issuing certificate authority of the ZyXEL Device's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the ZyXEL Device's factory default certificate is the ZyXEL Device itself since the certificate is a self-signed certificate.
  - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
  - To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix G on page 457 for details.
- The actual IP address of the HTTPS server (the IP address of the ZyXEL Device's port that you are trying to access) does not match the common name specified in the ZyXEL Device's HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your ZyXEL Device sends to HTTPS clients.

  2a Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.

  2b Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (see Figure 76 on page 136 for an example).

Use this procedure to have the ZyXEL Device use a certificate with a common name that matches the ZyXEL Device's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

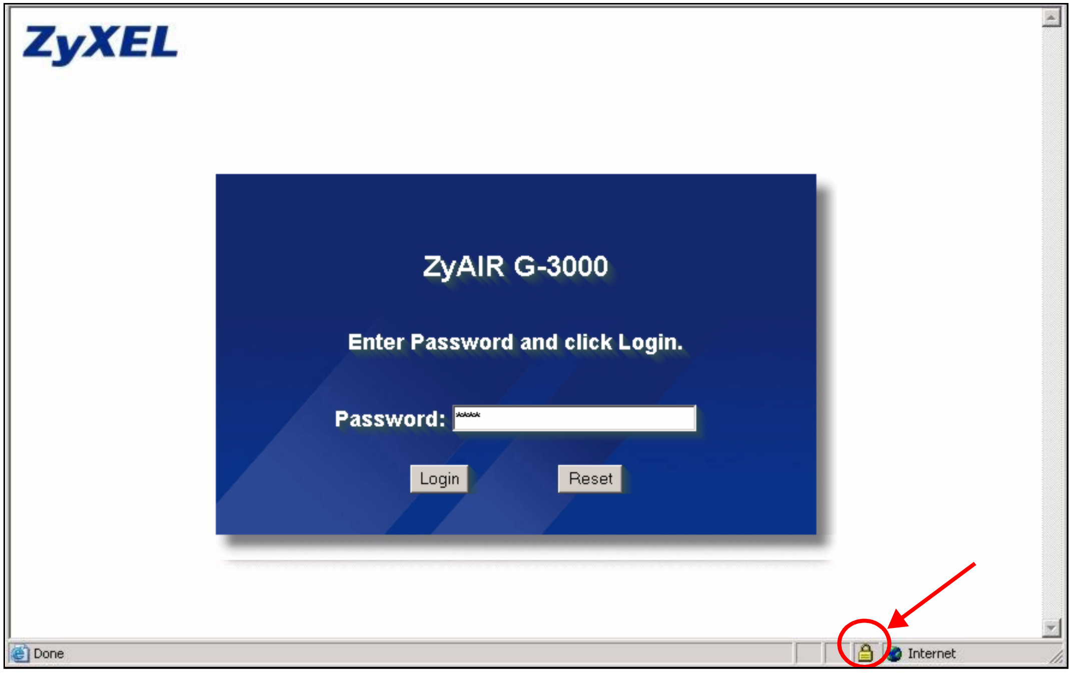
2a Create a new certificate for the ZyXEL Device that uses the IP address (of the ZyXEL Device's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.167.1, create a certificate that uses 192.168.167.1 as the common name.

2b Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

11.6.4 Login Screen

After you accept the certificate, the ZyXEL Device login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

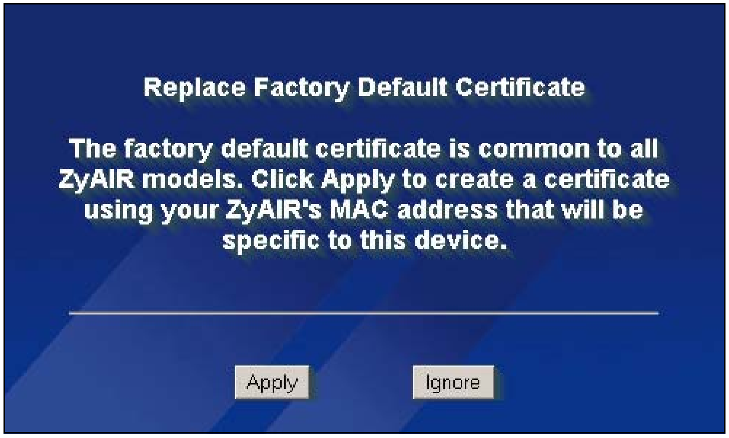
Figure 74 Example: Lock Denoting a Secure Connection)



Click **Login** and you then see the next screen.

The factory default certificate is a common default certificate for all ZyXEL Device models.

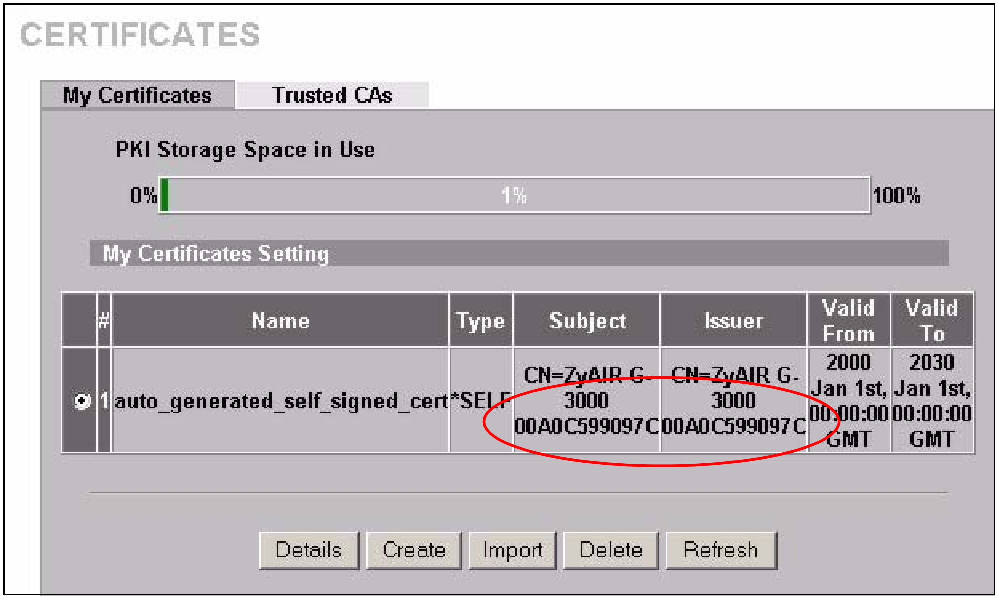
Figure 75 Replace Certificate


Replace Factory Default Certificate

The factory default certificate is common to all ZyAIR models. Click Apply to create a certificate using your ZyAIR's MAC address that will be specific to this device.

Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

Figure 76 Device-specific Certificate



CERTIFICATES

PKI Storage Space in Use

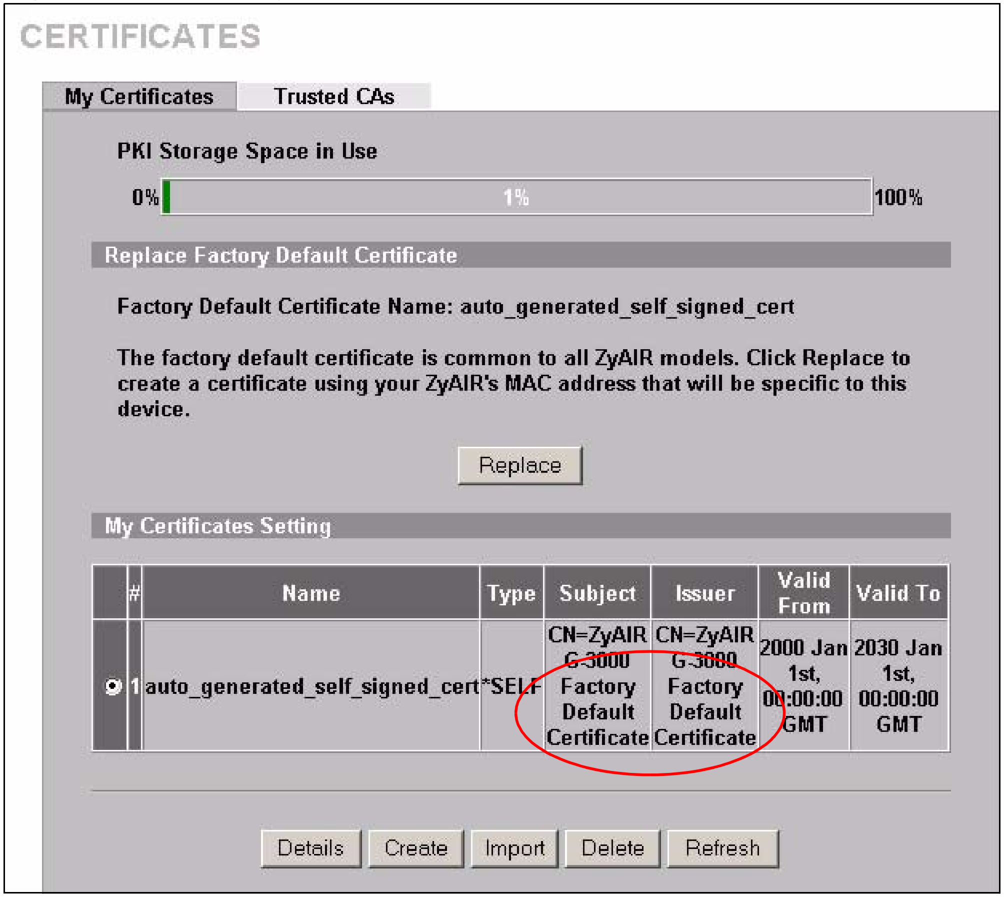
0% 1% 100%

My Certificates Setting

	#	Name	Type	Subject	Issuer	Valid From	Valid To
●	1	auto_generated_self_signed_cert	*SELF	CN=ZyAIR G-3000 00A0C599097C	CN=ZyAIR G-3000 00A0C599097C	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT

Click **Ignore** in the **Replace Certificate** screen to use the common ZyXEL Device certificate. You will then see this information in the **My Certificates** screen.

Figure 77 Common ZyXEL Device Certificate



CERTIFICATES

PKI Storage Space in Use

0% 1% 100%

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to all ZyAIR models. Click Replace to create a certificate using your ZyAIR's MAC address that will be specific to this device.

My Certificates Setting

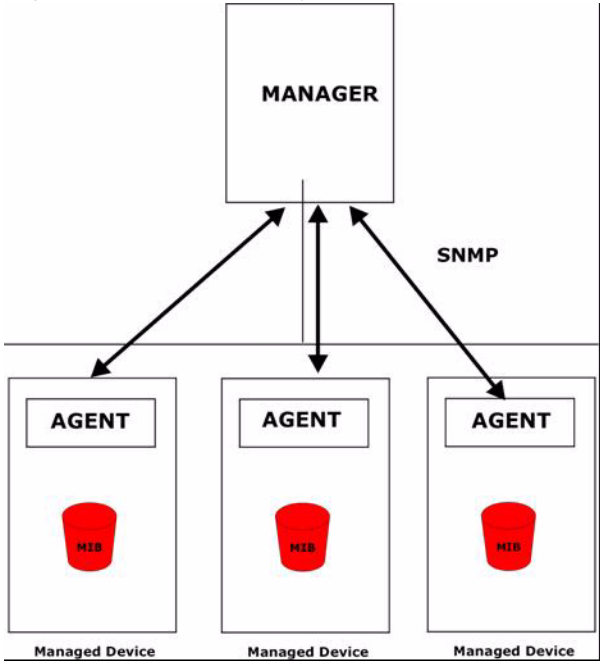
	#	Name	Type	Subject	Issuer	Valid From	Valid To
●	1	auto_generated_self_signed_cert	*SELF	CN=ZyAIR G-3000 Factory Default Certificate	CN=ZyAIR G-3000 Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT

11.7 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

SNMP is only available if TCP/IP is configured.

Figure 78 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

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

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

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

11.7.1 Supported MIBs

The ZyXEL Device supports MIB II that is defined in RFC-1213 and RFC-1215 as well as the proprietary ZyXEL private MIB. The purpose of the MIBs is to let administrators collect statistical data and monitor status and performance.

11.7.2 SNMP Traps

The ZyXEL Device can send the following traps to the SNMP manager.

Table 40 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
Generic Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent after booting (power on). This trap is defined in RFC-1215.
warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent after booting (software reboot). This trap is defined in RFC-1215.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure (defined in *RFC-1215*)	1.3.6.1.6.3.1.1.5.5	The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password). Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps.
Traps defined in the ZyXEL Private MIB.		
whyReboot	1.3.6.1.4.1.890.1.5.13.0.1	This trap is sent with the reason for restarting before the system reboots (warm start). "System reboot by user!" is added for an intentional reboot (for example, download new files, CI command "sys reboot"). If the system reboots because of fatal errors, a code for the error is listed.
pwStaAssociation	1.3.6.1.4.1.890.1.9.2.3.1.1	This trap is sent when a wireless client has successfully connected to the AP. The MAC address of the wireless client and the ESSID are listed.

Table 40 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
pwWlanStaDisassociation	1.3.6.1.4.1.890.1.9.2.3.1.2	This trap is sent when a wireless client has disconnected from the AP. The MAC address of the wireless client and the ESSID are listed.
pwWlanStaAuthFail	1.3.6.1.4.1.890.1.9.2.3.2.1	This trap is sent when a wireless client has failed to connect to the AP. The MAC address of the wireless client, the ESSID and the reason are listed.
pwTFTPStatus	1.3.6.1.4.1.890.1.9.2.3.3.1	This trap is sent to indicate the status and result of a TFTP client session that has ended.

11.8 SNMP Traps

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the ZyXEL Device’s physical ports.

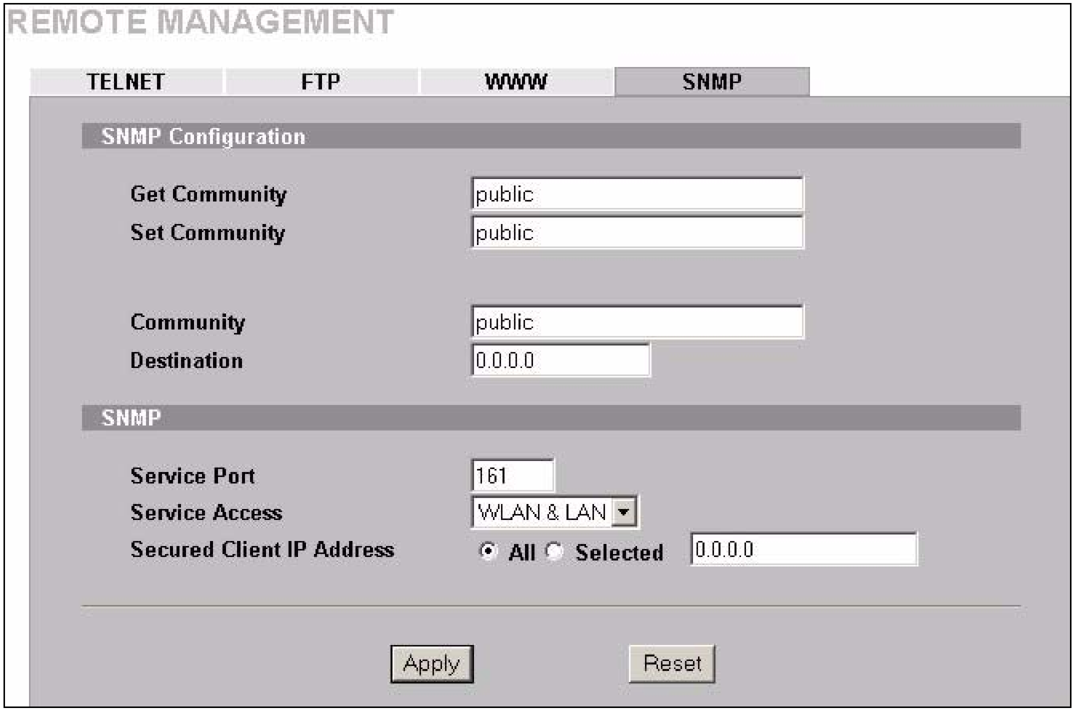
Table 41 SNMP Interface Index to Physical Port Mapping

INTERFACE TYPE	PHYSICAL PORT
enet0	WLAN
enet1	Ethernet port

11.8.1 Configuring SNMP

To change your ZyXEL Device’s SNMP settings, click **REMOTE MGMT**, then the **SNMP** tab. The screen appears as shown.

Figure 79 Remote Management: SNMP



SNMP Configuration

Get Community: public

Set Community: public

Community: public

Destination: 0.0.0.0

SNMP

Service Port: 161

Service Access: WLAN & LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 42 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

12

Auth Server

This chapter describes how to use the internal RADIUS server to authenticate wireless clients or other AP's in other wireless networks.For more background information on RADIUS, see Section 7.2 on page 88. This feature is not available on all models.

12.1 Auth Server Overview

The ZyXEL Device has a built-in RADIUS server that can authenticate wireless clients or other AP's in other wireless networks.

The ZyXEL Device can function as an AP and as a RADIUS server at the same time.

PEAP (Protected EAP) and MD5 authentication is implemented on the internal RADIUS server using simple username and password methods over a secure TLS connection. See the Appendix for more information on the types of EAP authentication and the internal RADIUS authentication method used in your ZyXEL Device.

Figure 80 ZyXEL Device Authenticates Wireless Stations

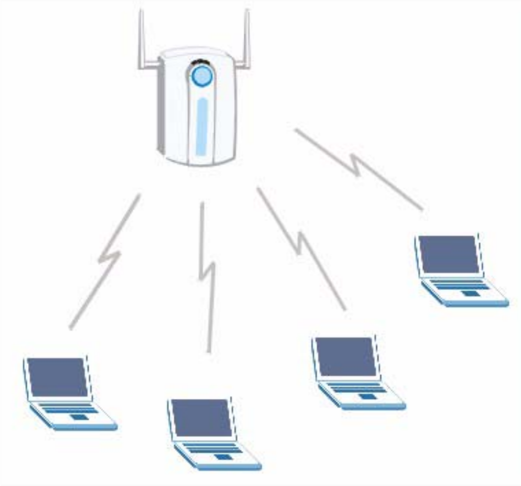


Figure 81 ZyXEL Device Authenticates other AP's

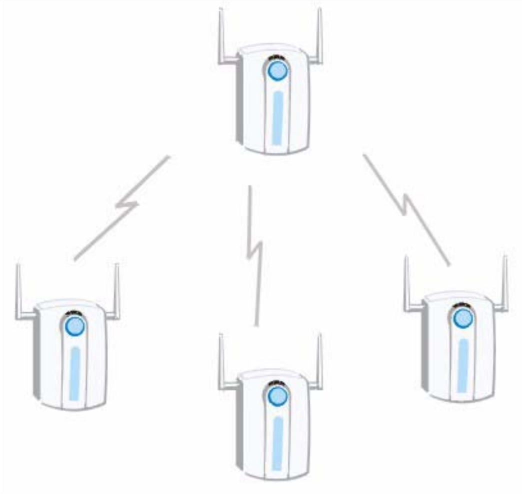


Table 43 Internal RADIUS Server

LABEL	DESCRIPTION
Setting	Use the **Setting** screen to display information about the ZyXEL Device's certificate and to activate the internal RADIUS server on your ZyXEL Device.
Trusted AP	Use the Trusted AP screen to configure which trusted AP's you can authenticate. You can authenticate up to 31 AP's using the ZyXEL Device's internal RADIUS.
Trusted Users	Use the **Trusted Users** screen to configure which wireless stations you can authenticate The ZyXEL Device internal RADIUS server can authenticate up to 32 wireless clients.

12.2 Internal RADIUS Server Setting

The **INTERNAL RADIUS SERVER Setting** screen displays information about certificates. The certificates are used by wireless clients to authenticate the RADIUS server. Information matching the certificate is held on the wireless clients utility, for example, Funk Software's Odyssey client. A password and user name on the utility must match the **Trusted Users** list so that the RADIUS server can be authenticated.

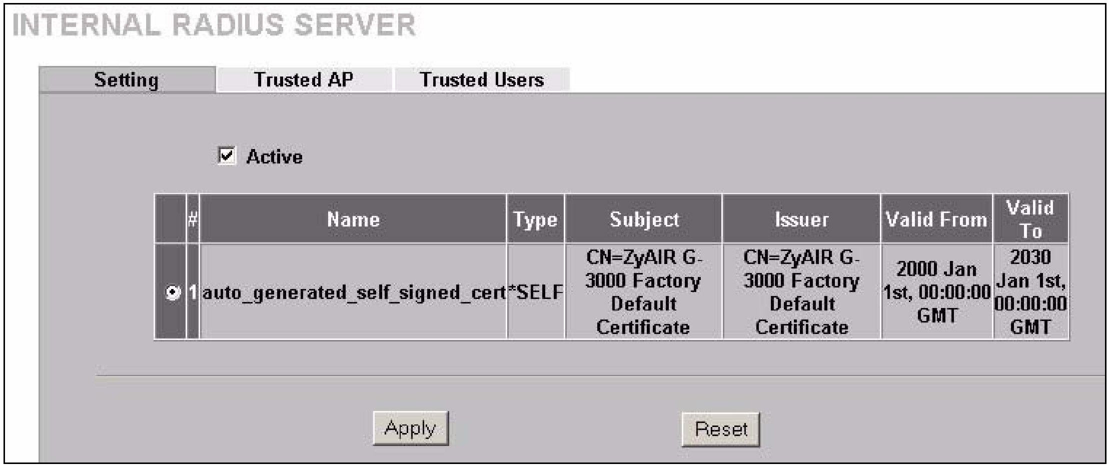
ZyXEL recommends that you replace the factory default certificate with one that uses your ZyXEL Device's MAC address. This can be done when you first log in to the ZyXEL Device or in the **Advanced** web configurator **Certificates** screen.

The internal RADIUS server does not support domain accounts (DOMAIN/user). When you configure your Windows XP SP2 Wireless Zero Configuration PEAP/MS-CHAPv2 settings, deselect the **Use Windows logon name and password** check box. When authentication begins, a pop-up dialog box requests you to type a **Name**, **Password** and **Domain** of the RADIUS server. Specify a **Name** and **Password** only, do not specify a domain.

Refer to the My Certificates section in the Certifications chapter for information on how to replace, add or remove certificates.

Click the **AUTH SERVER** link under **ADVANCED** and then the **Setting** tab. The screen appears as shown.

Figure 82 Internal RADIUS Server Setting Screen



INTERNAL RADIUS SERVER

☑ Active

	#	Name	Type	Subject	Issuer	Valid From	Valid To
●	1	auto_generated_self_signed_cert	*SELF	CN=ZyAIR G-3000 Factory Default Certificate	CN=ZyAIR G-3000 Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT

The following table describes the labels in this screen.

Table 44 My Certificates

LABEL	DESCRIPTION
Active	Select the **Active** check box to have the ZyXEL Device use its internal RADIUS server to authenticate wireless clients or other AP's.
#	This field displays the certificate index number. The certificates are listed in alphabetical order. Certificates can be added or removed in the **Advanced Certificate** screens. The internal RADIUS server uses one of the certificates listed in this screen to authenticate each wireless client. The exact certificate used, depends on the certificate information configured on the wireless client.
Name	This field displays the name used to identify this certificate. The ZyXEL Device has an **auto_generated_self_signed_cert** by factory default. The factory default certificate is common to all ZyXEL Device's that use certificates. You can replace the certificate when you log into the ZyXEL Device, see the section Introducing the Web Configurator or you can go to the **Certificates** configuration screen, see the Certificates chapter.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.

Table 44 My Certificates (continued)

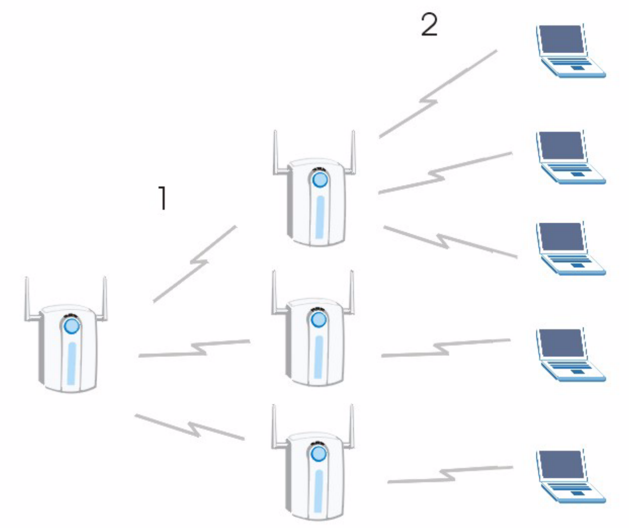
LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Apply	Click **Apply** to have the ZyXEL Device use certificates to authenticate wireless clients.
Reset	Click **Reset** to start configuring this screen afresh.

12.3 Trusted AP Overview

A trusted AP is an AP that uses the ZyXEL Device's internal RADIUS server to authenticate it's wireless clients.

The following shows how this is done in two phases.

Figure 83 Trusted AP Overview



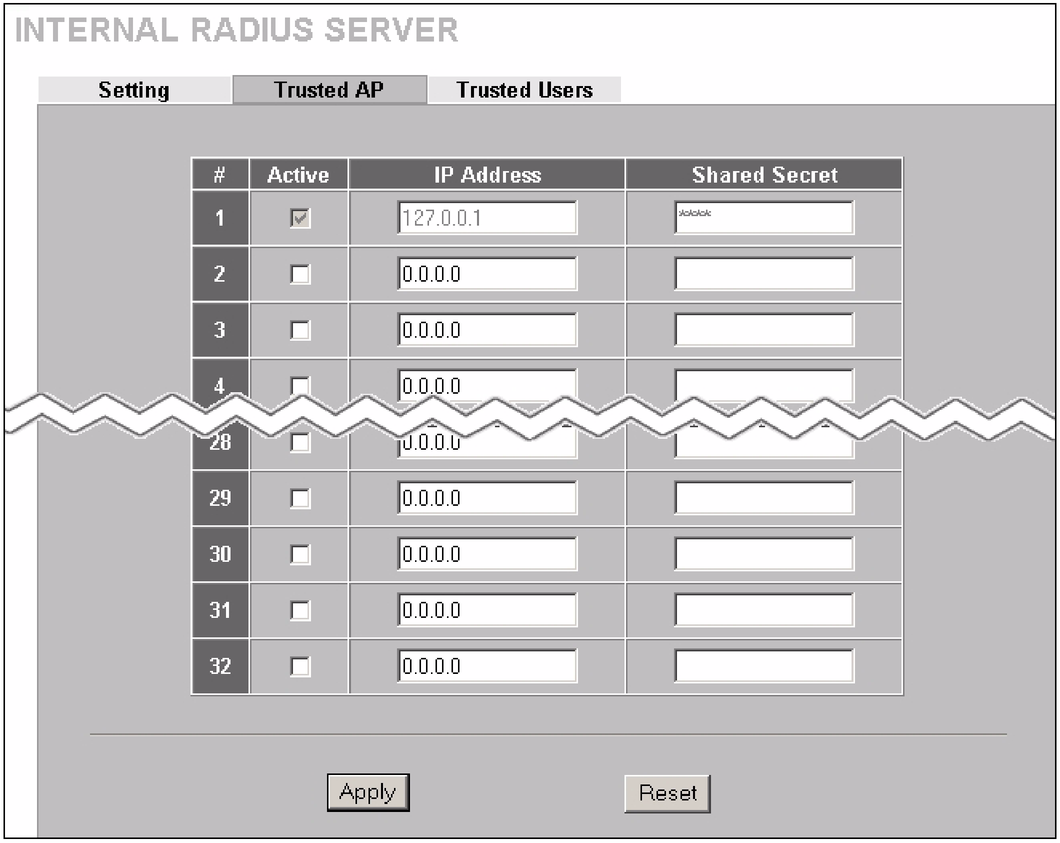
1 Configure an IP address and shared secret in the **Trusted AP** database to authenticate an AP as a trusted AP.

2 Configure wireless client user names and passwords in the **Trusted Users** database to use a trusted AP as a relay between the RADIUS server and the wireless clients. The wireless clients can then be authenticated by the RADIUS server.

12.4 Configuring Trusted AP

To configure trusted AP's on the ZyXEL Device's internal RADIUS, click the **AUTH SERVER** link under **ADVANCED** and then the **Trusted AP** tab. The screen appears as shown.

Figure 84 Trusted AP Screen



#	Active	IP Address	Shared Secret
1	☑	127.0.0.1	****
2	☐	0.0.0.0	
3	☐	0.0.0.0	
4	☐	0.0.0.0	
28	☐	0.0.0.0	
29	☐	0.0.0.0	
30	☐	0.0.0.0	
31	☐	0.0.0.0	
32	☐	0.0.0.0	

The following table describes the labels in this screen.

Table 45 Trusted AP

LABEL	DESCRIPTION
#	This field displays the trusted AP index number.
Active	Select this check box to have the ZyXEL Device use the **IP Address** and **Shared Secret** to authenticate a trusted AP.
IP Address	Type the IP network address of the trusted AP in dotted decimal notation.
Shared Secret	Enter a password (up to 31 alphanumeric characters, no spaces) to be shared between the trusted AP and the ZyXEL Device. Note: The first trusted AP fields are reserved for the ZyXEL Device. They are grayed out and therefore cannot be configured. The shared secret must be the same on the trusted AP and your ZyXEL Device. The shared secret is not sent over the network. The shared secret is used to encrypt messages from and to the ZyXEL Device. Both the IP address and shared secret of the trusted AP can be configured in the “external RADIUS” server fields of the trusted AP.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to begin configuring this screen afresh.

12.5 Trusted Users Overview

A trusted user is a wireless client within the ZyXEL Device’s wireless network. See Section on page 122 to change your ZyXEL Device’s trusted users.

13

Certificates

This chapter gives background information about public-key certificates and explains how to use them.

13.1 Certificates Overview

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

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

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

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

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

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

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

13.1.1 Advantages of Certificates

Certificates offer the following benefits.

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

13.2 Self-signed Certificates

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

13.3 Verifying a Certificate

Before you import a trusted CA certificate into the ZyXEL Device, you should verify that you have the actual certificate. This is especially important since the ZyXEL Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

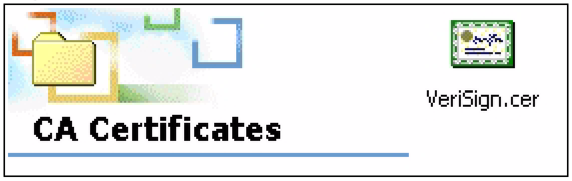
13.3.1 Checking the Fingerprint of a Certificate on Your Computer

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

1 Browse to where you have the certificate saved on your computer.

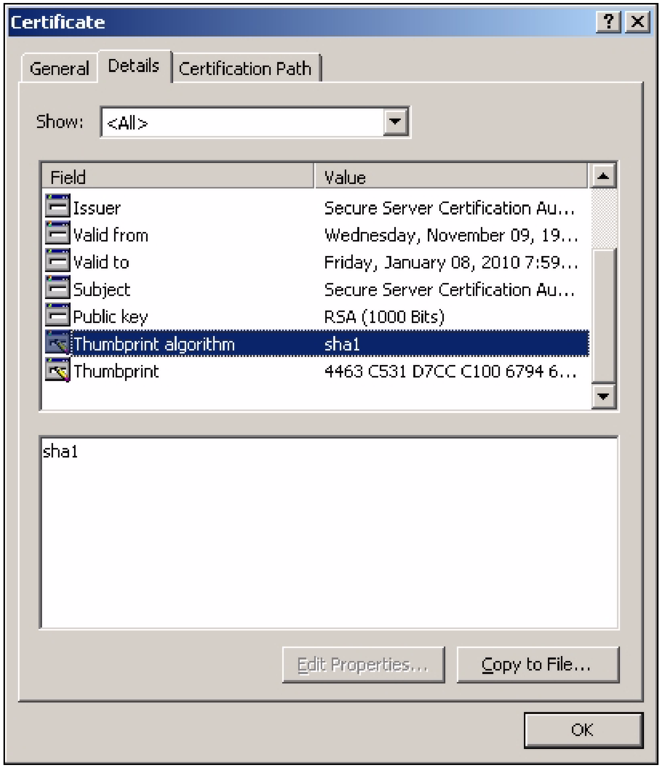
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 85 Certificates on Your Computer



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

Figure 86 Certificate Details



Show: <All>

Field	Value
Issuer	Secure Server Certification Au...
Valid from	Wednesday, November 09, 19...
Valid to	Friday, January 08, 2010 7:59...
Subject	Secure Server Certification Au...
Public key	RSA (1000 Bits)
Thumbprint algorithm	sha1
Thumbprint	4463 C531 D7CC C100 6794 6...

sha1

4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

13.4 Configuration Summary

This section summarizes how to manage certificates.

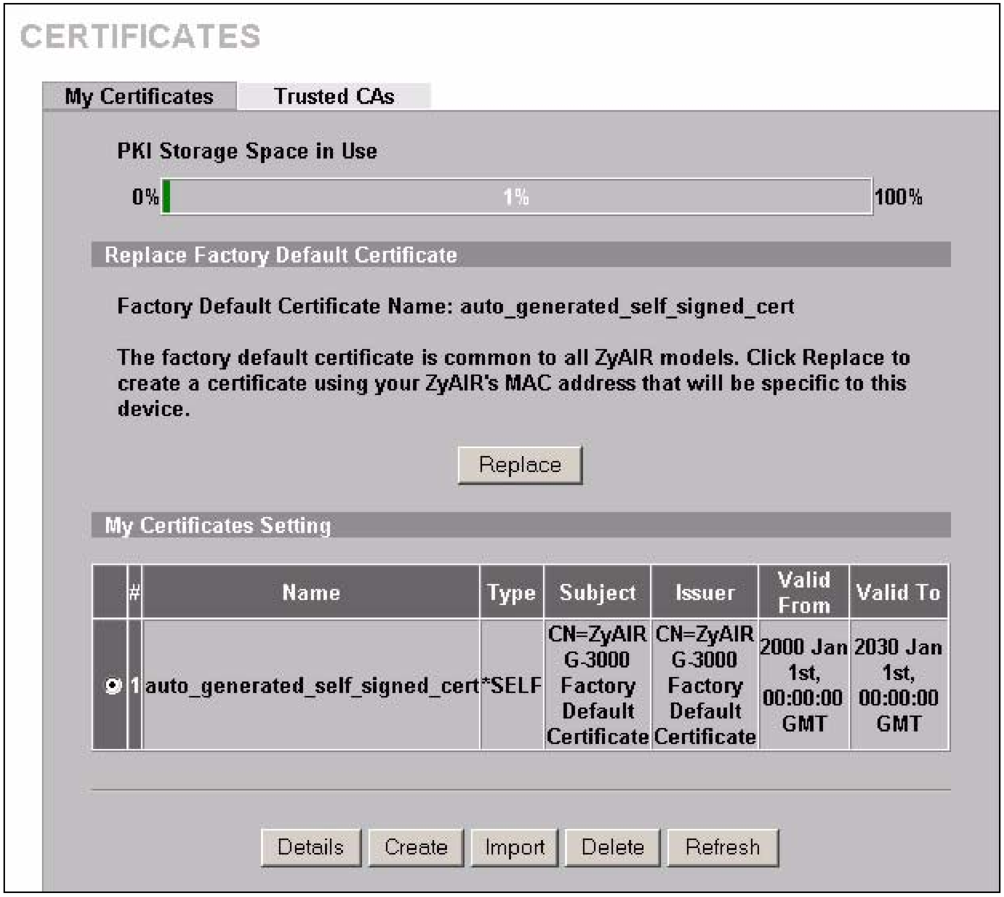
Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyXEL Devices' CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the ZyXEL Device.

13.5 My Certificates

Click **CERTIFICATES** > **My Certificates** to open the ZyXEL Device's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

Figure 87 My Certificates



CERTIFICATES

PKI Storage Space in Use

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to all ZyAIR models. Click Replace to create a certificate using your ZyAIR's MAC address that will be specific to this device.

My Certificates Setting

	#	Name	Type	Subject	Issuer	Valid From	Valid To
●	1	auto_generated_self_signed_cert	*SELF	CN=ZyAIR G-3000 Factory Default Certificate	CN=ZyAIR G-3000 Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT

The following table describes the labels in this screen.

Table 46 My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the ZyXEL Device has the factory default certificate. The factory default certificate is common to all ZyXEL Devices that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyXEL Device's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.

Table 46 My Certificates (continued)

LABEL	DESCRIPTION
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Details	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows ***SELF** in the **Type** field. 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the ***SELF** certificate. 2. Click the details icon next to another self-signed certificate (see the description on the **Create** button if you need to create a self-signed certificate). 3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box. 4. Click **Apply** to save the changes and return to the **My Certificates** screen. 5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now. Note that subsequent certificates move up by one when you take this action
Create	Click **Create** to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.
Import	Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.
Delete	Click **Delete** to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Refresh	Click **Refresh** to display the current validity status of the certificates.

13.6 Certificate File Formats

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

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

13.7 Importing a Certificate

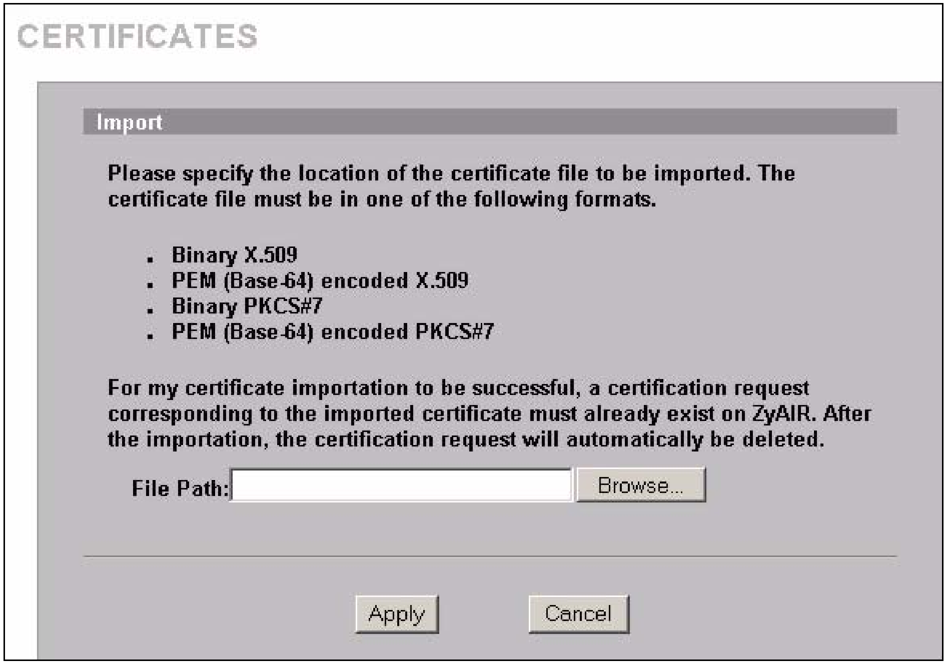
Click **CERTIFICATES** > **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyXEL Device.

You can import only a certificate that matches a corresponding certification request that was generated by the ZyXEL Device.

The certificate you import replaces the corresponding request in the My Certificates screen.

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

Figure 88 My Certificate Import



Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyAIR. After the importation, the certification request will automatically be deleted.

The following table describes the labels in this screen.

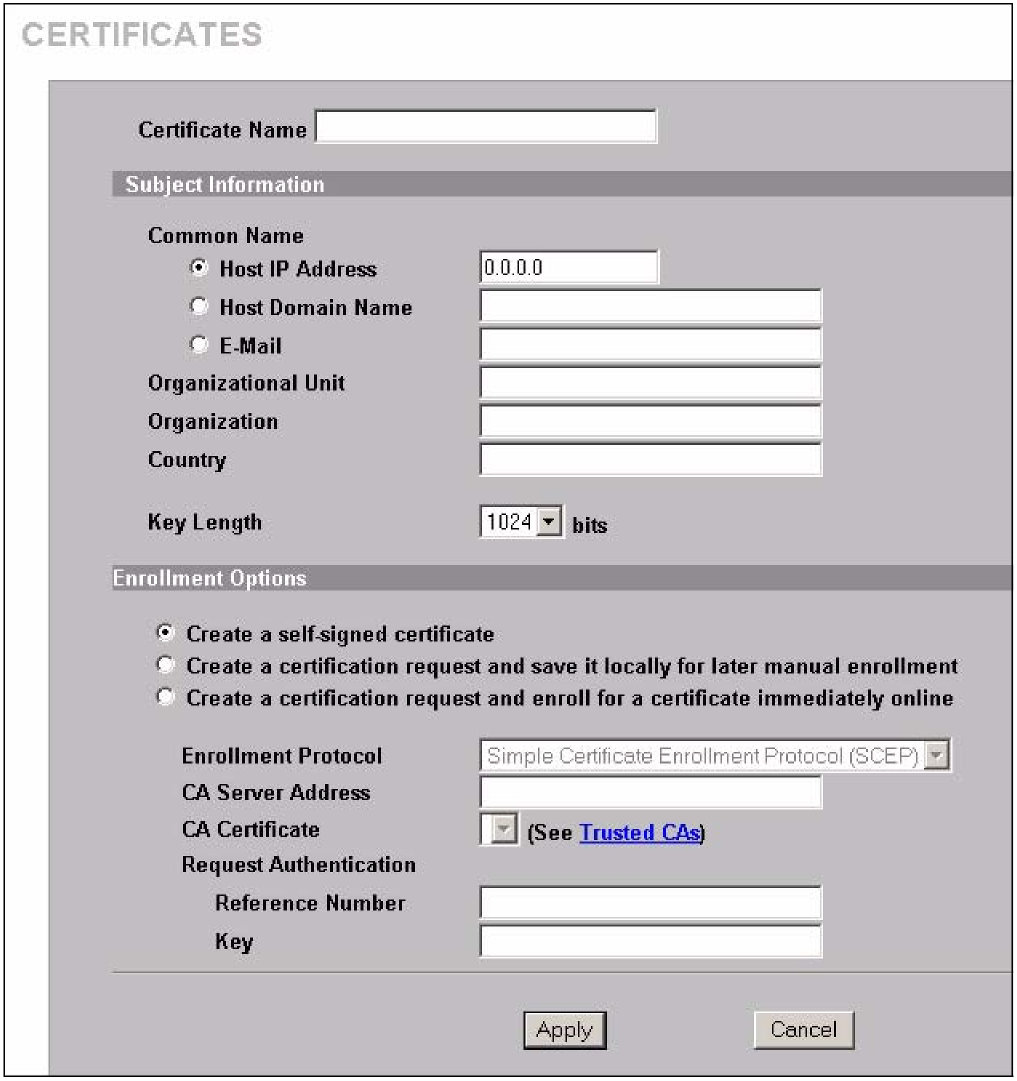
Table 47 My Certificate Import

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 certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

13.8 Creating a Certificate

Click **CERTIFICATES** > **My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the ZyXEL Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request, see the following figure.

Figure 89 My Certificate Create



CERTIFICATES

Certificate Name

Subject Information

Common Name

● Host IP Address 0.0.0.0

○ Host Domain Name

○ E-Mail

Organizational Unit

Organization

Country

Key Length 1024 bits

Enrollment Options

● Create a self-signed certificate

○ Create a certification request and save it locally for later manual enrollment

○ Create a certification request and enroll for a certificate immediately online

Enrollment Protocol Simple Certificate Enrollment Protocol (SCEP)

CA Server Address

CA Certificate (See Trusted CAs)

Request Authentication

Reference Number

Key

The following table describes the labels in this screen.

Table 48 My Certificate Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.

Table 48 My Certificate Create (continued)

LABEL	DESCRIPTION
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the ZyXEL Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the ZyXEL Device generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (Section 13.9 on page 156) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the ZyXEL Device generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SECP enrollment protocol.
Key	Type the key that the certification authority gave you.

Table 48 My Certificate Create (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyXEL Device is generating the self-signed certificate or certification request.

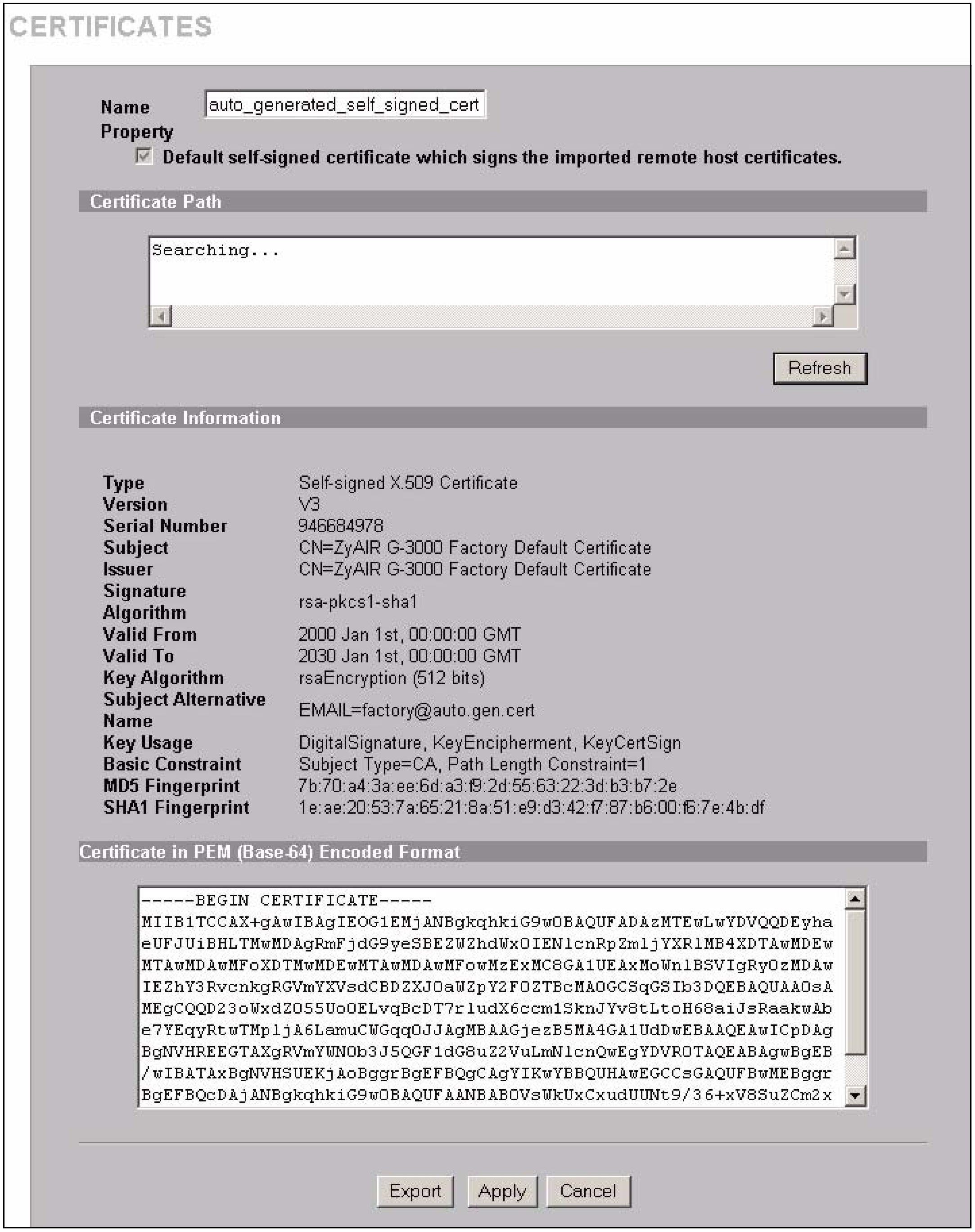
After the ZyXEL Device successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyXEL Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyXEL Device to enroll a certificate online.

13.9 My Certificate Details

Click **CERTIFICATES** > **My Certificates** to open the **My Certificates** screen (Figure 87 on page 150). Click the details button to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyXEL Device uses to sign the trusted remote host certificates that you import to the ZyXEL Device.

Figure 90 My Certificate Details



Name: auto_generated_self_signed_cert

Property

☑ Default self-signed certificate which signs the imported remote host certificates.

```
Searching...
```

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946684978
Subject	CN=ZyAIR G-3000 Factory Default Certificate
Issuer	CN=ZyAIR G-3000 Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=factory@auto.gen.cert
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	7b:70:a4:3a:ee:6d:a3:f9:2d:55:63:22:3d:b3:b7:2e
SHA1 Fingerprint	1e:ae:20:53:7a:65:21:8a:51:e9:d3:42:f7:87:b6:00:f6:7e:4b:df

```
-----BEGIN CERTIFICATE-----
MIIB1TCCAX+gAwIBAgIEOG1EMjANBgkqhkiG9w0BAQUFADAzMTEwLwYDVQQDEyha
eUFJUiBHLTMwMDAgRmFjdG9yeSBEZWZhdWx0IENlcnRpZmljYXRlMB4XDTAwMDEw
MTAwMDAwMFoXDTMwMDEwMTAwMDAwMFowMzExMC8GA1UEAxMoWnlBSVIgRy0zMDAw
IEZhY3RvcnkgRGVmYXVsdCBDZXJ0aWZpY2F0ZTBcMA0GCSqGSIb3DQEBAQUAA0sA
MEgCQQD23oWxdZ055UoOELvqBcDT7rludX6ccm1SknJYv8tLtoH68aiJsRaakwAb
e7YEqyRtwTMpljA6LamuCWGqq0JJAgMBAAGjezB5MA4GA1UdDwEBAAQEAwICpDAg
BgNVHREEGTAXgRVmYWN0b3J5QGF1dG8uZ2VuLmNlcnQwEgYDVR0TAQEABAgwBgEB
/wIBATAxBgNVHSUEKjAoBggrBgEFBQgCAgYIKwYBBQUHAwEGCCsGAQUFBwMEBggr
BgEFBQcDAjANBgkqhkiG9w0BAQUFAANBAB0VsWkUxCxudUUNt9/36+xV8SuZCm2x
```

The following table describes the labels in this screen.

Table 49 My Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyXEL Device use this certificate to sign the trusted remote host certificates that you import to the ZyXEL Device. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certificate Path	Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyXEL Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyXEL Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyXEL Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).

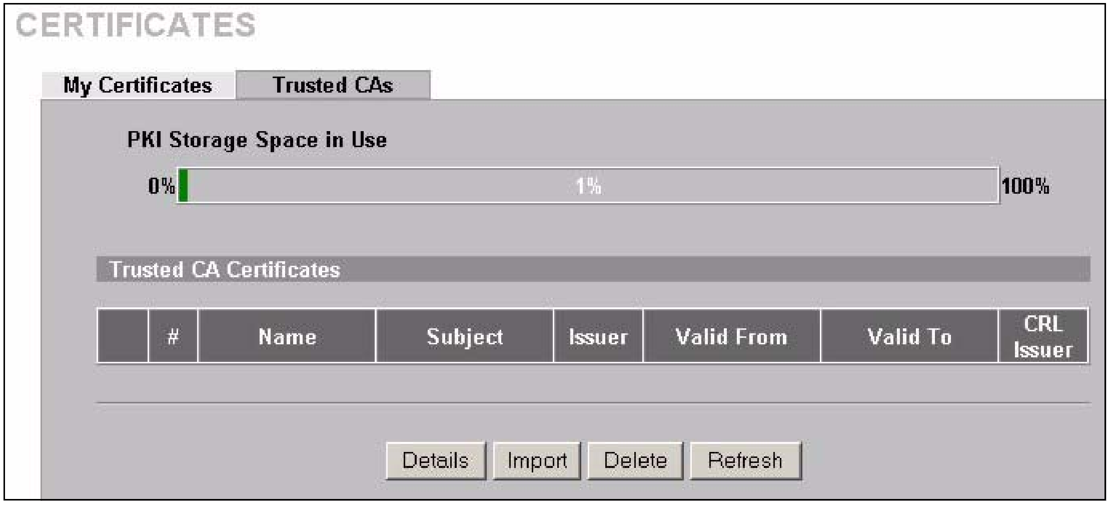
Table 49 My Certificate Details (continued)

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate owner‘s IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate’s key can be used. For example, “DigitalSignature” means that the key can be used to sign certificates and “KeyEncipherment” means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority’s certificate and “Path Length Constraint=1” means that there can only be one certification authority in the certificate’s path.
MD5 Fingerprint	This is the certificate’s message digest that the ZyXEL Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate’s message digest that the ZyXEL Device calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority’s web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

13.10 Trusted CAs

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

Figure 91 Trusted CAs



	#	Name	Subject	Issuer	Valid From	Valid To	CRL Issuer

The following table describes the labels in this screen.

