P-2900-4HB

Cable Router

User's Guide

Default Login Details	
IP Address	192.168.1.1
Password	1234

Firmware Version 3.40
Edition 1, 3/2009

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

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

Related Documentation

- Quick Start Guide

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

- Support Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

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

User Guide Feedback

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

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

E-mail: techwriters@zyxel.com.tw

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.

- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

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

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

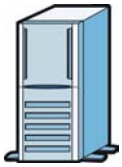
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-2900-4HB may be referred to as the "ZyXEL Device", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

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

ZyXEL Device 	Computer 	Notebook computer 
Server 	Telephone 	Switch 
Router 	Internet 	

Safety Warnings

- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- Make sure that the cable system is grounded so as to provide some protection against voltage surges.
- CAUTION: RISK OF EXPLOSION IF BATTERIES ARE REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.

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

Contents Overview

Table of Contents

PART I
Introduction and Configuration

1

Getting To Know Your ZyXEL Device