Table 50 Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (CRL)** check box in the certificate's details screen to have the ZyXEL Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Details	Click **Details** to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.

Table 50 Trusted CAs (continued)

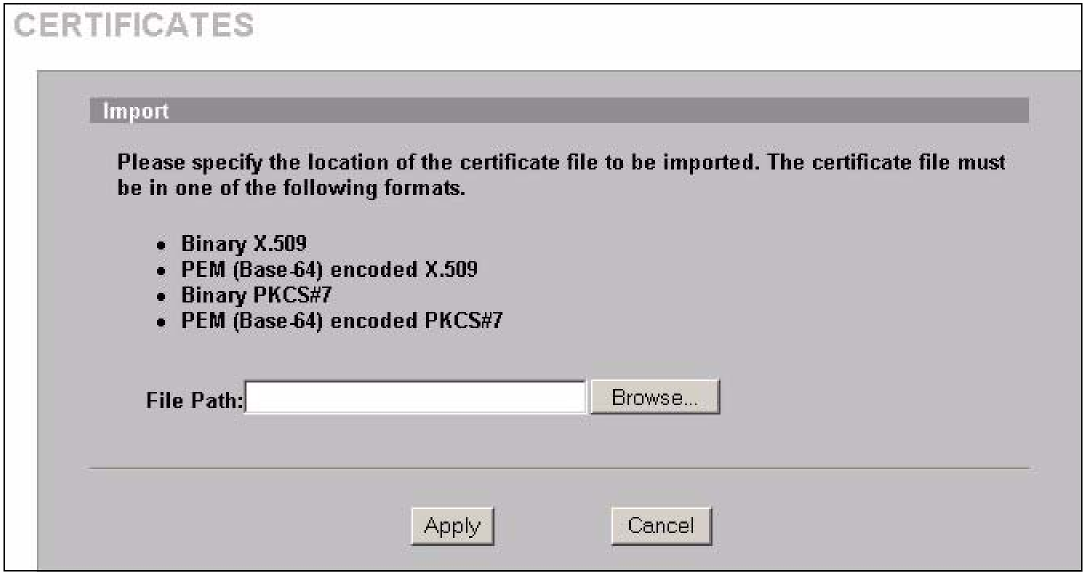
LABEL	DESCRIPTION
Delete	Click **Delete** to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Refresh	Click this button to display the current validity status of the certificates.

13.11 Importing a Trusted CA's Certificate

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyXEL Device, see the following figure.

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

Figure 92 Trusted CA Import



Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

The following table describes the labels in this screen.

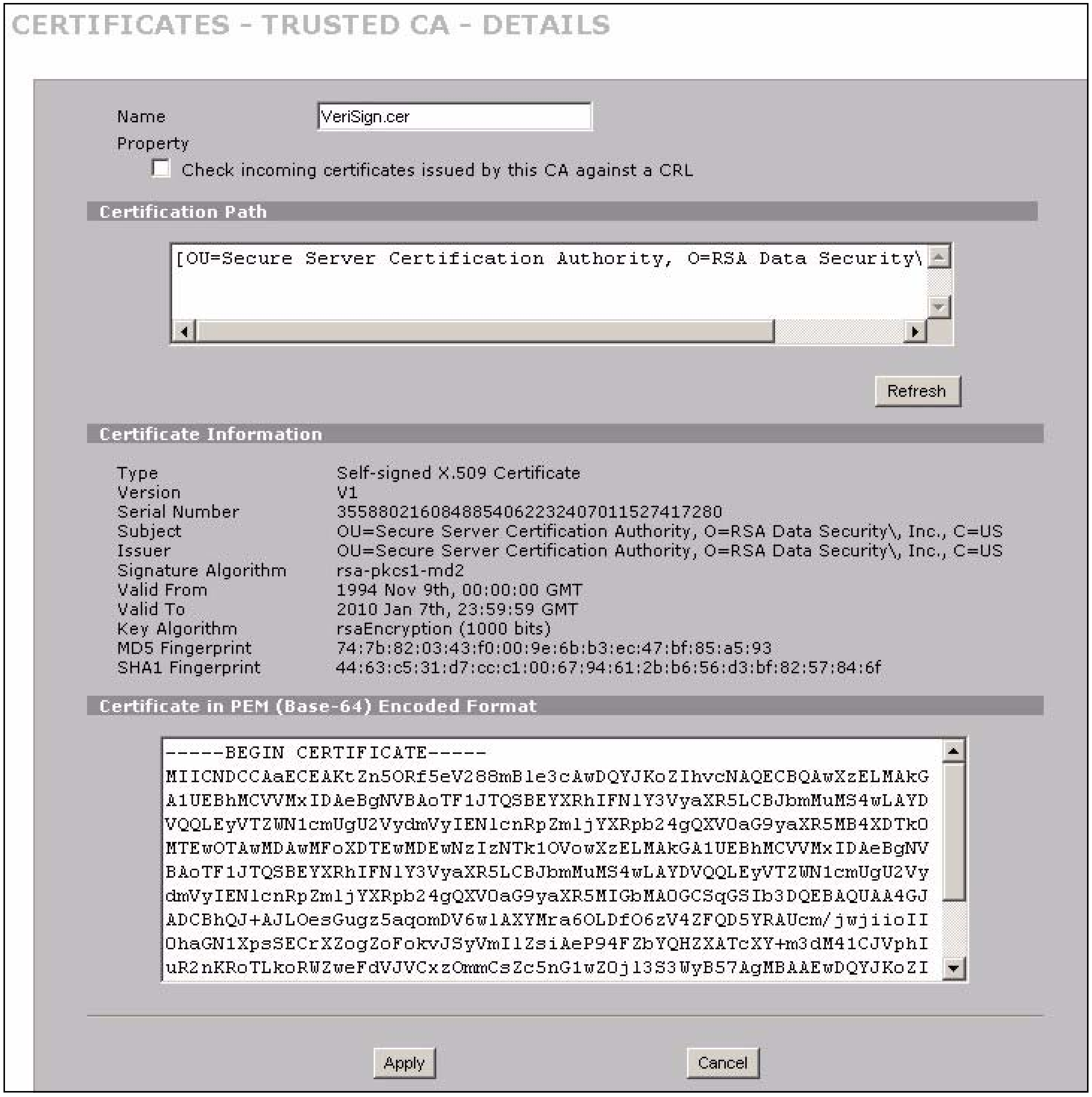
Table 51 Trusted CA Import

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 certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

13.12 Trusted CA Certificate Details

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 93 Trusted CA Details



CERTIFICATES - TRUSTED CA - DETAILS

Name: VeriSign.cer

Property

□ Check incoming certificates issued by this CA against a CRL

Certification Path

```
[OU=Secure Server Certification Authority, O=RSA Data Security\
```

Certificate Information

Type	Self-signed X.509 Certificate
Version	V1
Serial Number	3558802160848854062232407011527417280
Subject	OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US
Issuer	OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US
Signature Algorithm	rsa-pkcs1-md2
Valid From	1994 Nov 9th, 00:00:00 GMT
Valid To	2010 Jan 7th, 23:59:59 GMT
Key Algorithm	rsaEncryption (1000 bits)
MD5 Fingerprint	74:7b:82:03:43:f0:00:9e:6b:b3:ec:47:bf:85:a5:93
SHA1 Fingerprint	44:63:c5:31:d7:cc:c1:00:67:94:61:2b:b6:56:d3:bf:82:57:84:6f

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN CERTIFICATE-----
MIICNDCCAaECEAKtZn5ORf5eV288mBle3cAwDQYJKoZIhvcNAQECBQAwXzELMAkG
A1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMS4wLAYD
VQQLEyVTZWN1cmUgU2VydmVyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTk0
MTEwOTAwMDAwMFoXDTEwMDEwNzIzNTk1OVowXzELMAkGA1UEBhMCVVMxIDAeBgNV
BAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMS4wLAYDVQQLEyVTZWN1cmUgU2Vy
dmVyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIGbMA0GCSqGSIb3DQEBAQUAA4GJ
ADCBhQJ+AJLOesGugz5aqomDV6wlAXYMra6OLDfO6zV4ZFQD5YRAUcm/jwjiioII
0haGN1XpsSECrXZogZoFokvJSyVmIlZsiAeP94FZbYQHZXATcXY+m3dM41CJVphI
uR2nKRoTLkoRWZweFdVJVCxzOmmCsZc5nG1wZ0jl3S3WyB57AgMBAAEwDQYJKoZI
```

The following table describes the labels in this screen.

Table 52 Trusted CA Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the ZyXEL Device check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the ZyXEL Device not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyXEL Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).

Table 52 Trusted CA Details (continued)

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Apply	Click **Apply** to save your changes back to the ZyXEL Device. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

14

Log Screens

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

14.1 Configuring View Log

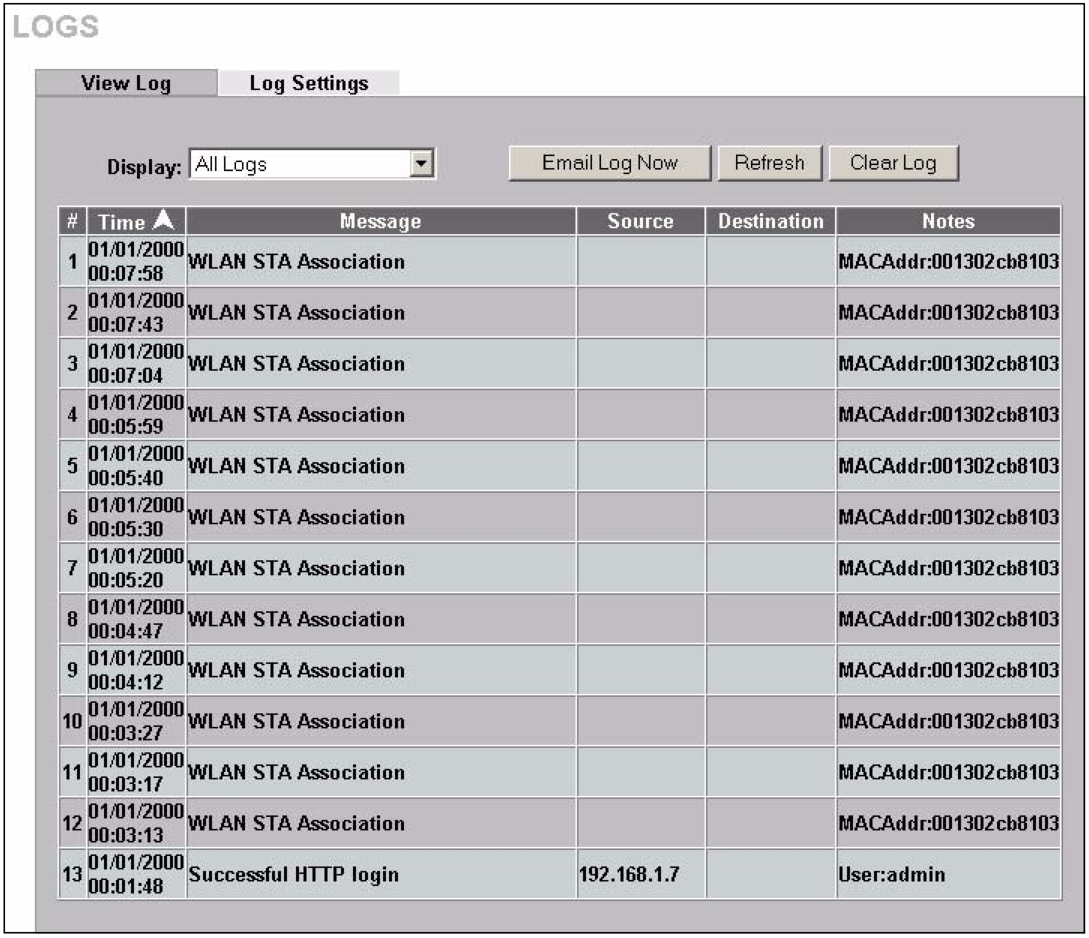
The web configurator allows you to look at all of the ZyXEL Device's logs in one location.

Click **LOGS > View Log**. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Figure 95 on page 167). Options include logs about system maintenance, system errors and access control.

You can view logs and alert messages in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

Figure 94 View Log



Display: All Logs

#	Time	Message	Source	Destination	Notes
1	01/01/2000 00:07:58	WLAN STA Association			MACAddr:001302cb8103
2	01/01/2000 00:07:43	WLAN STA Association			MACAddr:001302cb8103
3	01/01/2000 00:07:04	WLAN STA Association			MACAddr:001302cb8103
4	01/01/2000 00:05:59	WLAN STA Association			MACAddr:001302cb8103
5	01/01/2000 00:05:40	WLAN STA Association			MACAddr:001302cb8103
6	01/01/2000 00:05:30	WLAN STA Association			MACAddr:001302cb8103
7	01/01/2000 00:05:20	WLAN STA Association			MACAddr:001302cb8103
8	01/01/2000 00:04:47	WLAN STA Association			MACAddr:001302cb8103
9	01/01/2000 00:04:12	WLAN STA Association			MACAddr:001302cb8103
10	01/01/2000 00:03:27	WLAN STA Association			MACAddr:001302cb8103
11	01/01/2000 00:03:17	WLAN STA Association			MACAddr:001302cb8103
12	01/01/2000 00:03:13	WLAN STA Association			MACAddr:001302cb8103
13	01/01/2000 00:01:48	Successful HTTP login	192.168.1.7		User:admin

The following table describes the labels in this screen.

Table 53 View Log

LABEL	DESCRIPTION
Display	Select a log category from the drop down list box to display logs within the selected category. To view all logs, select **All Logs**. The number of categories shown in the drop down list box depends on the selection in the **Log Settings** page.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.

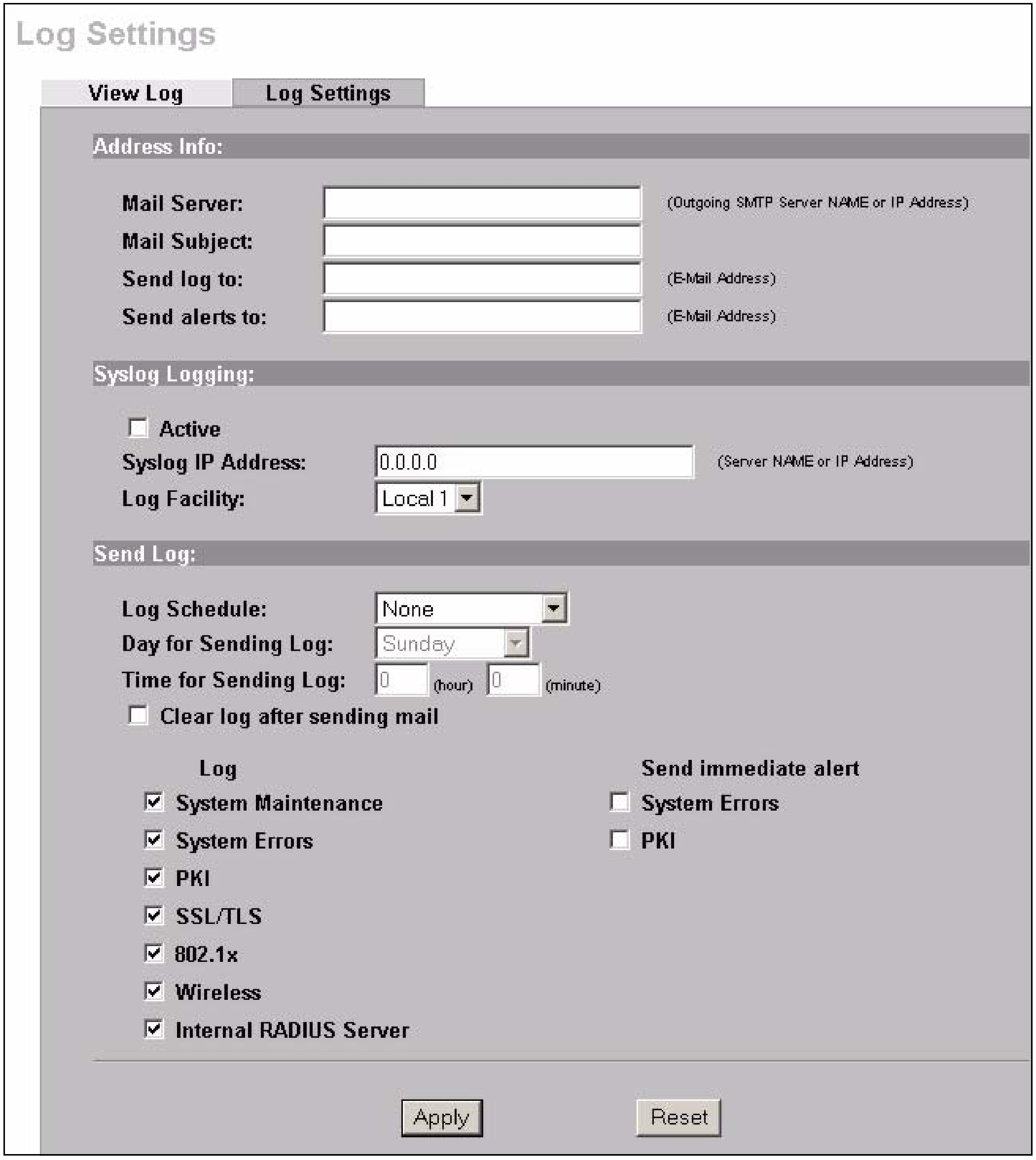
14.2 Configuring Log Settings

To change your ZyXEL Device's log settings, click **LOGS** > **Log Settings**. The screen appears as shown.

Use the **Log Settings** screen to configure to where and when the ZyXEL Device is to send the logs and which logs and/or immediate alerts it is to send.

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

Figure 95 Log Settings



Log Settings

Address Info:

Mail Server: (Outgoing SMTP Server NAME or IP Address)
Mail Subject:
Send log to: (E-Mail Address)
Send alerts to: (E-Mail Address)

Syslog Logging:

☐ Active
Syslog IP Address: 0.0.0.0 (Server NAME or IP Address)
Log Facility: Local 1

Send Log:

Log Schedule: None
Day for Sending Log: Sunday
Time for Sending Log: 0 (hour) 0 (minute)
☐ Clear log after sending mail

Log	Send immediate alert
☑ System Maintenance	☐ System Errors
☑ System Errors	☐ PKI
☑ PKI	
☑ SSL/TLS	
☑ 802.1x	
☑ Wireless	
☑ Internal RADIUS Server	

The following table describes the labels in this screen.

Table 54 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends.
Send Log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts to	Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	This field is only available when you select **Weekly** in the **Log Schedule** field. Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select the categories of alerts for which you want the ZyXEL Device to immediately send e-mail alerts.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to reconfigure all the fields in this screen.

14.3 Example Log Messages

This section provides descriptions of some example log messages.

Table 55 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`DHCP client gets %s`	A DHCP client got a new IP address from the DHCP server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`SMT Login Successfully`	Someone has logged on to the router's SMT interface.
`SMT Login Fail`	Someone has failed to log on to the router's SMT interface.
`WEB Login Successfully`	Someone has logged on to the router's web configurator interface.
`WEB Login Fail`	Someone has failed to log on to the router's web configurator interface.
`TELNET Login Successfully`	Someone has logged on to the router via telnet.
`TELNET Login Fail`	Someone has failed to log on to the router via telnet.
`FTP Login Successfully`	Someone has logged on to the router via FTP.
`FTP Login Fail`	Someone has failed to log on to the router via FTP.

Table 56 ICMP Notes

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

Table 56 ICMP Notes (continued)

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

Table 57 Sys log

LOG MESSAGE	DESCRIPTION
`Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>"`	This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts.

14.4 Log Commands

Go to the command interpreter interface (see Section 26.1 on page 249 for how to access and use the commands).

14.4.1 Configuring What You Want the ZyXEL Device to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyXEL Device is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

Table 58 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
error	0, 1, 2, 3
mten	0, 1
Use `0` to not record logs for that category, `1` to record only logs for that category, `2` to record only alerts for that category, and `3` to record both logs and alerts for that category.	

Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

14.4.2 Displaying Logs

Use the `sys logs display` command to show all of the logs in the ZyXEL Device's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual ZyXEL Device log category.

Use the `sys logs clear` command to erase all of the ZyXEL Device's logs.

14.5 Log Command Example

This example shows how to set the ZyXEL Device to record the error logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category error 3
ras> sys logs save
ras> sys logs display access

#.    time                source              destination           notes    message
0  | 11/11/2002 15:10:12 | 172.22.3.80:137  |  172.22.255.255:137  |  ACCESS   BLOCK
```

15

VLAN

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

15.1 VLAN

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

15.1.1 Management VLAN ID

The Management VLAN ID identifies the “management VLAN”. A device must be a member of this “management VLAN” in order to access and manage the ZyXEL Device. If a device is not a member of this VLAN, then that device cannot manage the ZyXEL Device.

If no devices are in the management VLAN, then you will not be able to access the ZyXEL Device through the network. If the ZyXEL Device has no console port, you will have to restore the default configuration file.

15.1.2 VLAN Tagging

The ZyXEL Device supports IEEE 802.1q VLAN tagging. Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header of a frame to identify VLAN membership. The ZyXEL Device can identify VLAN tags for incoming Ethernet frames and add VLAN tags to outgoing Ethernet frames.

When VLAN is enabled, you must connect the ZyXEL Device to a VLAN-aware device that is a member of the management VLAN in order to manage it through the network. See the example of configuring a management VLAN (**Section 15.2.2 on page 176**) BEFORE you configure VLAN on the ZyXEL Device.

15.2 Configuring VLAN

The ZyXEL Device allows you to configure VLAN based on SSID profile (wireless VLAN), and / or based on your RADIUS server (RADIUS VLAN).

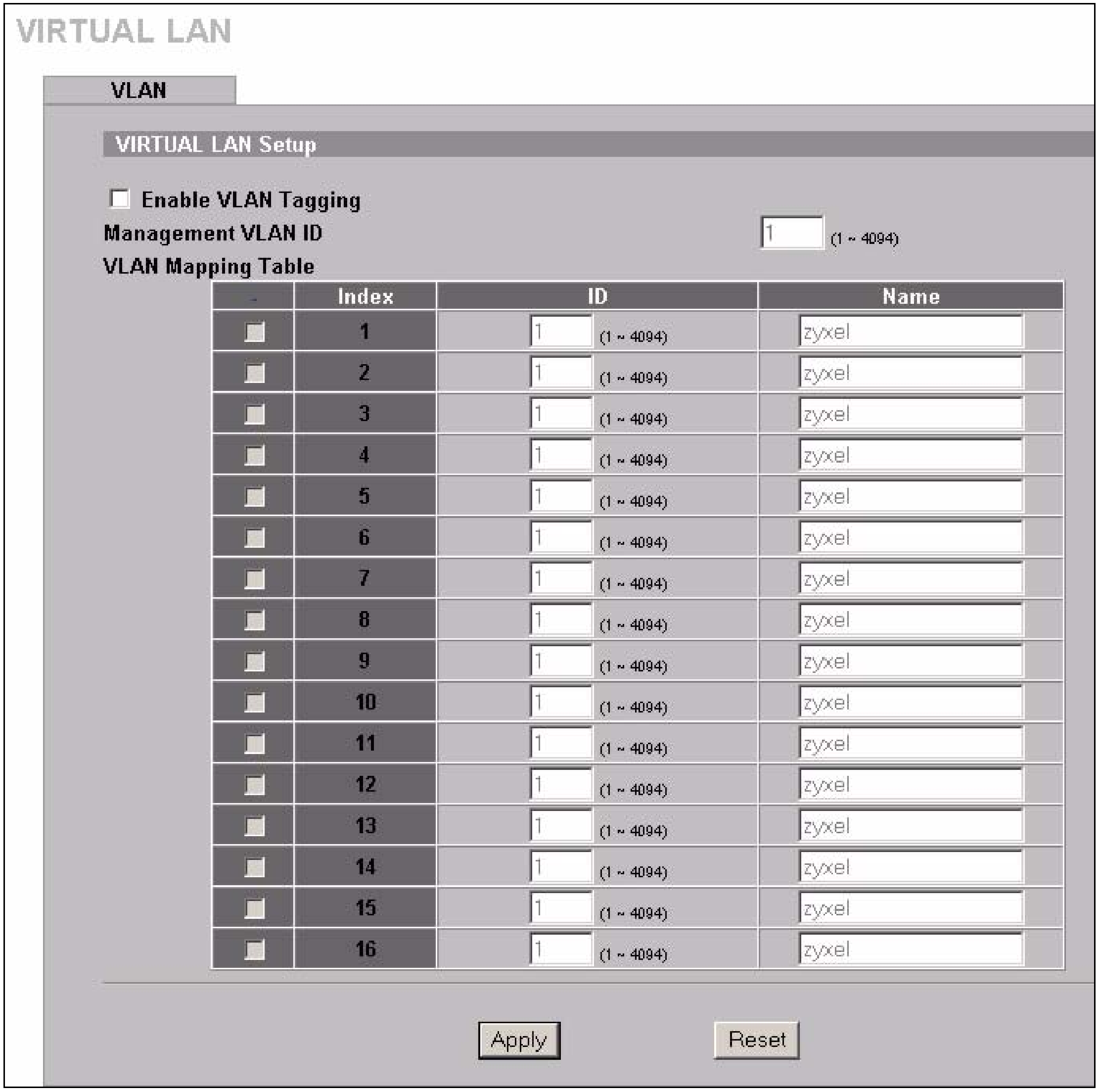
- When you use wireless VLAN, the ZyXEL Device tags all packets from an SSID with the VLAN ID you set in the **WIRELESS** > **SSID** > **Edit** screen.
- When you use the VLAN screen's mapping table, your RADIUS server assigns VLAN IDs to a user or user group's traffic based on the configuration in the **VLAN** screen.
- When you use wireless VLAN and the VLAN mapping table together, the ZyXEL Device first tries to assign VLAN IDs based on the VLAN IDs from the RADIUS server. If a client's user name does not match an entry in the VLAN mapping table, the ZyXEL Device assigns a VLAN ID based on the settings you set for the SSID. See Section 15.2.3 on page 178 for more information.

To use the VLAN mapping table, you must first turn on VLAN tagging and configure the management VLAN ID.

15.2.1 VLAN

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

Figure 96 VLAN



VIRTUAL LAN

VLAN

VIRTUAL LAN Setup

☐ Enable VLAN Tagging

Management VLAN ID 1 (1 ~ 4094)

VLAN Mapping Table

-	Index	ID	Name
☐	1	1 (1 ~ 4094)	zyxel
☐	2	1 (1 ~ 4094)	zyxel
☐	3	1 (1 ~ 4094)	zyxel
☐	4	1 (1 ~ 4094)	zyxel
☐	5	1 (1 ~ 4094)	zyxel
☐	6	1 (1 ~ 4094)	zyxel
☐	7	1 (1 ~ 4094)	zyxel
☐	8	1 (1 ~ 4094)	zyxel
☐	9	1 (1 ~ 4094)	zyxel
☐	10	1 (1 ~ 4094)	zyxel
☐	11	1 (1 ~ 4094)	zyxel
☐	12	1 (1 ~ 4094)	zyxel
☐	13	1 (1 ~ 4094)	zyxel
☐	14	1 (1 ~ 4094)	zyxel
☐	15	1 (1 ~ 4094)	zyxel
☐	16	1 (1 ~ 4094)	zyxel

The following table describes the labels in this screen

Table 59 WIRELESS VLAN

FIELD	DESCRIPTION
Enable VIRTUAL LAN	Select this box to enable VLAN tagging.
Management VLAN ID	Enter a number from 1 to 4094 to define this VLAN group. At least one device in your network must belong to this VLAN group in order to manage the ZyXEL Device. Note: Mail and FTP servers must have the same management VLAN ID to communicate with the ZyXEL Device. See Section 15.2.2 on page 176 for more information.

Table 59 WIRELESS VLAN

FIELD	DESCRIPTION
VLAN Mapping Table	Use this table to map names to VLAN IDs so that the RADIUS server can assign each user or user group a mapped VLAN ID. See your RADIUS server documentation for more information on configuring VLAN ID attributes. See Section 15.2.3 on page 178 for more information.
Index	Select a check box to enable the VLAN mapping profile.
ID	Type a VLAN ID. Incoming traffic from the WLAN is authorized and assigned a VLAN ID before it is sent to the LAN.
Name	Type a name to have the ZyXEL Device check for specific VLAN attributes on incoming messages from the RADIUS server. Access-accept packets sent by the RADIUS server contain VLAN related attributes. The configured **Name** fields are checked against these attributes. If a configured **Name** field matches these attributes, the corresponding VLAN ID is added to packets sent from this user to the LAN. If the VLAN-related attributes sent by the RADIUS server do not match a configured **Name** field, a wireless station is assigned the wireless VLAN ID associated with its SSID.
Apply	Click this to save your changes to the ZyXEL Device.
Reset	Click this to return this screen to its last-saved settings.

15.2.2 Configuring Management VLAN Example

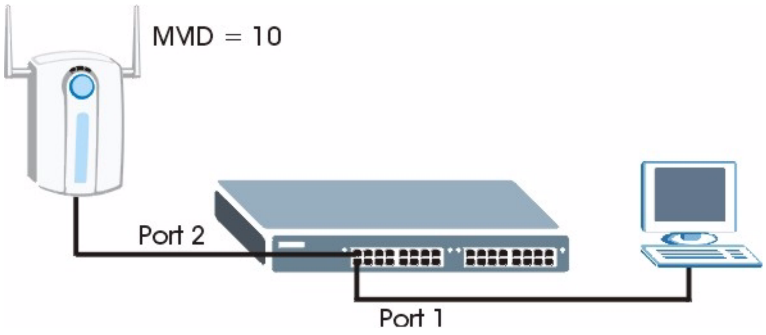
This section shows you how to create a VLAN on an Ethernet switch.

By default, the port on the ZyXEL Device is a member of the management VLAN (VLAN ID 1). The following procedure shows you how to configure a tagged VLAN.

If you misconfigure the management VLAN and lock yourself out from performing in-band management you will need to reset the ZyXEL Device.

On an Ethernet switch, create a VLAN that has the same management VLAN ID as the ZyXEL Device. The following figure has the ZyXEL Device connected to port 2 of the switch and your computer connected to port 1. The management VLAN ID is ten.

Figure 97 Management VLAN Configuration Example



Perform the following steps in the switch web configurator:

1 Click **VLAN** under **Advanced Application**.

2 Click **Static VLAN**.

3 Select the **ACTIVE** check box.

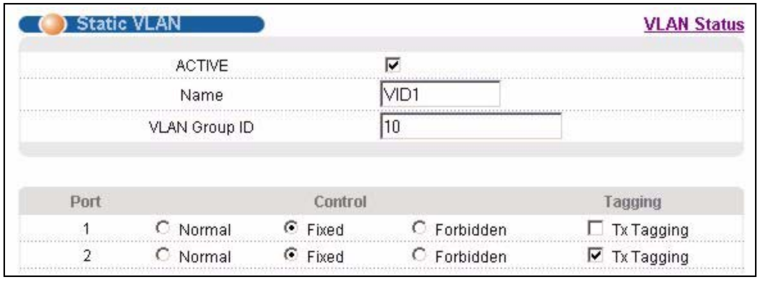
4 Type a **Name** for the VLAN ID.

5 Type a **VLAN Group ID**. This should be the same as the management VLAN ID on the ZyXEL Device.

6 Enable **Tx Tagging** on the port which you want to connect to the ZyXEL Device. Disable **Tx Tagging** on the port you are using to connect to your computer.

7 Under **Control**, select **Fixed** to set the port as a member of the VLAN.

Figure 98 VLAN-Aware Switch - Static VLAN

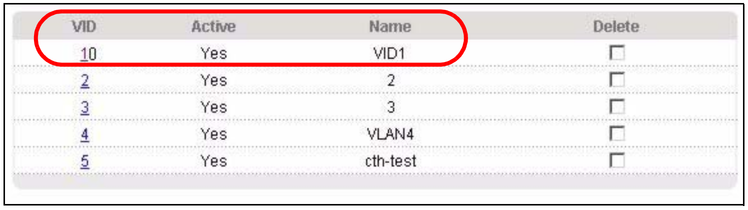


ACTIVE	☑
Name	VID1
VLAN Group ID	10

Port	Control			Tagging
1	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
2	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging

8 Click **Apply**. The following screen displays.

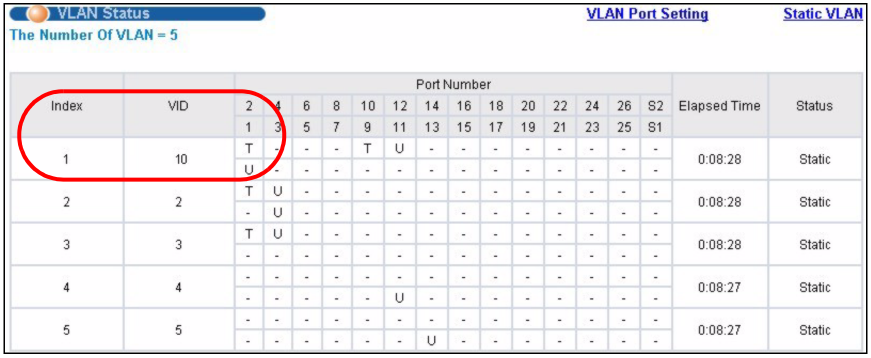
Figure 99 VLAN-Aware Switch



VID	Active	Name	Delete
10	Yes	VID1	□
2	Yes	2	□
3	Yes	3	□
4	Yes	VLAN4	□
5	Yes	cth-test	□

9 Click **VLAN Status** to display the following screen.

Figure 100 VLAN-Aware Switch - VLAN Status



The Number Of VLAN = 5

Index	VID	Port Number														Elapsed Time	Status
		2	4	6	8	10	12	14	16	18	20	22	24	26	S2		
		1	3	5	7	9	11	13	15	17	19	21	23	25	S1		
1	10	T	-	-	-	T	U	-	-	-	-	-	-	-	-	0:08:28	Static
		U	-	-	-	-	-	-	-	-	-	-	-	-	-		
2	2	T	U	-	-	-	-	-	-	-	-	-	-	-	-	0:08:28	Static
		-	U	-	-	-	-	-	-	-	-	-	-	-	-		
3	3	T	U	-	-	-	-	-	-	-	-	-	-	-	-	0:08:28	Static
		-	-	-	-	-	-	-	-	-	-	-	-	-	-		
4	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:08:27	Static
		-	-	-	-	-	U	-	-	-	-	-	-	-	-		
5	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:08:27	Static
		-	-	-	-	-	-	U	-	-	-	-	-	-	-		

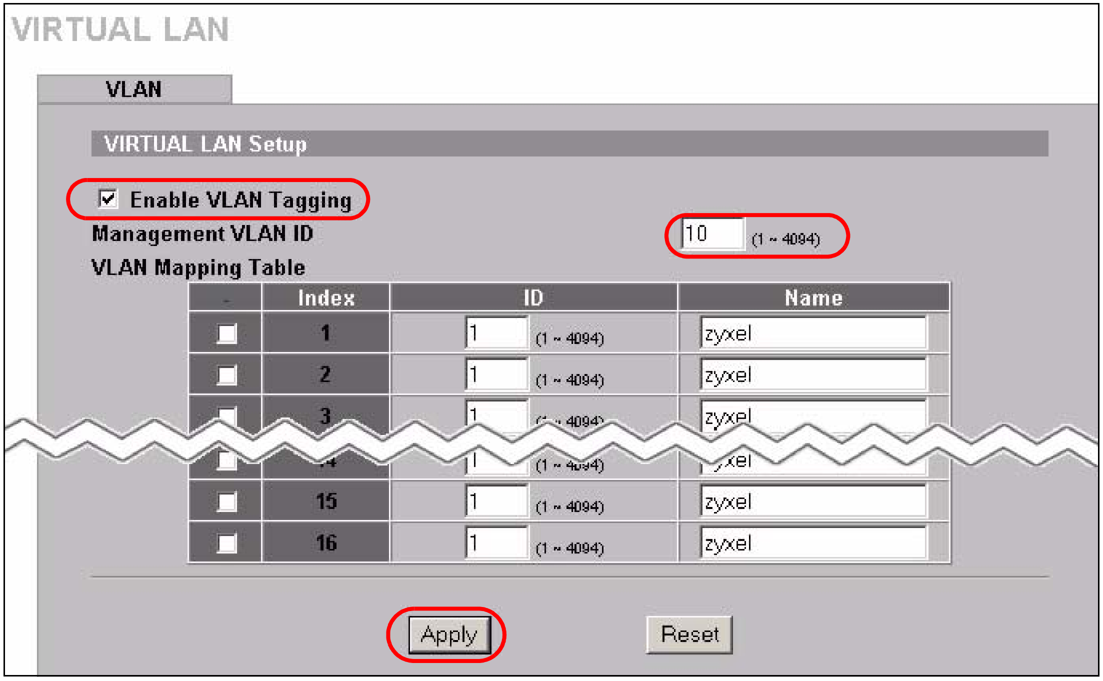
Follow the instructions in the Quick Start Guide to set up your ZyXEL Device for configuration. The ZyXEL Device should be connected to the VLAN-aware switch. In the above example, the switch is using port 1 to connect to your computer and port 2 to connect to the ZyXEL Device: Figure 97 on page 176.

1 In the ZyXEL Device web configurator click **VLAN** to open the VLAN setup screen.

2 Select the **Enable VLAN Tagging** check box and type a **Management VLAN ID** (10 in this example) in the field provided.

3 Click **Apply**.

Figure 101 VLAN Setup



VIRTUAL LAN

VLAN

VIRTUAL LAN Setup

☑ Enable VLAN Tagging

Management VLAN ID 10 (1 ~ 4094)

VLAN Mapping Table

	Index	ID	Name
□	1	1 (1 ~ 4094)	zyxel
□	2	1 (1 ~ 4094)	zyxel
□	3	1 (1 ~ 4094)	zyxel
□	14	1 (1 ~ 4094)	zyxel
□	15	1 (1 ~ 4094)	zyxel
□	16	1 (1 ~ 4094)	zyxel

4 The ZyXEL Device attempts to connect with a VLAN-aware device. You can now access and mange the ZyXEL Device though the Ethernet switch.

If you do not connect the ZyXEL Device to a correctly configured VLAN-aware device, you will lock yourself out of the ZyXEL Device. If this happens, you must reset the ZyXEL Device to access it again.

15.2.3 Configuring Microsoft's IAS Server Example

Dynamic VLAN assignment can be used with the ZyXEL Device. Dynamic VLAN assignment allows network administrators to assign a specific VLAN (configured on the ZyXEL Device) to an individual's Windows User Account. When a wireless station is successfully authenticated to the network, it is automatically placed into it's respective VLAN.

ZyXEL uses the following standard RADIUS attributes returned from Microsoft's IAS RADIUS service to place the wireless station into the correct VLAN:

Table 60 Standard RADIUS Attributes

ATTRIBUTE NAME	TYPE	VALUE
Tunnel-Type	064	13 (decimal) – VLAN

Table 60 Standard RADIUS Attributes

ATTRIBUTE NAME	TYPE	VALUE
Tunnel-Medium-Type	065	6 (decimal) – 802
Tunnel-Private-Group-ID	081	<vlan-name> (string) – either the **Name** you enter in the ZyXEL Device's **VLAN > RADIUS VLAN** screen or the number. See Figure 113 on page 185.

The following occurs under Dynamic VLAN Assignment:

1. When you configure your wireless credentials, the ZyXEL Device sends the information to the IAS server using RADIUS protocol.
2. Authentication by the RADIUS server is successful.
3. The RADIUS server sends three attributes related to this feature.
4. The ZyXEL Device compares these attributes with the VLAN screen mapping table.
   - **4a** If the **Name**, for example "VLAN 20" is found, the mapped VLAN ID is used.
   - **4b** If the **Name** is not found in the mapping table, the string in the **Tunnel-Private-Group-ID** attribute is considered as a number ID format, for example 2493. The range of the number ID (Name:string) is between 1 and 4094.
   - **4c** If **a** or **b** are not matched, the ZyXEL Device uses the VLAN ID configured in the **WIRELESS VLAN** screen and the wireless station. This **VLAN ID** is independent and hence different to the **ID** in the VLAN screen.

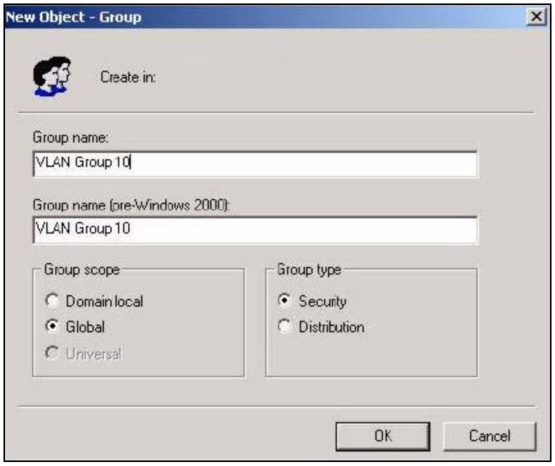
15.2.3.1 Configuring VLAN Groups

To configure a VLAN group you must first define the VLAN Groups on the Active Directory server and assign the user accounts to each VLAN Group.

1. Using the Active Directory Users and Computers administrative tool, create the VLAN Groups that will be used for each VLAN ID. One VLAN Group must be created for each VLAN defined on the ZyXEL Device. The VLAN Groups must be created as Global/ Security groups.

- Type a name for the **VLAN Group** that describes the VLAN Group's function.
- Select the **Global** Group scope parameter check box.
- Select the **Security** Group type parameter check box.
- Click **OK**.

Figure 102 New Global Security Group



Group name: VLAN Group 10

Group name (pre-Windows 2000): VLAN Group 10

Group scope: ○ Domain local ● Global ○ Universal

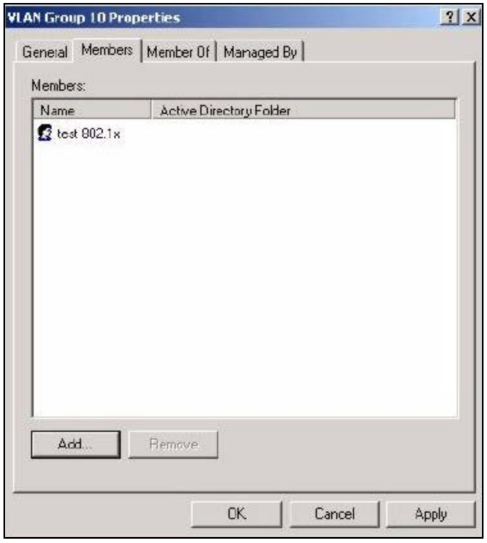
Group type: ● Security ○ Distribution

2 In **VLAN Group ID Properties**, click the **Members** tab.

- The IAS uses group memberships to determine which user accounts belong to which VLAN groups. Click the **Add** button and configure the VLAN group details.

3 Repeat the previous step to add each VLAN group required.

Figure 103 Add Group Members



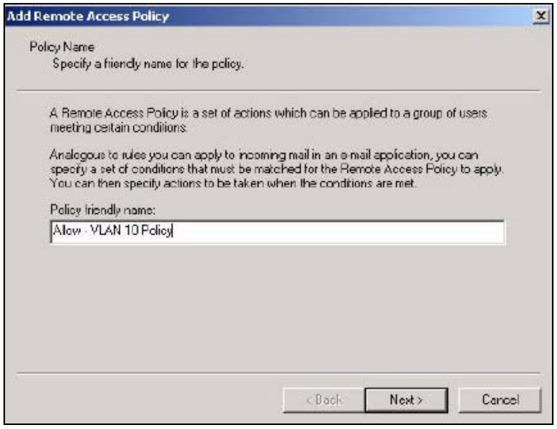
15.2.3.2 Configuring Remote Access Policies

Once the VLAN Groups have been created, the IAS Remote Access Policy needs to be defined. This allows the IAS to compare the user account being authenticated against the group memberships of each VLAN Group.

1 Using the **Remote Access Policy** option on the Internet Authentication Service management interface, create a new VLAN Policy for each VLAN Group defined in the previous section. The order of the remote access policies is important. The most specific policies should be placed at the top of the policy list and the most general at the bottom. For example, if the Day-And-Time Restriction policy is still present, it should be moved to the bottom or deleted to allow the VLAN Group policies to take precedence.

- Right click **Remote Access Policy** and select **New Remote Access Policy**.
- Enter a **Policy friendly name** that describes the policy. Each Remote Access Policy will be matched to one VLAN Group. An example may be, **Allow - VLAN 10 Policy**.
- Click **Next**.

Figure 104 New Remote Access Policy for VLAN Group



Add Remote Access Policy

Policy Name
Specify a friendly name for the policy.

A Remote Access Policy is a set of actions which can be applied to a group of users meeting certain conditions.

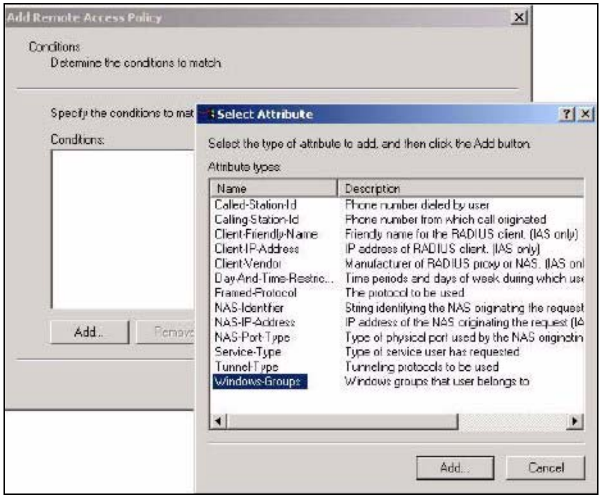
Analogous to rules you can apply to incoming mail in an e-mail application, you can specify a set of conditions that must be matched for the Remote Access Policy to apply. You can then specify actions to be taken when the conditions are met.

Policy friendly name: Allow - VLAN 10 Policy

2 The **Conditions** window displays. Select **Add** to add a condition for this policy to act on.

3 In the **Select Attribute** screen, click **Windows-Groups** and the **Add** button.

Figure 105 Specifying Windows-Group Condition



Add Remote Access Policy

Conditions
Determine the conditions to match.

Specify the conditions to mat

Conditions:

Select Attribute

Select the type of attribute to add, and then click the Add button.

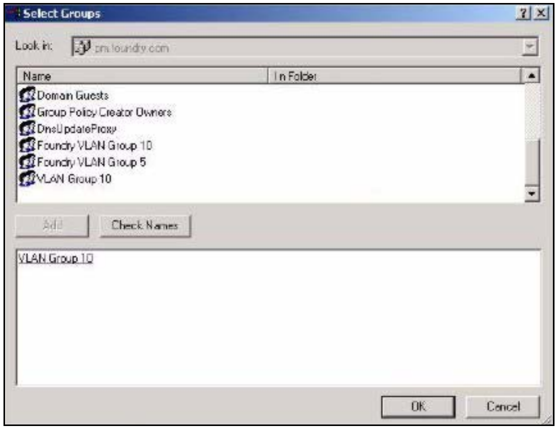
Attribute types:

Name	Description
Called-Station-Id	Phone number dieled by user
Calling-Station-Id	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client. (IAS only)
Client-IP-Address	IP address of RADIUS client. (IAS only)
Client-Vendor	Manufacturer of RADIUS proxy or NAS. (IAS onl
Day-And-Time-Restric...	Time periods and days of week during which use
Framed-Protocol	The protocol to be used
NAS-Identifier	String identifying the NAS originating the request
NAS-IP-Address	IP address of the NAS originating the request (IA
NAS-Port-Type	Type of physical port used by the NAS originatin
Service-Type	Type of service user has requested
Tunnel-Type	Tunneling protocols to be used
Windows-Groups	Windows groups that user belongs to

4 The **Select Groups** window displays. Select a remote access policy and click the **Add** button. The policy is added to the field below. Only one VLAN Group should be associated with each policy.

5 Click **OK** and **Next** in the next few screens to accept the group value.

Figure 106 Adding VLAN Group



Select Groups

Look in: pm.foundry.com

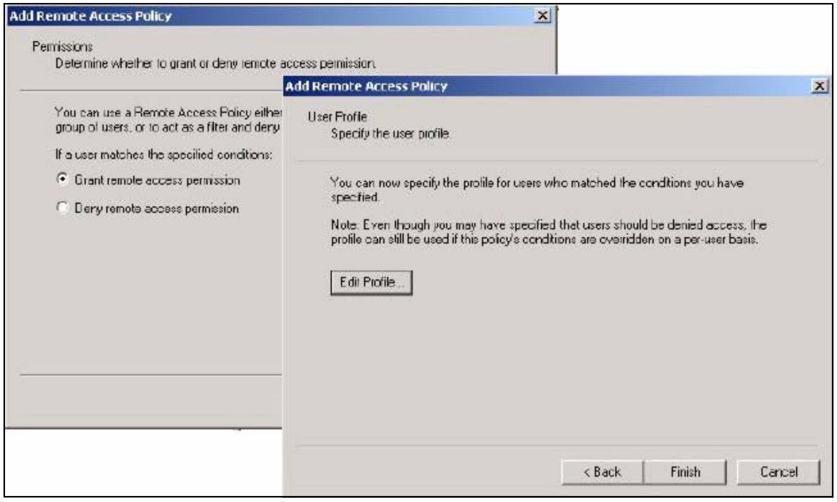
Name	In Folder
Domain Guests	
Group Policy Creator Owners	
DnsUpdateProxy	
Foundry VLAN Group 10	
Foundry VLAN Group 5	
VLAN Group 10	

VLAN Group 10

6 When the **Permissions** options screen displays, select **Grant remote access permission**.

- Click **Next** to grant access based on group membership.
- Click the **Edit Profile** button.

Figure 107 Granting Permissions and User Profile Screens



Permissions
Determine whether to grant or deny remote access permission.

You can use a Remote Access Policy eithe
group of users, or to act as a filter and deny

If a user matches the specified conditions:

● Grant remote access permission

○ Deny remote access permission

User Profile
Specify the user profile.

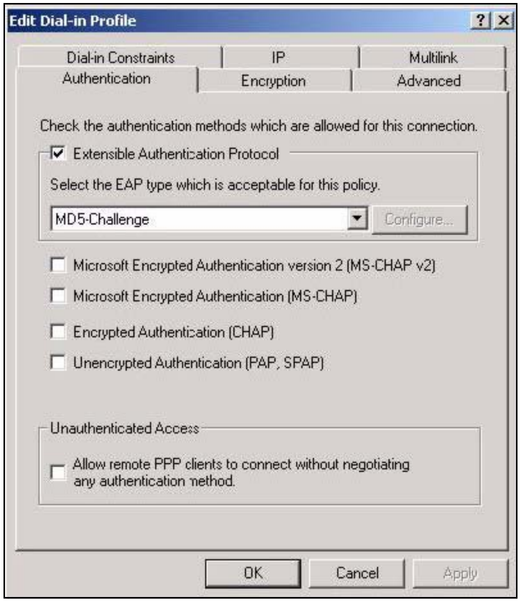
You can now specify the profile for users who matched the conditions you have specified.

Note: Even though you may have specified that users should be denied access, the profile can still be used if this policy's conditions are overridden on a per-user basis.

7 The **Edit Dial-in Profile** screen displays. Click the **Authentication** tab and select the **Extensible Authentication Protocol** check box.

- Select an EAP type depending on your authentication needs from the drop-down list box.
- Clear the check boxes for all other authentication types listed below the drop-down list box.

Figure 108 Authentication Tab Settings



Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

MD5-Challenge

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ Microsoft Encrypted Authentication (MS-CHAP)

□ Encrypted Authentication (CHAP)

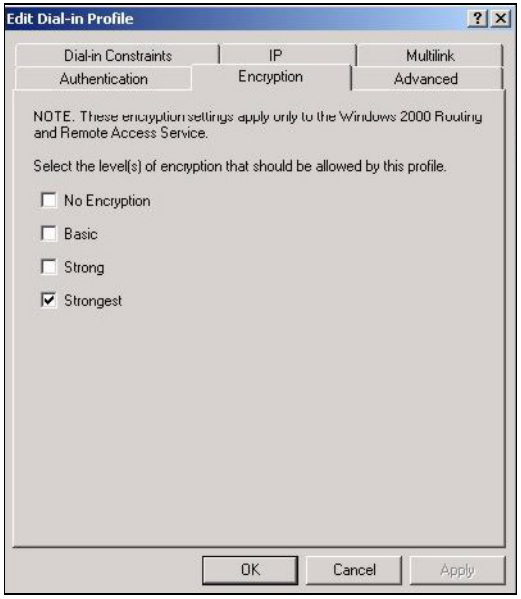
□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

□ Allow remote PPP clients to connect without negotiating any authentication method.

8 Click the **Encryption** tab. Select the **Strongest** encryption option. This step is not required for EAP-MD5, but is performed as a safeguard.

Figure 109 Encryption Tab Settings



Edit Dial-in Profile

NOTE. These encryption settings apply only to the Windows 2000 Routing and Remote Access Service.

Select the level(s) of encryption that should be allowed by this profile.

☐ No Encryption

☐ Basic

☐ Strong

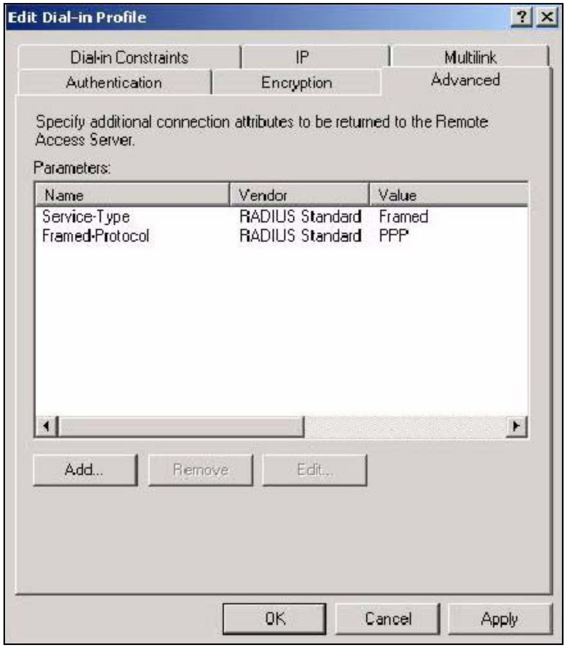
☑ Strongest

9 Click the **IP** tab and select the **Client may request an IP address** check box for DHCP support.

10 Click the **Advanced** tab. The current default parameters returned to the ZyXEL Device should be **Service-Type** and **Framed-Protocol**.

- Click the **Add** button to add an additional three RADIUS VLAN attributes required for 802.1X Dynamic VLAN Assignment.

Figure 110 Connection Attributes Screen



Edit Dial-in Profile

Specify additional connection attributes to be returned to the Remote Access Server.

Parameters:

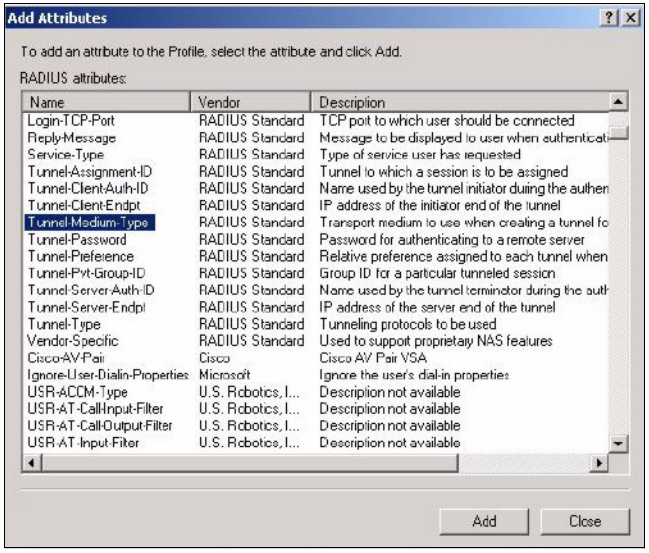
Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Framed-Protocol	RADIUS Standard	PPP

11 The RADIUS Attribute screen displays. From the list, three RADIUS attributes will be added:

- Tunnel-Medium-Type
- Tunnel-Pvt-Group-ID

  - Tunnel-Type
- Click the **Add** button
- Select **Tunnel-Medium-Type**
- Click the **Add** button.

Figure 111 RADIUS Attribute Screen



Add Attributes

To add an attribute to the Profile, select the attribute and click Add.

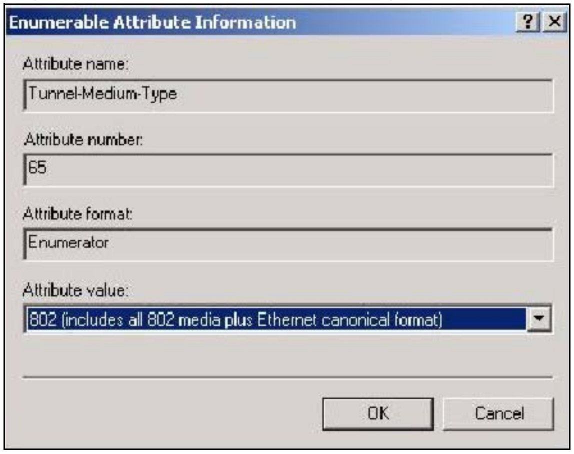
RADIUS attributes:

Name	Vendor	Description
Login-TCP-Port	RADIUS Standard	TCP port to which user should be connected
Reply-Message	RADIUS Standard	Message to be displayed to user when authenticati
Service-Type	RADIUS Standard	Type of service user has requested
Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned
Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authen
Tunnel-Client-Endpt	RADIUS Standard	IP address of the initiator end of the tunnel
Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel fo
Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server
Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when
Tunnel-Pvt-Group-ID	RADIUS Standard	Group ID for a particular tunneled session
Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the auth
Tunnel-Server-Endpt	RADIUS Standard	IP address of the server end of the tunnel
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features
Cisco-AV-Pair	Cisco	Cisco AV Pair VSA
Ignore-User-Dialin-Properties	Microsoft	Ignore the user's dial-in properties
USR-ACCM-Type	U.S. Robotics, I...	Description not available
USR-AT-Call-Input-Filter	U.S. Robotics, I...	Description not available
USR-AT-Call-Output-Filter	U.S. Robotics, I...	Description not available
USR-AT-Input-Filter	U.S. Robotics, I...	Description not available

12 The **Enumerable Attribute Information** screen displays. Select the **802** value from the **Attribute value** drop-down list box.

- Click **OK**.

Figure 112 802 Attribute Setting for Tunnel-Medium-Type



Enumerable Attribute Information

Attribute name: Tunnel-Medium-Type

Attribute number: 65

Attribute format: Enumerator

Attribute value: 802 (includes all 802 media plus Ethernet canonical format)

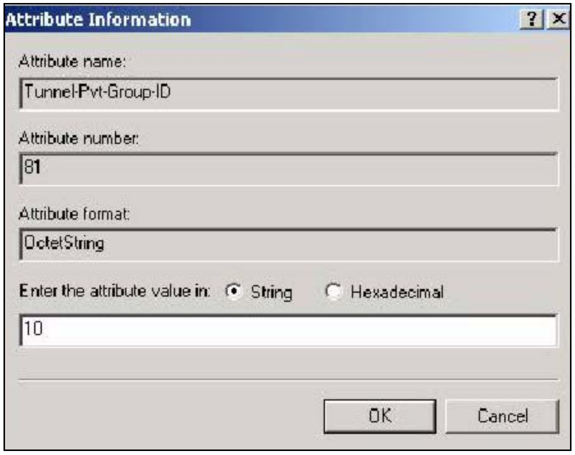
13 Return to the **RADIUS Attribute Screen** shown as Figure 111 on page 184.

- Select **Tunnel-Pvt-Group-ID.**
- Click **Add**.

14 The **Attribute Information** screen displays.

- In the **Enter the attribute value in:** field select **String** and type a number in the range 1 to 4094 or a **Name** for this policy. This **Name** should match a name in the VLAN mapping table on the ZyXEL Device. Wireless stations belonging to the VLAN Group specified in this policy will be given a VLAN **ID** specified in the ZyXEL Device VLAN table.
- Click **OK**.

Figure 113 VLAN ID Attribute Setting for Tunnel-Pvt-Group-ID



Attribute Information

Attribute name: Tunnel-Pvt-Group-ID

Attribute number: 81

Attribute format: OctetString

Enter the attribute value in: ● String ○ Hexadecimal

10

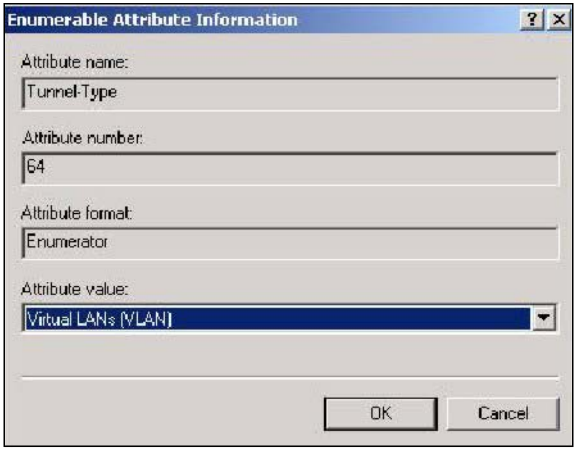
15 Return to the **RADIUS Attribute Screen** shown as Figure 111 on page 184.

- Select **Tunnel-Type**.
- Click **Add**.

16 The **Enumerable Attribute Information** screen displays.

- Select **Virtual LANs (VLAN)** from the attribute value drop-down list box.
- Click **OK**.

Figure 114 VLAN Attribute Setting for Tunnel-Type



Enumerable Attribute Information

Attribute name: Tunnel-Type

Attribute number: 64

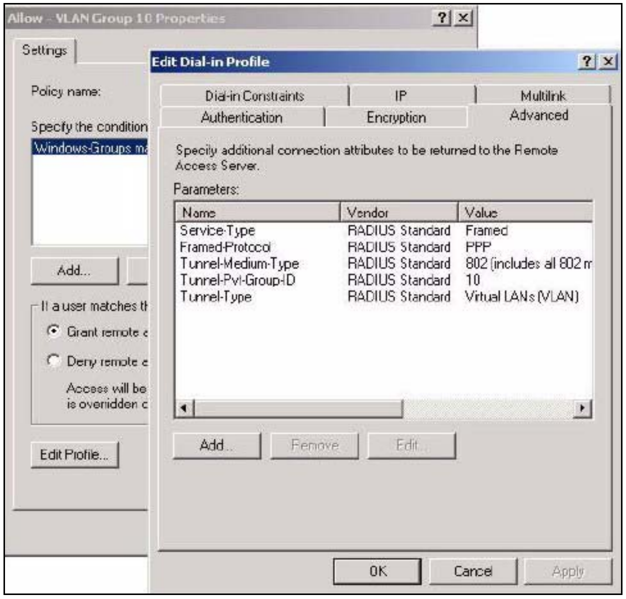
Attribute format: Enumerator

Attribute value: Virtual LANs (VLAN)

17 Return to the **RADIUS Attribute Screen** shown as Figure 111 on page 184.

- Click the **Close** button.
- The completed **Advanced** tab configuration should resemble the following screen.

Figure 115 Completed Advanced Tab



Specify additional connection attributes to be returned to the Remote Access Server.

Parameters:

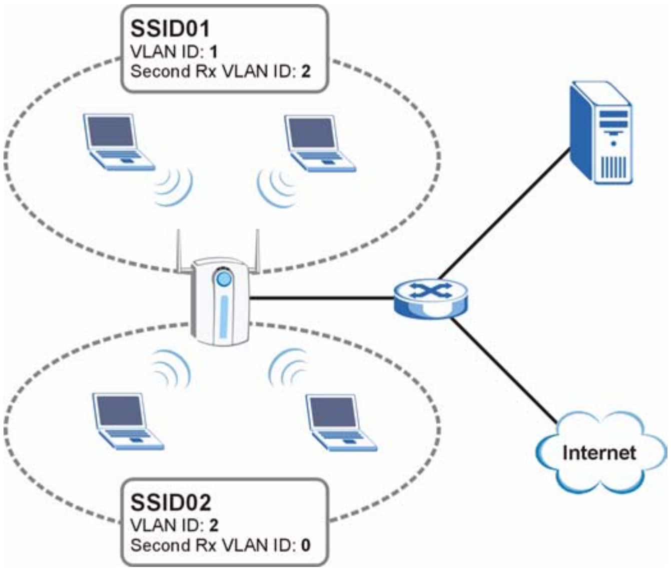
Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Framed-Protocol	RADIUS Standard	PPP
Tunnel-Medium-Type	RADIUS Standard	802 (includes all 802 m
Tunnel-Pvt-Group-ID	RADIUS Standard	10
Tunnel-Type	RADIUS Standard	Virtual LANs (VLAN)

Repeat the Configuring Remote Access Policies procedure for each VLAN Group defined in the Active Directory. Remember to place the most general Remote Access Policies at the bottom of the list and the most specific at the top of the list.

15.2.4 Second Rx VLAN ID Example

In this example, the ZyXEL Device is configured to tag packets from **SSID01** with VLAN ID 1 and tag packets from **SSID02** with VLAN ID 2. **VLAN 1** and **VLAN 2** have access to a server, **S**, and the Internet, as shown in the following figure.

Figure 116 Second Rx VLAN ID Example



Packets sent from the server **S** back to the switch are tagged with a VLAN ID (incoming VLAN ID). These incoming VLAN packets are forwarded to the ZyXEL Device. The ZyXEL Device compares the VLAN ID in the packet header with each SSID's configured VLAN ID and second Rx VLAN ID settings.

In this example, **SSID01**'s second Rx VLAN ID is set to **2**. All incoming packets tagged with VLAN ID **2** are forwarded to **SSID02**, and also to **SSID01**. However, **SSID02** has no second Rx VLAN ID configured, and the ZyXEL Device forwards only packets tagged with VLAN ID **2** to it.

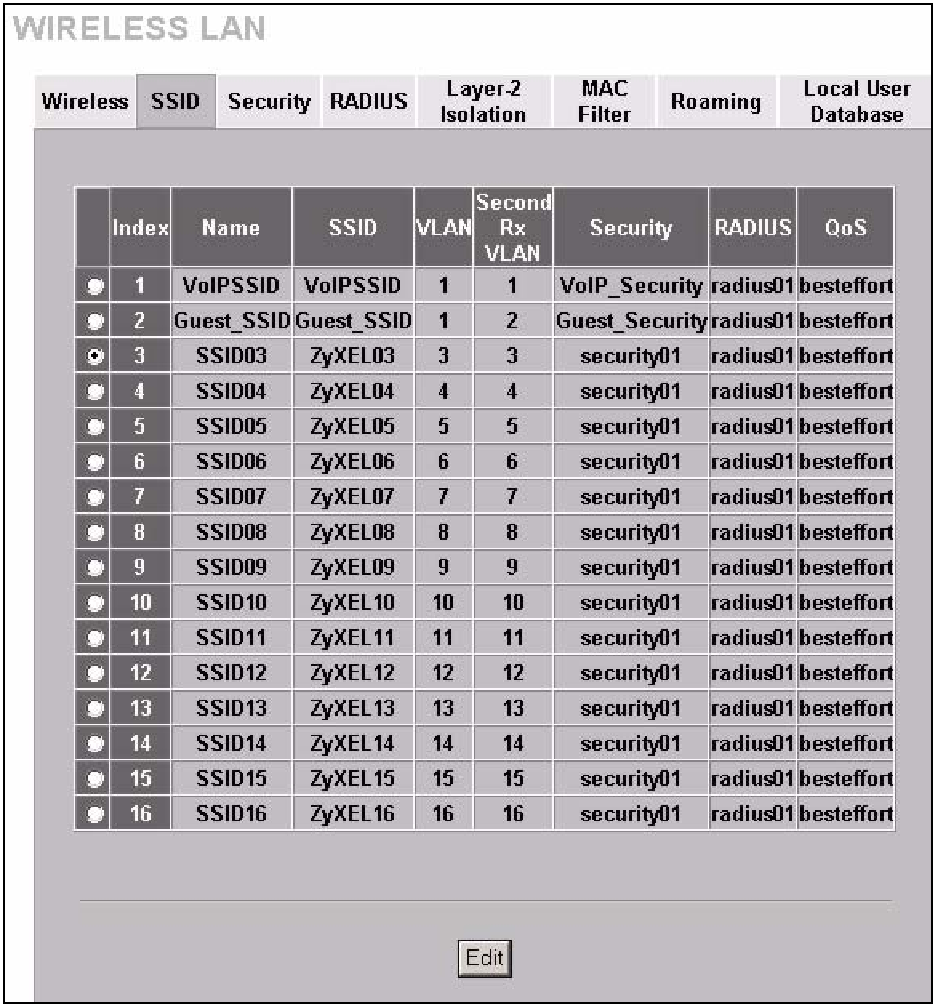
15.2.4.1 Second Rx VLAN Setup Example

The following steps show you how to configure a VLAN ID and second Rx VLAN ID for a third SSID (**SSID03**) on the ZyXEL Device.

This example has the ZyXEL Device tag outgoing packets from clients in **SSID03** with a **VLAN ID** of **3**, and forward incoming packets with a **VLAN ID** of **3** or **4** to **SSID03**.

1. Log into the Web Configurator.
2. Click **WIRELESS** > **SSID**.
3. Select the radio button for the SSID profile you want to configure (**SSID03** in this example) and click **Edit**.
4. Select the SSID profile you want to configure (**SSID03** in this example), and enter the **VLAN ID** number (between 1 and 4094).
5. Enter a **Second Rx VLAN ID**. The following screen shows **SSID03** tagged with a **VLAN ID** of **3** and a **Second Rx VLAN ID** of **4**. Click **Apply**.

Figure 117 Configuring SSID: Second Rx VLAN ID Example



	Index	Name	SSID	VLAN	Second Rx VLAN	Security	RADIUS	QoS
○	1	VoIPSSID	VoIPSSID	1	1	VoIP_Security	radius01	besteffort
○	2	Guest_SSID	Guest_SSID	1	2	Guest_Security	radius01	besteffort
●	3	SSID03	ZyXEL03	3	3	security01	radius01	besteffort
○	4	SSID04	ZyXEL04	4	4	security01	radius01	besteffort
○	5	SSID05	ZyXEL05	5	5	security01	radius01	besteffort
○	6	SSID06	ZyXEL06	6	6	security01	radius01	besteffort
○	7	SSID07	ZyXEL07	7	7	security01	radius01	besteffort
○	8	SSID08	ZyXEL08	8	8	security01	radius01	besteffort
○	9	SSID09	ZyXEL09	9	9	security01	radius01	besteffort
○	10	SSID10	ZyXEL10	10	10	security01	radius01	besteffort
○	11	SSID11	ZyXEL11	11	11	security01	radius01	besteffort
○	12	SSID12	ZyXEL12	12	12	security01	radius01	besteffort
○	13	SSID13	ZyXEL13	13	13	security01	radius01	besteffort
○	14	SSID14	ZyXEL14	14	14	security01	radius01	besteffort
○	15	SSID15	ZyXEL15	15	15	security01	radius01	besteffort
○	16	SSID16	ZyXEL16	16	16	security01	radius01	besteffort

6 If VLAN is not already enabled, click **VLAN** and select **Enable Virtual LAN**. You also need to set up the **Management VLAN ID** (see Section 15.1.1 on page 173).

If no devices are in the management VLAN, then you will not be able to access the ZyXEL Device through the network. If the ZyXEL Device has no console port, you will have to restore the default configuration file.

16

Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

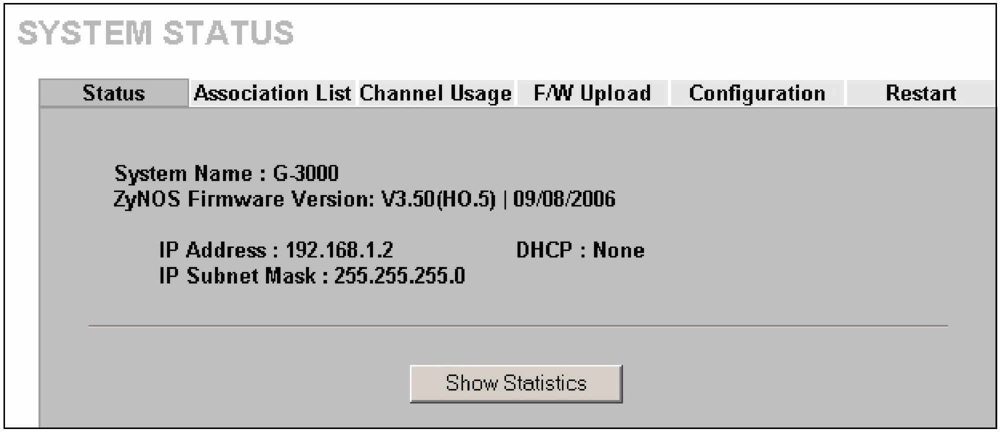
16.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyXEL Device.

16.2 System Status Screen

Click **MAINTENANCE** to open the **System Status** screen, where you can use to monitor your ZyXEL Device. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.

Figure 118 System Status



SYSTEM STATUS

System Name : G-3000
ZyNOS Firmware Version: V3.50(HO.5) | 09/08/2006

IP Address : 192.168.1.2 DHCP : None
IP Subnet Mask : 255.255.255.0

The following table describes the labels in this screen.

Table 61 System Status

LABEL	DESCRIPTION
System Name	This is the **System Name** you can configure in the **SYSTEM** > **General** screen. It is for identification purposes
ZyNOS Firmware Version	This is the ZyNOS Firmware version and date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
IP Address	This is the Ethernet port IP address.

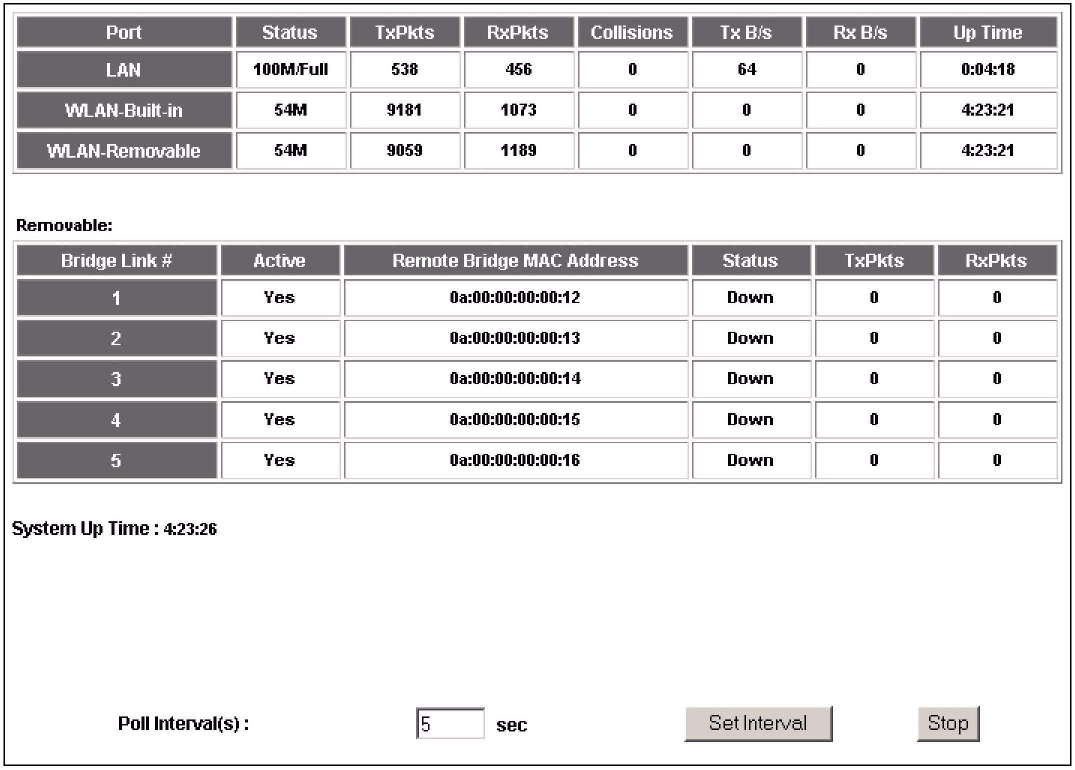
Table 61 System Status

LABEL	DESCRIPTION
IP Subnet Mask	This is the Ethernet port subnet mask.
DHCP	This is the Ethernet port DHCP role - **Client** or **None**.
Show Statistics	Click **Show Statistics** to see router performance statistics such as number of packets sent and number of packets received for each port.

16.2.1 System Statistics

Read-only information here includes port status, packet specific statistics and bridge link status. Also provided are "system up time" and "poll interval(s)". The **Poll Interval** field is configurable.

Figure 119 System Status: Show Statistics



Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M/Full	538	456	0	64	0	0:04:18
WLAN-Built-in	54M	9181	1073	0	0	0	4:23:21
WLAN-Removable	54M	9059	1189	0	0	0	4:23:21

Removable:

Bridge Link #	Active	Remote Bridge MAC Address	Status	TxPkts	RxPkts
1	Yes	0a:00:00:00:00:12	Down	0	0
2	Yes	0a:00:00:00:00:13	Down	0	0
3	Yes	0a:00:00:00:00:14	Down	0	0
4	Yes	0a:00:00:00:00:15	Down	0	0
5	Yes	0a:00:00:00:00:16	Down	0	0

System Up Time : 4:23:26

Poll Interval(s) : 5 sec

The following table describes the labels in this screen.

Table 62 System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the Ethernet port or wireless adapter.
Status	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect. This shows the transmission speed only for the wireless port.

Table 62 System Status: Show Statistics

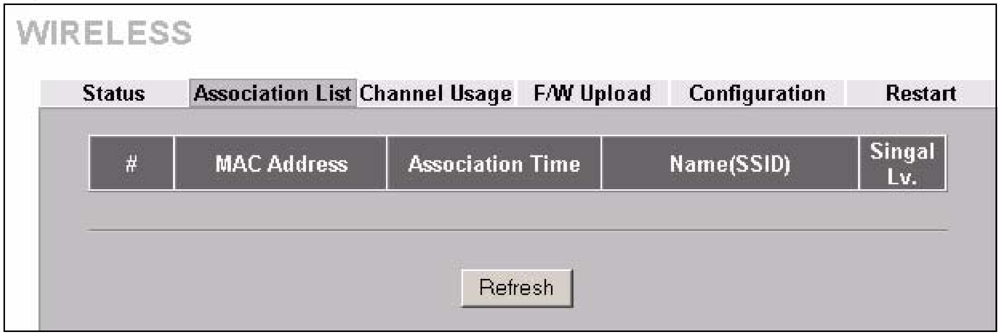
LABEL	DESCRIPTION
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This shows the transmission speed in bytes per second on this port.
Rx B/s	This shows the reception speed in bytes per second on this port.
Up Time	This is total amount of time the line has been up.
Bridge Link #	This is the index number of the bridge connection.
Active	This shows whether the bridge connection is activated or not.
Remote Bridge MAC Address	This is the MAC address of the peer device in bridge mode.
Status	This shows the current status of the bridge connection, which can be **Up** or **Down**.
TxPkts	This is the number of transmitted packets on the wireless bridge.
RxPkts	This is the number of received packets on the wireless bridge.
System Up Time	This is the total time the ZyXEL Device has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics.
Set Interval	Click this button to apply the new poll interval you entered above.
Stop	Click this button to stop refreshing statistics.

16.3 Association List

View the wireless stations that are currently associated with the ZyXEL Device in the **Association List** screen.

Click **MAINTENANCE** and then the **Association List** tab to display the screen as shown next.

Figure 120 Association List



The following table describes the labels in this screen.

Table 63 Association List

LABEL	DESCRIPTION
Stations	
#	This is the index number of an associated wireless station.

Table 63 Association List

LABEL	DESCRIPTION
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyXEL Device.
Name (SSID)	This field displays the SSID to which the wireless station is associated.
WDS Link This screen displays when bridge mode is activated on the ZyXEL Device.	
Link No	This field displays the index number of a bridge connection on the WDS.
MAC Address	This field displays a remote bridge MAC address.
Link Time	This field displays the WDS link up-time.
Privacy	This field displays whether traffic on the WDS is encrypted or not.
Refresh	Click **Refresh** to reload the screen.

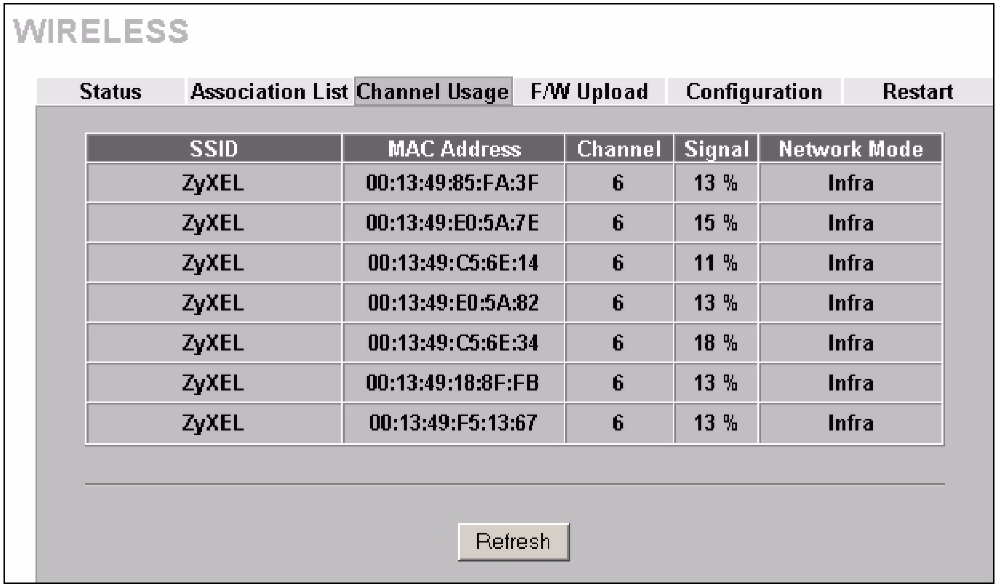
16.4 Channel Usage

The **Channel Usage** screen shows whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.

Click **MAINTENANCE** and then the **Channel Usage** tab to display the screen shown next.

Wait a moment while the ZyXEL Device compiles the information.

Figure 121 Channel Usage



SSID	MAC Address	Channel	Signal	Network Mode
ZyXEL	00:13:49:85:FA:3F	6	13 %	Infra
ZyXEL	00:13:49:E0:5A:7E	6	15 %	Infra
ZyXEL	00:13:49:C5:6E:14	6	11 %	Infra
ZyXEL	00:13:49:E0:5A:82	6	13 %	Infra
ZyXEL	00:13:49:C5:6E:34	6	18 %	Infra
ZyXEL	00:13:49:18:8F:FB	6	13 %	Infra
ZyXEL	00:13:49:F5:13:67	6	13 %	Infra

The following table describes the labels in this screen.

Table 64 Channel Usage

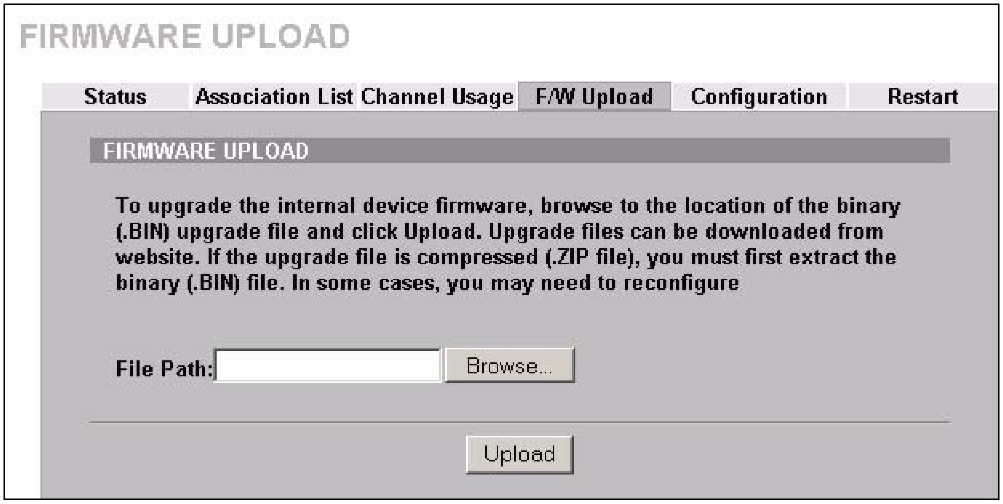
LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the Wireless Configuration and Roaming chapter for more information on basic service sets (BSS) and extended service sets (ESS).
MAC Address	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.
Channel	This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.
Signal	This field displays the strength of the AP's signal. If you must choose a channel that's currently in use, choose one with low signal strength for minimum interference.
Network Mode	"Network mode" in this screen refers to your wireless LAN infrastructure (refer to the Wireless LAN chapter) and security setup.
Refresh	Click **Refresh** to reload the screen.

16.5 F/W Upload Screen

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

Click **MAINTENANCE** > **F/W Upload**. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 122 Firmware Upload



To upgrade the internal device 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

File Path:

The following table describes the labels in this screen.

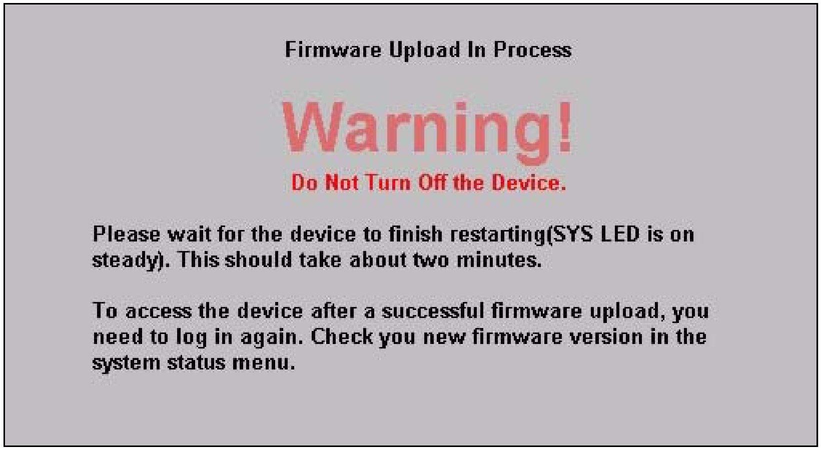
Table 65 Firmware Upload

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!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 123 Firmware Upload In Process



Firmware Upload In Process

Warning!

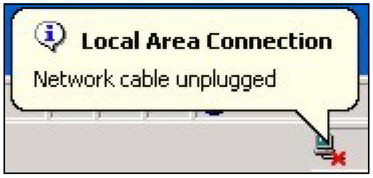
Do Not Turn Off the Device.

Please wait for the device to finish restarting(SYS LED is on steady). This should take about two minutes.

To access the device after a successful firmware upload, you need to log in again. Check you new firmware version in the system status menu.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 124 Network Temporarily Disconnected



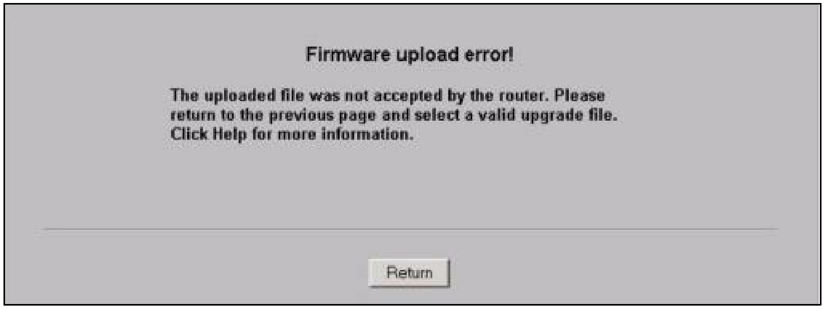
Local Area Connection

Network cable unplugged

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

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 125 Firmware Upload Error



Firmware upload error!

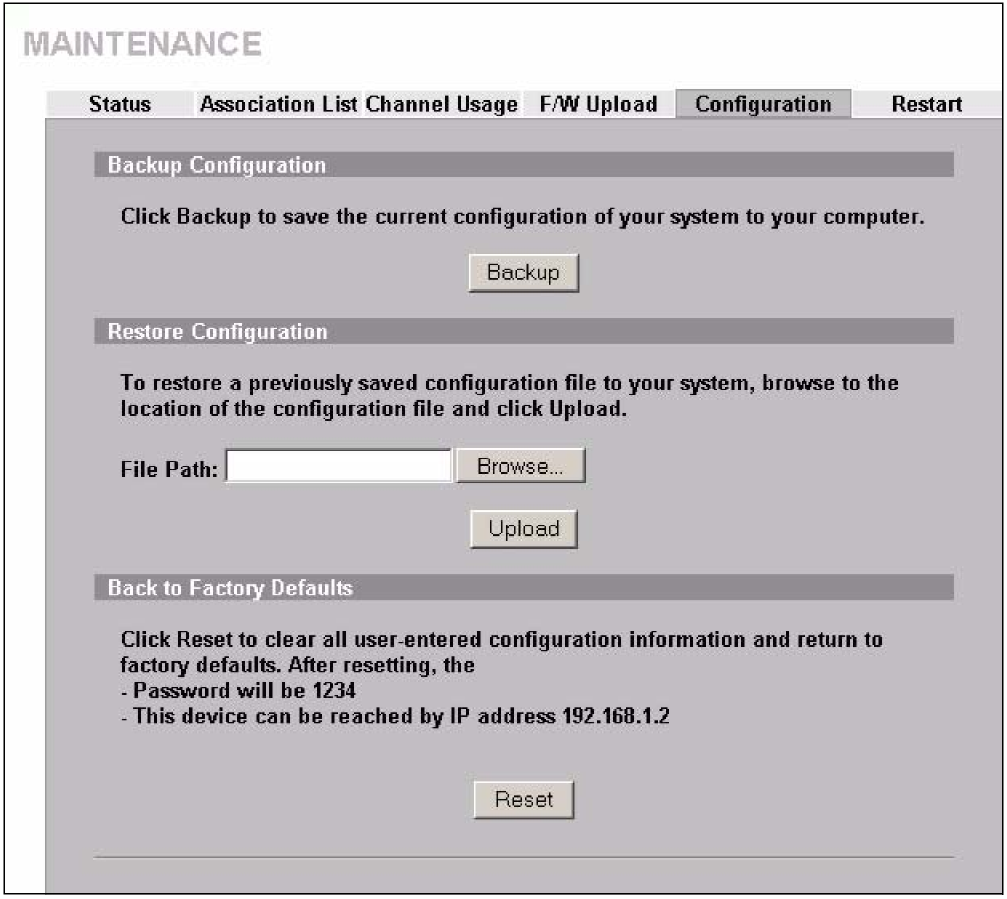
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

16.6 Configuration Screen

See Chapter 25 on page 237 for information on how to transfer configuration files using FTP/ TFTP commands.

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

Figure 126 Configuration



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

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

File Path:

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- This device can be reached by IP address 192.168.1.2

16.6.1 Backup Configuration

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

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

16.6.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

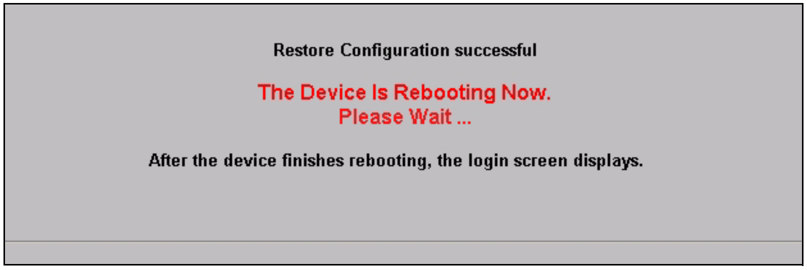
Table 66 Restore Configuration

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

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

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 127 Configuration Upload Successful



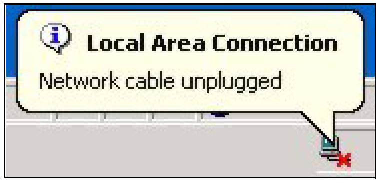
Restore Configuration successful

The Device Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 128 Network Temporarily Disconnected

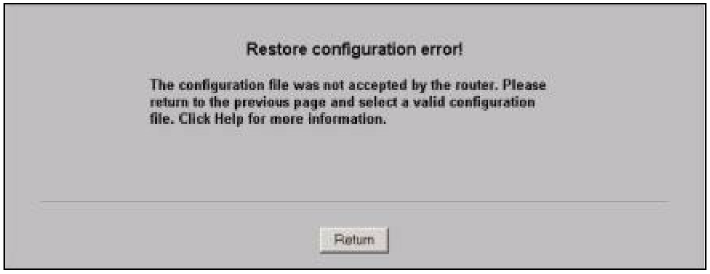


Local Area Connection
Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.2). See your Quick Start Guide for details on how to set up your computer's IP address.

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

Figure 129 Configuration Upload Error



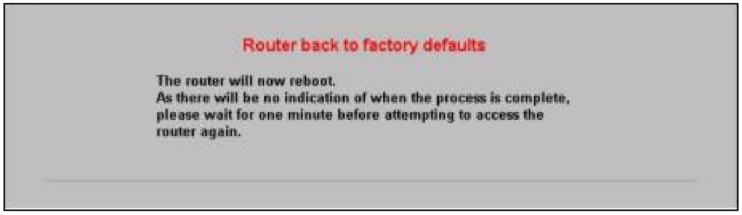
Restore configuration error!

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

16.6.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 130 Reset Warning Message



Router back to factory defaults

The router 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.

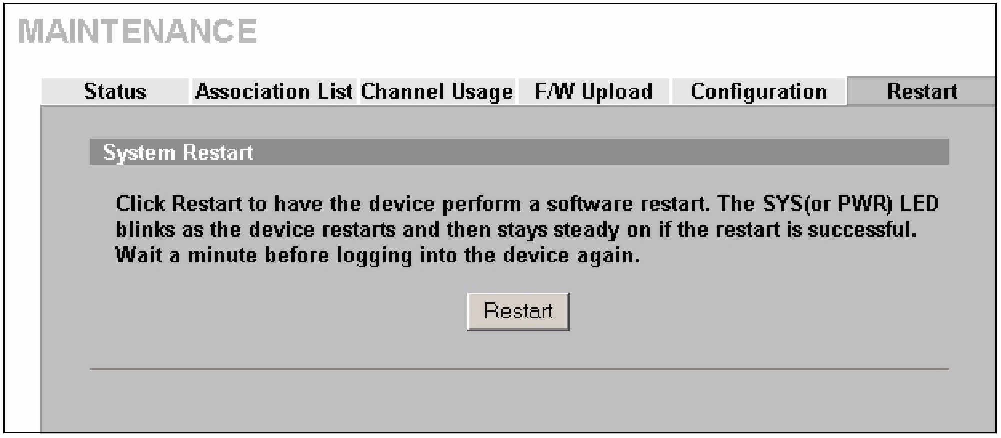
You can also press the **RESET** button to reset your ZyXEL Device to its factory default settings. Refer to Section 2.3 on page 43 for more information.

16.7 Restart Screen

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

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

Figure 131 Restart Screen



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.

PART III
SMT and Troubleshooting

17

Introducing the SMT

This chapter describes how to access the SMT (System Management Terminal) and provides an overview of its menus.

17.1 Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the Quick Start Guide. Not available on all models.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

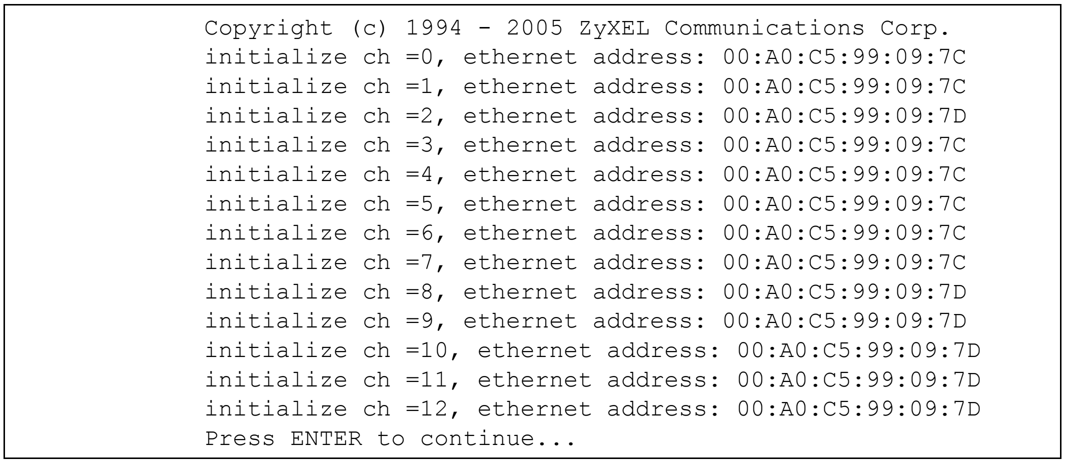
- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

17.1.1 Initial Screen

When you turn on your ZyXEL Device, it performs several internal tests as well as line initialization.

After the tests, the ZyXEL Device asks you to press [ENTER] to continue, as shown next.

Figure 132 Initial Screen



```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:A0:C5:99:09:7C
initialize ch =1, ethernet address: 00:A0:C5:99:09:7C
initialize ch =2, ethernet address: 00:A0:C5:99:09:7D
initialize ch =3, ethernet address: 00:A0:C5:99:09:7C
initialize ch =4, ethernet address: 00:A0:C5:99:09:7C
initialize ch =5, ethernet address: 00:A0:C5:99:09:7C
initialize ch =6, ethernet address: 00:A0:C5:99:09:7C
initialize ch =7, ethernet address: 00:A0:C5:99:09:7C
initialize ch =8, ethernet address: 00:A0:C5:99:09:7D
initialize ch =9, ethernet address: 00:A0:C5:99:09:7D
initialize ch =10, ethernet address: 00:A0:C5:99:09:7D
initialize ch =11, ethernet address: 00:A0:C5:99:09:7D
initialize ch =12, ethernet address: 00:A0:C5:99:09:7D
Press ENTER to continue...
```

The login screen appears after you press [ENTER], prompting you to enter the password.

17.2 Connect to your ZyXEL Device Using Telnet

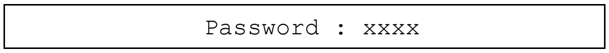
To telnet into your ZyXEL Device, in Windows, click **Start** (usually in the bottom left corner), **Run** and then type “telnet 192.168.1.2” (the default IP address) and click **OK**.

17.3 Entering the Password

For your first login, enter the default password “1234”. As you type the password, the screen displays an asterisk “*” for each character you type.

Whether or not you use administrator authentication on RADIUS, you still use the local system password to log in via the console port.

Figure 133 Login



```
                Password : xxxx
```

After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your ZyXEL Device will automatically log you out. You will then have to log into the ZyXEL Device again. You can use the web configurator or the CI commands to change the inactivity time out period.

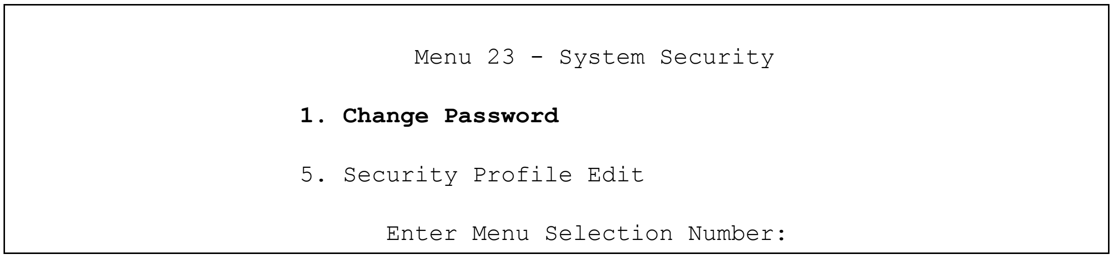
17.4 Changing the System Password

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to Section 17.4 on page 202 and Section 2.3 on page 43.

Change the ZyXEL Device’s default password by following the steps shown next.

1 From the main menu, enter 23 to display **Menu 23 – System Security**.

Figure 134 Menu 23 System Security

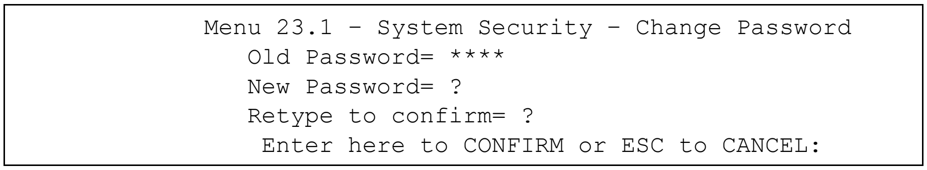


```
                            Menu 23 - System Security

                    1. Change Password

                    5. Security Profile Edit

                          Enter Menu Selection Number:
```

2 Enter 1 to display **Menu 23.1 – System Security – Change Password** as shown next.

3 Type your existing system password in the **Old Password** field, and press [ENTER].

Figure 135 Menu 23.1 System Security: Change Password



```
              Menu 23.1 - System Security - Change Password
                 Old Password= ****
                 New Password= ?
                 Retype to confirm= ?
                  Enter here to CONFIRM or ESC to CANCEL:
```

4 Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].

5 Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an asterisk "*" for each character you type.

17.5 Navigating the SMT Interface

You can use the SMT to configure and monitor your ZyXEL Device.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 67 Main Menu Commands

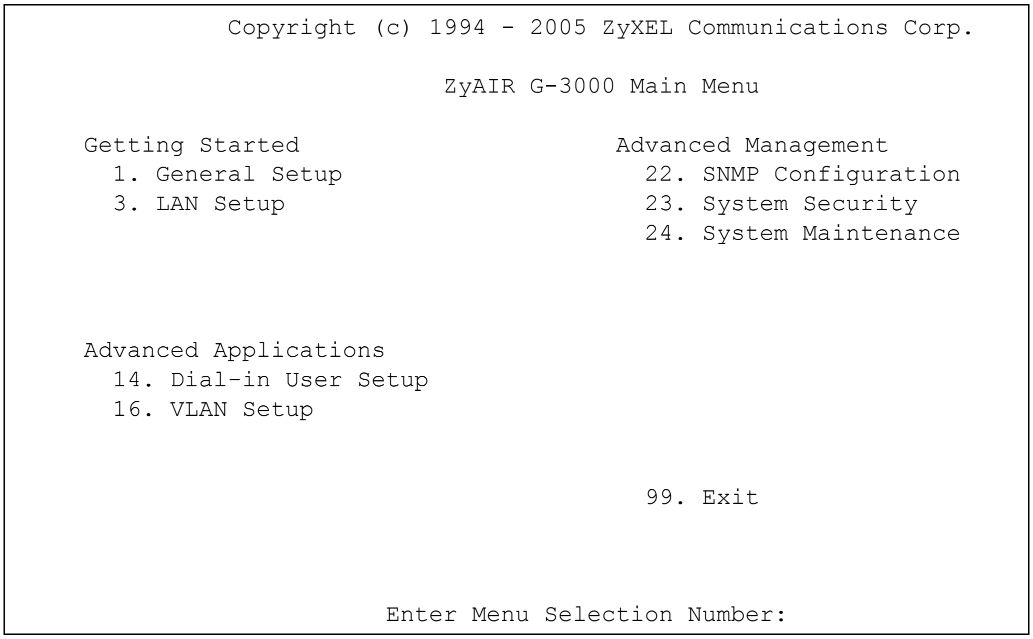
OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?> or **ChangeMe**	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with **ChangeMe** must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.

Table 67   Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

Figure 136   SMT Main Menu



```
               Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

                               ZyAIR G-3000 Main Menu

     Getting Started                      Advanced Management
       1. General Setup                     22. SNMP Configuration
       3. LAN Setup                         23. System Security
                                            24. System Maintenance



     Advanced Applications
       14. Dial-in User Setup
       16. VLAN Setup



                                            99. Exit



                           Enter Menu Selection Number:
```

17.5.1 SMT Main Menu Summary

The following table briefly describes the SMT main menus.

Table 68   Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
3	LAN Setup	Use this menu to set up your LAN and WLAN connection.
14	Dial-in User Setup	Use this menu to set up local user profiles on the ZyXEL Device.
16	VLAN Setup	Use this menu to set up your VLAN ID.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password and configure your wireless LAN security profiles.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
99	Exit	Use this to exit the SMT.

17.6 SMT Menus Overview

The following table gives you an overview of your ZyXEL Device's various SMT menus.

Table 69 SMT Menus Overview

MENUS	SUB MENUS	
1 General Setup	1.1 Configure Dynamic DNS	
3 LAN Setup	3.2 TCP/IP Setup	
	3.5 Wireless LAN Setup	3.5.1 WLAN MAC Address Filter
		3.5.2 Roaming Configuration
		3.5.4 Bridge Link Configuration
		3.5.5 - Layer-2 Isolation
		3.5.6 SSID Profile Edit
14 Dial-in User Setup	14. Edit Dial-in User	
16 VLAN Setup		
22 SNMP Configuration	22.1 SNMP	
23 System Password	23.1 System Password	
	23.5 Security Profile Edit	
24 System Maintenance	24.1 System Status	
	24.2 System Information and Console Port Speed	24.2.1 System Information
		24.2.2 Console Port Speed
	24.3 Log and Trace	
	24.4 Diagnostic	
	24.5 Backup Configuration	
	24.6 Restore Configuration	
	24.7 Upload Firmware	24.7.1 Upload System Firmware
		24.7.2 Upload System Configuration File
	24.8 Command Interpreter Mode	
	24.10 Time and Date Setting	
	24.11 Remote Management Setup	

18

General Setup

The chapter shows you the information on general setup.

18.1 General Setup

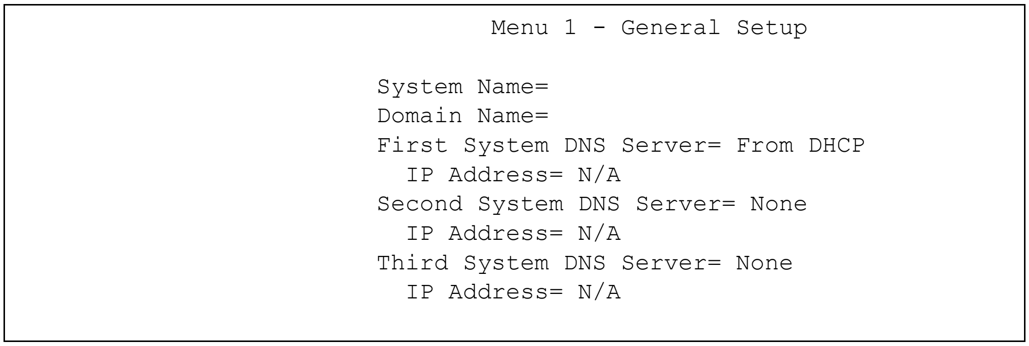
Menu 1 – General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyXEL Device via DHCP.

18.1.1 Procedure To Configure Menu 1

Enter 1 in the Main Menu to open **Menu 1 – General Setup** as shown next.

Figure 137 Menu 1 General Setup



```
                           Menu 1 - General Setup

                   System Name=
                   Domain Name=
                   First System DNS Server= From DHCP
                     IP Address= N/A
                   Second System DNS Server= None
                     IP Address= N/A
                   Third System DNS Server= None
                     IP Address= N/A
```

Fill in the required fields. Refer to the following table for more information about these fields.

Table 70 Menu 1 General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes “-” and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.

Table 70 Menu 1 General Setup

FIELD	DESCRIPTION
First/Second/Third System DNS Server	Press [SPACE BAR] to select **From DHCP**, **User Defined** or **None** and press [ENTER]. These fields are not available on all models.
IP Address	Enter the IP addresses of the DNS servers. This field is available when you select **User-Defined** in the field above.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

19

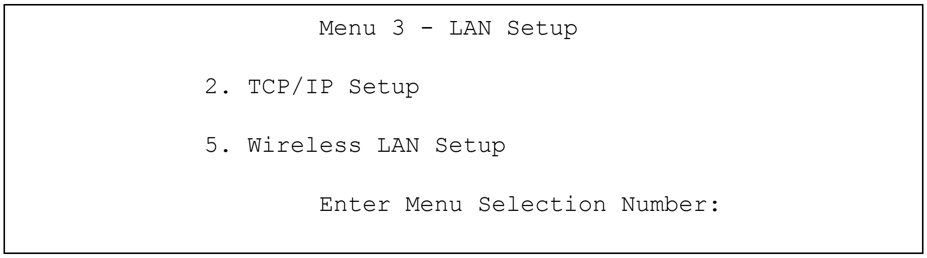
LAN Setup

This chapter shows you how to configure the LAN on your ZyXEL Device.

19.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 – LAN Setup**. From the main menu, enter 3 to display menu 3.

Figure 138 Menu 3 LAN Setup



```
                      Menu 3 - LAN Setup

              2. TCP/IP Setup

              5. Wireless LAN Setup

                      Enter Menu Selection Number:
```

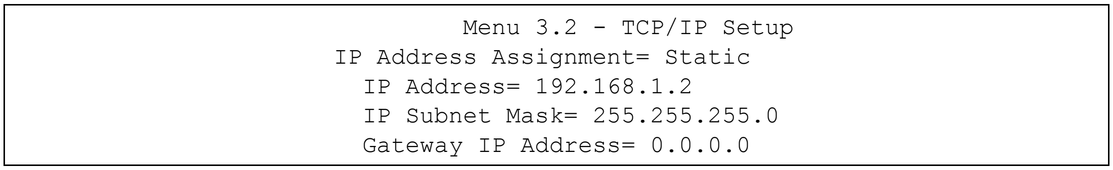
Detailed explanation about the LAN Setup menu is given in the next chapter.

19.2 TCP/IP Ethernet Setup

Use menu 3.2 to configure your ZyXEL Device for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3-LAN Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2-TCP/IP Setup**, as shown next:

Figure 139 Menu 3.2 TCP/IP Setup



```
                         Menu 3.2 - TCP/IP Setup
                IP Address Assignment= Static
                  IP Address= 192.168.1.2
                  IP Subnet Mask= 255.255.255.0
                  Gateway IP Address= 0.0.0.0
```

Follow the instructions in the following table on how to configure the fields in this menu.

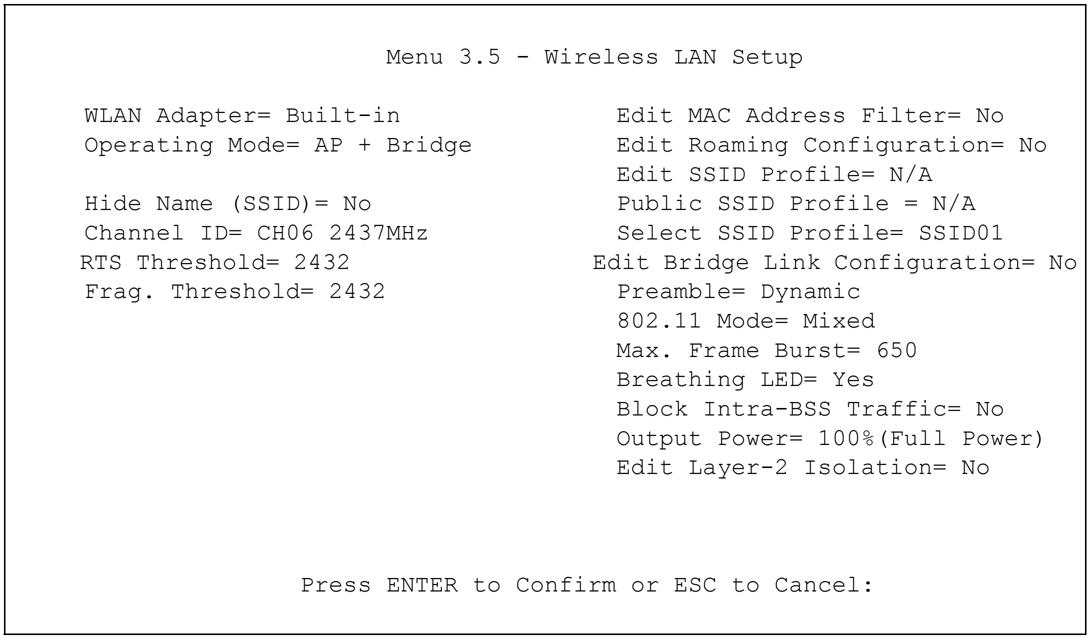
Table 71 Menu 3.2 TCP/IP Setup

FIELD	DESCRIPTION
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** to have the ZyXEL Device obtain an IP address from a DHCP server. You must know the IP address assigned to the ZyXEL Device (by the DHCP server) to access the ZyXEL Device again. Select **Static** to give the ZyXEL Device a fixed, unique IP address. Enter a subnet mask appropriate to your network and the gateway IP address if applicable.
IP Address	Enter the (LAN) IP address of your ZyXEL Device in dotted decimal notation
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same network segment as your ZyXEL Device.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

19.3 Wireless LAN Setup

Use menu 3.5 to set up your ZyXEL Device as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

Figure 140 Menu 3.5 Wireless LAN Setup



```
                        Menu 3.5 - Wireless LAN Setup

     WLAN Adapter= Built-in                Edit MAC Address Filter= No
     Operating Mode= AP + Bridge           Edit Roaming Configuration= No
                                           Edit SSID Profile= N/A
     Hide Name (SSID)= No                  Public SSID Profile = N/A
     Channel ID= CH06 2437MHz              Select SSID Profile= SSID01
     RTS Threshold= 2432                 Edit Bridge Link Configuration= No
     Frag. Threshold= 2432                 Preamble= Dynamic
                                           802.11 Mode= Mixed
                                           Max. Frame Burst= 650
                                           Breathing LED= Yes
                                           Block Intra-BSS Traffic= No
                                           Output Power= 100%(Full Power)
                                           Edit Layer-2 Isolation= No



                  Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 72 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
WLAN Adapter	Press [SPACE BAR] and select **Built-in** to configure settings for your ZyXEL Device's the internal WLAN card. Press [SPACE BAR] and select **Removable** to configure settings for your ZyXEL Device's WLAN card in the extension card slot.
Operating Mode	Press [SPACE BAR] and select **Access Point**, **Bridge / Repeater** or **AP + Bridge**. This field is not available on all models.
Name (SSID)	The SSID (Service Set IDentity) identifies the AP to which the wireless stations associate. Wireless stations associating to the AP must have the same SSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters. This field is only available when you select **Access Point** or **AP + Bridge** in the **Operating Mode** field.
Hide Name (SSID)	Press [SPACE BAR] and select **Yes** to hide the SSID in the outgoing data frame so an intruder cannot obtain the SSID through scanning.
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.
Frag. Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Edit MAC Address Filter	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 3.5.1 - WLAN MAC Address Filter**.
Edit Roaming Configuration	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 3.5.2 - Roaming Configuration**.
Edit SSID Profile	This field is available when you select AP, AP+bridge or MESSID as the operating mode. Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 3.5.6 - SSID Profile Edit**.
Public SSID Profile	The public SSID setting apply with the MESSID operating mode. Configure the public SSID settings in the web configurator SSID screen (see Section 8.2.2 on page 111). You do not need to configure this field. The setting in this field does not apply.
Select SSID Profile	This field is available when you select AP or AP+bridge as the operating mode. Press [SPACE BAR] to select a SSID for the ZyXEL Device to use.
Edit Bridge Link Configuration	Use [SPACE BAR] to choose **Yes** and press [ENTER] to go to **Menu 3.5.4 - Bridge Link Configuration**.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** and **Dynamic**. The default setting is **Long**. See the section on preamble for more information.
802.11 Mode	Select **B Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **G Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.

Table 72 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the ZyXEL Device transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.
Breathing LED	Select Yes to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyXEL Device is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyXEL Device is on and data is being transmitted/received.
Block Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the same BSS. Select **No** to allow Intra-BSS traffic, select **Yes** to block all Intra-BSS traffic. Note: The setting automatically changes from **No** to **Yes** if you enable layer-2 isolation in the web configurator. Change it back to **No** if you want to allow intra-BSS traffic.
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of APs within an area, decrease the output power of the ZyXEL Device to reduce interference with other APs.The options are 17dBm (50mW), 15dBm (32mW), 13dBm (20mW), 11dBm (12.6mW) or 7dBm (5mW) for IEEE802.11b mode and 13dBm (20mW), 11dBm (12.6mW), 9dBm (7.9mW), 7dBm (5mW) or 3dBm (2mW) for IEEE802.11g mode.
Edit Layer-2 Isolation	Use [SPACE BAR] to choose **Yes** and press [ENTER] to go to **Menu 3.5.5 - Layer-2 Isolation**.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

19.3.1 Configuring MAC Address Filter

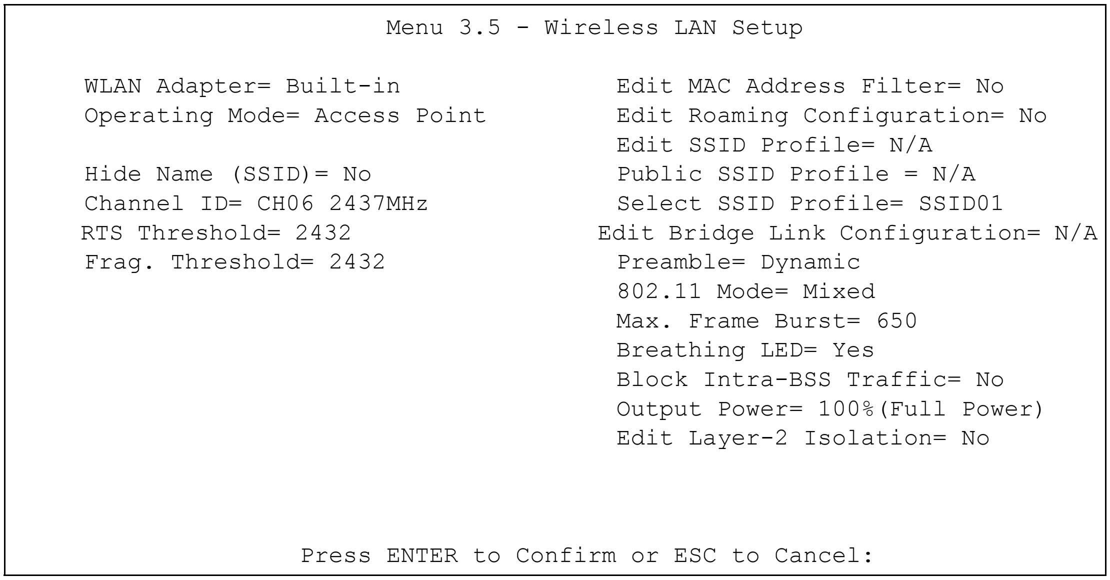
Your ZyXEL Device checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your ZyXEL Device.

1 From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

2 Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

Figure 141 Menu 3.5 Wireless LAN Setup

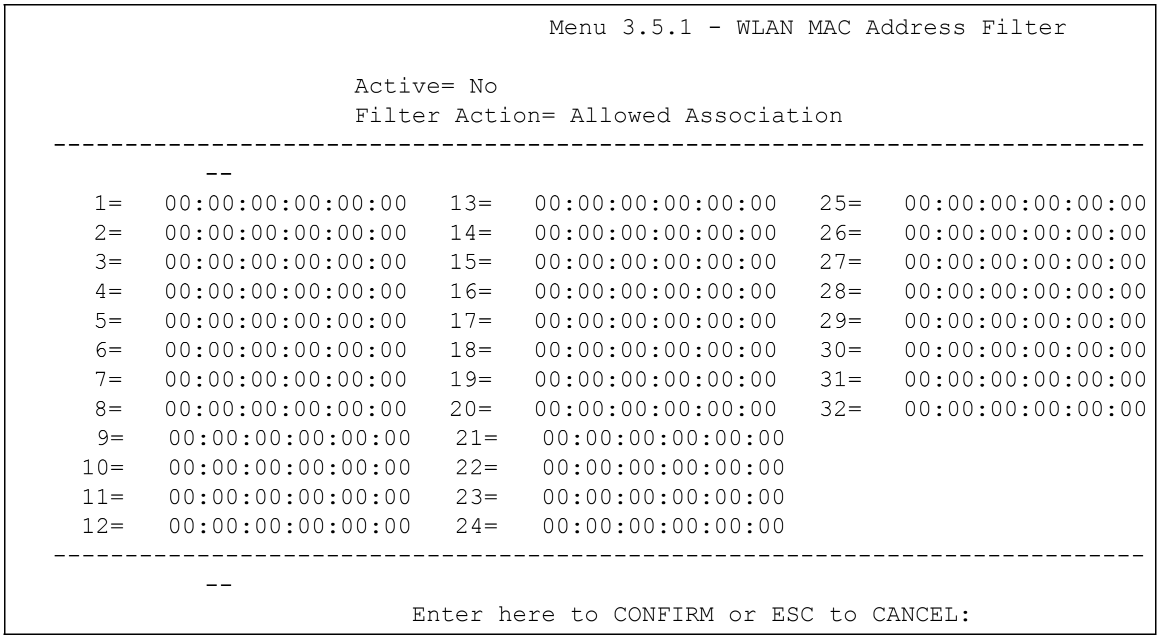


```
                          Menu 3.5 - Wireless LAN Setup

     WLAN Adapter= Built-in                Edit MAC Address Filter= No
     Operating Mode= Access Point          Edit Roaming Configuration= No
                                           Edit SSID Profile= N/A
     Hide Name (SSID)= No                  Public SSID Profile = N/A
     Channel ID= CH06 2437MHz              Select SSID Profile= SSID01
     RTS Threshold= 2432                  Edit Bridge Link Configuration= N/A
     Frag. Threshold= 2432                 Preamble= Dynamic
                                           802.11 Mode= Mixed
                                           Max. Frame Burst= 650
                                           Breathing LED= Yes
                                           Block Intra-BSS Traffic= No
                                           Output Power= 100%(Full Power)
                                           Edit Layer-2 Isolation= No



                    Press ENTER to Confirm or ESC to Cancel:
```

3 Press [SPACE BAR] to select **Access Point** or **AP + Bridge** in the **Operating Mode** field and press [ENTER].

4 In the **Edit MAC Address Filter** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.1 – WLAN MAC Address Filter** displays as shown next.

Figure 142 Menu 3.5.1 WLAN MAC Address Filter



```
                                   Menu 3.5.1 - WLAN MAC Address Filter

                    Active= No
                    Filter Action= Allowed Association
 ----------------------------------------------------------------------------
           --
    1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
    2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
    3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
    4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
    5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
    6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
    7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
    8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
    9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
   10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
   11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
   12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
 ----------------------------------------------------------------------------
           --
                        Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 73 Menu 3.5.1 WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the ZyXEL Device, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, **Allowed Association**, permits association with the ZyXEL Device. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
1..32	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyXEL Device in these address fields.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

19.3.2 Configuring Roaming

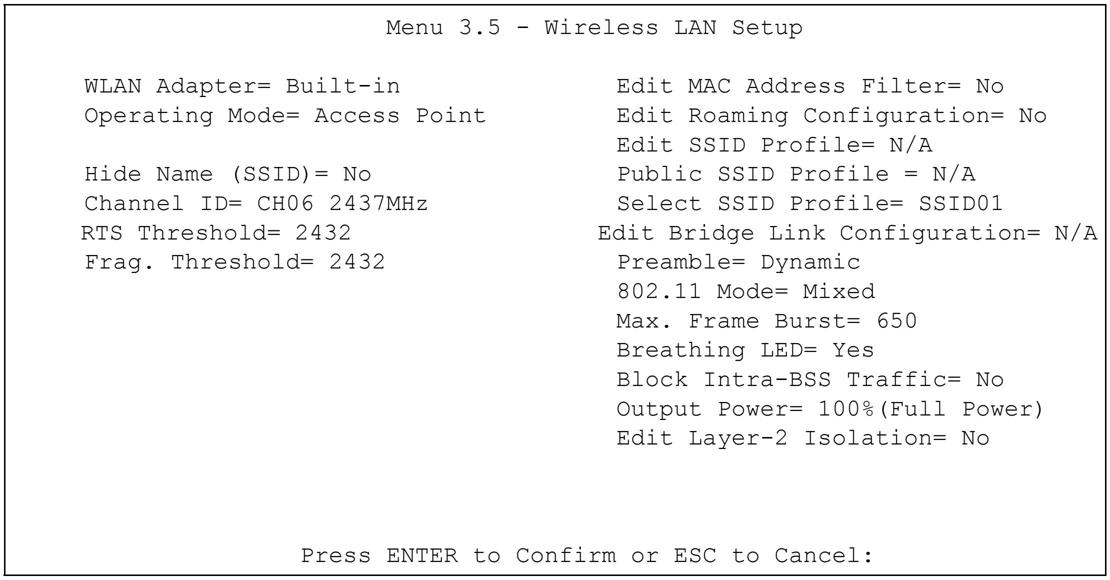
The roaming feature allows wireless LAN users to move between the coverage areas of different access points in a wireless LAN.

Follow the steps below to configure roaming on your ZyXEL Device.

1 From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

2 Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

Figure 143 Menu 3.5 Wireless LAN Setup

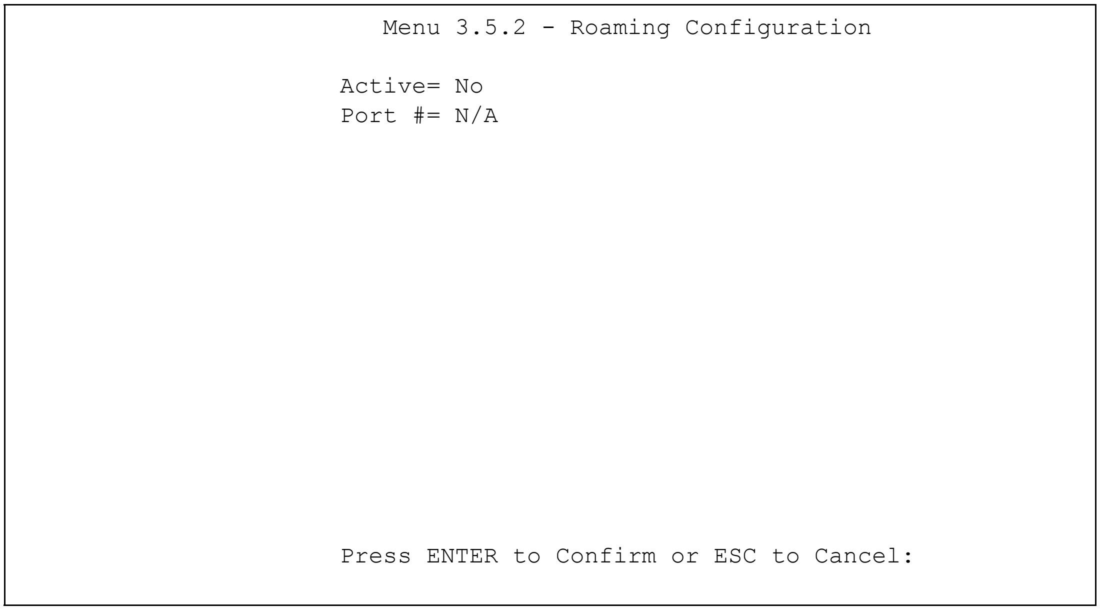


```
                          Menu 3.5 - Wireless LAN Setup

     WLAN Adapter= Built-in                 Edit MAC Address Filter= No
     Operating Mode= Access Point           Edit Roaming Configuration= No
                                            Edit SSID Profile= N/A
     Hide Name (SSID)= No                   Public SSID Profile = N/A
     Channel ID= CH06 2437MHz               Select SSID Profile= SSID01
     RTS Threshold= 2432                   Edit Bridge Link Configuration= N/A
     Frag. Threshold= 2432                  Preamble= Dynamic
                                            802.11 Mode= Mixed
                                            Max. Frame Burst= 650
                                            Breathing LED= Yes
                                            Block Intra-BSS Traffic= No
                                            Output Power= 100%(Full Power)
                                            Edit Layer-2 Isolation= No



                    Press ENTER to Confirm or ESC to Cancel:
```

3 Press [SPACE BAR] to select **Access Point, AP + Bridge** or **MESSID** in the **Operating Mode** field and press [ENTER].

4 In the **Edit Roaming Configuration** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.2 - Roaming Configuration** displays as shown next.

Figure 144 Menu 3.5.2 - Roaming Configuration



```
                         Menu 3.5.2 - Roaming Configuration

                      Active= No
                      Port #= N/A




















                      Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 74 Menu 3.5.2 - Roaming Configuration

FIELD	DESCRIPTION
Active	To enable roaming, press [SPACE BAR] to select **Yes** and press [ENTER]. This is useful if you have two or more APs on the same subnet. Note: All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.
Port #	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is 3517. Make sure this port is not used by other services.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

19.3.3 Configuring Bridge Link

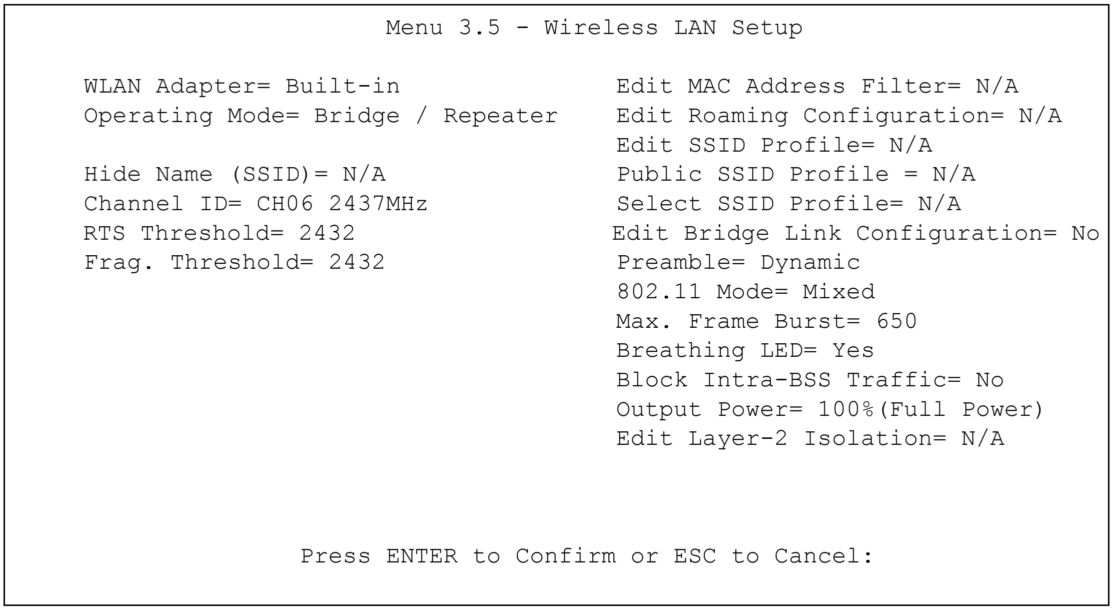
Follow the steps below to configure bridge link on your ZyXEL Device.

1 From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

2 Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

3 In the **Operating Mode** field, press [SPACE BAR] to select **Bridge / Repeater** or **AP + Bridge** and press [ENTER].

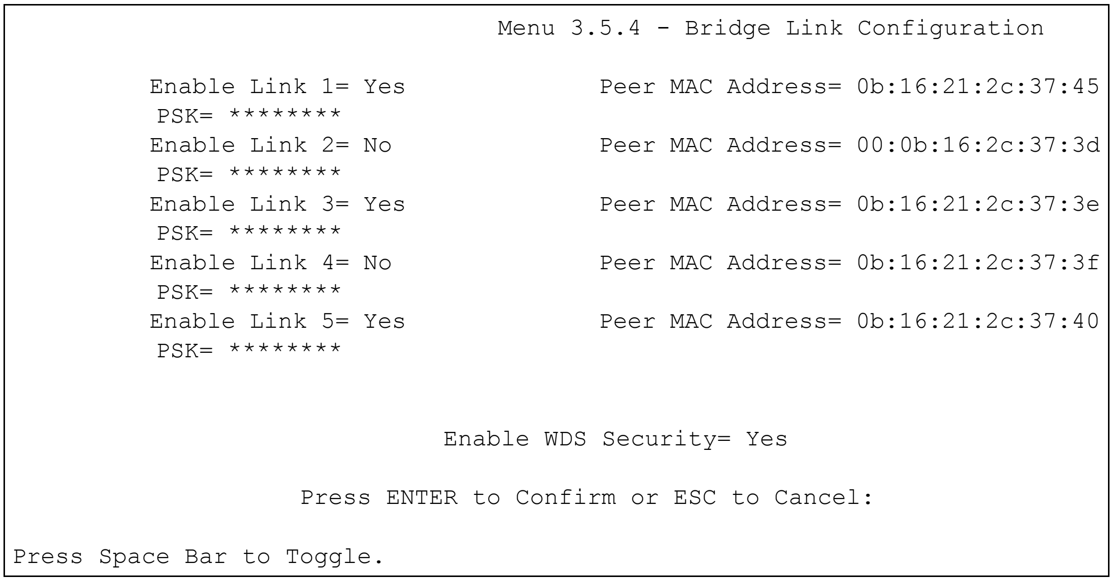
Figure 145 Menu 3.5 Wireless LAN Setup



```
                          Menu 3.5 - Wireless LAN Setup

     WLAN Adapter= Built-in                Edit MAC Address Filter= N/A
     Operating Mode= Bridge / Repeater     Edit Roaming Configuration= N/A
                                           Edit SSID Profile= N/A
     Hide Name (SSID)= N/A                 Public SSID Profile = N/A
     Channel ID= CH06 2437MHz              Select SSID Profile= N/A
     RTS Threshold= 2432                  Edit Bridge Link Configuration= No
     Frag. Threshold= 2432                 Preamble= Dynamic
                                           802.11 Mode= Mixed
                                           Max. Frame Burst= 650
                                           Breathing LED= Yes
                                           Block Intra-BSS Traffic= No
                                           Output Power= 100%(Full Power)
                                           Edit Layer-2 Isolation= N/A



                    Press ENTER to Confirm or ESC to Cancel:
```

4 Move the cursor to the **Edit Bridge Link Configuration** field. Press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.4 – Bridge Link Configuration** displays as shown next.

Figure 146 Menu 3.5.4 Bridge Link Configuration



```
                                Menu 3.5.4 - Bridge Link Configuration

          Enable Link 1= Yes             Peer MAC Address= 0b:16:21:2c:37:45
           PSK= ********
          Enable Link 2= No              Peer MAC Address= 00:0b:16:2c:37:3d
           PSK= ********
          Enable Link 3= Yes             Peer MAC Address= 0b:16:21:2c:37:3e
           PSK= ********
          Enable Link 4= No              Peer MAC Address= 0b:16:21:2c:37:3f
           PSK= ********
          Enable Link 5= Yes             Peer MAC Address= 0b:16:21:2c:37:40
           PSK= ********


                            Enable WDS Security= Yes

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

The following table describes the fields in this menu.

Table 75 Menu 3.5.4 Bridge Link Configuration

FIELD	DESCRIPTION
Enable Link 1 ~ 5	Press [SPACE BAR] to select **Yes** or **No** and press [ENTER].
Peer MAC Address	Type the MAC address of peer device in valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols)
Enable WDS Security	Select **Yes** to enable WDS on your ZyXEL Device. A Wireless Distribution System (WDS) is a wireless connection between two or more APs. When you select **Yes**, you are prompted to type a Pre-Shared Key (PSK) in the PSK fields of each bridge link you want to configure. The ZyXEL Device uses TKIP to encrypt traffic on the WDS between AP's. Note: Other AP's must use the same encryption method to enable WDS.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

19.3.4 Configuring Layer-2 Isolation

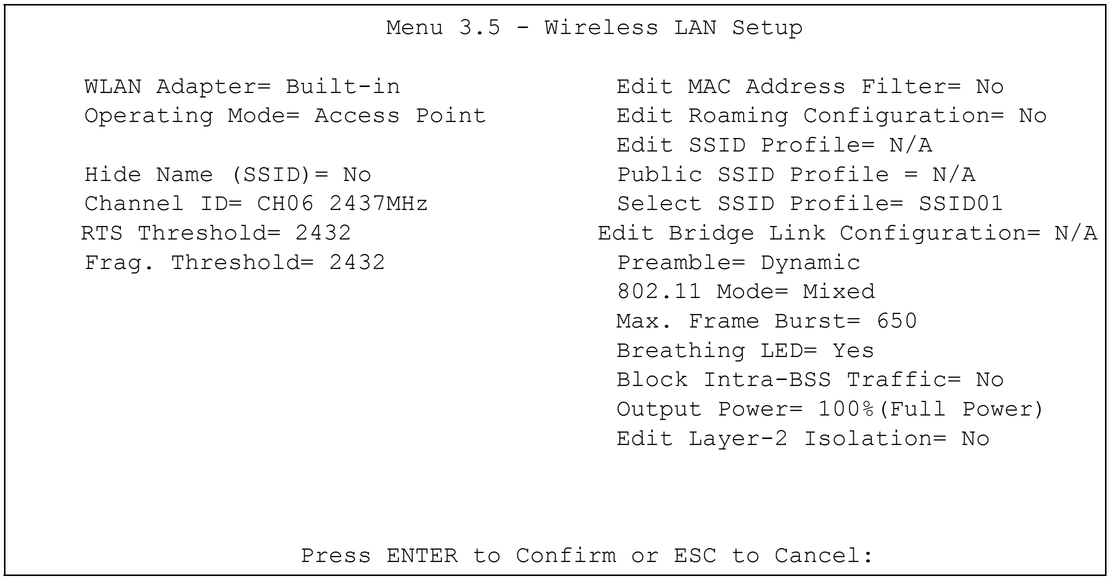
Use layer-2 isolation to prevent wireless clients associated with your ZyXEL Device from communicating with other wireless clients, APs, computers or routers in a network.

Follow the steps below to configure layer-2 isolation on your ZyXEL Device.

1 From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

2 Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

Figure 147 Menu 3.5 Wireless LAN Setup

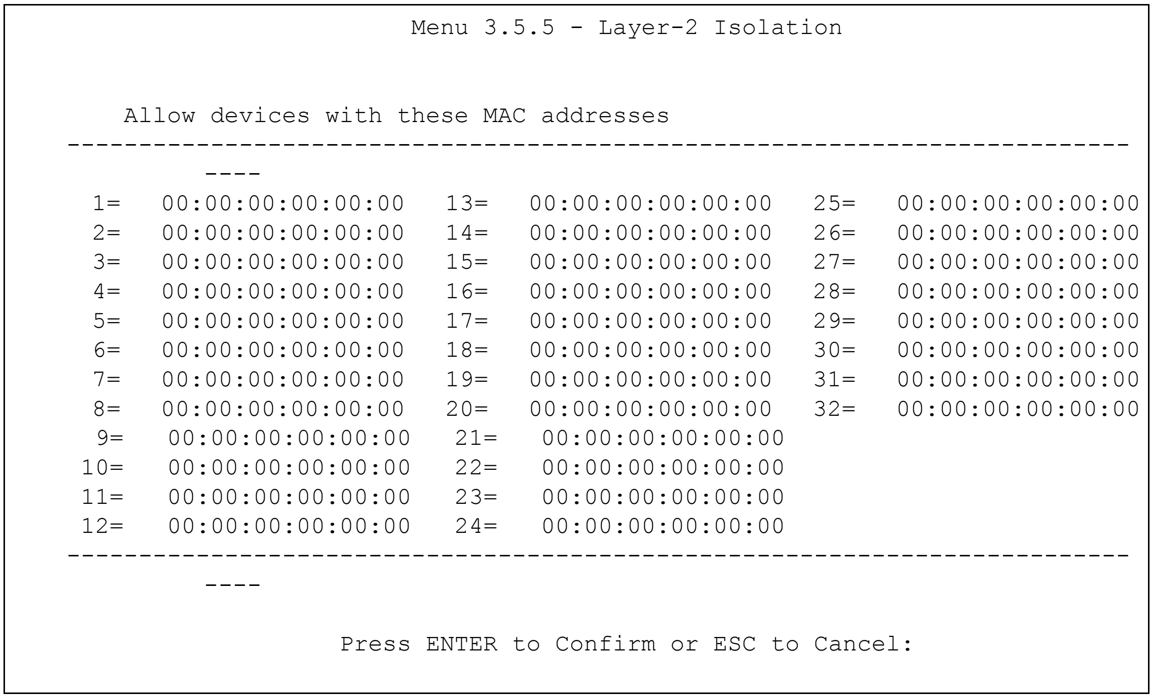


```
                        Menu 3.5 - Wireless LAN Setup

     WLAN Adapter= Built-in               Edit MAC Address Filter= No
     Operating Mode= Access Point         Edit Roaming Configuration= No
                                          Edit SSID Profile= N/A
     Hide Name (SSID)= No                 Public SSID Profile = N/A
     Channel ID= CH06 2437MHz             Select SSID Profile= SSID01
     RTS Threshold= 2432                 Edit Bridge Link Configuration= N/A
     Frag. Threshold= 2432                Preamble= Dynamic
                                          802.11 Mode= Mixed
                                          Max. Frame Burst= 650
                                          Breathing LED= Yes
                                          Block Intra-BSS Traffic= No
                                          Output Power= 100%(Full Power)
                                          Edit Layer-2 Isolation= No



                  Press ENTER to Confirm or ESC to Cancel:
```

3 Press [SPACE BAR] to select **Access Point, AP + Bridge** or **MESSID** in the **Operating Mode** field and press [ENTER].

4 In the **Edit Layer-2 Isolation** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.5 - Layer-2 Isolation** displays as shown next.

Figure 148 Menu 3.5.5 - Layer-2 Isolation



```
                          Menu 3.5.5 - Layer-2 Isolation


      Allow devices with these MAC addresses
  --------------------------------------------------------------------------
           ----
    1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
    2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
    3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
    4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
    5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
    6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
    7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
    8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
    9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
   10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
   11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
   12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
  --------------------------------------------------------------------------
           ----

                     Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 76 Menu 3.5.5 - Layer-2 Isolation

FIELD	DESCRIPTION
Allow devices with these MAC addresses	These are the MAC address of a wireless client, AP, computer or router. A wireless client associated with the ZyXEL Device can communicate with another wireless client, AP, computer or router only if the MAC addresses of those devices are listed in this table.
1..32	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyXEL Device in these address fields.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

19.3.5 Configuring SSID Profiles

When the ZyXEL Device is set to MESSID mode, you need to choose the SSID profile(s) you want to use in your wireless network (see Section 6.6 on page 78 for more information on operating modes).

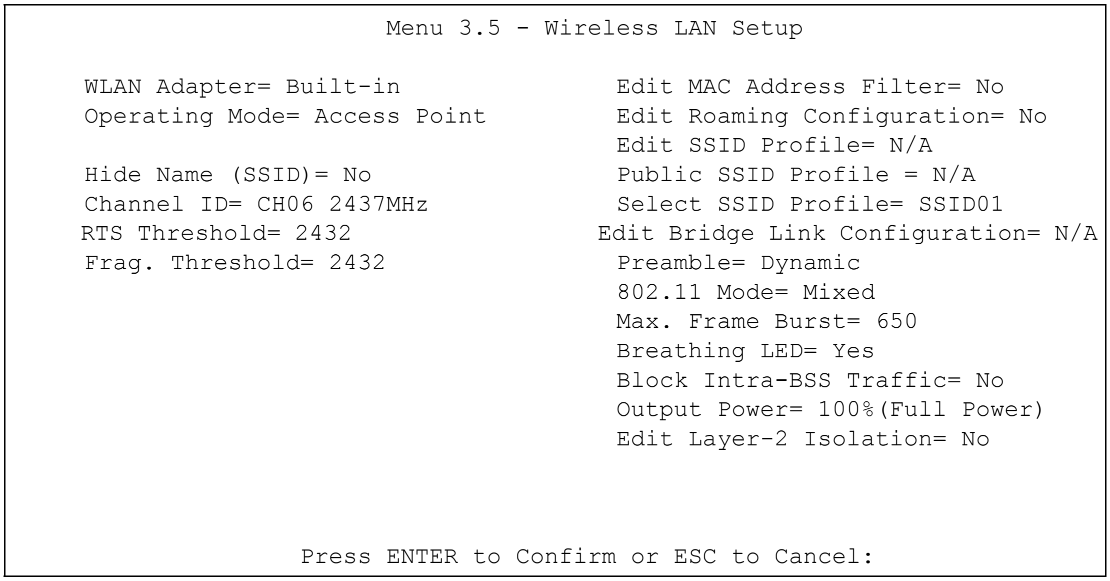
Follow the steps below to set which SSID profiles your ZyXEL Device uses.

1 From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

2 Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

3 Press [SPACE BAR] to select **MESSID** in the **Operating Mode** field and press [ENTER].

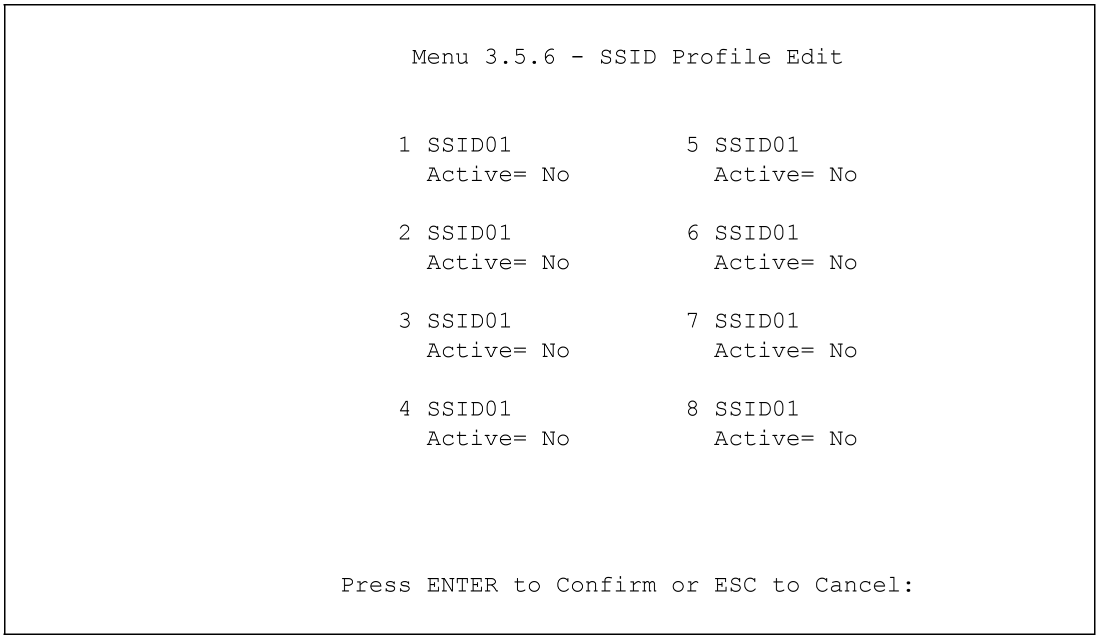
Figure 149 Menu 3.5 Wireless LAN Setup



```
                        Menu 3.5 - Wireless LAN Setup

     WLAN Adapter= Built-in                Edit MAC Address Filter= No
     Operating Mode= Access Point          Edit Roaming Configuration= No
                                           Edit SSID Profile= N/A
     Hide Name (SSID)= No                  Public SSID Profile = N/A
     Channel ID= CH06 2437MHz              Select SSID Profile= SSID01
    RTS Threshold= 2432                   Edit Bridge Link Configuration= N/A
     Frag. Threshold= 2432                 Preamble= Dynamic
                                           802.11 Mode= Mixed
                                           Max. Frame Burst= 650
                                           Breathing LED= Yes
                                           Block Intra-BSS Traffic= No
                                           Output Power= 100%(Full Power)
                                           Edit Layer-2 Isolation= No



                  Press ENTER to Confirm or ESC to Cancel:
```

4 In the **Edit SSID Profile** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.6 - SSID Profile Edit** displays as shown next.

Figure 150 Menu 3.5.6 - SSID Profile Edit



```
                          Menu 3.5.6 - SSID Profile Edit


                         1 SSID01             5 SSID01
                           Active= No           Active= No

                         2 SSID01             6 SSID01
                           Active= No           Active= No

                         3 SSID01             7 SSID01
                           Active= No           Active= No

                         4 SSID01             8 SSID01
                           Active= No           Active= No




                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 77 Menu 3.5.6 - SSID Profile Edit

FIELD	DESCRIPTION
1~8	An SSID profile is the set of parameters relating to one of the ZyXEL Device's ESSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating with the access point (AP) must have the same SSID. Press [SPACE BAR] and then [ENTER] to select the profile(s) of the SSIDs you want to use in your wireless network. Configure SSID profiles in the web configurator **SSID** screen. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or 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.
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable a SSID profile. Select **No** to disable the SSID profile.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

20

Dial-in User Setup

This chapter shows you how to create user accounts on the ZyXEL Device.

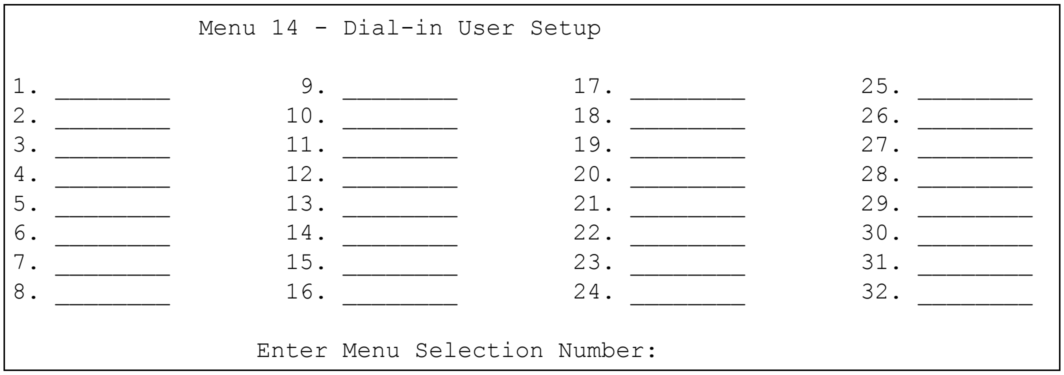
20.1 Dial-in User Setup

By storing user profiles locally, your ZyXEL Device is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your ZyXEL Device.

From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.

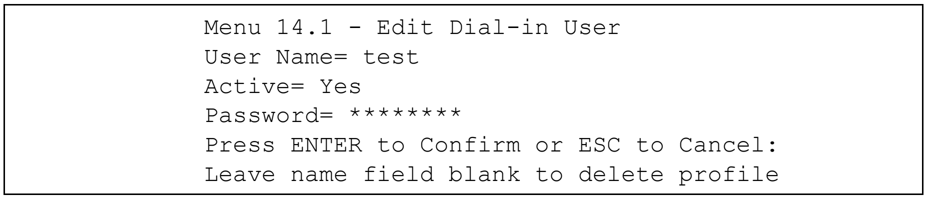
Figure 151 Menu 14- Dial-in User Setup



```
             Menu 14 - Dial-in User Setup

1. ________          9. ________          17. ________          25. ________
2. ________         10. ________          18. ________          26. ________
3. ________         11. ________          19. ________          27. ________
4. ________         12. ________          20. ________          28. ________
5. ________         13. ________          21. ________          29. ________
6. ________         14. ________          22. ________          30. ________
7. ________         15. ________          23. ________          31. ________
8. ________         16. ________          24. ________          32. ________

                 Enter Menu Selection Number:
```

Type a number and press [ENTER] to edit the user profile.

Figure 152 Menu 14.1- Edit Dial-in User



```
              Menu 14.1 - Edit Dial-in User
              User Name= test
              Active= Yes
              Password= ********
              Press ENTER to Confirm or ESC to Cancel:
              Leave name field blank to delete profile
```

The following table describes the fields in this screen.

Table 78 Menu 14.1- Edit Dial-in User

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

21

VLAN Setup

This chapter explains VLAN Setup menu 16. Refer to Chapter 15 on page 173 for background information on VLAN.

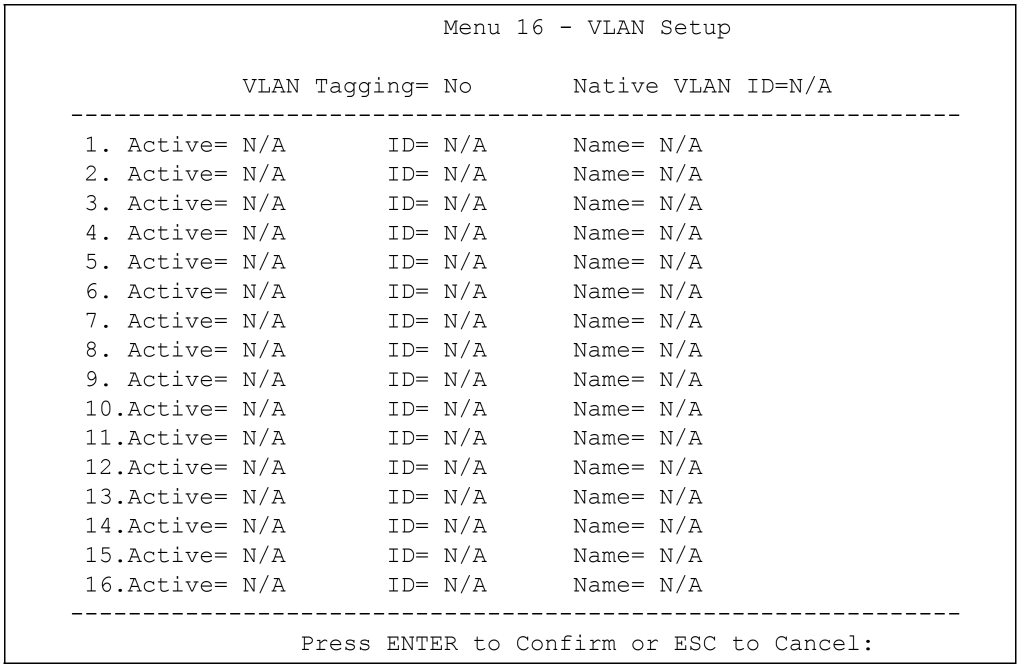
21.1 VLAN Setup

When VLAN is enabled, you must connect the ZyXEL Device to a VLAN-aware device that is a member of the management VLAN in order to manage it through the network. See the example of configuring a management VLAN Section 15.2.2 on page 176 before you configure VLAN on the ZyXEL Device.

If no devices are in the management VLAN, then you will not be able to access the ZyXEL Device through the network. If the ZyXEL Device has no console port, you will have to restore the default configuration file.

To setup VLAN, select option 16 from the main menu to open Menu 16 – VLAN Setup as shown next.

Figure 153 Menu 16 VLAN Setup



```
                          Menu 16 - VLAN Setup

            VLAN Tagging= No       Native VLAN ID=N/A
--------------------------------------------------------------
 1. Active= N/A       ID= N/A      Name= N/A
 2. Active= N/A       ID= N/A      Name= N/A
 3. Active= N/A       ID= N/A      Name= N/A
 4. Active= N/A       ID= N/A      Name= N/A
 5. Active= N/A       ID= N/A      Name= N/A
 6. Active= N/A       ID= N/A      Name= N/A
 7. Active= N/A       ID= N/A      Name= N/A
 8. Active= N/A       ID= N/A      Name= N/A
 9. Active= N/A       ID= N/A      Name= N/A
 10.Active= N/A       ID= N/A      Name= N/A
 11.Active= N/A       ID= N/A      Name= N/A
 12.Active= N/A       ID= N/A      Name= N/A
 13.Active= N/A       ID= N/A      Name= N/A
 14.Active= N/A       ID= N/A      Name= N/A
 15.Active= N/A       ID= N/A      Name= N/A
 16.Active= N/A       ID= N/A      Name= N/A
--------------------------------------------------------------
                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 79 Menu 16 VLAN Setup

FIELD	DESCRIPTION
VLAN Tagging	To enable VLAN tagging, press [SPACE BAR] to select **Yes** and press [ENTER].
Native VLAN ID	Enter a number from 1 to 4094. At least one device in your network must belong to this VLAN group in order to manage the ZyXEL Device. Mail and FTP servers must have the same management VLAN ID to communicate with the ZyXEL Device.
	Use this table to map names to VLAN IDs so that the RADIUS server can assign each user or user group a mapped VLAN ID. See your RADIUS server documentation for more information on configuring VLAN ID attributes. See Section 15.2.3 on page 178 for more information.
Active	To enable a SSID to VLAN mapping entry, press [SPACE BAR] to select **Yes** and press [ENTER].
ID	Enter a number from 1 to 4094 to define this VLAN group.
Name	Type a name to have the ZyXEL Device check for specific VLAN attributes on incoming messages from the RADIUS server. Access-accept packets sent by the RADIUS server contain VLAN related attributes. The configured **Name** fields are checked against these attributes. If a configured **Name** field matches these attributes, the corresponding VLAN ID is added to packets sent from this user to the LAN. If the VLAN-related attributes sent by the RADIUS server do not match a configured **Name** field, a wireless station is assigned the wireless VLAN ID associated with its SSID.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

22

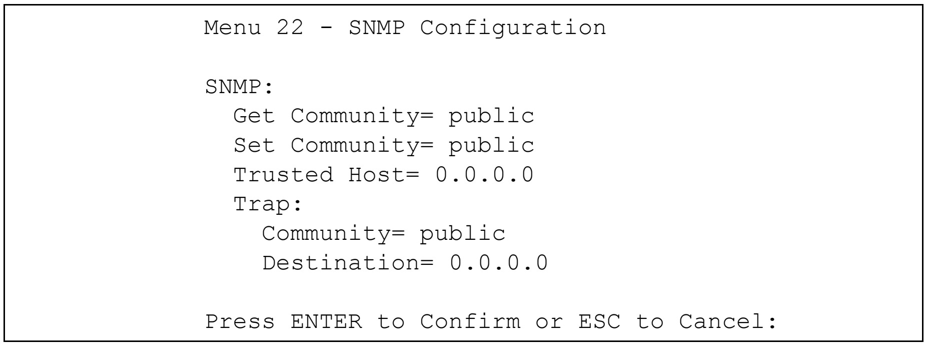
SNMP Configuration

This chapter explains SNMP Configuration menu 22. See the web configurator chapter on SNMP for background information.

22.1 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 – SNMP Configuration** as shown next. The "community" for Get, Set and Trap fields is SNMP terminology for password.

Figure 154 Menu 22 SNMP Configuration



```
              Menu 22 - SNMP Configuration

              SNMP:
                Get Community= public
                Set Community= public
                Trusted Host= 0.0.0.0
                Trap:
                  Community= public
                  Destination= 0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the SNMP configuration parameters.

Table 80 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the **Set Community**, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your ZyXEL Device will only respond to SNMP messages from this address. A blank (default) field means your ZyXEL Device will respond to all SNMP messages it receives, regardless of source.
Trap:	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.

Table 80 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

23

System Security

This chapter describes how to configure the ZyXEL Device's system password and wireless LAN security profiles.

23.1 System Password

See Section 17.4 on page 202 for how to change the system password.

23.2 Configuring Wireless Security Profiles

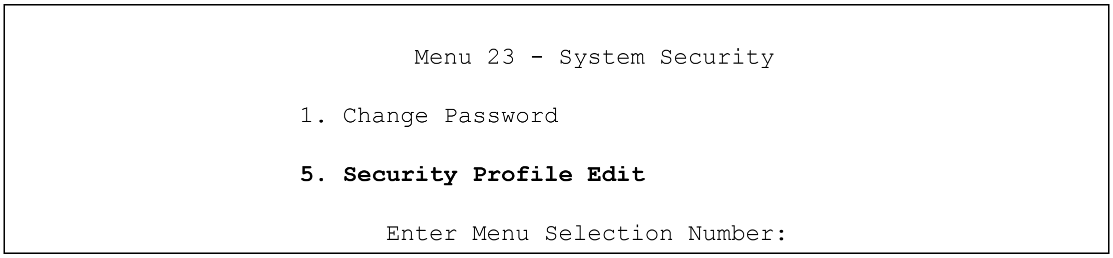
> The following screens are configurable only in **Access Point, AP+Bridge and MESSID** operating modes only.

Use SMT menu 23.5 create secure profiles. A security profile is a group of configuration settings which can be assigned to an SSID profile in the **SSID** configuration screen. See Chapter 7 on page 87 and Appendix E on page 295 for information on wireless security.

Do the following to change your ZyXEL Device's wireless security settings.

1 From the main menu, enter 23 to open **Menu 23 – System Security**.

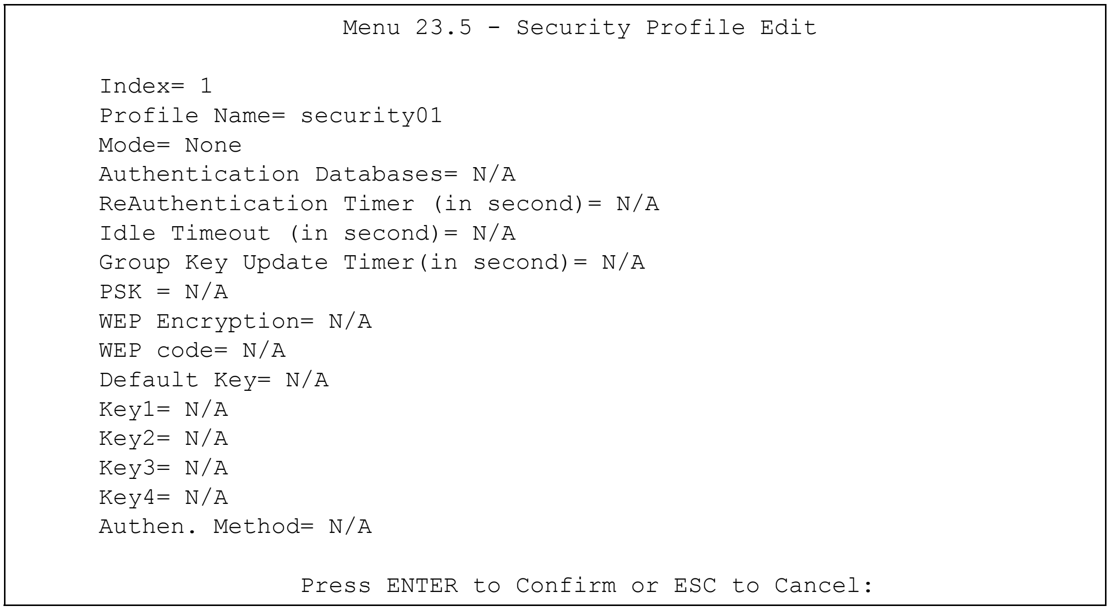
Figure 155 Menu 23 System Security



```
                         Menu 23 - System Security

                 1. Change Password

                 5. Security Profile Edit

                       Enter Menu Selection Number:
```

2 Enter 5 to display **Menu 23.5 - Security Profile Edit**. Menu 23 System Security

Figure 156 Menu 23.5 - Security Profile Edit



```
                        Menu 23.5 - Security Profile Edit

      Index= 1
      Profile Name= security01
      Mode= None
      Authentication Databases= N/A
      ReAuthentication Timer (in second)= N/A
      Idle Timeout (in second)= N/A
      Group Key Update Timer(in second)= N/A
      PSK = N/A
      WEP Encryption= N/A
      WEP code= N/A
      Default Key= N/A
      Key1= N/A
      Key2= N/A
      Key3= N/A
      Key4= N/A
      Authen. Method= N/A

                     Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu. Not all fields apply for each security mode.

Table 81 Menu 3.5.6 - SSID Profile Edit

FIELD	DESCRIPTION
Index	Press [SPACE BAR] and then [ENTER] to select the number of the security profile that you want to edit.
Profile Name	Type a name to identify this security profile.
Mode	Press [SPACE BAR] and then [ENTER] to select the security mode for this security profile. See Chapter 7 on page 87 for information on wireless security modes.
Authentication Databases	Press [SPACE BAR] and then [ENTER] to select which authentication databases the ZyXEL Device uses and in what order. Select **Local User Database Only** to have the system use the internal user account database. Select **RADIUS Only** to have the system use an external RADIUS server. Select **Local first then RADIUS** to have the system check the internal user account database first, and then the external RADIUS server if there is no match. Select **RADIUS first then Local** to have the system check the external RADIUS server first, and then the internal user account database if there is no match.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

Table 81 Menu 3.5.6 - SSID Profile Edit

FIELD	DESCRIPTION
Idle Timeout (in second)	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Group Key Update Timer(in second)	This is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. The ZyXEL Device default is 1800 seconds (30 minutes).
PSK	WPA-PSK and WPA2-PSK use a simple common password (called a pre-shared key or PSK), instead of user-specific credentials. Type a PSK from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
WEP Encryption	Press [SPACE BAR] and then [ENTER] to select **Disable** to allow wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
WEP code	Press [SPACE BAR] and then [ENTER] to select **ASCII** to enter ASCII characters as the WEP keys. Press [SPACE BAR] and then [ENTER] to select **HEX** to enter hexadecimal characters as the WEP keys. The preceding “0x” is entered automatically.
Default Key	Press [SPACE BAR] and then [ENTER] to select which of the four WEP keys the ZyXEL Device is to use for encryption.You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Key1~4	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").
Authen. Method	Press [SPACE BAR] and then [ENTER] to select **Auto**, **Open System** or **Shared Key** from the drop-down list box. The default setting is **Auto**.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

24

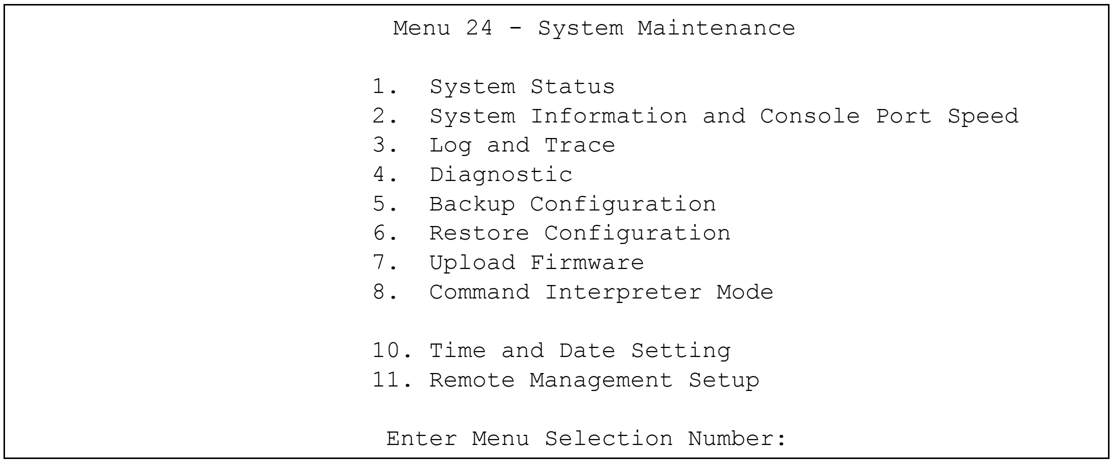
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu and press [ENTER] to open **Menu 24 – System Maintenance**, as shown in the following figure.

Figure 157 Menu 24 System Maintenance



```
                          Menu 24 - System Maintenance

                         1.  System Status
                         2.  System Information and Console Port Speed
                         3.  Log and Trace
                         4.  Diagnostic
                         5.  Backup Configuration
                         6.  Restore Configuration
                         7.  Upload Firmware
                         8.  Command Interpreter Mode

                         10. Time and Date Setting
                         11. Remote Management Setup

                          Enter Menu Selection Number:
```

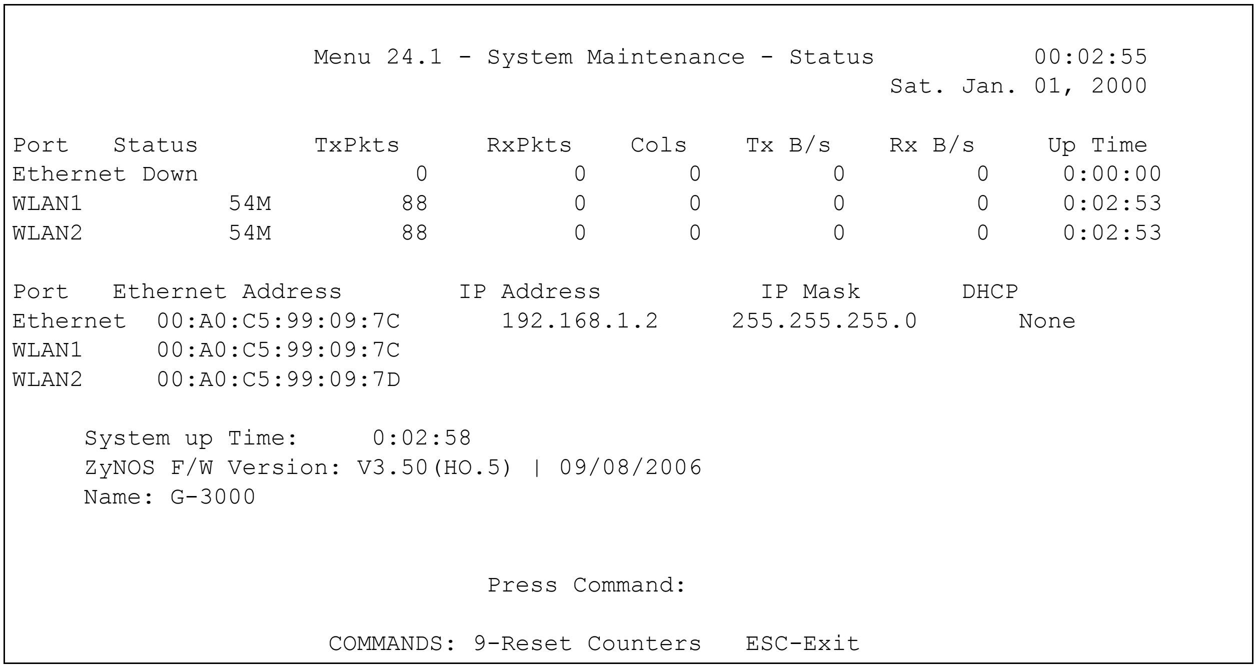
24.1 System Status

The first selection, **System Status** gives you information on the status and statistics of the ports, as shown next. **System Status** is a tool that can be used to monitor your ZyXEL Device. Specifically, it gives you information on your Ethernet and Wireless LAN status, and the number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 – System Maintenance.** From this menu, type 1**. System Status**. There are two commands in **Menu 24.1 – System Maintenance – Status**. Entering 9 resets the counters; pressing [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status** which are read-only and meant for diagnostic purposes.

Figure 158 Menu 24.1 System Maintenance: Status



```
                     Menu 24.1 - System Maintenance - Status           00:02:55
                                                               Sat. Jan. 01, 2000

Port   Status         TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
Ethernet Down               0           0       0         0         0     0:00:00
WLAN1          54M         88           0       0         0         0     0:02:53
WLAN2          54M         88           0       0         0         0     0:02:53

Port   Ethernet Address        IP Address           IP Mask       DHCP
Ethernet  00:A0:C5:99:09:7C       192.168.1.2     255.255.255.0       None
WLAN1     00:A0:C5:99:09:7C
WLAN2     00:A0:C5:99:09:7D

     System up Time:     0:02:58
     ZyNOS F/W Version: V3.50(HO.5) | 09/08/2006
     Name: G-3000


                                Press Command:

                      COMMANDS: 9-Reset Counters   ESC-Exit
```

The following table describes the fields present in this menu.

Table 82 Menu 24.1 System Maintenance: Status

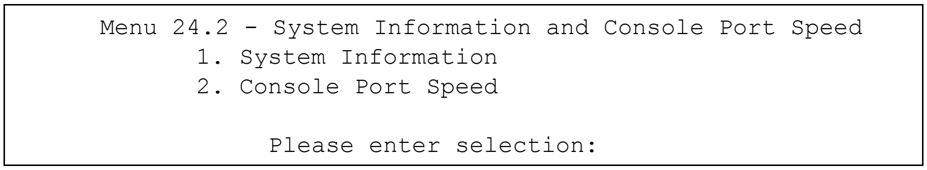
FIELD	DESCRIPTION
Port	This is the port, either Ethernet or wireless. For the G-3000, the built-in wireless adapter is WLAN1 and the removable wireless adapter is WLAN 2.
Status	This shows the status of the port's connection.
TxPkts	This is the number of transmitted packets to this remote node.
RxPkts	This is the number of received packets from this remote node.
Cols	This is the number of collisions on this connection.
Tx B/s	This shows the transmission rate in bytes per second.
Rx B/s	This shows the receiving rate in bytes per second.
Up Time	This is the time this channel has been connected to the current remote node.
Ethernet Address	This shows the MAC address of the port.
IP Address	This shows the IP address of the network device connected to the port.
IP Mask	This shows the subnet mask of the network device connected to the port.
DHCP	This shows the DHCP setting (None or Client) for the port.
System Up Time	This is the time the ZyXEL Device is up and running from the last reboot.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Name	This displays the device name.

24.2 System Information

To get to the System Information:

1. Enter 24 to display **Menu 24 – System Maintenance**.
2. Enter 2 to display **Menu 24.2 – System Information and Console Port Speed**.
3. From this menu you have two choices as shown in the next figure:

Figure 159 Menu 24.2 System Information and Console Port Speed



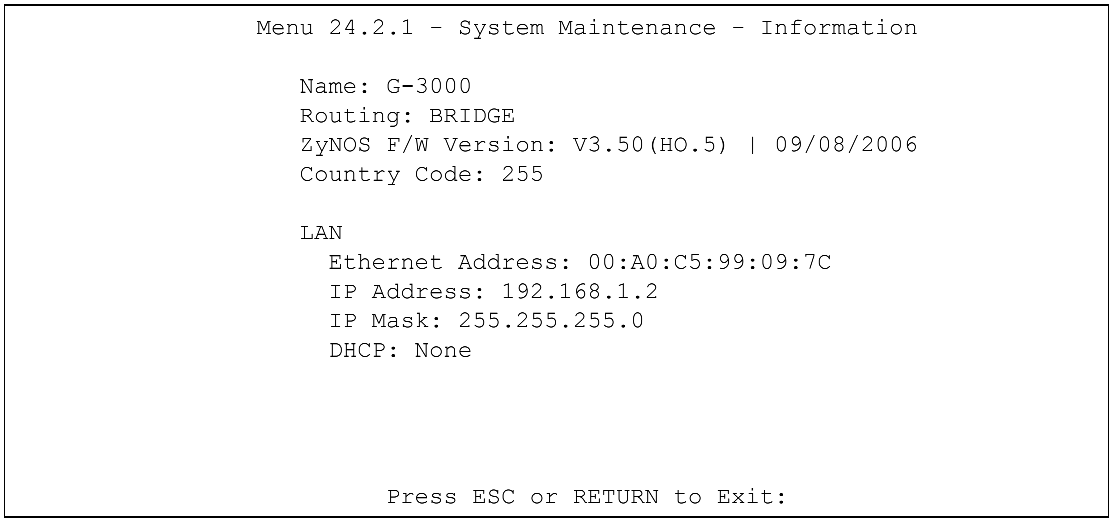
```
      Menu 24.2 - System Information and Console Port Speed
             1. System Information
             2. Console Port Speed

                  Please enter selection:
```

If you ZyXEL Device does not have an external console port, these settings are for an internal console port for support personnel only. Do not open the ZyXEL Device as it will void your warranty.

24.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

Figure 160 Menu 24.2.1 System Information: Information



```
                 Menu 24.2.1 - System Maintenance - Information

                    Name: G-3000
                    Routing: BRIDGE
                    ZyNOS F/W Version: V3.50(HO.5) | 09/08/2006
                    Country Code: 255

                    LAN
                      Ethernet Address: 00:A0:C5:99:09:7C
                      IP Address: 192.168.1.2
                      IP Mask: 255.255.255.0
                      DHCP: None




                             Press ESC or RETURN to Exit:
```

The following table describes the fields in this menu.

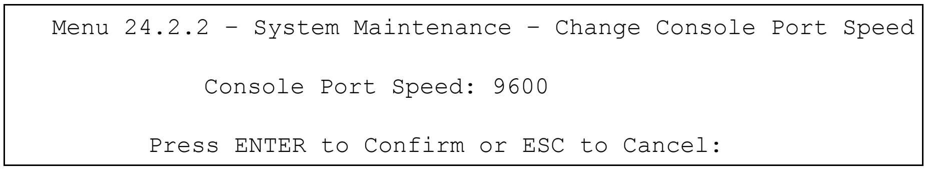
Table 83 Menu 24.2.1 System Maintenance: Information

FIELD	DESCRIPTION
Name	Displays the system name of your ZyXEL Device. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Country Code	Refers to the country code of the firmware.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your ZyXEL Device.
IP Address	This is the IP address of the ZyXEL Device in dotted decimal notation.
IP Mask	This shows the subnet mask of the ZyXEL Device.
DHCP	This field shows the DHCP setting of the ZyXEL Device.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

24.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your ZyXEL Device supports 9600 (default), 19200, 38400, 57600 and 115200 bps console port speeds. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

Figure 161 Menu 24.2.2 System Maintenance: Change Console Port Speed



```
  Menu 24.2.2 - System Maintenance - Change Console Port Speed

            Console Port Speed: 9600

        Press ENTER to Confirm or ESC to Cancel:
```

After you changed your ZyXEL Device's console port speed, you must also make the same change to the console port speed parameter of your communication software.

24.3 Log and Trace

Your ZyXEL Device provides error logs and trace records that are stored locally.

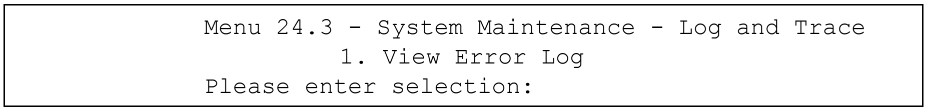
24.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

1 Type 24 in the main menu to display **Menu 24 – System Maintenance**.

2 From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

Figure 162 Menu 24.3 System Maintenance: Log and Trace

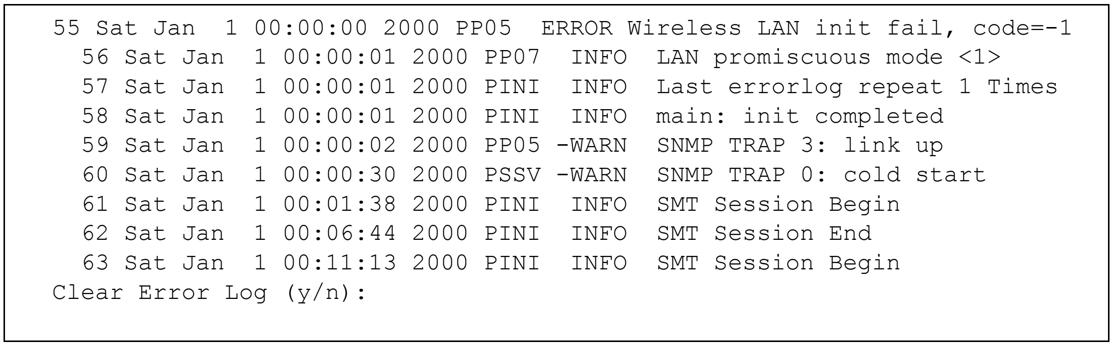


```
              Menu 24.3 - System Maintenance - Log and Trace
                       1. View Error Log
              Please enter selection:
```

3 Enter 1 from **Menu 24.3 – System Maintenance – Log and Trace** and press [ENTER] twice to display the error log in the system.

After the ZyXEL Device finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

Figure 163 Sample Error and Information Messages

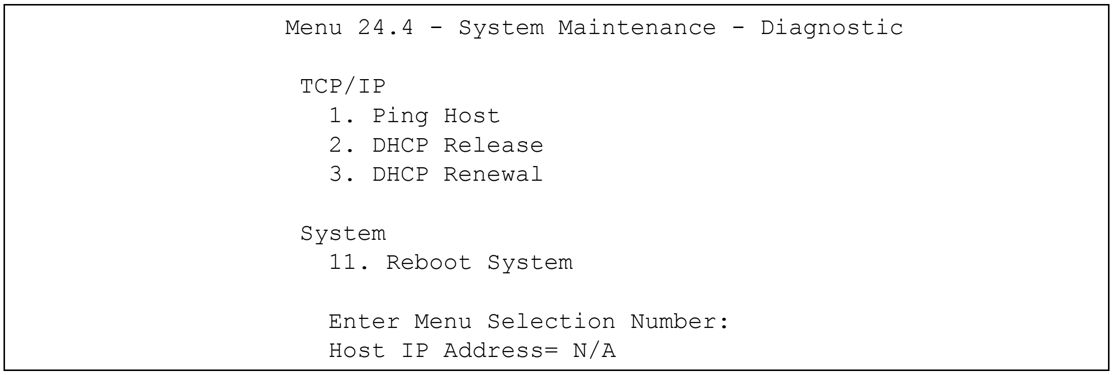


```
   55 Sat Jan  1 00:00:00 2000 PP05  ERROR Wireless LAN init fail, code=-1
     56 Sat Jan  1 00:00:01 2000 PP07  INFO  LAN promiscuous mode <1>
     57 Sat Jan  1 00:00:01 2000 PINI  INFO  Last errorlog repeat 1 Times
     58 Sat Jan  1 00:00:01 2000 PINI  INFO  main: init completed
     59 Sat Jan  1 00:00:02 2000 PP05 -WARN  SNMP TRAP 3: link up
     60 Sat Jan  1 00:00:30 2000 PSSV -WARN  SNMP TRAP 0: cold start
     61 Sat Jan  1 00:01:38 2000 PINI  INFO  SMT Session Begin
     62 Sat Jan  1 00:06:44 2000 PINI  INFO  SMT Session End
     63 Sat Jan  1 00:11:13 2000 PINI  INFO  SMT Session Begin
   Clear Error Log (y/n):
```

24.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyXEL Device to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Figure 164 Menu 24.4 System Maintenance: Diagnostic



```
                    Menu 24.4 - System Maintenance - Diagnostic

                     TCP/IP
                       1. Ping Host
                       2. DHCP Release
                       3. DHCP Renewal

                     System
                       11. Reboot System

                       Enter Menu Selection Number:
                       Host IP Address= N/A
```

Follow the procedure next to get to display this menu:

1 From the main menu, type 24 to open **Menu 24 – System Maintenance**.

2 From this menu, type 4. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

The following table describes the diagnostic tests available in menu 24.4 for your ZyXEL Device and the connections.

Table 84 Menu 24.4 System Maintenance Menu: Diagnostic

FIELD	DESCRIPTION
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
DHCP Release	Release the IP address assigned by the DHCP server.
DHCP Renewal	Get a new IP address from the DHCP server.
Reboot System	Reboot the ZyXEL Device.
Host IP Address	If you typed 1 to Ping Host, now type the address of the computer you want to ping.

25

Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files using the SMT screens.

25.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password and TCP/IP Setup, etc. It arrives from ZyXEL with a rom filename extension. Once you have customized the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyXEL Device.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file config.cfg.

If your [T]FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) will vary. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version.

Table 85 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the ZyXEL Device.

25.2 Backup Configuration

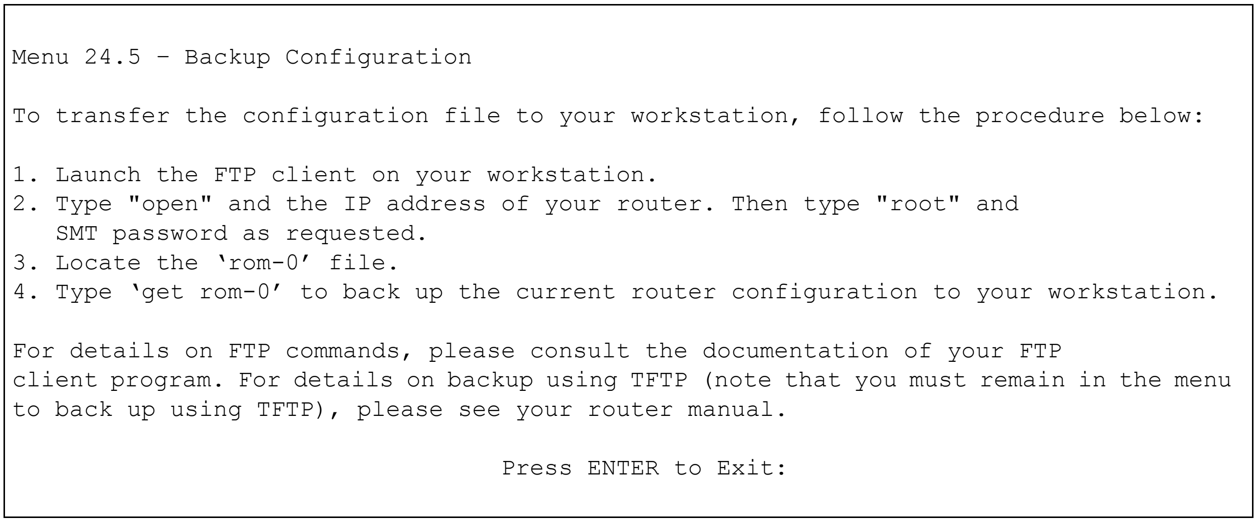
Option 5 from **Menu 24 – System Maintenance** allows you to backup the current configuration to your computer. Backup is highly recommended once your ZyXEL Device is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the terms “download” and “upload” are relative to the computer. Download means to transfer from the ZyXEL Device to the computer, while upload means from your computer to the ZyXEL Device.

25.2.1 Backup Configuration Using FTP

Enter 5 in **Menu 24 – System Maintenance** to get the following screen.

Figure 165 Menu 24.5 Backup Configuration

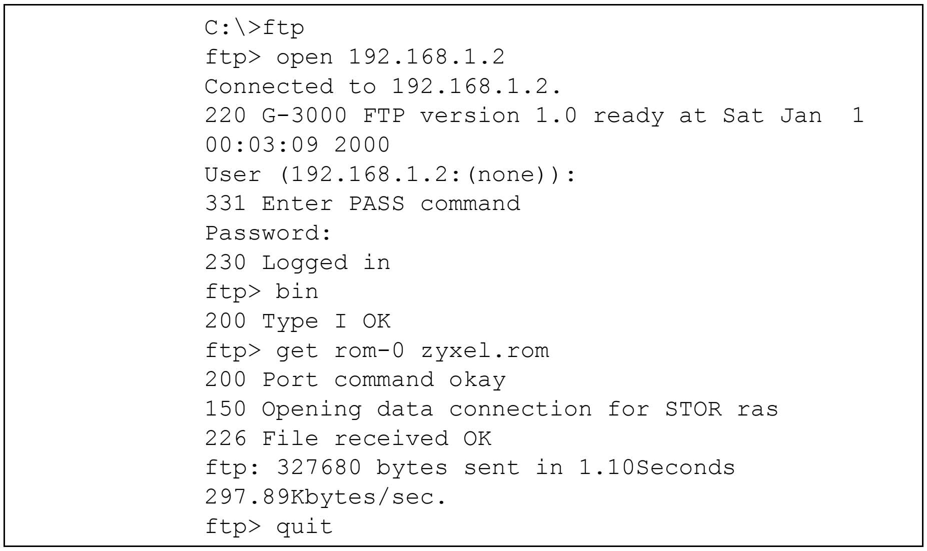


```
Menu 24.5 - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Locate the ‘rom-0’ file.
4. Type ‘get rom-0’ to back up the current router configuration to your workstation.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain in the menu
to back up using TFTP), please see your router manual.

                                  Press ENTER to Exit:
```

25.2.2 Using the FTP Command from the DOS Prompt

1. Launch the FTP client on your computer.
2. Enter "open" and the IP address of your ZyXEL Device.
3. Press [ENTER] when prompted for a username.
4. Enter your management password as requested. The default is 1234.
5. Enter "bin" to set transfer mode to binary.
6. Use "get" to transfer files from the ZyXEL Device to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the ZyXEL Device to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.
7. Enter "quit" to exit the FTP prompt.

Figure 166 FTP Session Example



```
C:\>ftp
ftp> open 192.168.1.2
Connected to 192.168.1.2.
220 G-3000 FTP version 1.0 ready at Sat Jan  1
00:03:09 2000
User (192.168.1.2:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

The following table describes some of the commands that you may see in third party FTP clients.

Table 86 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

25.2.3 Backup Configuration Using TFTP

The ZyXEL Device supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next:

1. Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.
5. Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is `rom-0` (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyXEL Device to the computer and “binary” to set binary transfer mode.

25.2.4 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyXEL Device IP address, “get” transfers the file source on the ZyXEL Device (rom-0 name of the configuration file on the ZyXEL Device) to the file destination on the computer and renames it config.rom.

The following table describes some of the fields that you may see in third party TFTP clients.

Table 87 General Commands for Third Party TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.2 is the ZyXEL Device’s default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the ZyXEL Device and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyXEL Device. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.

Table 87 General Commands for Third Party TFTP Clients

COMMAND	DESCRIPTION
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

25.2.5 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar. The console port does not apply to all models.

1 Display menu 24.5 and enter “y” at the following screen.

Figure 167 System Maintenance: Backup Configuration

```
              Ready to backup Configuration via Xmodem.
              Do you want to continue (y/n):
```

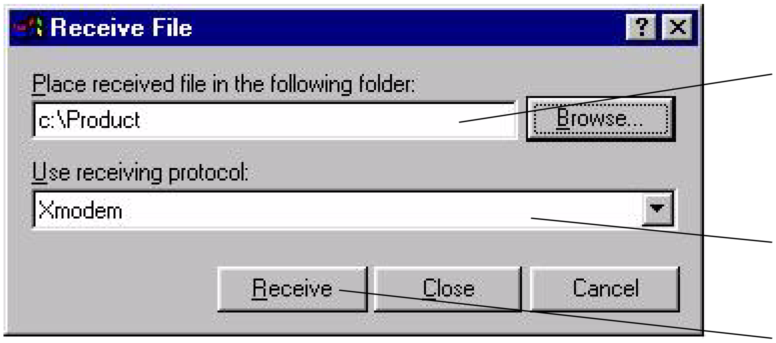
2 The following screen indicates that the Xmodem download has started.

Figure 168 System Maintenance: Starting Xmodem Download Screen

```
              You can enter ctrl-x to terminate operation any time.
              Starting XMODEM download...
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

Figure 169 Backup Configuration Example



Receive File

Place received file in the following folder: c:\Product

Use receiving protocol: Xmodem

Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

Figure 170 Successful Backup Confirmation Screen

```
              ** Backup Configuration completed. OK.
              ### Hit any key to continue.###
```

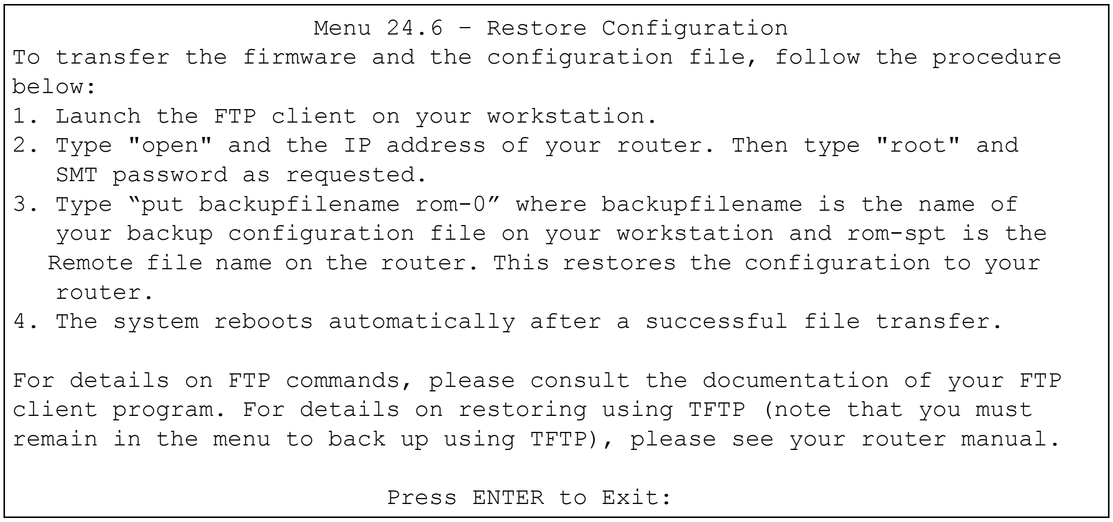
25.3 Restore Configuration

Menu 24.6 — System Maintenance – Restore Configuration allows you to restore the configuration via FTP or TFTP to your ZyXEL Device. The preferred method is FTP. Note that this function erases the current configuration before restoring the previous backup configuration; please do not attempt to restore unless you have a backup configuration stored on disk. To restore configuration using FTP or TFTP is the same as uploading the configuration file, please refer to the following sections on FTP and TFTP file transfer for more details. The ZyXEL Device restarts automatically after the file transfer is complete.

25.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

Figure 171 Menu 24.6 Restore Configuration



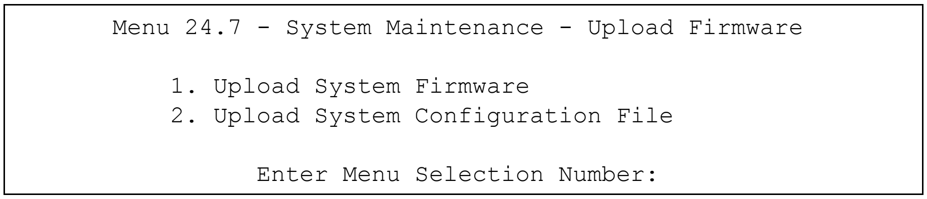
```
                     Menu 24.6 - Restore Configuration
To transfer the firmware and the configuration file, follow the procedure
below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Type “put backupfilename rom-0” where backupfilename is the name of
   your backup configuration file on your workstation and rom-spt is the
  Remote file name on the router. This restores the configuration to your
   router.
4. The system reboots automatically after a successful file transfer.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on restoring using TFTP (note that you must
remain in the menu to back up using TFTP), please see your router manual.

                          Press ENTER to Exit:
```

25.4 Uploading Firmware and Configuration Files

Menu 24.7 – System Maintenance – Upload Firmware allows you to upgrade the firmware and the configuration file.

WARNING! PLEASE WAIT A FEW MINUTES FOR RESTART AFTER FIRMWARE OR CONFIGURATION FILE UPLOAD. INTERRUPTING THE UPLOAD PROCESS MAY PERMANENTLY DAMAGE YOUR DEVICE.

Figure 172 Menu 24.7 System Maintenance: Upload Firmware



```
        Menu 24.7 - System Maintenance - Upload Firmware

            1. Upload System Firmware
            2. Upload System Configuration File

                  Enter Menu Selection Number:
```

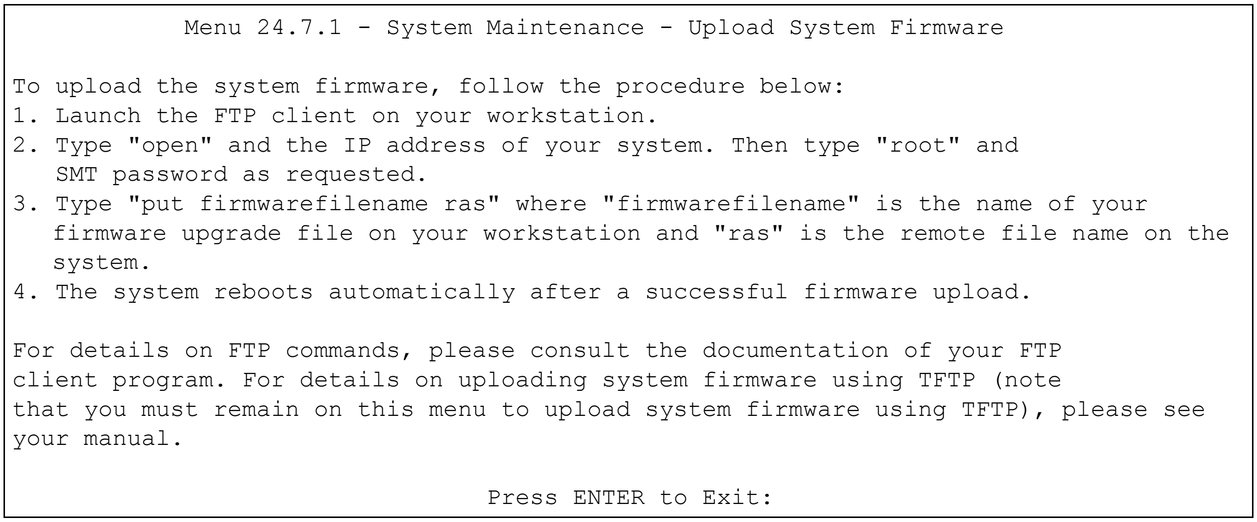
The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

25.4.1 Firmware Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyXEL Device, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 173 Menu 24.7.1 System Maintenance: Upload System Firmware

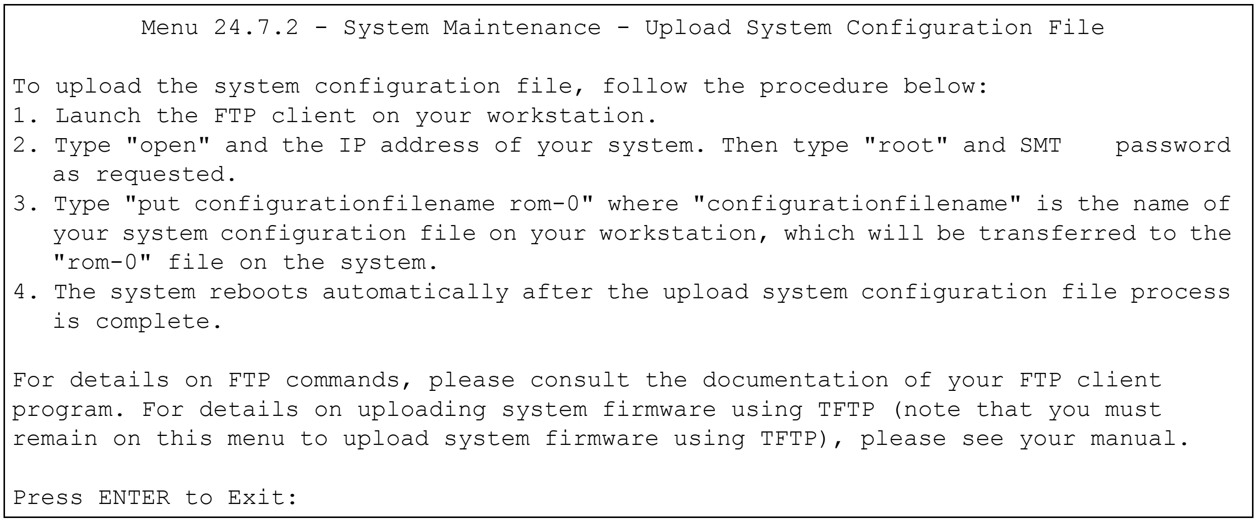


```
            Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put firmwarefilename ras" where "firmwarefilename" is the name of your
   firmware upgrade file on your workstation and "ras" is the remote file name on the
   system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP), please see
your manual.

                                 Press ENTER to Exit:
```

25.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 174 Menu 24.7.2 System Maintenance: Upload System Configuration File



```
         Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and SMT    password
   as requested.
3. Type "put configurationfilename rom-0" where "configurationfilename" is the name of
   your system configuration file on your workstation, which will be transferred to the
   "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration file process
   is complete.

For details on FTP commands, please consult the documentation of your FTP client
program. For details on uploading system firmware using TFTP (note that you must
remain on this menu to upload system firmware using TFTP), please see your manual.

Press ENTER to Exit:
```

To transfer the firmware and the configuration file, follow these examples:

25.4.3 Using the FTP command from the DOS Prompt Example

1 Launch the FTP client on your computer.

2 Enter “open” and the IP address of your ZyXEL Device.

3 Press [ENTER] when prompted for a username.

4 Enter your management password as requested. The default is 1234.

5 Enter “bin” to set transfer mode to binary.

6 Use “put” to transfer files from the computer to the ZyXEL Device for example “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyXEL Device and renames it “ras”. Similarly “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyXEL Device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

7 Enter “quit” to exit the FTP prompt.

Figure 175 FTP Session Example

```
C:\>ftp
ftp> open 192.168.1.2
Connected to 192.168.1.2.
220 G-3000 FTP version 1.0 ready at Sat Jan  1
00:03:09 2000
User (192.168.1.2:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

More commands that you may find in third party FTP clients are listed earlier in this chapter.

25.4.4 TFTP File Upload

The ZyXEL Device also supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next:

1. Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter the command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.
5. Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the firmware is “ras” and the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyXEL Device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

25.4.5 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyXEL Device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyXEL Device).

Commands that you may see in third party TFTP clients are listed earlier in this chapter.

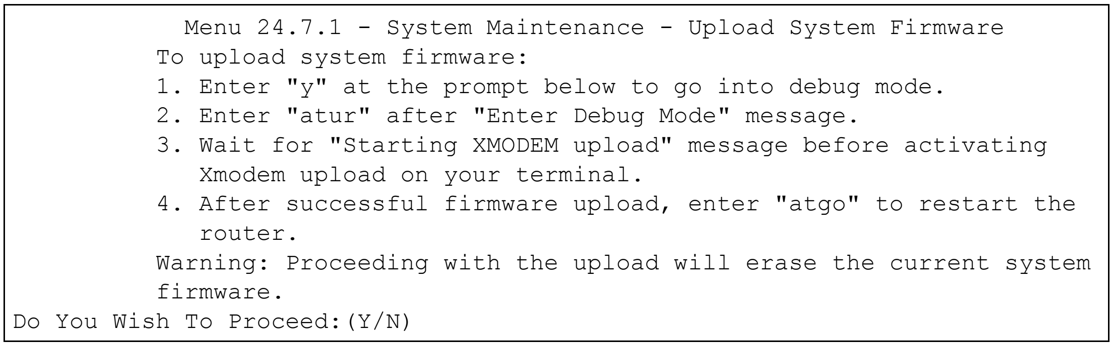
25.4.6 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyXEL Device. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyXEL Device via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload. The console port does not apply to all models.

25.4.7 Uploading Firmware File Via Console Port

Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 – System Maintenance – Upload System Firmware**, then follow the instructions as shown in the following screen. The console port does not apply to all models.

Figure 176 Menu 24.7.1 as seen using the Console Port



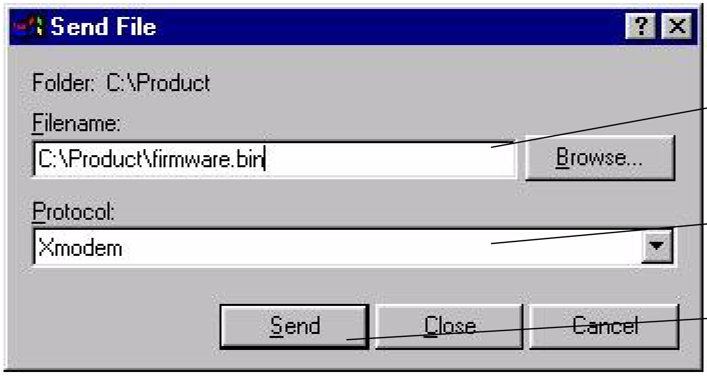
```
              Menu 24.7.1 - System Maintenance - Upload System Firmware
            To upload system firmware:
            1. Enter "y" at the prompt below to go into debug mode.
            2. Enter "atur" after "Enter Debug Mode" message.
            3. Wait for "Starting XMODEM upload" message before activating
               Xmodem upload on your terminal.
            4. After successful firmware upload, enter "atgo" to restart the
               router.
            Warning: Proceeding with the upload will erase the current system
            firmware.
Do You Wish To Proceed:(Y/N)
```

After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

25.4.8 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 177 Example Xmodem Upload



Send File

Folder: C:\Product

Filename: C:\Product\firmware.bin

Protocol: Xmodem

Type the firmware file's location, or click **Browse** to look for it.

Choose the **Xmodem** protocol.

Then click **Send**.

After the firmware upload process has completed, the ZyXEL Device will automatically restart.

25.4.9 Uploading Configuration File Via Console Port

The console port does not apply to all models.

1 Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 – System Maintenance – Upload System Configuration File**. Follow the instructions as shown in the next screen.

Figure 178 Menu 24.7.2 as seen using the Console Port

```
     Menu 24.7.2 - System Maintenance - Upload System Configuration File

          To upload system configuration file:
          1. Enter "y" at the prompt below to go into debug mode.
          2. Enter "atlc" after "Enter Debug Mode" message.
          3. Wait for "Starting XMODEM upload" message before activating
             Xmodem upload on your terminal.
          4. After successful firmware upload, enter "atgo" to restart the
             system.

          Warning:
          1. Proceeding with the upload will erase the current
             configuration file.
          2. The system's console port speed (Menu 24.2.2) may change
             when it is restarted; please adjust your terminal's speed
             accordingly. The password may change (menu 23), also.
          3. When uploading the DEFAULT configuration file, the console
             port speed will be reset to 9600 bps and the password to
             "1234".
                          Do You Wish To Proceed:(Y/N)
```

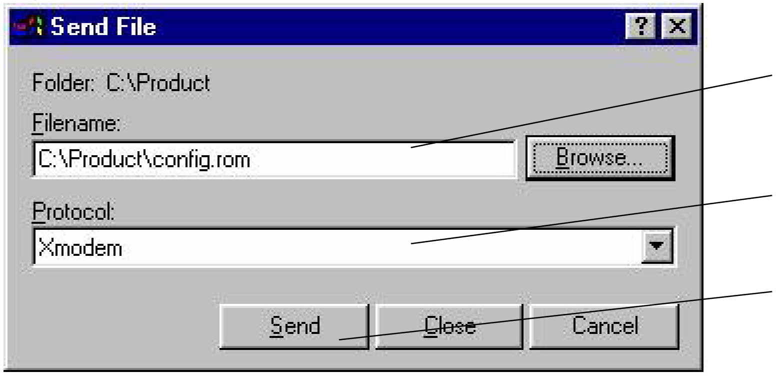
2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter "atgo" to restart the ZyXEL Device.

25.4.10 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 179 Example Xmodem Upload



Folder: C:\Product

Filename:
C:\Product\config.rom

Protocol:
Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

After the configuration upload process has completed, restart the ZyXEL Device by entering "atgo"

26

System Maintenance and Information

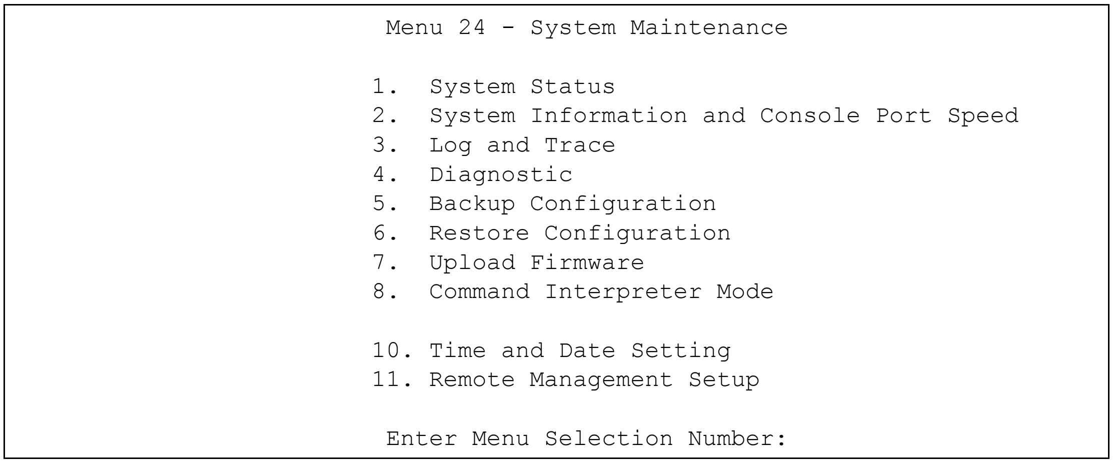
This chapter leads you through SMT menus 24.8 and 24.10.

26.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 – System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type "exit" to return to the SMT main menu when finished.

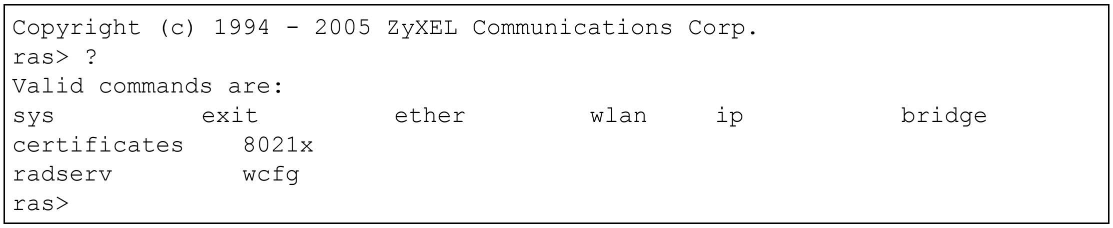
Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Figure 180 Menu 24 System Maintenance



```
                          Menu 24 - System Maintenance

                         1.  System Status
                         2.  System Information and Console Port Speed
                         3.  Log and Trace
                         4.  Diagnostic
                         5.  Backup Configuration
                         6.  Restore Configuration
                         7.  Upload Firmware
                         8.  Command Interpreter Mode

                         10. Time and Date Setting
                         11. Remote Management Setup

                          Enter Menu Selection Number:
```

Figure 181 Valid CI Commands



```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit         ether         wlan     ip           bridge
certificates    8021x
radserv         wcfg
ras>
```

26.1.1 Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

  For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

26.1.2 Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

26.1.3 Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password.

Table 88 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
sys pwderrtm	This command displays the brute-force guessing password protection settings.
sys pwderrtm 0	This command turns off the password’s protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
sys pwderrtm N	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

26.1.3.1 Configuring Brute-Force Password Guessing Protection: Example

```
sys pwderrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

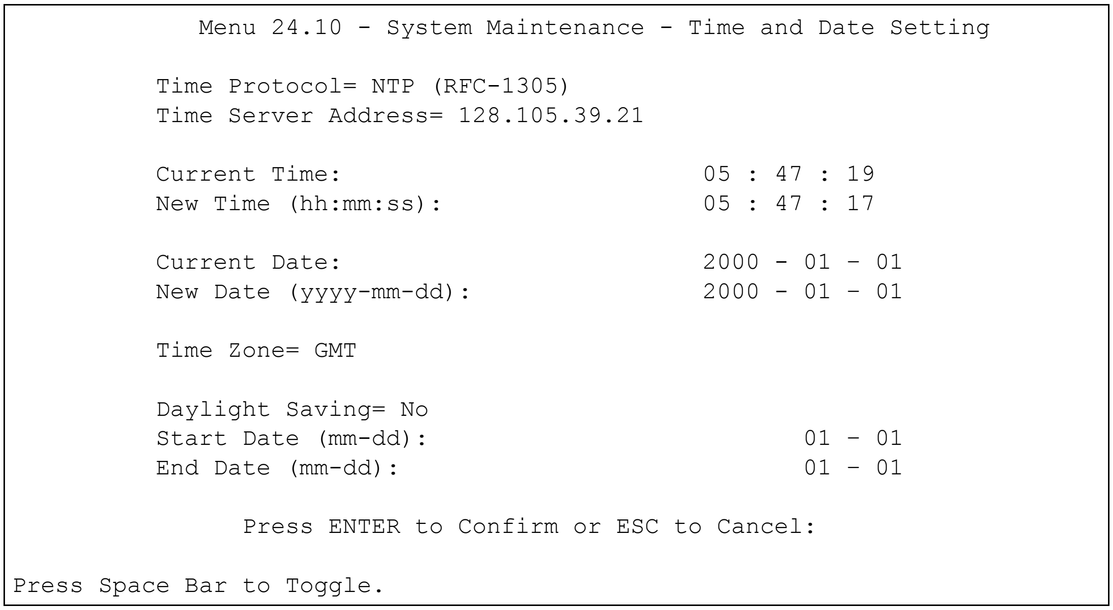
26.2 Time and Date Setting

The ZyXEL Device keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyXEL Device. Menu 24.10 allows you to update the time and date settings of your ZyXEL Device. The updated time is then displayed in the ZyXEL Device error logs.

1 Select menu 24 in the main menu to open **Menu 24 – System Maintenance**.

2 Then enter 10 to go to **Menu 24.10 – System Maintenance – Time and Date Setting** to update the time and date settings of your ZyXEL Device as shown in the following screen.

Figure 182 Menu 24.10 System Maintenance: Time and Date Setting



```
               Menu 24.10 - System Maintenance - Time and Date Setting

          Time Protocol= NTP (RFC-1305)
          Time Server Address= 128.105.39.21

          Current Time:                          05 : 47 : 19
          New Time (hh:mm:ss):                   05 : 47 : 17

          Current Date:                          2000 - 01 - 01
          New Date (yyyy-mm-dd):                 2000 - 01 - 01

          Time Zone= GMT

          Daylight Saving= No
          Start Date (mm-dd):                           01 - 01
          End Date (mm-dd):                             01 - 01

                Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

The following table describes the fields in this menu.

Table 89 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Time Protocol	Enter the time service protocol that your time server sends when you turn on the ZyXEL Device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None**. The default, enter the time manually.
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.

Table 89 System Maintenance: Time and Date Setting

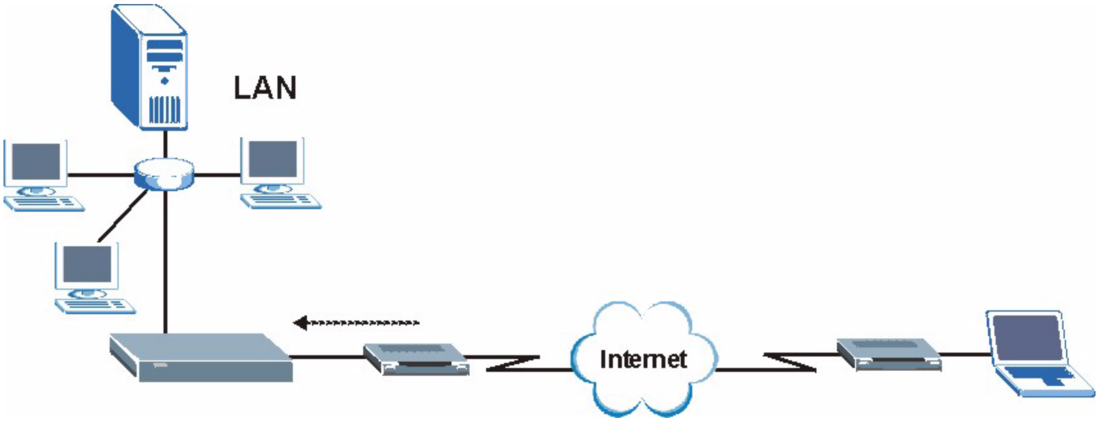
FIELD	DESCRIPTION
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose **Yes**.
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

26.3 Remote Management Setup

26.3.1 Telnet

You can configure your ZyXEL Device for remote Telnet access as shown next.

Figure 183 Telnet Configuration on a TCP/IP Network



26.3.2 FTP

You can upload and download ZyXEL Device firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

26.3.3 Web

You can use the ZyXEL Device’s embedded web configurator for configuration and file management. See the online help for details.

26.3.4 Remote Management Setup

Remote management setup is for managing Telnet, FTP and Web services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

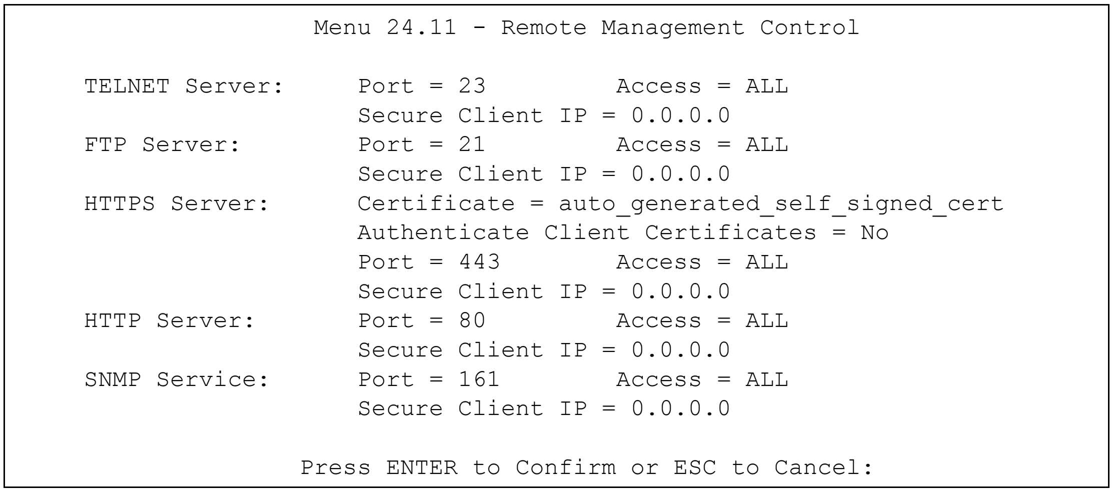
You can manage your ZyXEL Device from a remote location via:

Internet (**WLAN only**), the **LAN only**, **All** (LAN and WLAN) or **Disable** (neither).

If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

Enter 11, from menu 24, to display **Menu 24.11 - Remote Management Control** (shown next)

Figure 184 Menu 24.11 Remote Management Control



```
                    Menu 24.11 - Remote Management Control

     TELNET Server:      Port = 23         Access = ALL
                         Secure Client IP = 0.0.0.0
     FTP Server:         Port = 21         Access = ALL
                         Secure Client IP = 0.0.0.0
     HTTPS Server:       Certificate = auto_generated_self_signed_cert
                         Authenticate Client Certificates = No
                         Port = 443        Access = ALL
                         Secure Client IP = 0.0.0.0
     HTTP Server:        Port = 80         Access = ALL
                         Secure Client IP = 0.0.0.0
     SNMP Service:       Port = 161        Access = ALL
                         Secure Client IP = 0.0.0.0

                   Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 90 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION
TELNET Server: FTP Server: HTTPS Server: HTTP Server: SNMP Service:	Each of these read-only labels denotes a server or service that you may use to remotely manage the ZyXEL Device.
Port	This field shows the port number for the remote management service. You can change the port number for a service if needed, but you must use the same port number to use that service for remote management.
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**.

Table 90 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyXEL Device. Enter an IP address to restrict access to a client with a matching IP address.
Certificate	This field displays the name used to identify this certificate. The ZyXEL Device has an automatically generated self signed certificate by default. The factory default certificate is common to all ZyXEL Device's that use certificates. You can replace the certificate when you log into the ZyXEL Device (see Section 2.2 on page 41) or you can use the Certificates configuration screen (see Chapter 13 on page 147).
Authenticate Client Certificates	Select **Yes** by pressing [SPACE BAR]. The ZyXEL Device uses one of the certificates listed in the My Certificates screen to authenticate each wireless client. The exact certificate used depends on the certificate information configured on the wireless client.
Once you have filled in this menu, press [ENTER] to save your configuration, or press [ESC] to cancel.	

26.3.5 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1 You have disabled that service in menu 24.11.

2 The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.

3 There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.

4 There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

26.4 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your ZyXEL Device will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

27

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

27.1 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.

27.2 ZyXEL Device Access and Login

? I forgot the IP address for the ZyXEL Device.

1 The default IP address is **192.168.1.2**.

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

3 If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 43.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 43.

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 192.168.1.2.
   - If you changed the IP address (Section 10.3 on page 124), 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.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Section 27.1 on page 255.

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 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 your Quick Start Guide.

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 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.
- You may also need to clear your Internet browser's cache. In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Option**s screen. In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it.
- If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address). In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.

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

1 Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.
2 You cannot log in to the web configurator while someone is using the SMT or Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.
3 Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.
4 If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 43.

I cannot access the SMT.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

27.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 27.1 on page 255.
2 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3 If you are trying to access the Internet wirelessly, make sure the wireless settings on the wireless client are the same as the settings on the AP.
4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5 If the problem continues, contact your ISP.

? I cannot access the Internet anymore. I had access to the Internet (with the 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.
2 Reboot the ZyXEL 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. 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 is weak, 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 (microwaves, other wireless networks, and so on).
3 Reboot the ZyXEL Device.
4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

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

PART IV Appendices and Index

A

Product Specifications

Hardware and Firmware Specifications

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

Table 91 Hardware Specifications

Power Specification	G-3000: 12 V DC, 1.2 A G-3000H: 12 V DC, 1.5 A
Reset button	Returns all settings to their factory defaults.
Ethernet Port	• 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.
Extension Card Slot	The G-3000 has an extension card slot for adding a second wireless LAN adapter.
Console Port	The G-3000 has a PS/2 console port.
Power over Ethernet (PoE)	IEEE 802.3af compliant.
Wireless LAN Output Power	Here are the power ranges represented by the percentages to which you can set the output power. G-3000: 100%(Full Power): <11b>17dBm/<11g>13dBm (<11b>50mW/<11g>20mW), 50%: <11b>15dBm/<11g>11dBm (<11b>32mW/<11g>12.6mW), 25%: <11b>13dBm/<11g>9dBm (<11b>20mW/<11g>7.9mW), 12.5%: <11b>11dBm/<11g>7dBm (<11b>12.6mW/<11g>5mW), G-3000H: • 100%(Full Power) <11b>17dBm/<11g>13dBm (<11b>50mW/<11g>20mW), • 50% <11b>15dBm/<11g>11dBm (<11b>32mW/<11g>12.6mW), • 25% <11b>13dBm/<11g>9dBm (<11b>20mW/<11g>7.9mW), • 12.5% <11b>11dBm/<11g>7dBm (<11b>12.6mW/<11g>5mW).
External Antenna	Two 2dBi (Max) Dual detachable antennas with reverse SMA connectors. When you face the front of the ZyXEL Device, the antenna on the right is the main antenna. The main antenna can both transmit and receive. The antenna on the left only receives.
Operation Temperature	G-3000: 0 ~ 50 ° C G-3000H: 5° C ~ 50° C
Storage Temperature	G-3000 -30: ~ 60 ° C G-3000H: -20° C ~ 55° C
Operation Humidity	G-3000: 20% to 95% (Non-condensing) G-3000H: 10% to 90% (Non-condensing)

Table 91 Hardware Specifications

Storage Humidity	G-3000: 20% to 95% (Non-condensing) G-3000H: 5% to 95% (Non-condensing)
Dimensions (W x D x H)	G-3000: 212.5mm (L) x 138.5mm (W) x 52mm (H) G-3000H: 152 mm (L) x 92 mm (W) x 42 mm (H)
Distance between the centers of wall-mounting holes on the device's back.	G-3000: 80 mm G-3000H: 60 mm
Screw size for wall-mounting	6mm ~ 8mm (0.24" ~ 0.31") head width.

Table 92 Firmware Specifications

FEATURE	DESCRIPTION
Wireless LAN Standards	IEEE 802.11b, IEEE 802.11g, Wi-Fi certificate
Wireless Security	WEP, WPA(2), WPA(2)-PSK, 802.1x
Internal RADIUS Server	The G-3000 has a built-in RADIUS server that can authenticate wireless clients or other AP's in other wireless networks. The G-3000 can function as an AP and as a RADIUS server at the same time.
Layer 2 isolation	Prevents wireless clients associated with your ZyXEL Device from communicating with other wireless clients, APs, computers or routers in a network.
Multiple ESSID (MESSID)	MESSID mode allows the ZyXEL Device to operate up to 8 different wireless networks (ESSs) simultaneously, each with independently-configurable wireless and security settings.
VLAN	802.1Q VLAN tagging.
STP (Spanning Tree Protocol) / RSTP (Rapid STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP-compliant bridges in your network to ensure that only one path exists between any two stations on the network.
WMM QoS	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic.
Certificates	The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.
SSL Passthrough	SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https" instead of "http". The ZyXEL Device allows SSL connections to take place through the ZyXEL Device.
MAC Address Filter	Your ZyXEL Device checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.
Wireless Association List	With the wireless association list, you can see the list of the wireless stations that are currently using the ZyXEL Device to access your wired network.
Logging and Tracing	Built-in message logging and packet tracing.
Embedded FTP and TFTP Servers	The embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.

Table 92 Firmware Specifications

FEATURE	DESCRIPTION
Auto Configuration	Administrators can use text configuration files to configure the wireless LAN settings for multiple APs. The AP can automatically get a configuration file from a TFTP server at start up or after renewing DHCP client information.
Administrator Authentication on RADIUS	This feature lets a RADIUS server authenticate management logins to the device. This is useful if you need to regularly change a password that you use to manage several devices.
SNMP	SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manger station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

Power Adaptor Specifications

G-3000 Power Adaptor Specifications

Table 93 G-3000 NORTH AMERICAN PLUG STANDARDS

AC Power Adaptor Model	AD48-1201200DUY
Input Power	AC120Volts/60Hz/0.25A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1950, CSA C22.2 No.234-M90)

Table 94 G-3000 NORTH AMERICAN PLUG STANDARDS

AC Power Adaptor Model	DV-121A2-5720
Input Power	AC120Volts/60Hz/27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223-M91)

Table 95 G-3000 EUROPEAN PLUG STANDARDS

AC Power Adaptor Model	AD-1201200DV
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950)

Table 96 G-3000 United Kingdom PLUG STANDARDS

AC Power Adaptor Model	AD-1201200DK
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950, BS7002)

Table 97 G-3000 Japan PLUG STANDARDS

AC Power Adaptor Model	JOD-48-1124
Input Power	AC100Volts/ 50/60Hz/ 27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	T-Mark (Japan Dentori)

Table 98 G-3000 Australia and New Zealand plug standards

AC Power Adaptor Model	AD-1201200DS or AD-121200DS
Input Power	AC240Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	NATA (AS 3260)

G-3000H Power Adaptor Specifications

Table 99 G-3000H North American Plug Standards

AC Power Adaptor Model	ADS6818-1812-W 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5A, 18W
Power Consumption	6 W Max
Safety Standards	UL, CUL (UL60950 Third Edition, CSA C22.2 No. 60950)

Table 100 G-3000H European Plug Standards

AC Power Adaptor Model	ADS6818-1812-B 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	TUV-GS, CE (EN 60950)

Table 101 G-3000H United Kingdom Plug Standards

AC Power Adaptor Model	ADS6818-1812-D 1215
Input Power	100~240 Volts AC, 50~60 Hz,0.5 A

Table 101 G-3000H United Kingdom Plug Standards

Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	TUV-GS (BS EN 60950)

Table 102 G-3000H Australia and New Zealand Plug Standards

AC Power Adaptor Model	ADS6818-1812-A 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	DOFT (AS/NZS 60950, AS/NZSB 3112:1-2)

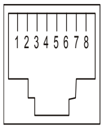
Power over Ethernet Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.-7.

Table 103 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Table 104 Power over Ethernet Injector RJ-45 Port Pin Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT
	1	Output Transmit Data +
	2	Output Transmit Data -
	3	Receive Data +
	4	Power +
	5	Power +
	6	Receive Data -
	7	Power -
	8	Power -

B

Setting up Your Computer's IP Address

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

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

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

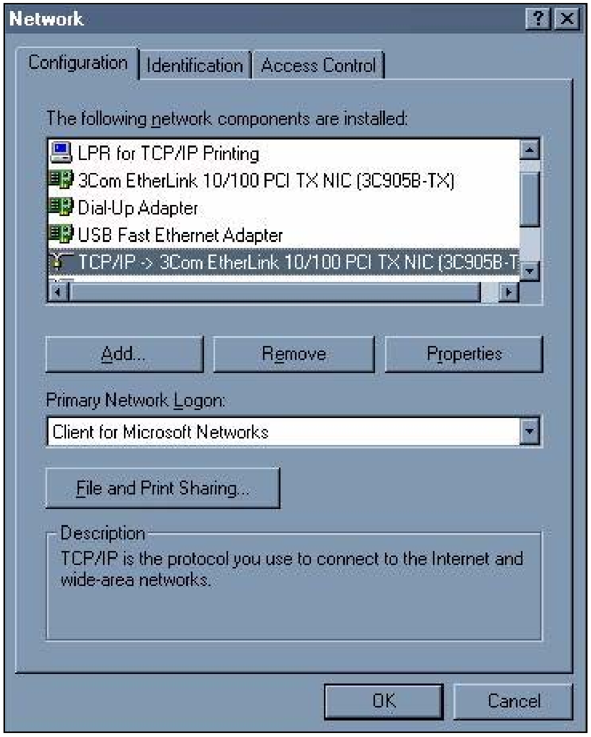
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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

Windows 95/98/Me

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

Figure 185 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

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

Primary Network Logon:

Client for Microsoft Networks

Description

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

Installing Components

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

If you need the adapter:

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

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

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

If you need TCP/IP:

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

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

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

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

If you need Client for Microsoft Networks:

1 Click **Add**.

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

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

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

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

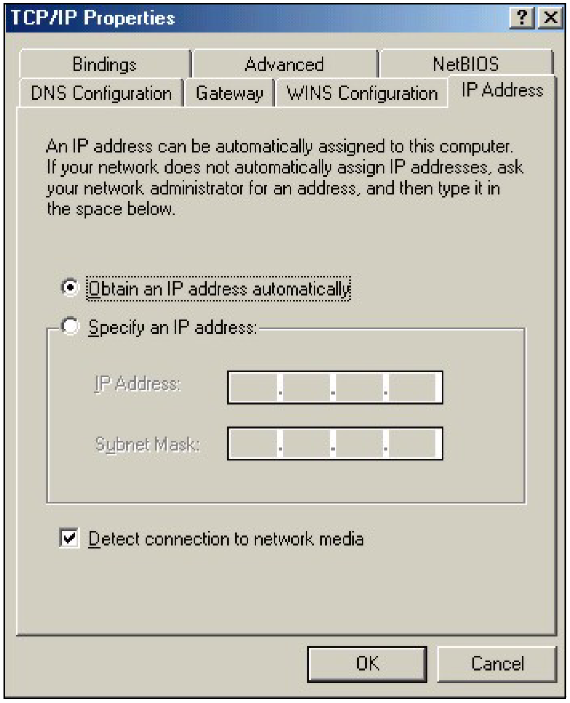
Configuring

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

2 Click the **IP Address** tab.

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

Figure 186 Windows 95/98/Me: TCP/IP Properties: IP Address



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

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

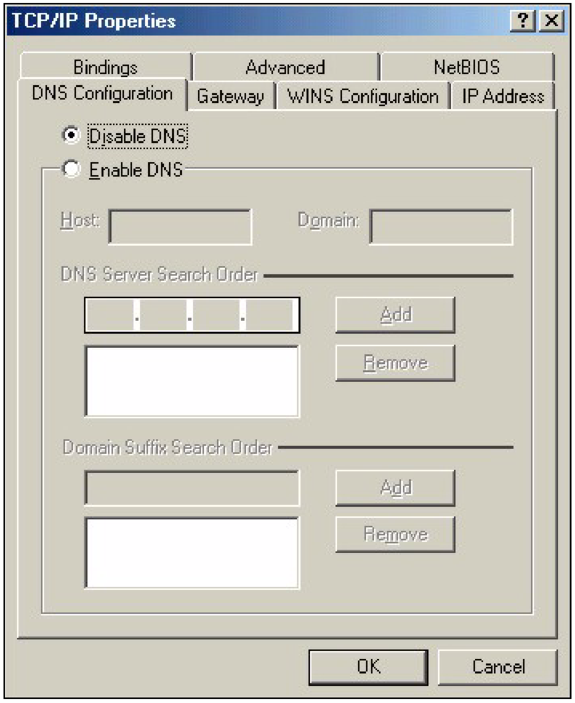
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

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

Figure 187 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



Chosen setting: ● Disable DNS

4 Click the **Gateway** tab.

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

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

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

7 Turn on your ZyXEL Device and restart your computer when prompted.

Verifying Settings

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

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

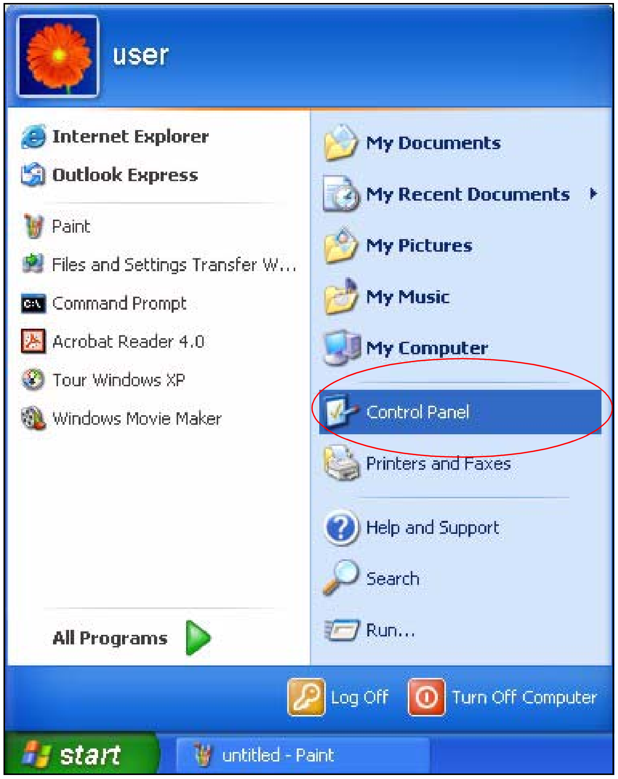
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

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

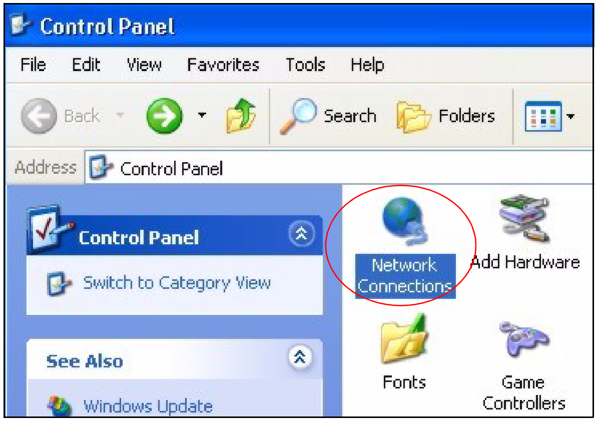
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 188 Windows XP: Start Menu



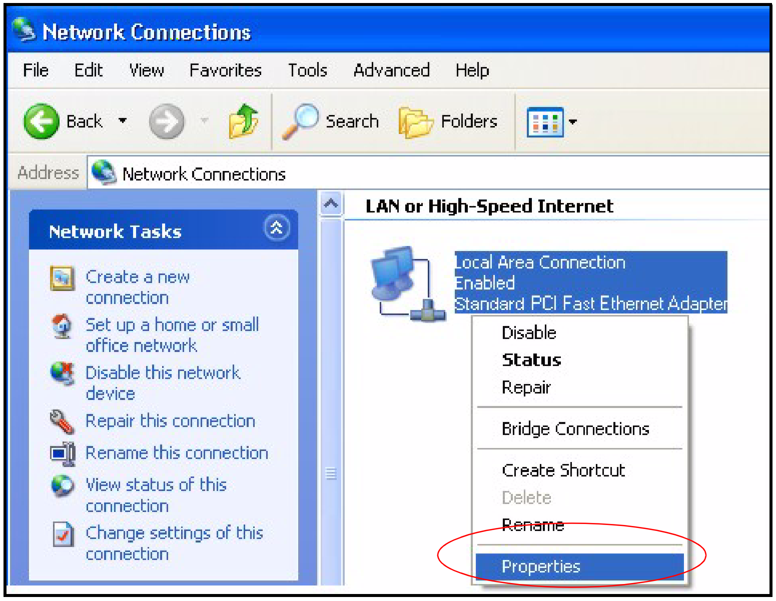
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 189 Windows XP: Control Panel



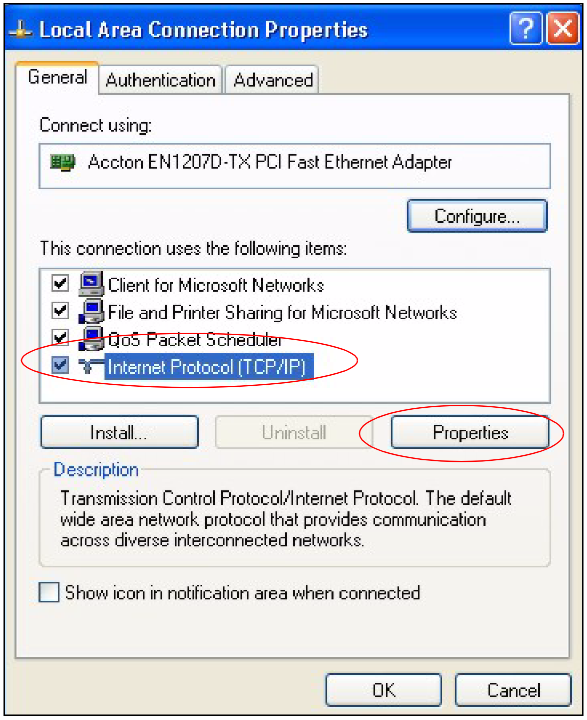
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 190 Windows XP: Control Panel: Network Connections: Properties


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

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

Figure 191 Windows XP: Local Area Connection Properties


Local Area Connection Properties
General Authentication Advanced
Configure...
Install... Uninstall Properties
OK Cancel

Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

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

Description

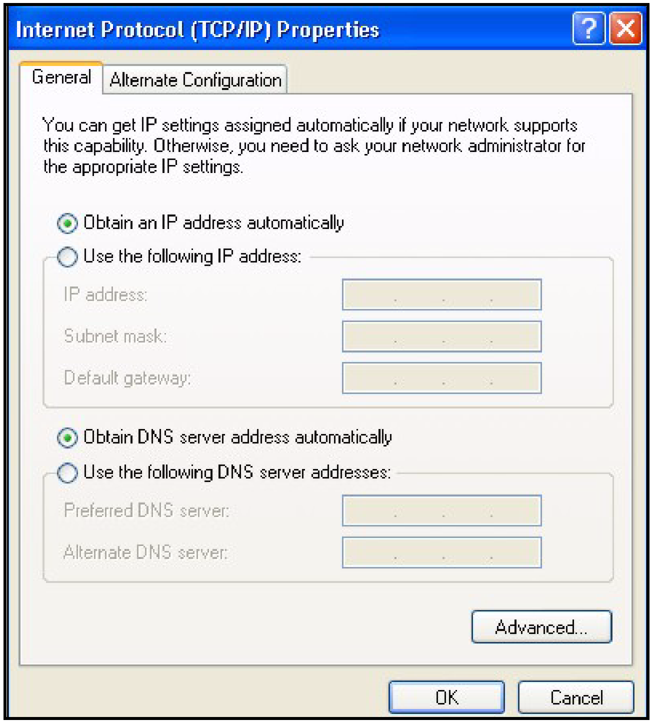
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

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

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

Figure 192 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

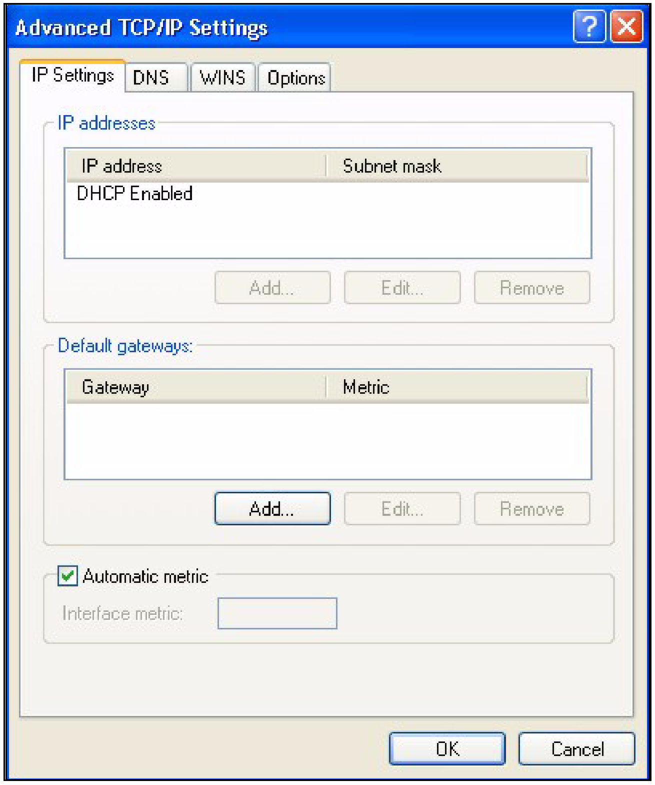
Alternate DNS server: . . .

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

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

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

Figure 193 Windows XP: Advanced TCP/IP Properties

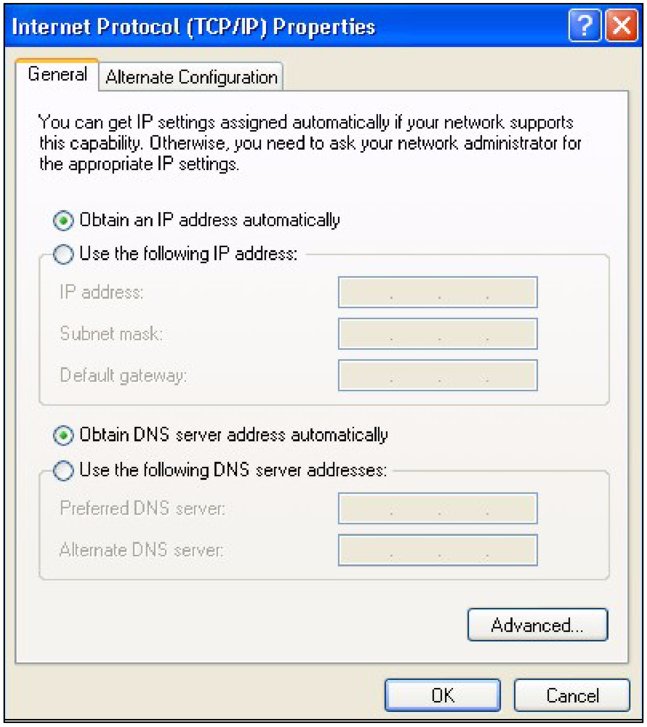


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

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

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

Figure 194 Windows XP: Internet Protocol (TCP/IP) Properties



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

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

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

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

Verifying Settings

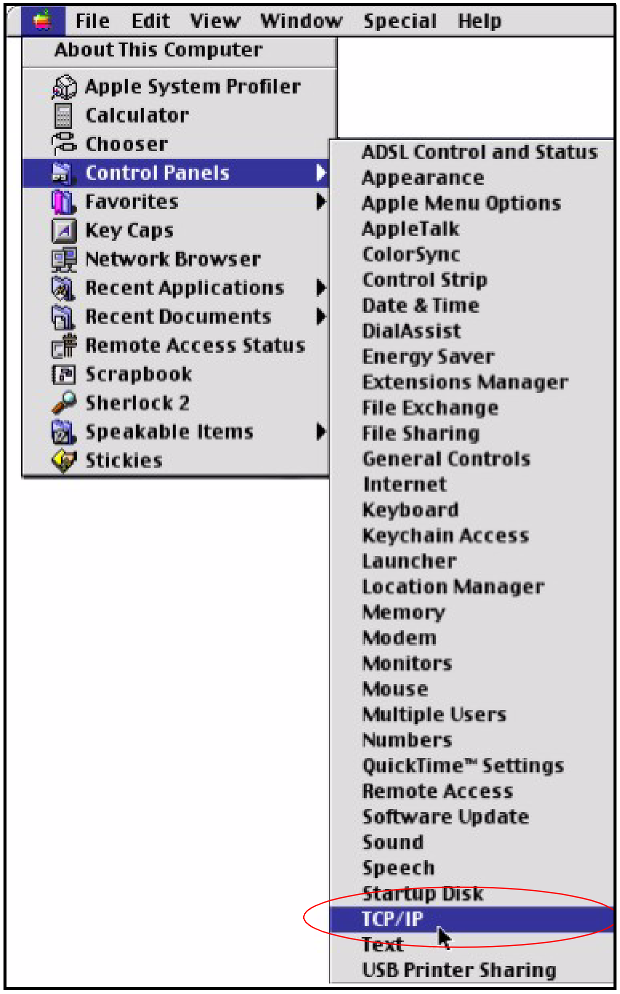
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

Macintosh OS 8/9

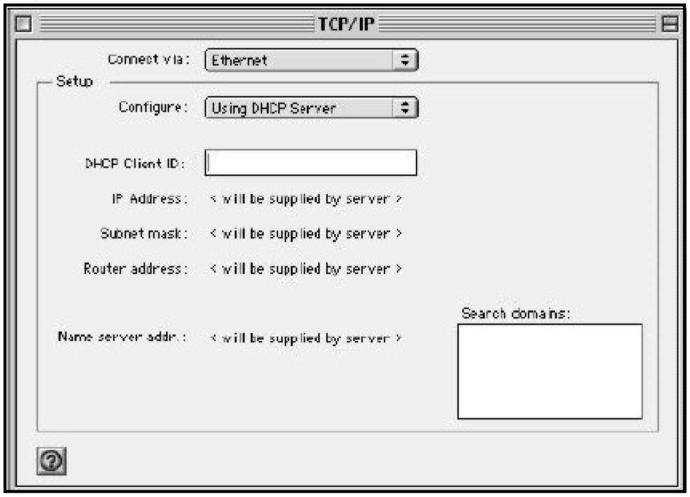
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 195 Macintosh OS 8/9: Apple Menu



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

Figure 196 Macintosh OS 8/9: TCP/IP


TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

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

Search domains:

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

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

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

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

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

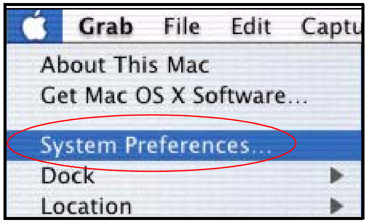
Verifying Settings

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

Macintosh OS X

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

Figure 197 Macintosh OS X: Apple Menu

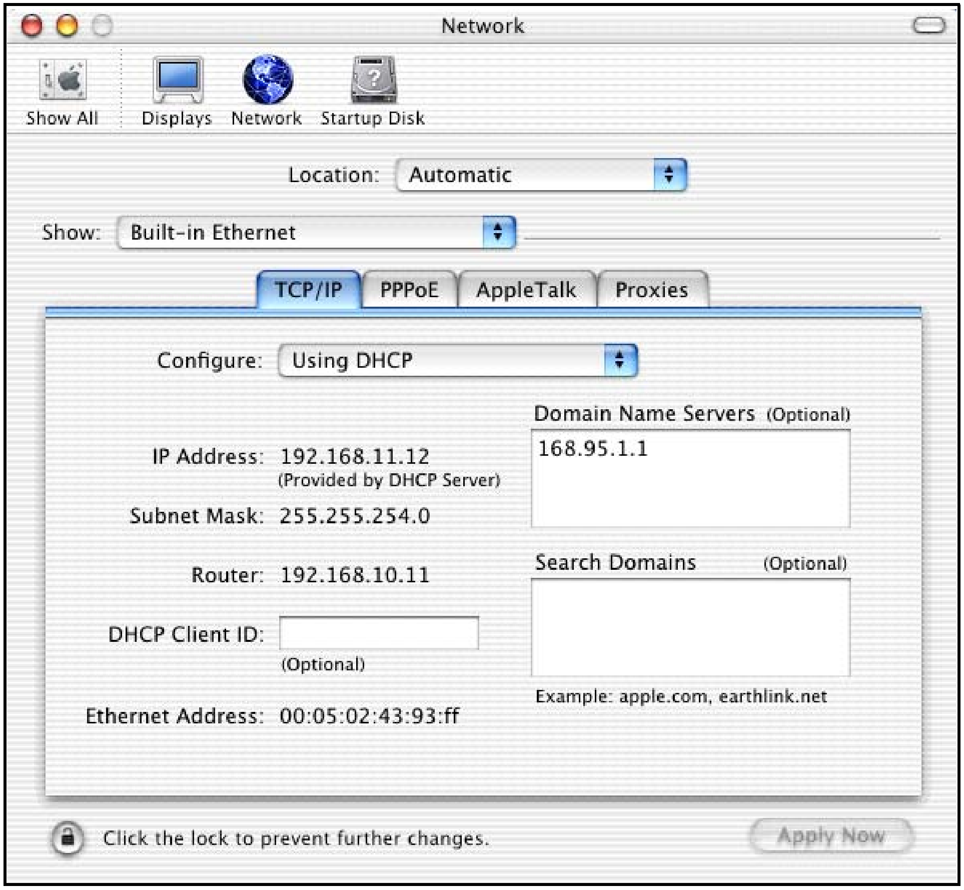


2 Click **Network** in the icon bar.

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

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

Figure 198 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

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

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

4 For statically assigned settings, do the following:
- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

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

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

Verifying Settings

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

Linux

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

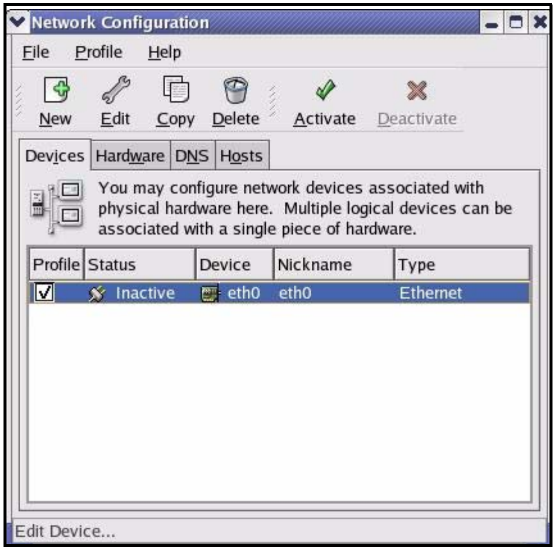
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

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

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

Figure 199 Red Hat 9.0: KDE: Network Configuration: Devices



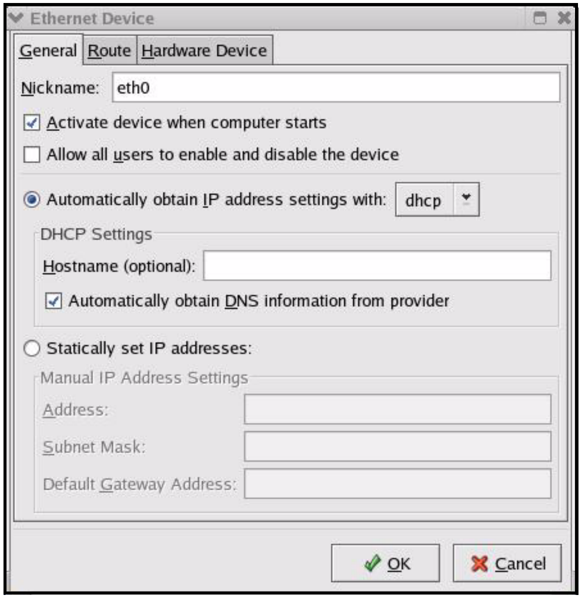
You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

Edit Device...

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

Figure 200 Red Hat 9.0: KDE: Ethernet Device: General



Nickname: eth0

☑ Activate device when computer starts

☐ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

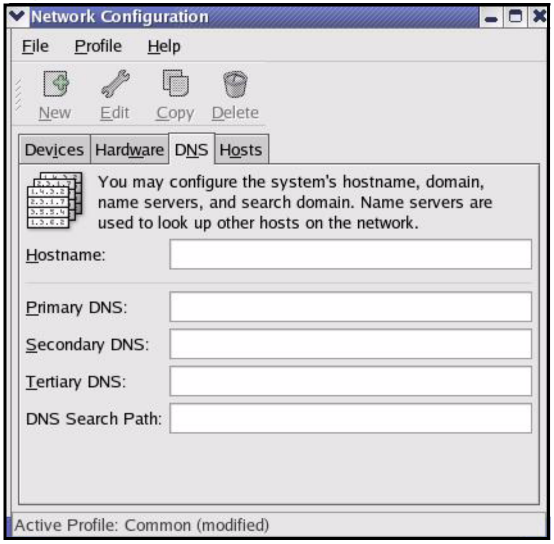
Default Gateway Address:

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

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

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

Figure 201 Red Hat 9.0: KDE: Network Configuration: DNS



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

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

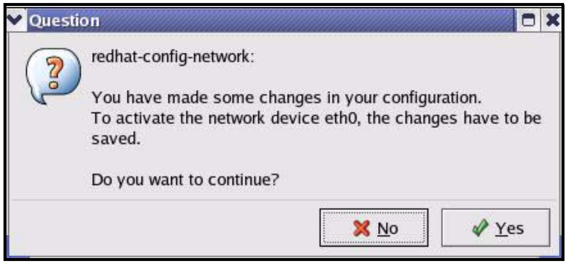
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

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

Figure 202 Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

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

Do you want to continue?

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

Using Configuration Files

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

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

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 203 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 204 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 205 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

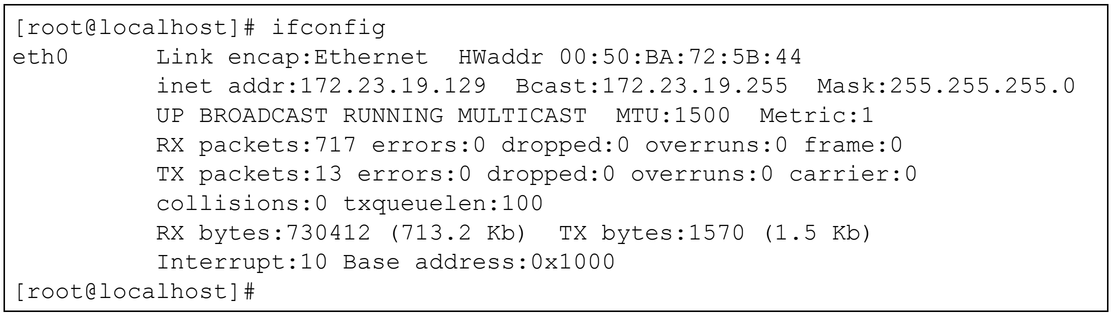
Figure 206 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                    [OK]
Shutting down loopback interface:                [OK]
Setting network parameters:                      [OK]
Bringing up loopback interface:                  [OK]
Bringing up interface eth0:                      [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 207 Red Hat 9.0: Checking TCP/IP Properties



```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

C

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

Introduction to IP Addresses

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

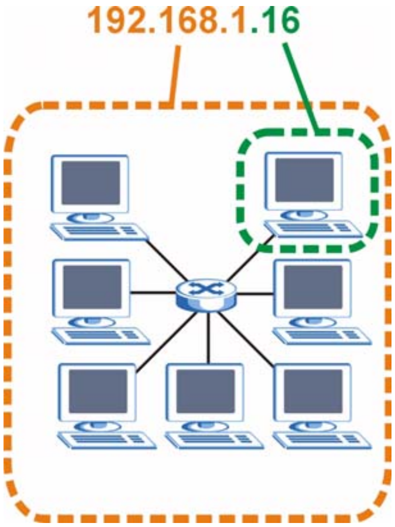
Structure

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

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

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

Figure 208 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 105 Subnet Masks

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

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

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

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

Table 106 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 107 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 108 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 108 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

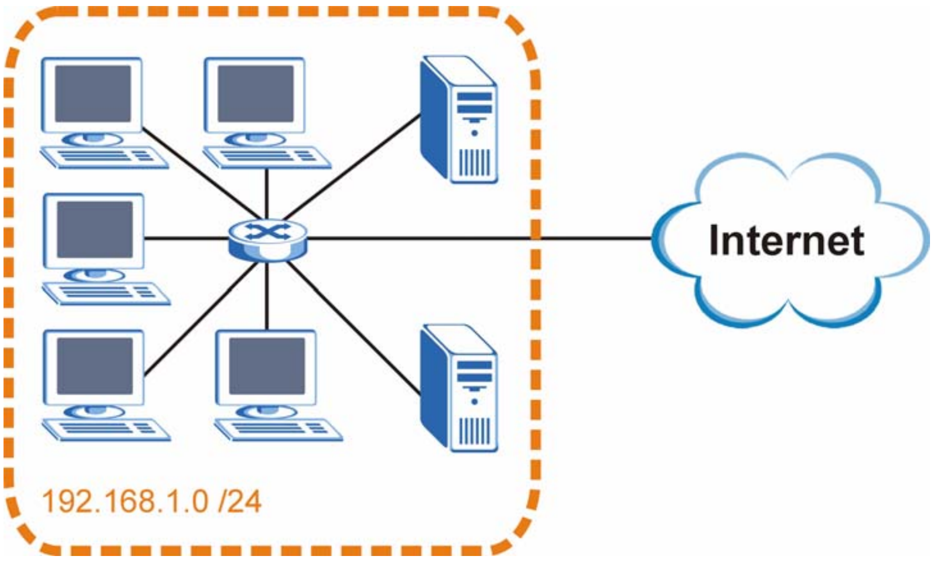
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 209 Subnetting Example: Before Subnetting

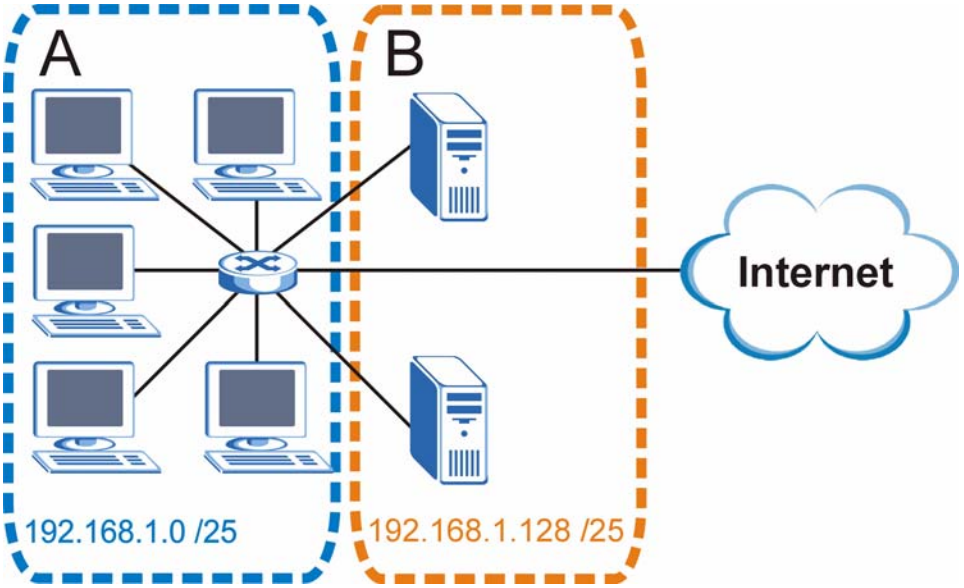


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 210 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 – 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 109 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 110 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 111 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 112 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 113 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 113 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 114 24-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 115 16-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 115 16-bit Network Number Subnet Planning (continued)

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

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

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

Private IP Addresses

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

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

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

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

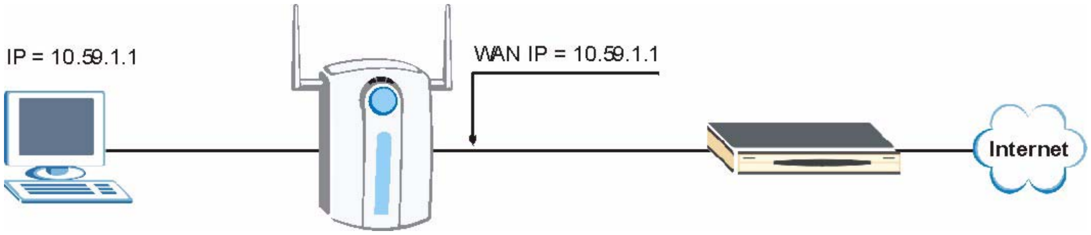
IP Address Assignment Conflicts

This appendix describes situations where IP address conflicts may occur. Subscribers with duplicate IP addresses will not be able to access the Internet.

Case A: The ZyXEL Device is using the same LAN and WAN IP addresses

The following figure shows an example where the ZyXEL Device is using a WAN IP address that is the same as the IP address of a computer on the LAN.

Figure 211 IP Address Conflicts: Case A

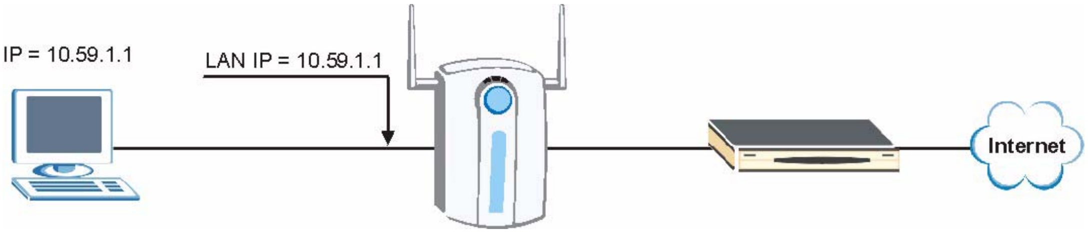


You must set the ZyXEL Device to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyXEL Device. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyXEL Device use a public WAN IP address.

Case B: The ZyXEL Device LAN IP address conflicts with the DHCP client IP address

In the following figure, the ZyXEL Device is acting as a DHCP server. The ZyXEL Device assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

Figure 212 IP Address Conflicts: Case B

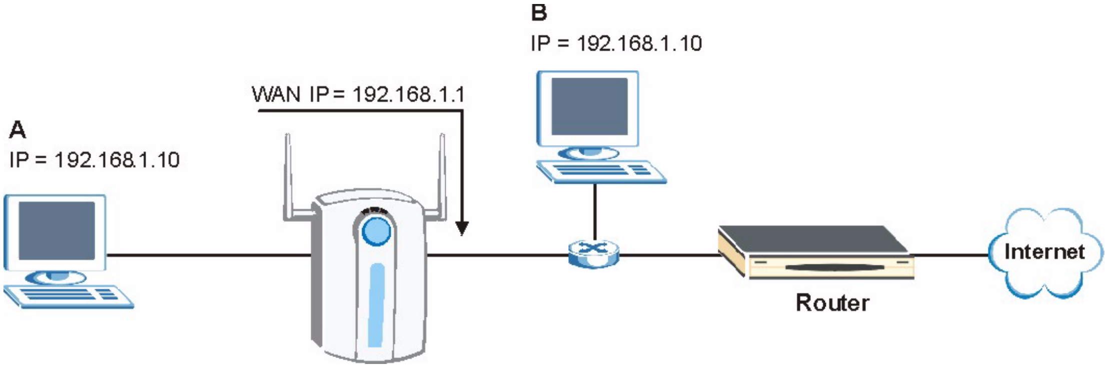


To solve this problem, make sure the ZyXEL Device LAN IP address is not in the DHCP IP address pool.

Case C: The Subscriber IP address is the same as the IP address of a network device

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the ZyXEL Device.

Figure 213 IP Address Conflicts: Case C



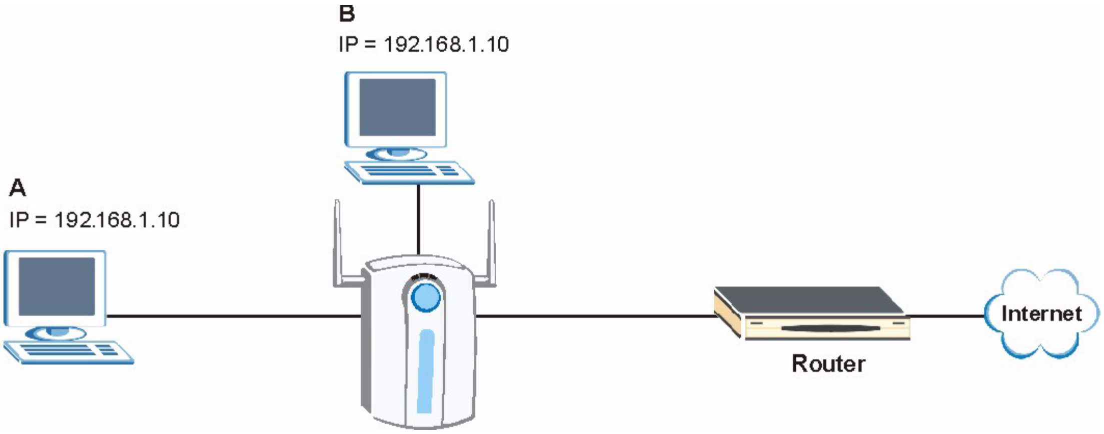
You must set the ZyXEL Device to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyXEL Device. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyXEL Device uses a public WAN IP address.

Case D: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the ZyXEL Device allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the ZyXEL Device DHCP server assigns to another subscriber acting as a DHCP client.

In this case, the subscribers are not able to access the Internet.

Figure 214 IP Address Conflicts: Case D



This problem can be solved by adding a VLAN-enabled switch or set the computers to obtain IP addresses dynamically.

E

Wireless LANs

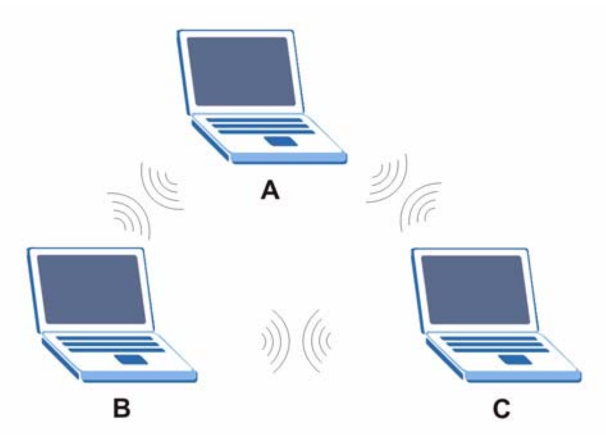
Wireless LAN Topologies

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

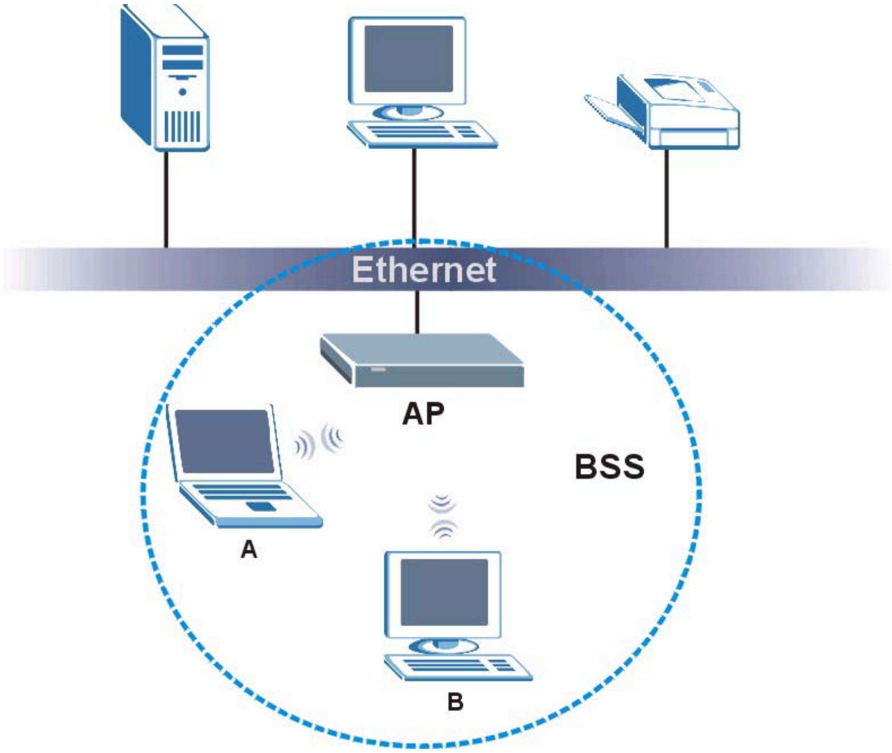


BSS

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 216 Basic Service Set



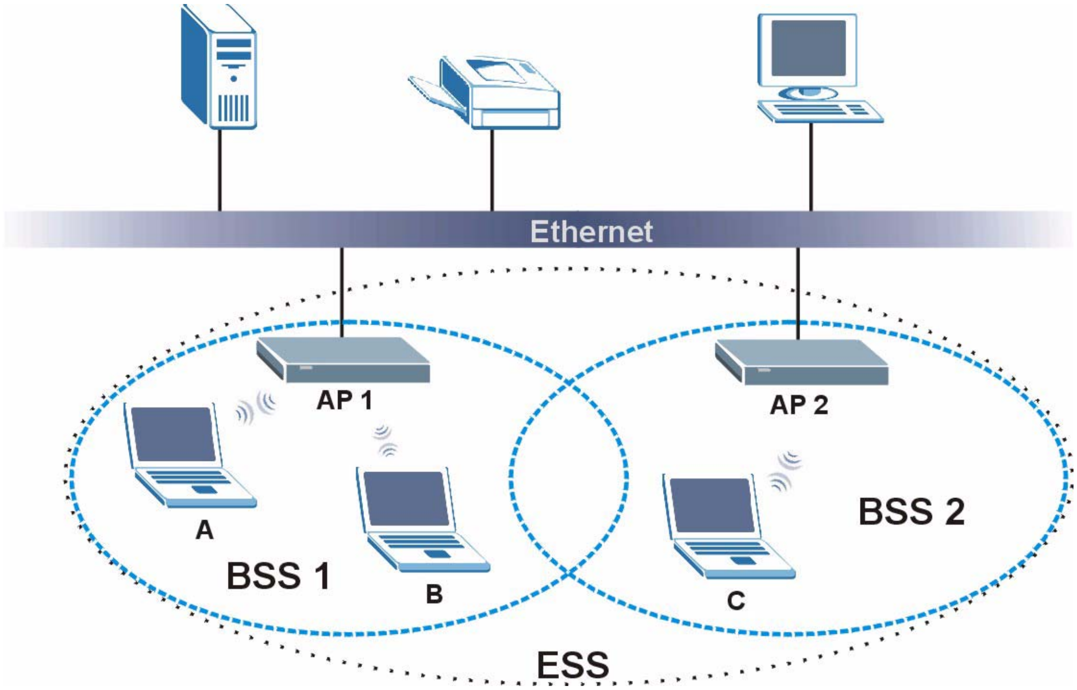
ESS

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 217 Infrastructure WLAN



Channel

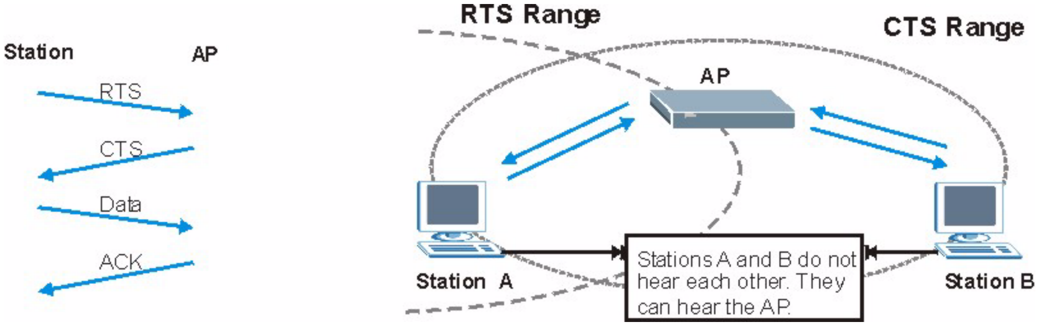
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

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

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 218 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 802.11b/g compliant wireless adapters support long preamble, but not all support short preamble.

Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.

Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.

Select **Dynamic** to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble.

The AP and the wireless adapters 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 116 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 117 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 screen. You may still configure and store keys here, 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 118 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.

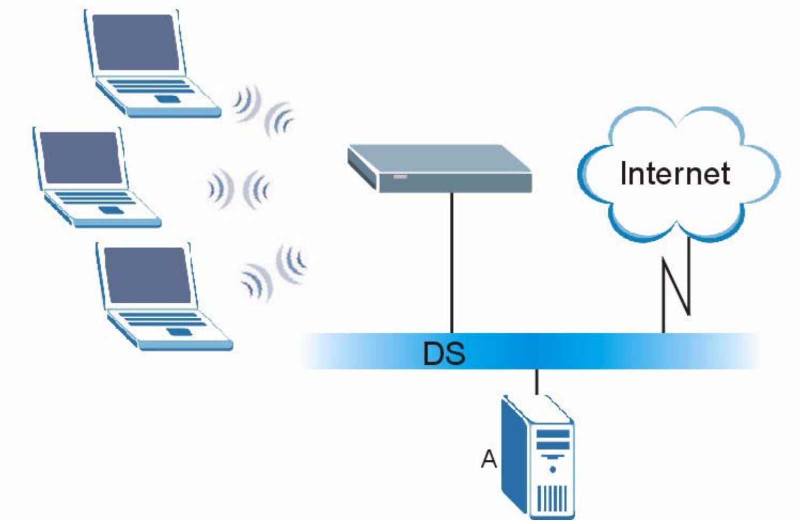
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 219 WPA(2) with RADIUS Application Example



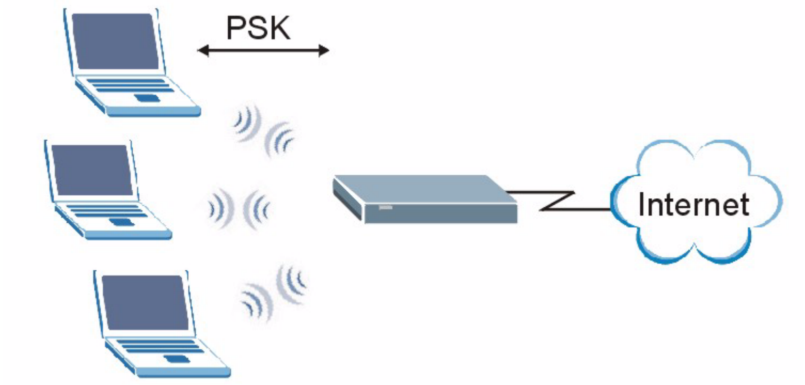
WPA(2)-PSK Application Example

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 (only) allows it to join the network if the password matches.
3. The AP and wireless clients use the pre-shared key to generate a common PMK (Pairwise Master Key).

4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 220 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 119 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) 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.

Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

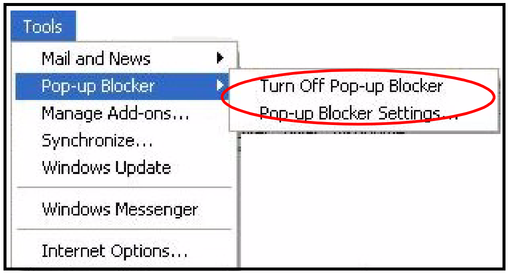
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 221 Pop-up Blocker

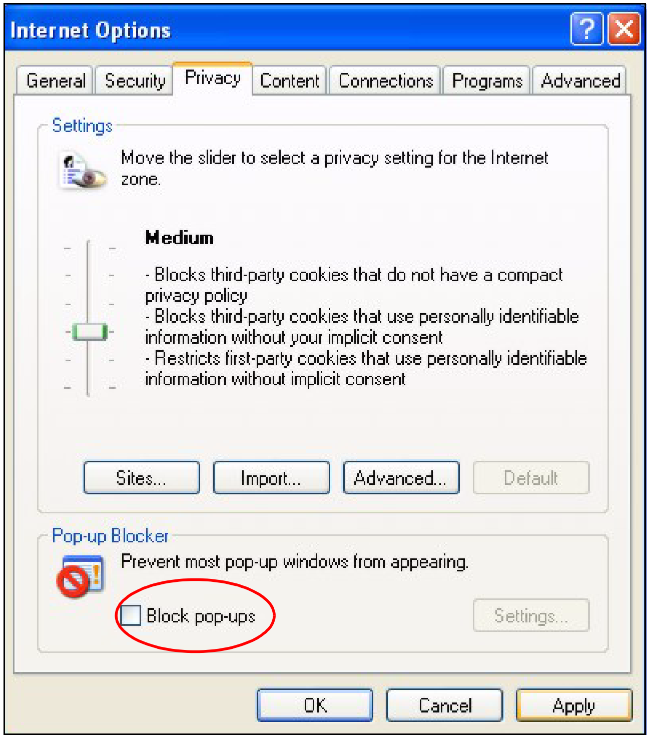


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 222 Internet Options: Privacy



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

Medium

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

Prevent most pop-up windows from appearing.

□ Block pop-ups

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

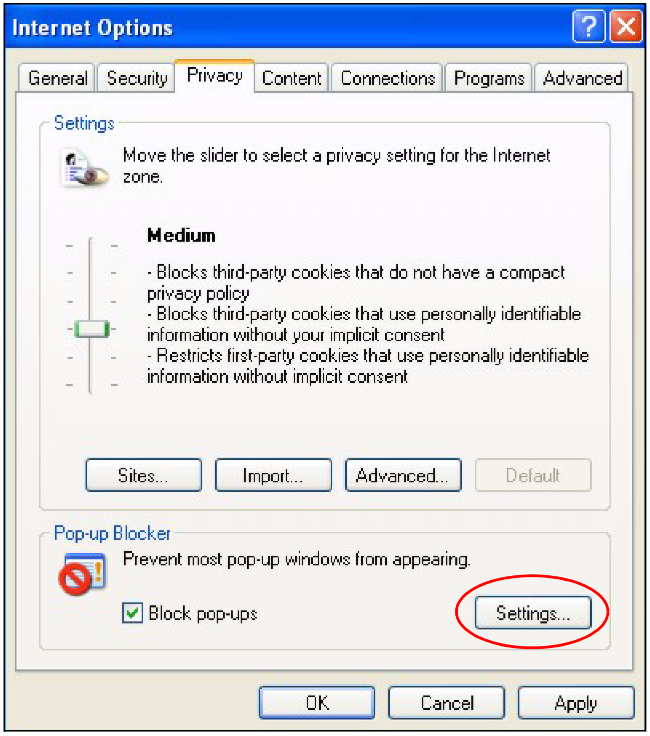
Enable pop-up Blockers with Exceptions

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

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

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

Figure 223 Internet Options: Privacy



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

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

Medium

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

Sites... | Import... | Advanced... | Default

Pop-up Blocker

Prevent most pop-up windows from appearing.

☑ Block pop-ups

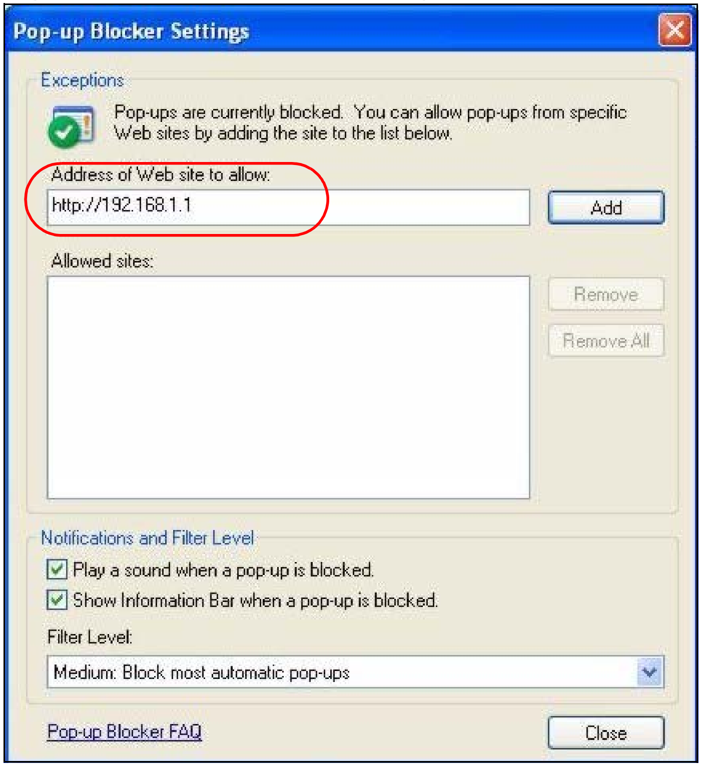
Settings...

OK | Cancel | Apply

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

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

Figure 224 Pop-up Blocker Settings



Pop-up Blocker Settings

Exceptions

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

Address of Web site to allow:

http://192.168.1.1

Add

Allowed sites:

Remove

Remove All

Notifications and Filter Level

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

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

Filter Level:

Medium: Block most automatic pop-ups

Pop-up Blocker FAQ

Close

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

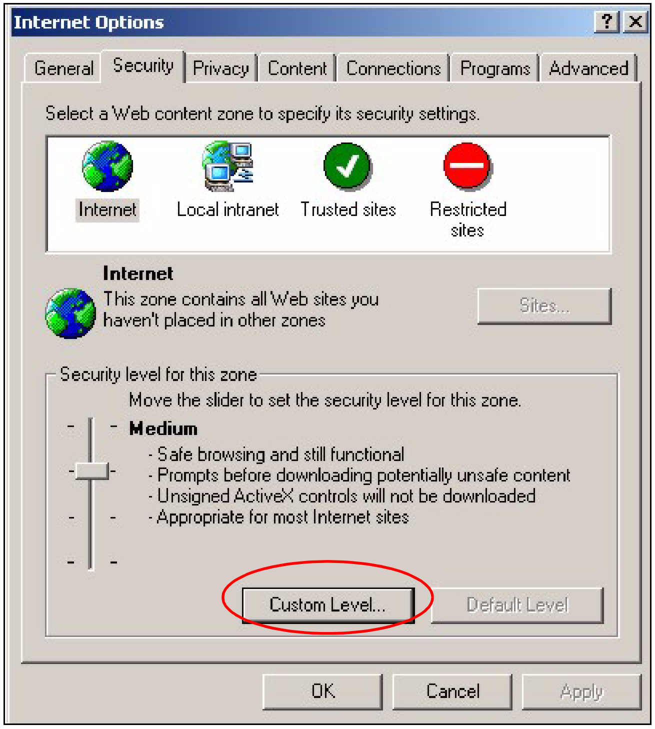
6 Click **Apply** to save this setting.

JavaScripts

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

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

Figure 225 Internet Options: Security



Select a Web content zone to specify its security settings.

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

Security level for this zone

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

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

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

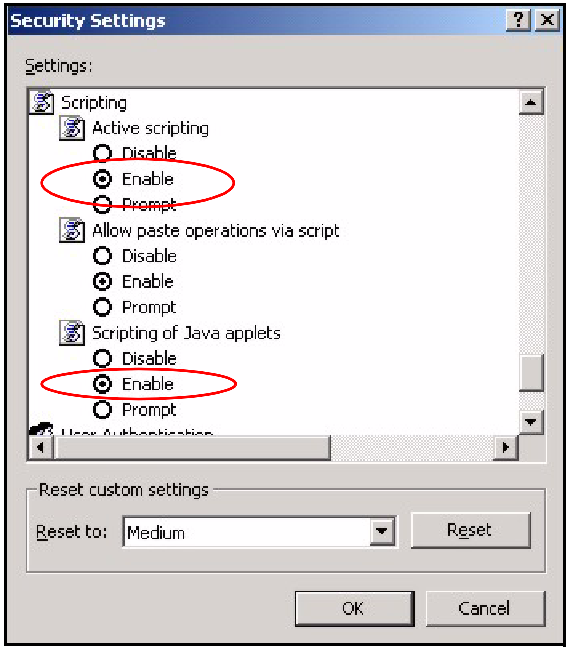
3 Scroll down to **Scripting**.

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

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

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

Figure 226 Security Settings - Java Scripting



Security Settings

Settings:

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

User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

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

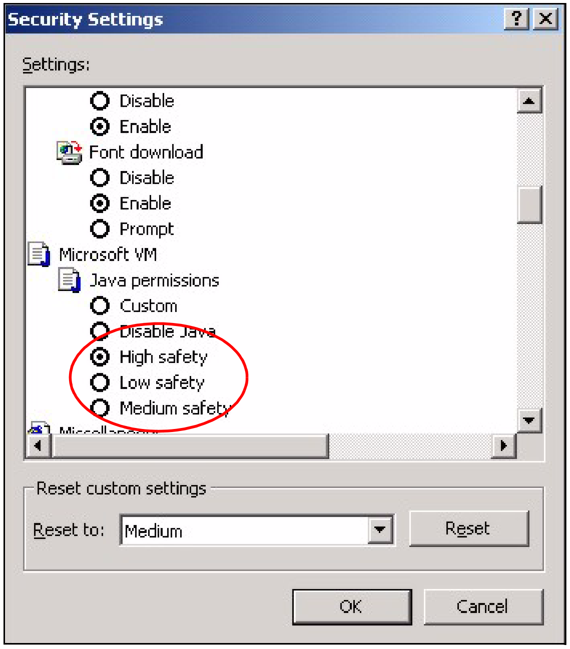
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

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

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

Figure 227 Security Settings - Java



Security Settings

Settings:

- ○ Disable
- ● Enable

Font download
- ○ Disable
- ● Enable
- ○ Prompt

Microsoft VM
- Java permissions
  - ○ Custom
  - ○ Disable Java
  - ● High safety
  - ○ Low safety
  - ○ Medium safety

Miscellaneous

Reset custom settings

Reset to: Medium

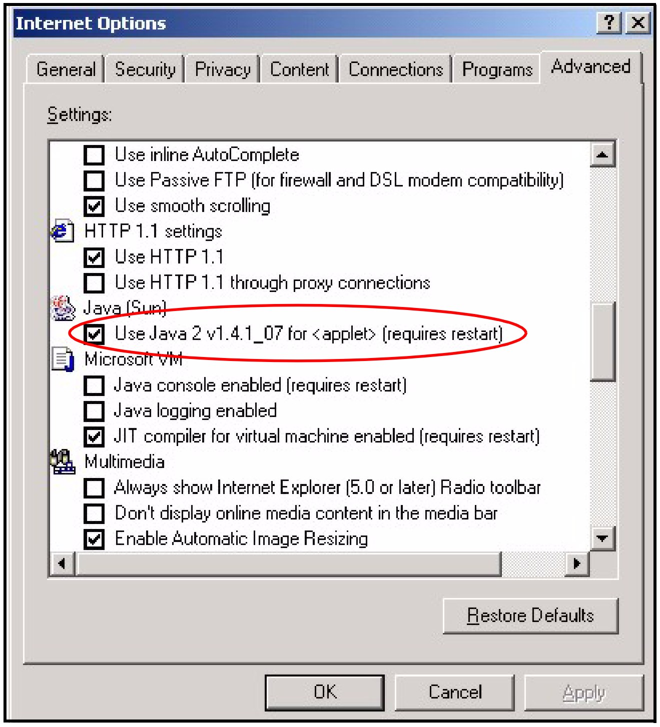
JAVA (Sun)

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

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

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

Figure 228 Java (Sun)



☐ Use inline AutoComplete
☐ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
☐ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
☐ Java console enabled (requires restart)
☐ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
☐ Always show Internet Explorer (5.0 or later) Radio toolbar
☐ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

G

Importing Certificates

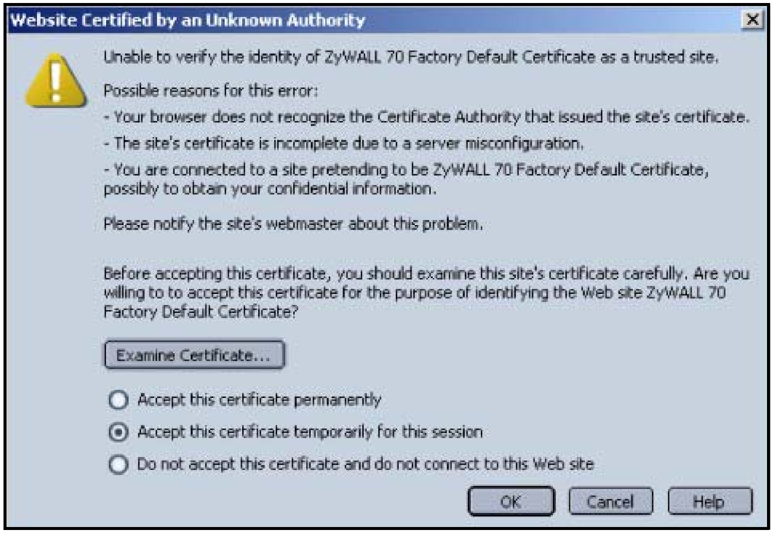
This appendix shows importing certificates examples using Internet Explorer 5.

Import ZyXEL Device Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the ZyXEL Device's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

Figure 229 Security Certificate



Website Certified by an Unknown Authority

Unable to verify the identity of ZyWALL 70 Factory Default Certificate as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be ZyWALL 70 Factory Default Certificate, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site ZyWALL 70 Factory Default Certificate?

○ Accept this certificate permanently
● Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this Web site

Importing the ZyXEL Device's Certificate into Internet Explorer

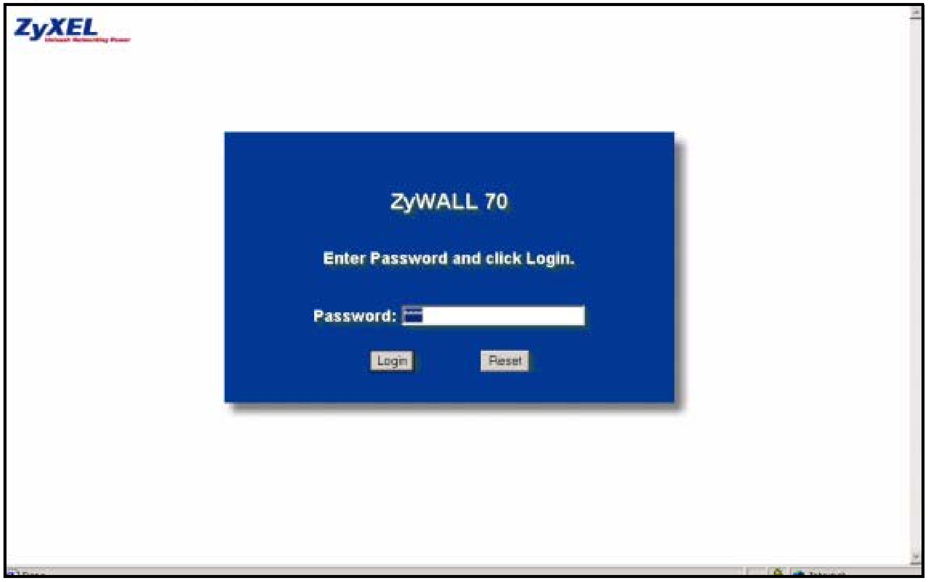
For Internet Explorer to trust a self-signed certificate from the ZyXEL Device, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a ZyXEL Device certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the ZyXEL Device's (self-signed) server certificate into your operating system as a trusted certification authority.

1 In Internet Explorer, double click the lock shown in the following screen.

Figure 230 Login Screen



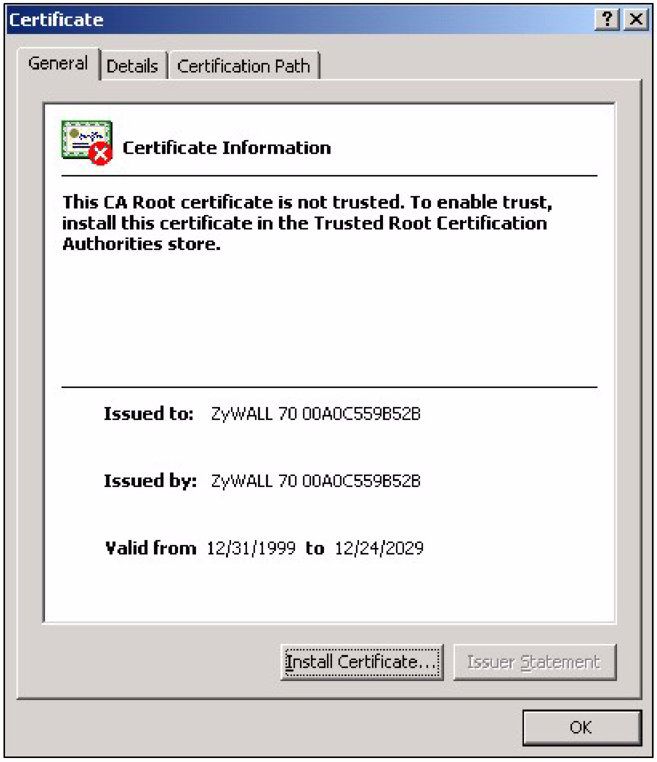
ZyWALL 70

Enter Password and click Login.

Password:

2 Click **Install Certificate** to open the **Install Certificate** wizard.

Figure 231 Certificate General Information before Import



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

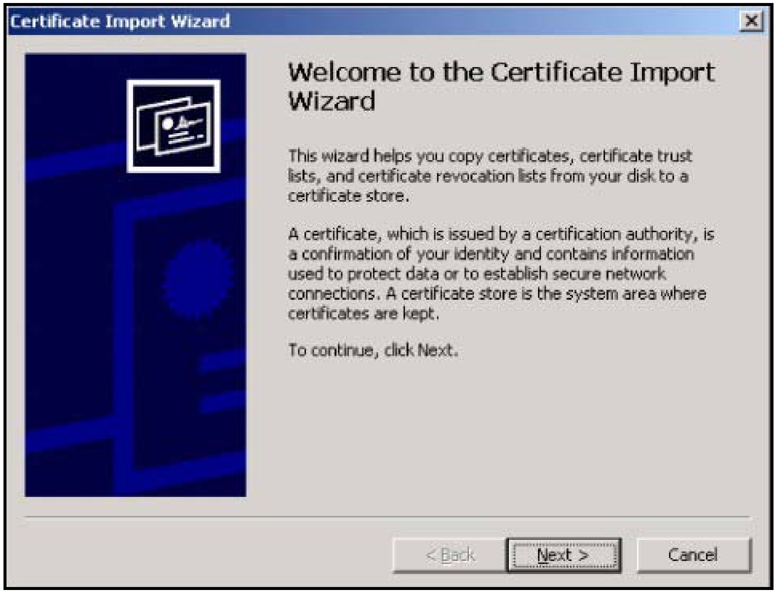
Issued to: ZyWALL 70 00A0C559B52B

Issued by: ZyWALL 70 00A0C559B52B

Valid from 12/31/1999 **to** 12/24/2029

3 Click **Next** to begin the **Install Certificate** wizard.

Figure 232 Certificate Import Wizard 1



Certificate Import Wizard

Welcome to the Certificate Import Wizard

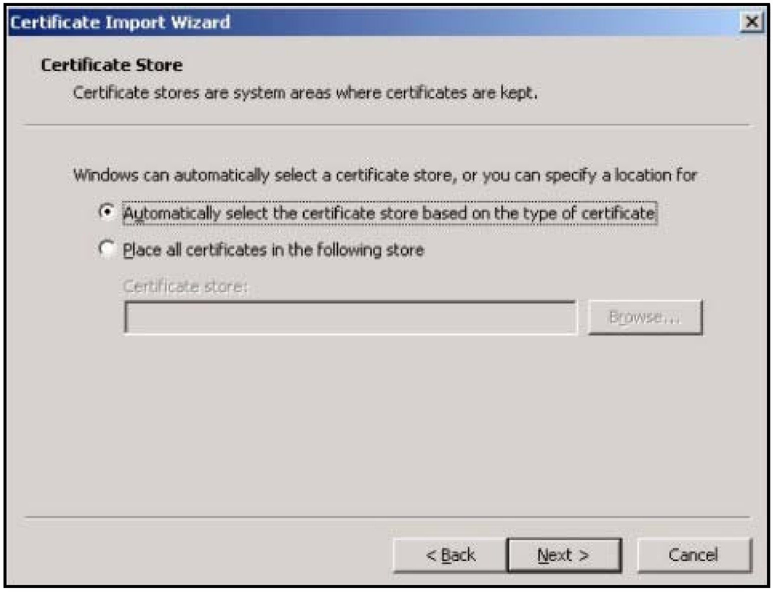
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4 Select where you would like to store the certificate and then click **Next**.

Figure 233 Certificate Import Wizard 2



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

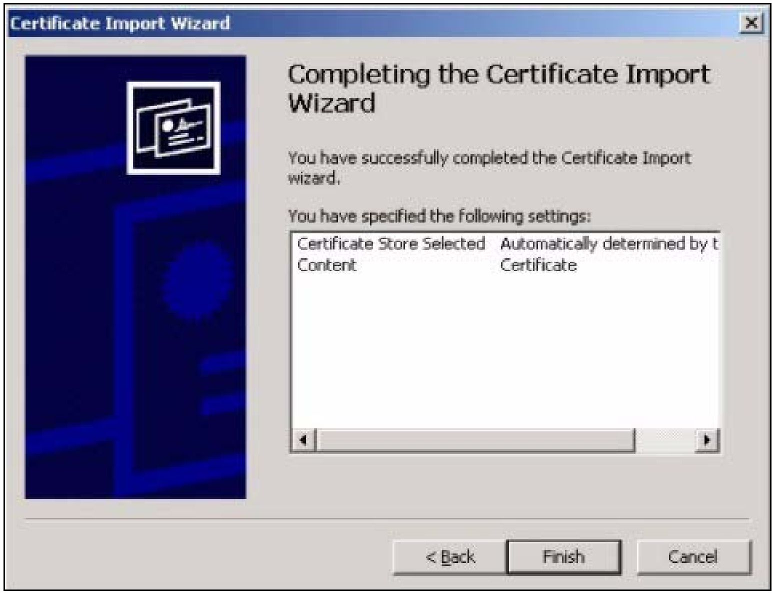
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5 Click **Finish** to complete the **Import Certificate** wizard.

Figure 234 Certificate Import Wizard 3



Certificate Import Wizard

Completing the Certificate Import Wizard

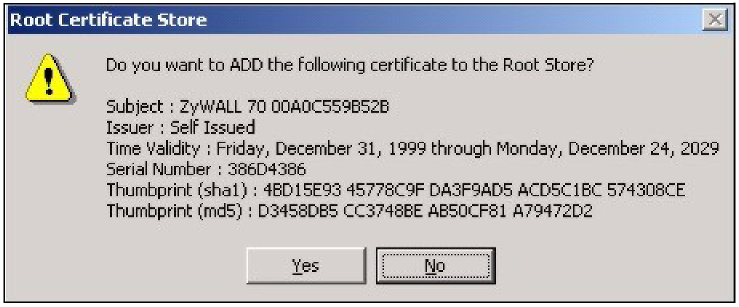
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

6 Click **Yes** to add the ZyXEL Device certificate to the root store.

Figure 235 Root Certificate Store

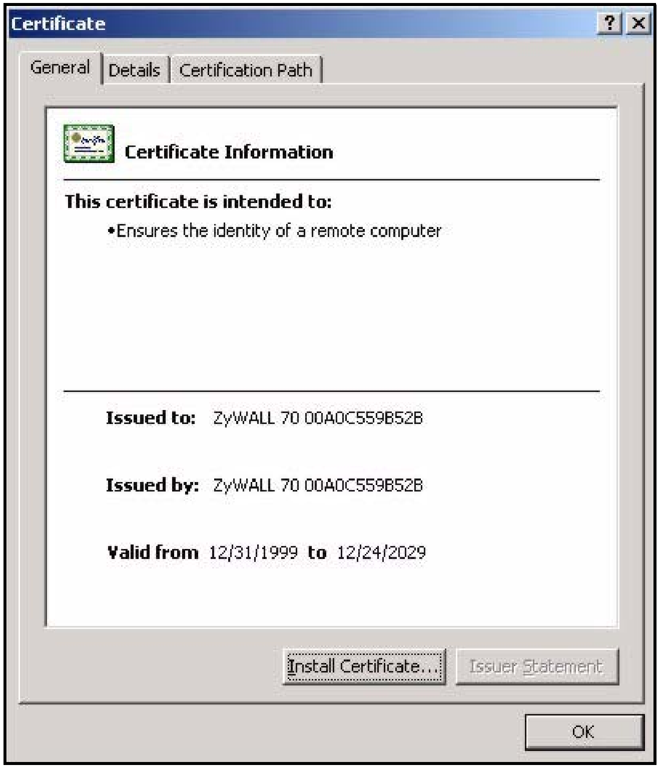


Root Certificate Store

Do you want to ADD the following certificate to the Root Store?

Subject : ZyWALL 70 00A0C559B52B
Issuer : Self Issued
Time Validity : Friday, December 31, 1999 through Monday, December 24, 2029
Serial Number : 386D4386
Thumbprint (sha1) : 4BD15E93 45778C9F DA3F9AD5 ACD5C1BC 574308CE
Thumbprint (md5) : D3458DB5 CC3748BE AB50CF81 A79472D2

Figure 236 Certificate General Information after Import



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer

Issued to: ZyWALL 70 00A0C559B52B

Issued by: ZyWALL 70 00A0C559B52B

Valid from 12/31/1999 to 12/24/2029

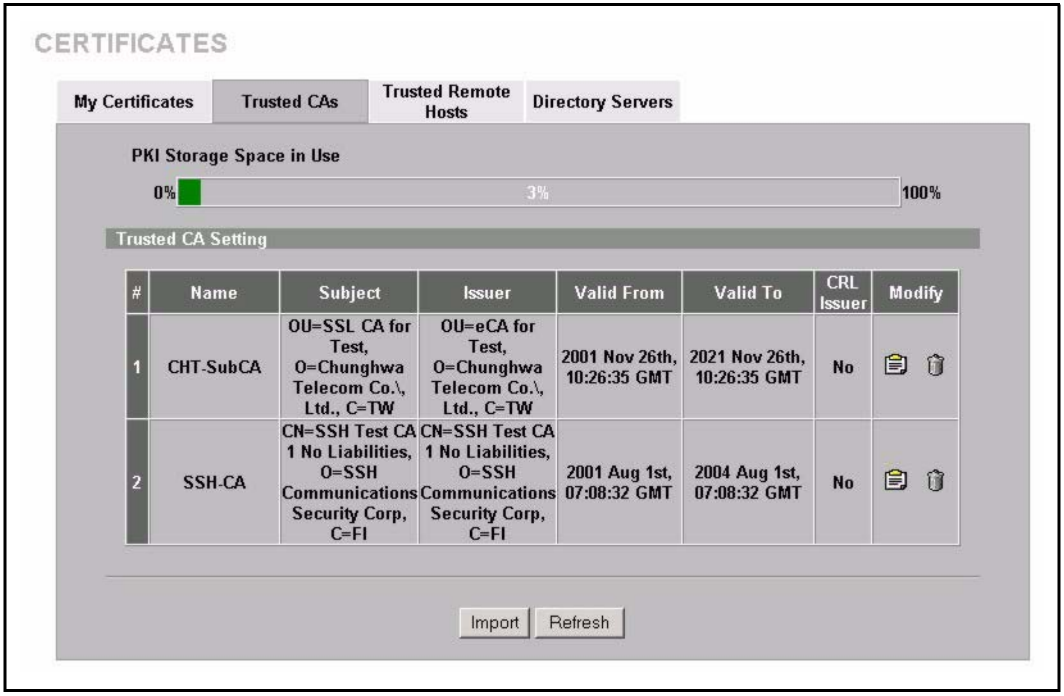
Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyXEL Device.

You must have imported at least one trusted CA to the ZyXEL Device in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyXEL Device (see the ZyXEL Device’s **Trusted CA** web configurator screen).

Figure 237 ZyXEL Device Trusted CA Screen



PKI Storage Space in Use

0% 🟩 3% 100%

Trusted CA Setting

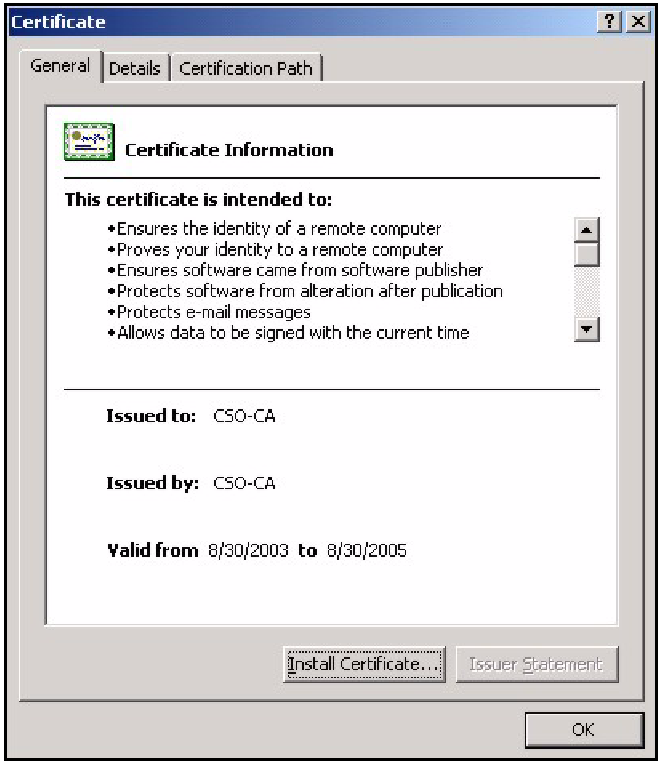
#	Name	Subject	Issuer	Valid From	Valid To	CRL Issuer	Modify
1	CHT-SubCA	OU=SSL CA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW	OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW	2001 Nov 26th, 10:26:35 GMT	2021 Nov 26th, 10:26:35 GMT	No	📋 🗑
2	SSH-CA	CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI	CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI	2001 Aug 1st, 07:08:32 GMT	2004 Aug 1st, 07:08:32 GMT	No	📋 🗑

The CA sends you a package containing the CA’s trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

Installing the CA’s Certificate

1 Double click the CA’s trusted certificate to produce a screen similar to the one shown next.

Figure 238 CA Certificate Example



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

Issued to: CSO-CA

Issued by: CSO-CA

Valid from 8/30/2003 to 8/30/2005

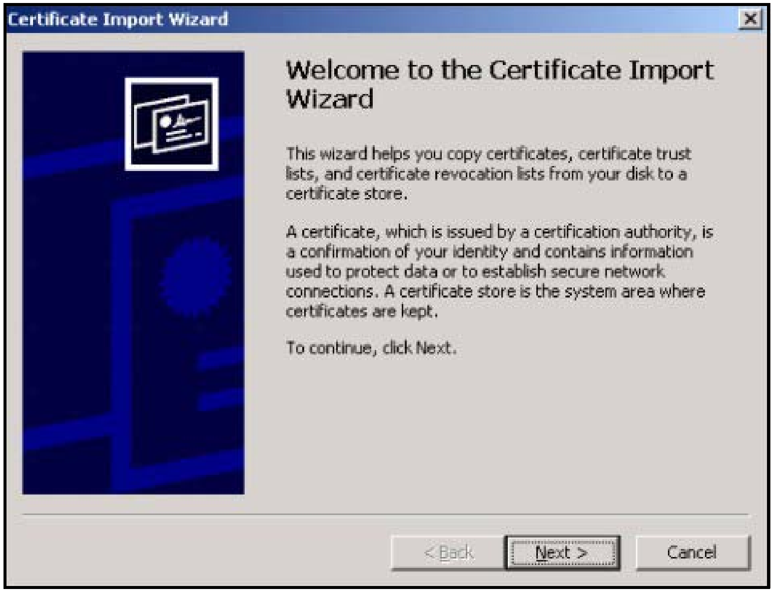
2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

Figure 239 Personal Certificate Import Wizard 1



Welcome to the Certificate Import Wizard

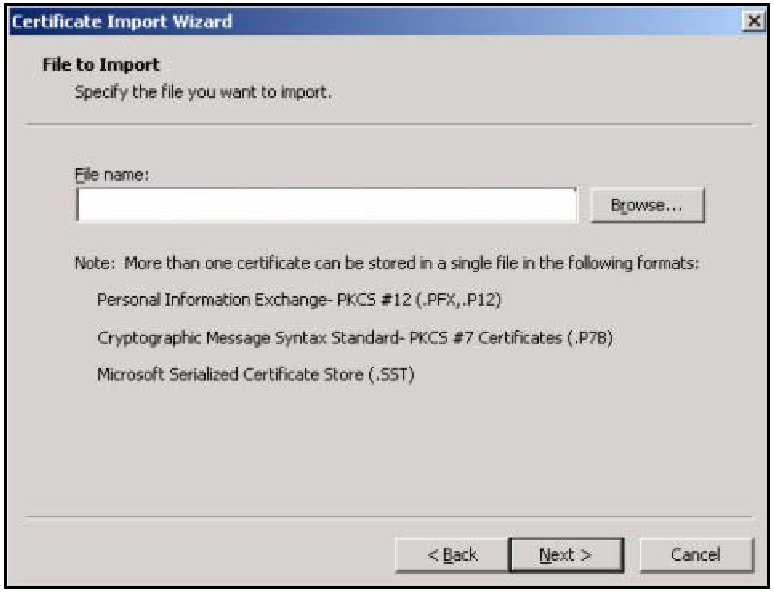
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

Figure 240 Personal Certificate Import Wizard 2



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

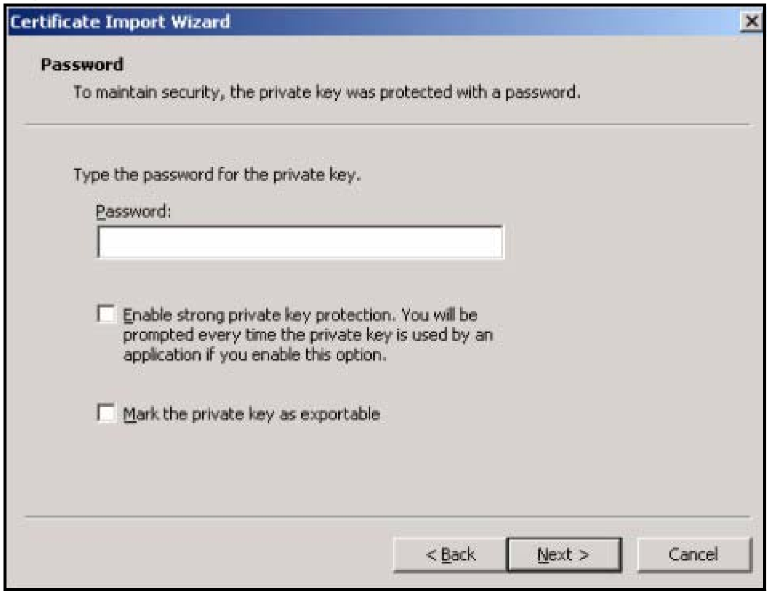
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

3 Enter the password given to you by the CA.

Figure 241 Personal Certificate Import Wizard 3



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

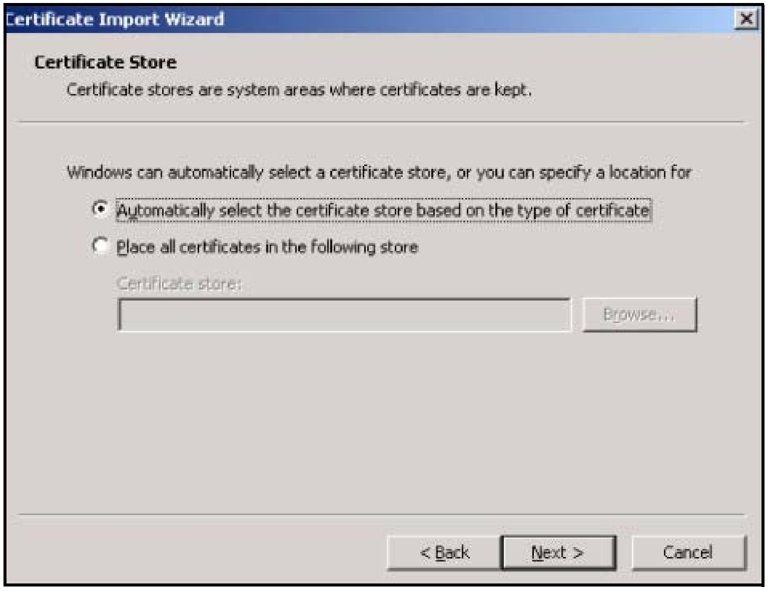
Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark the private key as exportable

4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

Figure 242 Personal Certificate Import Wizard 4



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

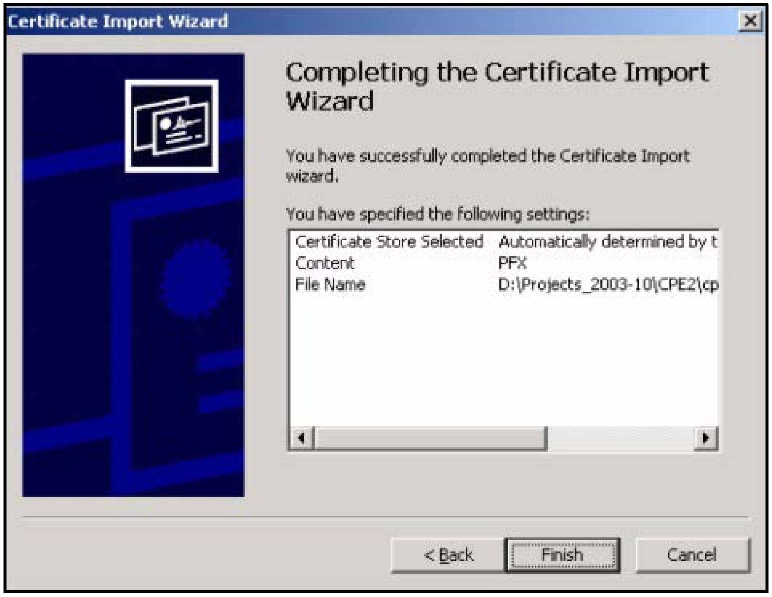
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5 Click **Finish** to complete the wizard and begin the import process.

Figure 243 Personal Certificate Import Wizard 5



Certificate Import Wizard

Completing the Certificate Import Wizard

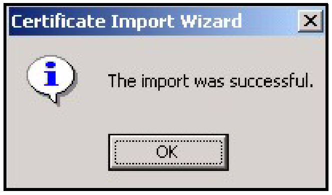
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	D:\Projects_2003-10\CPE2\cp

6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 244 Personal Certificate Import Wizard 6



Certificate Import Wizard

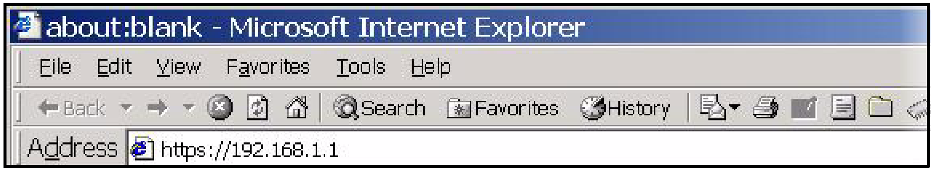
The import was successful.

Using a Certificate When Accessing the ZyXEL Device Example

Use the following procedure to access the ZyXEL Device via HTTPS.

1 Enter ‘https://ZyXEL Device IP Address/ in your browser’s web address field.

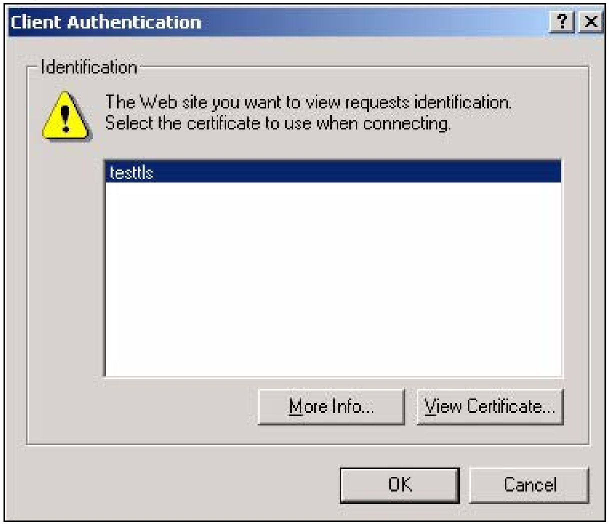
Figure 245 Access the ZyXEL Device Via HTTPS


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address

https://192.168.1.1

2 When **Authenticate Client Certificates** is selected on the ZyXEL Device, the following screen asks you to select a personal certificate to send to the ZyXEL Device. This screen displays even if you only have a single certificate as in the example.

Figure 246 SSL Client Authentication

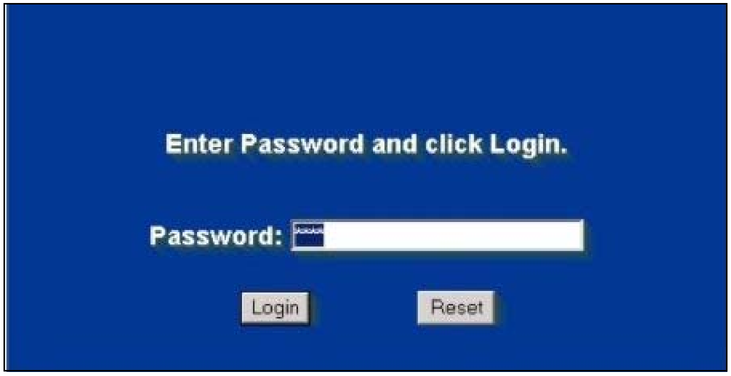


The Web site you want to view requests identification.
Select the certificate to use when connecting.

testtls

3 You next see the ZyXEL Device login screen.

Figure 247 ZyXEL Device Secure Login Screen



Enter Password and click Login.

Password:

H

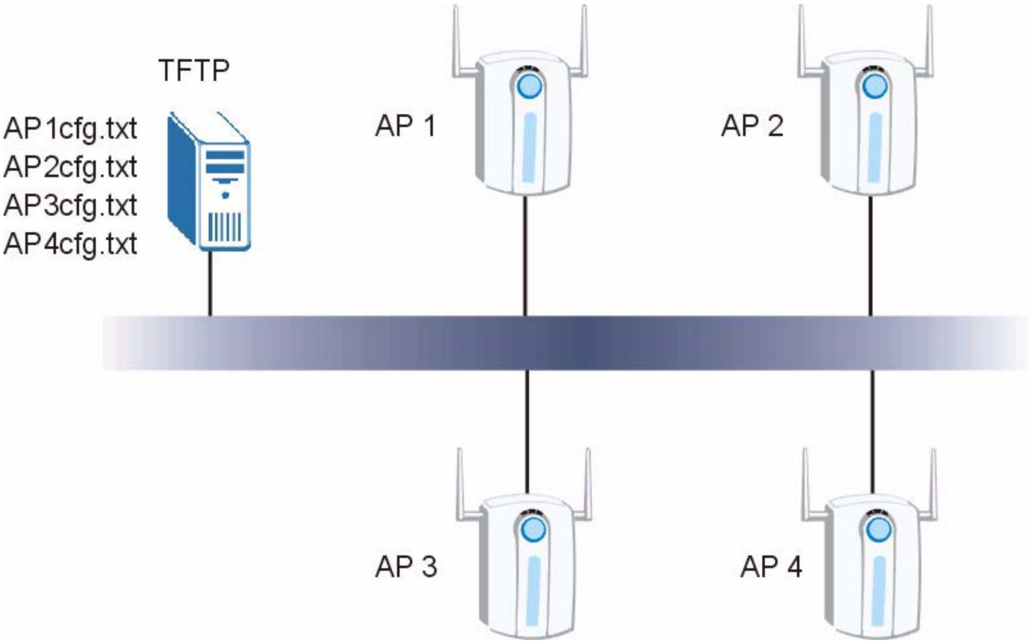
Text File Based Auto Configuration

This chapter describes how administrators can use text configuration files to configure the wireless LAN settings for multiple APs.

Text File Based Auto Configuration Overview

You can use plain text configuration files to configure the wireless LAN settings on multiple APs. The AP can automatically get a configuration file from a TFTP server at startup or after renewing DHCP client information.

Figure 248 Text File Based Auto Configuration



Use one of the following methods to give the AP the IP address of the TFTP server where you store the configuration files and the name of the configuration file that it should download.

You can have a different configuration file for each AP. You can also have multiple APs use the same configuration file.

If adjacent APs use the same configuration file, you should leave out the channel setting since they could interfere with each other's wireless traffic.

Auto Configuration by DHCP

A DHCP response can use options 66 and 67 to assign a TFTP server IP address and a filename. If the AP is configured as a DHCP client, these settings can be used to perform auto configuration.

Table 120 Auto Configuration by DHCP

COMMAND	DESCRIPTION
`wcfg autocfg dhcp [enable | disable]`	Turn configuration of TFTP server IP address and filename through DHCP on or off.

If this feature is enabled and the DHCP response provides a TFTP server IP address and a filename, the AP will try to download the file from the specified TFTP server. The AP then uses the file to configure wireless LAN settings.

Not all DHCP servers allow you to specify options 66 and 67.

Manual Configuration

Use the following command to manually configure a TFTP server IP address and a file name for the AP to use for auto provisioning whenever the AP starts up. See Section 26.1 on page 249 for how to access the Command Interpreter (CI).

Table 121 Manual Configuration

COMMAND	DESCRIPTION
`wcfg autocfg server [IP] [filename]`	Specify the TFTP server IP address and file name from which the AP is to download a configuration file whenever the AP starts up.

Configuration Via SNMP

You can configure and trigger the auto configuration remotely via SNMP.

Use the following procedure to have the AP download the configuration file.

Table 122 Configuration via SNMP

STEPS	MIB VARIABLE	VALUE
Step 1	pwTftpServer	Set the IP address of the TFTP server.
Step 2	pwTftpFileName	Set the file name, for example, g3000hcfg.txt.
Step 3	pwTftpFileType	Set to 3 (text configuration file).
Step 4	pwTftpOpCommand	Set to 2 (download).

Verifying Your Configuration File Upload Via SNMP

You can use SNMP management software to display the configuration file version currently on the device by using the following MIB.

Table 123 Displaying the File Version

ITEM	OBJECT ID	DESCRIPTION
pwCfgVersion	1.3.6.1.4.1.890.1.9.1.2	This displays the current configuration file version.

Troubleshooting Via SNMP

If you have any difficulties with the configuration file upload, you can try using the following MIB 10 to 20 seconds after using SNMP to have the AP download the configuration file.

Table 124 Displaying the File Version

ITEM	OBJECT ID	DESCRIPTION
pwTftpOpStatus	1.3.6.1.4.1.890.1.9.1.6	This displays the current operating status of the TFTP client.

Configuration File Format

The text based configuration file must use the following format.

Figure 249 Configuration File Format

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 1 xxx
wcfg security save
wcfg ssid 1 xxx
wcfg ssid save
```

The first line must be `!#ZYXEL PROWLAN.`

The second line must specify the file version. The AP compares the file version with the version of the last configuration file that it downloaded. If the version of the downloaded file is the same or smaller (older), the AP ignores the file. If the version of the downloaded file is larger (newer), the AP uses the file.

Configuration File Rules

You can only use the `wlan` and `wcfg` commands in the configuration file. The AP ignores other ZyNOS commands but continues to check the next command.

The AP ignores any improperly formatted commands and continues to check the next line.

If there are any errors while processing the configuration file, the AP generates a message with the line number and reason for the first error (subsequent errors during the processing of an individual configuration file are not recorded). You can use SNMP management software to display the message by using the following MIB.

Table 125 Displaying the Auto Configuration Status

ITEM	OBJECT ID	DESCRIPTION
pwAutoCfgMessage	1.3.6.1.4.1.890.1.9.1.9	Auto configuration status message string

The commands will be executed line by line just like if you entered them in a console or Telnet CI session. Be careful to ensure the integrity of the whole AP configuration. If there are existing settings in the AP, the newly loaded configuration file will either coexist with the previous settings or replace them.

You can zip each configuration file. You must use the store compression method and a .zip file extension. When zipping a configuration file, you can also add password protection using the same password that you use to log into the AP.

wcfg Command Configuration File Examples

These example configuration files use the `wcfg` command to configure security and SSID profiles.

Figure 250 WEP Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 11
wcfg security 1 name Test-wep
wcfg security 1 security wep
wcfg security 1 wep keysize 64 ascii
wcfg security 1 wep key1 abcde
wcfg security 1 wep key2 bcdef
wcfg security 1 wep key3 cdefg
wcfg security 1 wep key4 defgh
wcfg security 1 wep keyindex 1
wcfg security save
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 1 l2iolation disable
wcfg ssid 1 macfilter disable
wcfg ssid save
```

Figure 251 802.1X Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 2 name Test-8021x
wcfg security 2 mode  8021x-static128
wcfg security 2 wep key1 abcdefghijklm
wcfg security 2 wep key2 bcdefghijklmn
wcfg security 2 wep keyindex 1
wcfg security 2 reauthtime 1800
wcfg security 2 idletime 3600
wcfg security save
wcfg radius 2 name radius-rd
wcfg radius 2 primary 172.23.3.4 1812 1234 enable
wcfg radius 2 backup 172.23.3.5 1812 1234 enable
wcfg radius save
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 2 qos 4
wcfg ssid 2 l2isolation disable
wcfg ssid 2 macfilter disable
wcfg ssid save
```

Figure 252 WPA-PSK Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 13
wcfg security 3 name Test-wpapsk
wcfg security 3 mode wpapsk
wcfg security 3 passphrase qwertyuiop
wcfg security 3 reauthtime 1800
wcfg security 3 idletime 3600
wcfg security 3 groupkeytime 1800
wcfg security save
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 3 qos 4
wcfg ssid 3 l2siolation disable
wcfg ssid 3 macfilter disable
wcfg ssid save
```

Figure 253 WPA Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 14
wcfg security 4 name Test-wpa
wcfg security 4 mode wpa
wcfg security 4 reauthtime 1800
wcfg security 4 idletime 3600
wcfg security 4 groupkeytime 1800
wcfg security save
wcfg radius 4 name radius-rd1
wcfg radius 4 primary 172.0.20.38 1812 20 enable
wcfg radius 4 backup 172.0.20.39 1812 20 enable
wcfg radius save
wcfg ssid 4 name ssid-wpa
wcfg ssid 4 security Test-wpa
wcfg ssid 4 qos 4
wcfg ssid 4 l2isolation disable
wcfg ssid 4 macfilter disable
wcfg ssid save
```

wlan Command Configuration File Example

This example configuration file uses the `wlan` command to configure the AP to use the security and SSID profiles from the `wcfg` command configuration file examples and general wireless settings. You could actually combine all of this chapter’s example configuration files into a single configuration file. Remember that the commands are applied in order. So for example, you would place the commands that create security and SSID profiles before the commands that tell the AP to use those profiles.

Figure 254 wlan Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 15
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 4 name ssid-wpa2psk
wcfg ssid 4 security Test-wpa2psk
wcfg ssid save
!line starting with '!' is comment
!change to channel 8
wlan chid 8
!change operating mode -> AP mode,
!then select ssid-wep as running WLAN profile
wlan opmode 0
wlan ssidprofile ssid-wep
!change operating mode -> MESSID mode,
!then select ssid-wpapsk, ssid-wpa2psk as running WLAN profiles
wlan opmode 3
wlan ssidprofile ssid-wpapsk ssid-wpa2psk
! set output power level to 50%
wlan output power 2
```

I

Wireless LAN Manager

This appendix shows you how to install and use the Wireless LAN Manager.

The Wireless LAN Manager (WLM) software simplifies SNMP based firmware and configuration file upgrades on the AP. WLM is an Element Manager System (EMS) plug-in for SNMPc management software. The Wireless LAN Manager is referred to here as the EMS.

The EMS uses ZyXEL's proprietary Management Information Base (MIB). The proprietary MIB file is included on the CD with the EMS. You can also find it in the zipped file that contains the current firmware file. You can download the current firmware from www.zyxel.com.

System Requirements

These are the system requirements for operating the EMS software.

- CPU: Intel Pentium 4, 1.6 GHz or above
- Memory (RAM): 1 GB or more
- Hard Disk free space: 20 MB or more
- Screen Resolution: 1024x768 pixels
- Ethernet Adaptor: 10/100 Mbps
- Operating System: Windows 2000 (with service pack 1), Windows XP or Windows Server 2003 and all using NTFS file system.
- Castle Rock's SNMPc 7.

EMS Installation Overview

The following gives an overview of what you need to do to install the EMS:

1 Install SNMPc. See the documentation that comes with your SNMPc for information.
2 Install the EMS.
3 Add custom MIB files in SNMPc.
4 Locate device(s) that you want the EMS to manage.

Installing the EMS

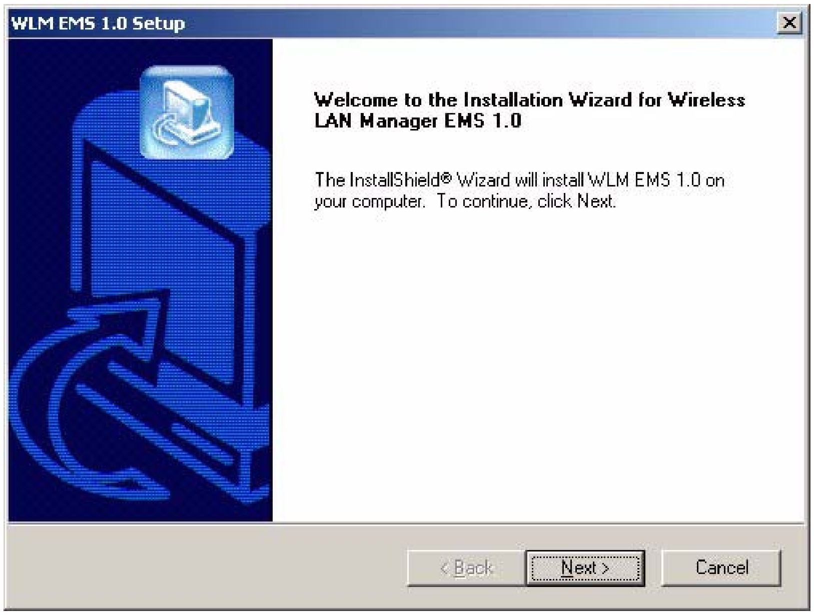
Follow the steps below to install the EMS server on a computer.

1 Install SNMPc if it is not already installed. See the user's guide for more information.

2 Insert the CD. The CD auto-runs. Click the **Tools** link and then the **WLM EMS** link. Otherwise you can go to the **WLM EMS** folder and double-click **Setup.exe**.

3 A **Welcome** screen displays. Click **Next** to continue.

Figure 255 EMS Installation Wizard: Welcome Screen



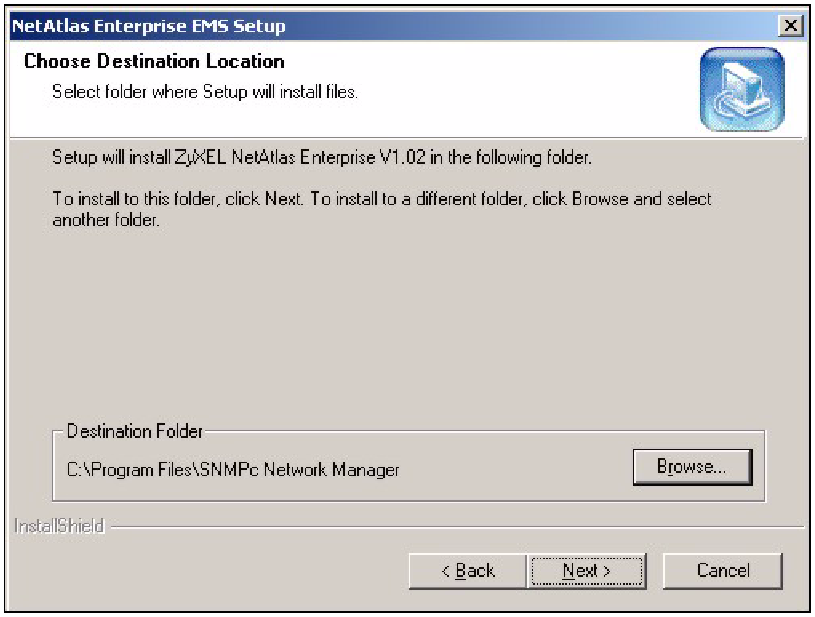
WLM EMS 1.0 Setup

Welcome to the Installation Wizard for Wireless LAN Manager EMS 1.0

The InstallShield® Wizard will install WLM EMS 1.0 on your computer. To continue, click Next.

4 You must select the same directory where you installed SNMPc. Click **Browse** if it's different from the destination folder shown. Click **Next** to continue.

Figure 256 EMS Installation Wizard: Choose Destination Screen



NetAtlas Enterprise EMS Setup

Choose Destination Location

Select folder where Setup will install files.

Setup will install ZyXEL NetAtlas Enterprise V1.02 in the following folder.

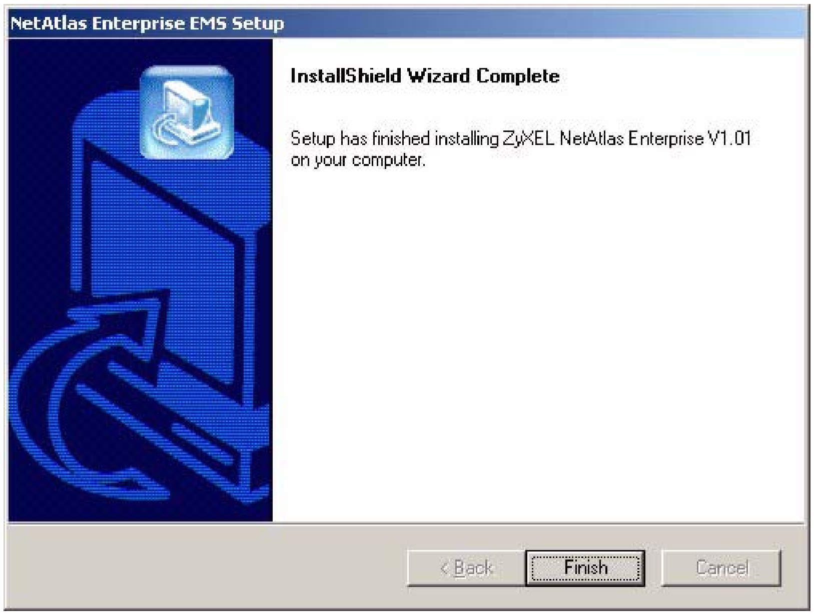
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\SNMPc Network Manager

5 When the installation process is complete, a screen displays as shown. Click **Finish**.

Figure 257 EMS Installation Wizard: Complete Screen



NetAtlas Enterprise EMS Setup

InstallShield Wizard Complete

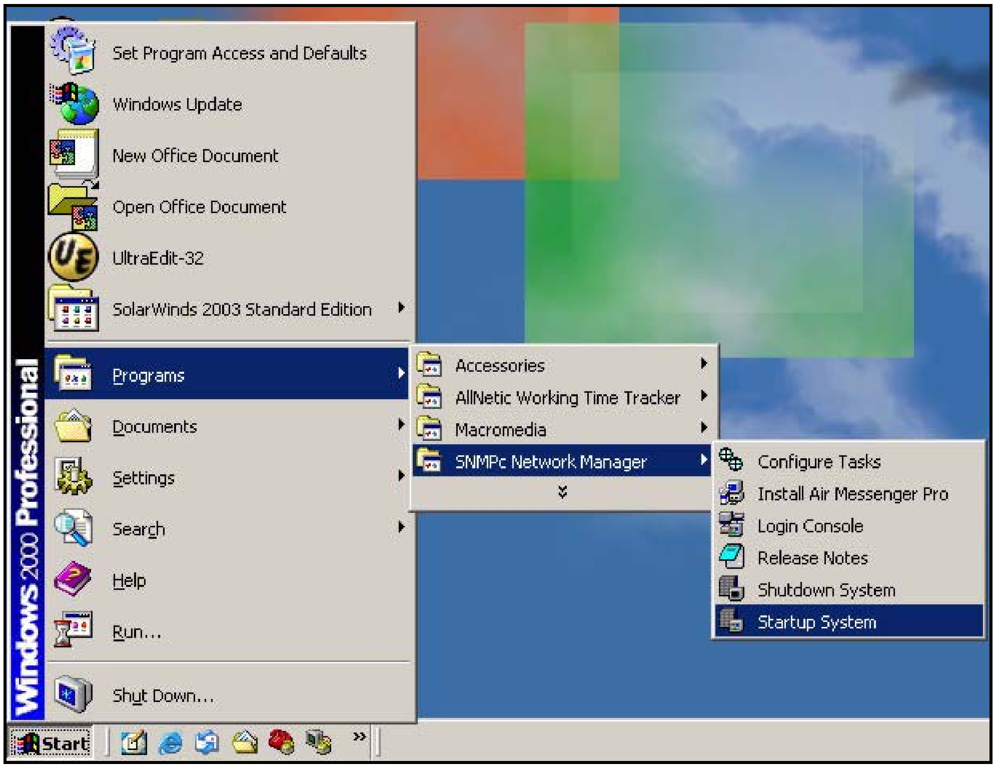
Setup has finished installing ZyXEL NetAtlas Enterprise V1.01 on your computer.

SNMPc Network Manager Startup

Use the following steps to set whether or not SNMPc starts automatically each time you turn on your computer.

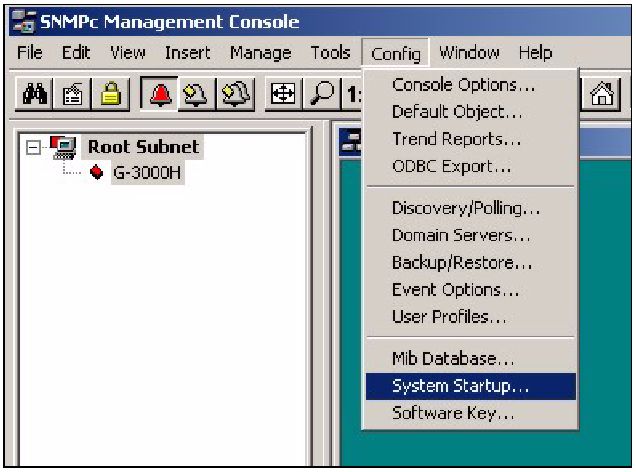
1 Click **Start, Programs, SNMPc Network Manager, Startup System** to manually start the SNMPc network manager.

Figure 258   Starting the SNMPc Network Manager



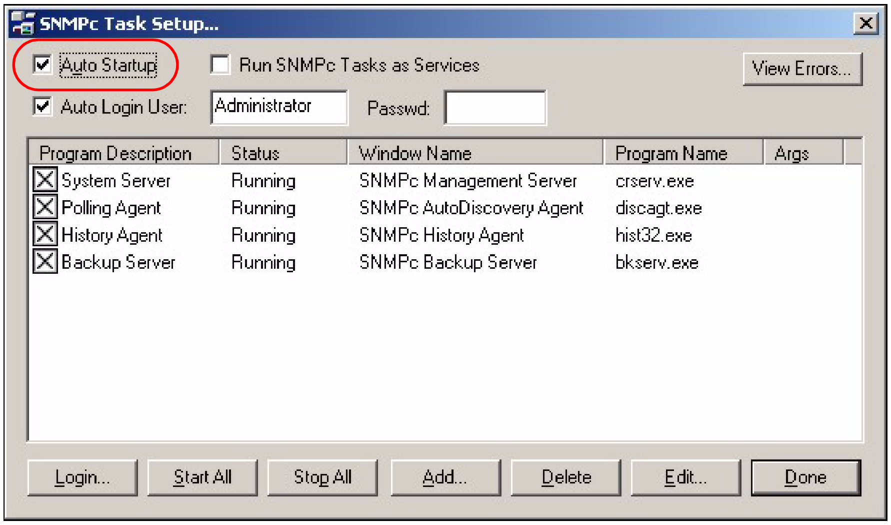
2 Click **Config**, **System Startup...**.

Figure 259   Accessing the SNMPc Startup Settings



3 Select **Auto Startup** check box if you want SNMPc to automatically start each time you turn on your computer, otherwise clear it. Click **Close**.

Figure 260 SNMPc Task Setup Screen



☑ Auto Startup

□ Run SNMPc Tasks as Services

☑ Auto Login User: Administrator

Passwd:

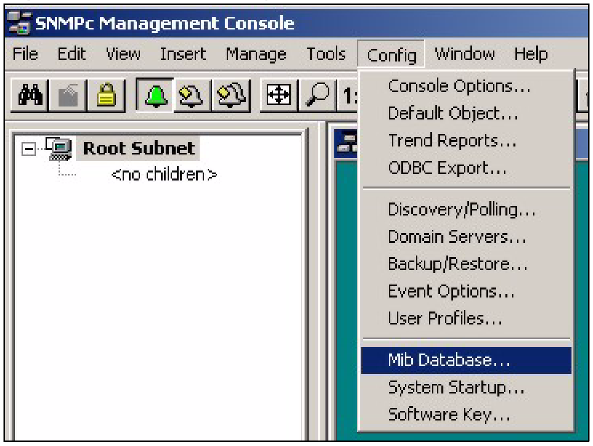
Program Description	Status	Window Name	Program Name	Args
☒ System Server	Running	SNMPc Management Server	crserv.exe	
☒ Polling Agent	Running	SNMPc AutoDiscovery Agent	discagt.exe	
☒ History Agent	Running	SNMPc History Agent	hist32.exe	
☒ Backup Server	Running	SNMPc Backup Server	bkserv.exe	

Adding MIBs

The Management Information Base (MIB) is designed for holding management information on systems (such as the AP) that the standard MIB does not include.

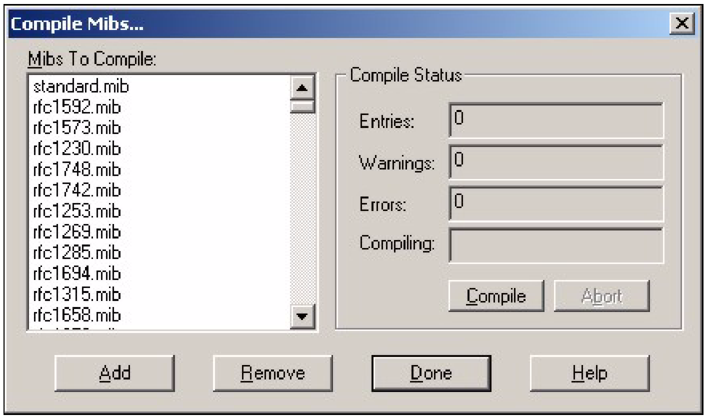
1 From the SNMPc Network Manager main screen, click **Config**, **Mib Database**.

Figure 261 Accessing the Compile Mibs Screen



2 In the **Compile Mibs** screen that displays, click **Add**.

Figure 262   Compile Mibs Screen



Compile Mibs...

Mibs To Compile:

standard.mib
rfc1592.mib
rfc1573.mib
rfc1230.mib
rfc1748.mib
rfc1742.mib
rfc1253.mib
rfc1269.mib
rfc1285.mib
rfc1694.mib
rfc1315.mib
rfc1658.mib

Compile Status

Entries: 0

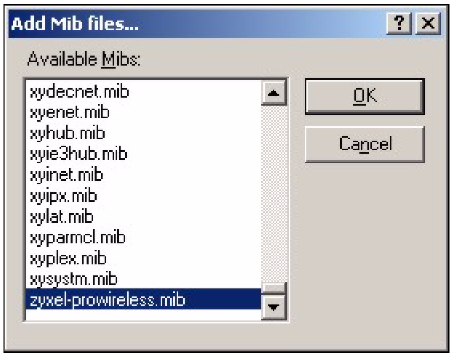
Warnings: 0

Errors: 0

Compiling:

3 The **Add Mib files...** screen opens. Select **zyxel-prowireless.mib** in the list box and click OK.

Figure 263   Add Mib files Screen



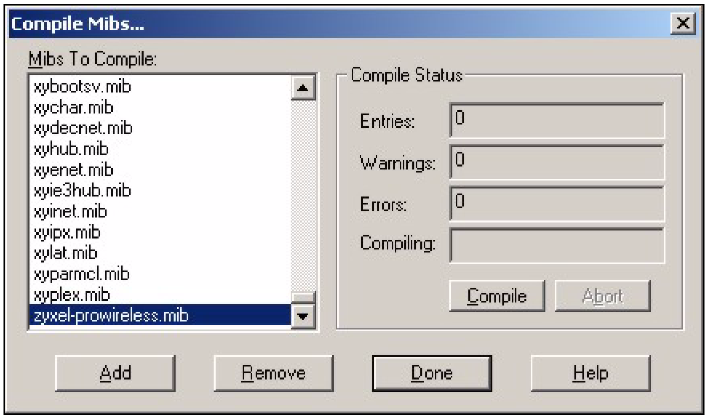
Add Mib files...

Available Mibs:

xydecnet.mib
xyenet.mib
xyhub.mib
xyie3hub.mib
xyinet.mib
xyipx.mib
xylat.mib
xyparmcl.mib
xyplex.mib
xysystm.mib
zyxel-prowireless.mib

4 In the **Compile Mibs** screen, click **Compile**.

Figure 264   Compile Mibs Screen



Compile Mibs...

Mibs To Compile:

xybootsv.mib
xychar.mib
xydecnet.mib
xyhub.mib
xyenet.mib
xyie3hub.mib
xyinet.mib
xyipx.mib
xylat.mib
xyparmcl.mib
xyplex.mib
zyxel-prowireless.mib

Compile Status

Entries: 0

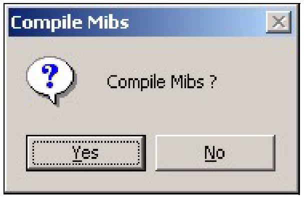
Warnings: 0

Errors: 0

Compiling:

5 Click **Yes** when asked to confirm.

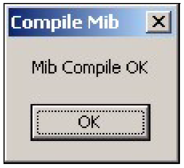
Figure 265 Compile Mibs Confirm Screen


Compile Mibs

Compile Mibs ?

6 This screen appears after the compiling finishes. Click **OK**.

Figure 266 Compile Mib OK Screen


Compile Mib

Mib Compile OK

7 Finally click **Done** in the **Compile Mibs** screen.

Proprietary MIBs

The following objects are contained in the **zyxel-prowireless.mib**.

Table 126 Proprietary MIBs

ITEMS	OBJECT ID (OID)	DESCRIPTION
pwCommon	1.3.6.1.4.1.890.1.9.1	AP status monitoring, firmware/configuration file upload / download.
pwTraps	1.3.6.1.4.1.890.1.9.2	Sets the device to send (or not send) SNMP traps.
pwStation	1.3.6.1.4.1.890.1.9.3	Displays the associated stations.
pwAPDetect	1.3.6.1.4.1.890.1.9.4	Displays the neighboring APs. You need to configure the timer to update the AP list.
pwWlanControl	1.3.6.1.4.1.890.1.9.5	Sets WLAN related parameters, Currently it can set the MAC filter and transmission power.

Finding Your Device

You can add your device(s) manually or have the SNMPc Network Manager find the new device(s) automatically using auto-discovery.

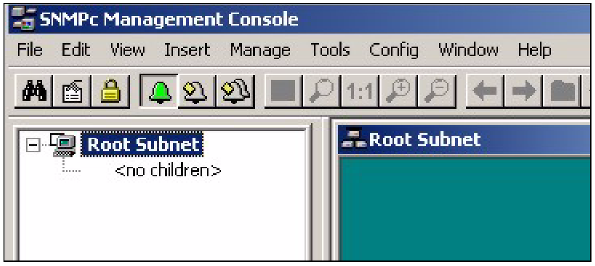
Auto-discovery can be slow and generates extra network traffic. For a large network you may prefer to add devices manually.

Add Device(s) Manually

Follow the steps below to add your device(s) manually.

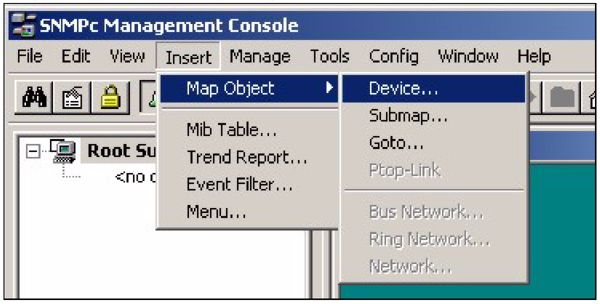
1 Select the **Root Subnet**.

Figure 267   Selecting the Root Subnet



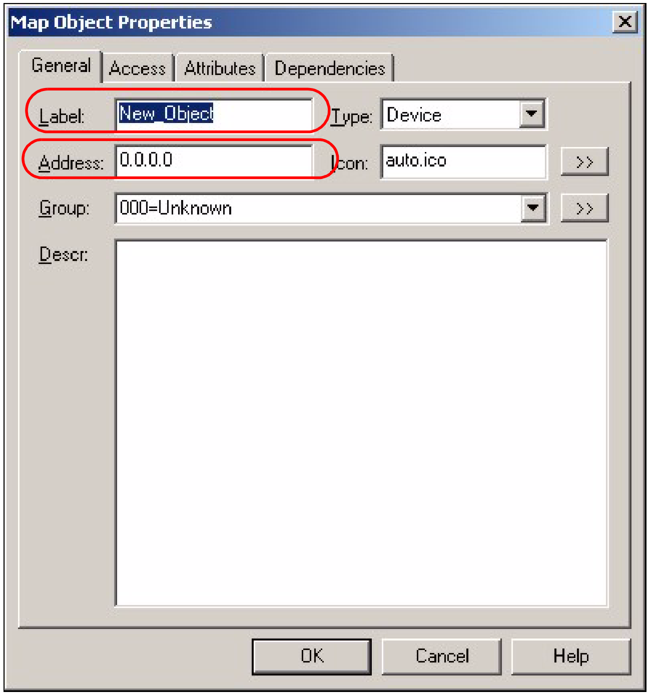
2   Click **Insert**, **MAP Object**, **Device**.

Figure 268   Accessing the MAP Object Properties Screen



3   In the **MAP Object Properties** screen, enter a descriptive device name and IP address for the device.

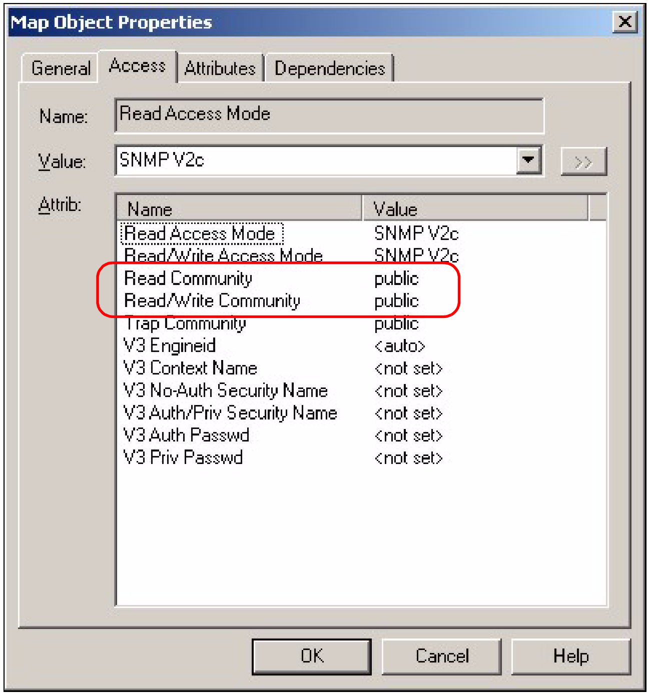
Figure 269   MAP Object Properties: General



Label: New_Object
Type: Device
Address: 0.0.0.0
Icon: auto.ico
Group: 000=Unknown

4   Click the **Access** tab.

Figure 270 MAP Object Properties: Access



Name: Read Access Mode

Value: SNMP V2c

Attrib:

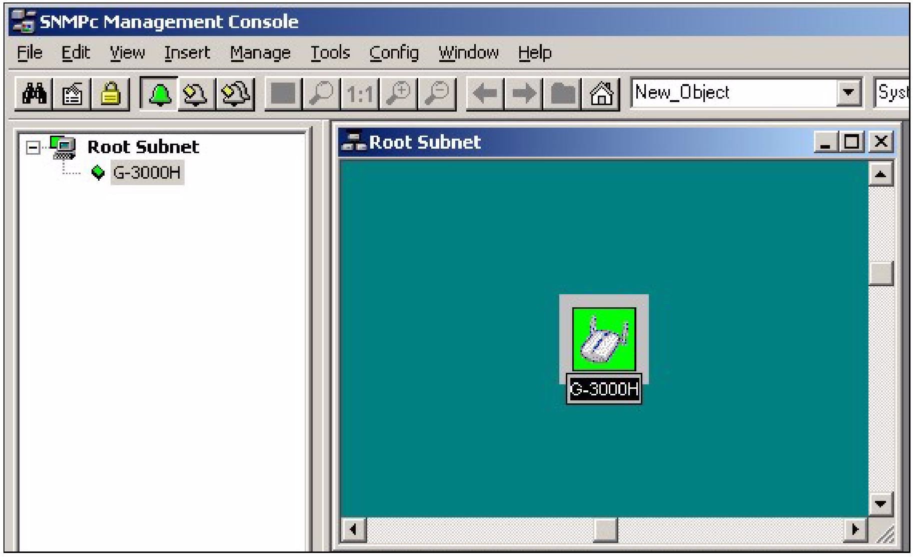
Name	Value
Read Access Mode	SNMP V2c
Read/Write Access Mode	SNMP V2c
Read Community	public
Read/Write Community	public
Trap Community	public
V3 Engineid	<auto>
V3 Context Name	<not set>
V3 No-Auth Security Name	<not set>
V3 Auth/Priv Security Name	<not set>
V3 Auth Passwd	<not set>
V3 Priv Passwd	<not set>

5 Change the read and write communities (passwords) to match the ones you use in your AP. Then click **OK**.

For security purposes, it is strongly recommended to change the Read Community and Read/Write Community on your AP. Write down this information and keep in a safe place so you will not forget it later.

6 An icon displays for the device.

Figure 271 Device Icon

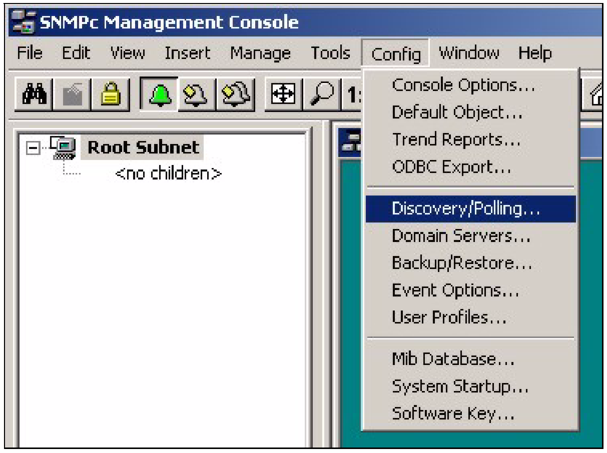


Device Auto-Discovery

Do the following to enable auto-discovery.

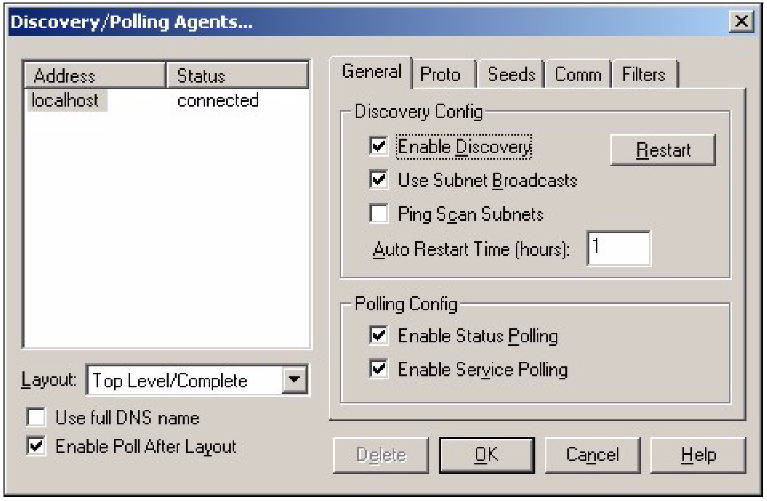
1 Click **Config**, **Discovery/Polling**.

Figure 272 Accessing the Discovery/Polling Agents Screen



2 Select the **Enable Discovery** check box and click **OK**.

Figure 273 Discovery/Polling Agents Screen



Address	Status
localhost	connected

Discovery Config

☑ Enable Discovery

☑ Use Subnet Broadcasts

☐ Ping Scan Subnets

Auto Restart Time (hours): 1

Polling Config

☑ Enable Status Polling

☑ Enable Service Polling

Layout: Top Level/Complete

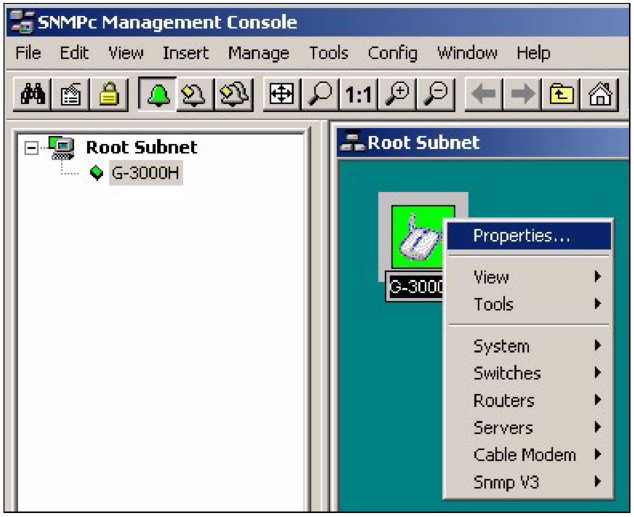
☐ Use full DNS name

☑ Enable Poll After Layout

3 After the device has been found, an icon and label appear in the network manager view window. Right-click the device icon and select **Properties**.

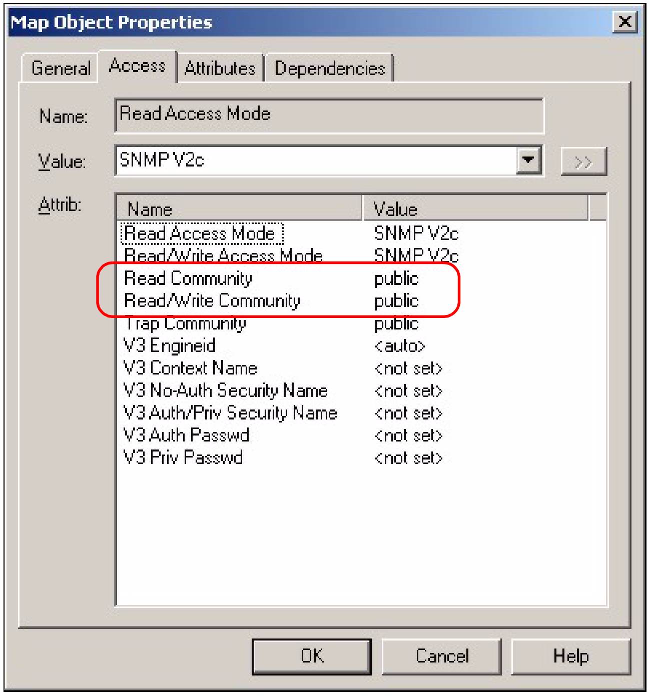
Auto-discovery may take hours for a large and complex network.

Figure 274 Device Icon



4 The **MAP Object Properties** screen opens. Click the **Access** tab.

Figure 275 MAP Object Properties: Access



Name: Read Access Mode

Value: SNMP V2c

Attrib:

Name	Value
Read Access Mode	SNMP V2c
Read/Write Access Mode	SNMP V2c
Read Community	public
Read/Write Community	public
Trap Community	public
V3 Engineid	<auto>
V3 Context Name	<not set>
V3 No-Auth Security Name	<not set>
V3 Auth/Priv Security Name	<not set>
V3 Auth Passwd	<not set>
V3 Priv Passwd	<not set>

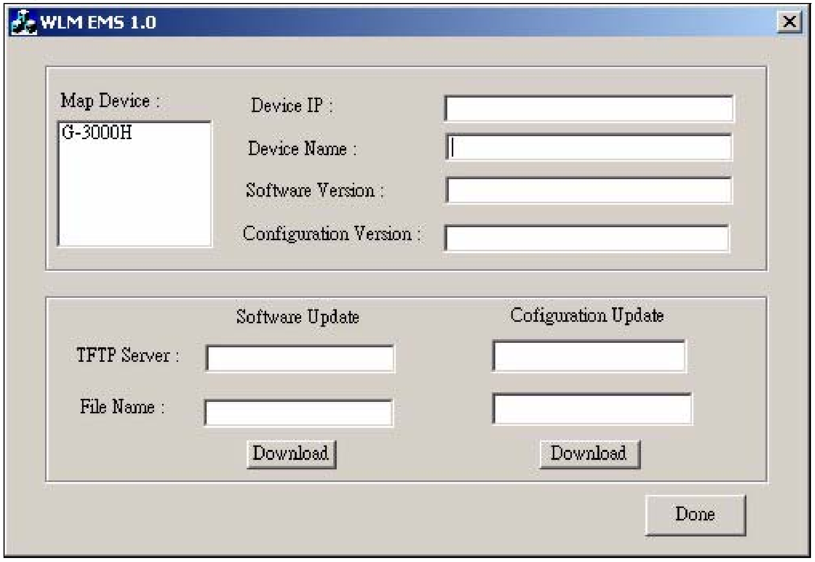
5 Change the read and write communities (passwords) to match the ones you use in your AP. Then click **OK**.

For security purposes, it is strongly recommended to change the Read Community and Read/Write Community on your AP. Write down this information and keep in a safe place so you will not forget it later.

Accessing the EMS

In the SNMPc main screen, double-click the device icon to open the **WLM EMS** screen. Use this screen to view the current firmware and text configuration file versions on an AP. You can also upload firmware and text configuration files from a TFTP server to a specific AP. This is also referred to as text file based auto configuration.

Figure 276 WLM EMS Screen



Map Device : G-3000H

Troubleshooting

1 SNMPc and/or EMS will not install properly

- Make sure that the computer on which you want to install the SNMPc and EMS meets the minimum hardware and software requirements.
- Shut down any running services or applications which may affect the installation.
- Remove any previous versions of SNMP software from your computer.
- Re-install SNMPc and EMS in that order.

2 I cannot find my device in the SNMPc Management screen.

- Check that you have added and compiled the MIBs correctly (see Section on page 339). Make sure you follow the instructions exactly.
- Check that the map object properties are correct for initial installation; see Section on page 341. Make sure the IP address entered is the IP address of the switch you want to manage via the EMS.
- If you want to use auto-discovery, make sure you have it enabled; see Section on page 344.
- Make sure that the computer you have installed the EMS on, is connected to the network where the device is located.
- Make sure your computer’s Ethernet card is working properly.
- Make sure that the device you want to manage is connected to the network and operating properly.

- If the problem still persists, uninstall and re-install the EMS software.

Legal Information

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用
者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現
有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍
受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。

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 networks 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.

K

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.

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 Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: 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 Site: www.zyxel.co.cr
- FTP Site: 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 Site: 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 Site: 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 Site: 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 Site: 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: +49-2405-6909-0
- Fax: +49-2405-6909-99
- Web Site: 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 Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

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 Site: www.us.zyxel.com
- FTP Site: 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 Site: 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 Site: 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 Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª 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 Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

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 Site: 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 Site: www.zyxel.co.uk
- FTP Site: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK, Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

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

Index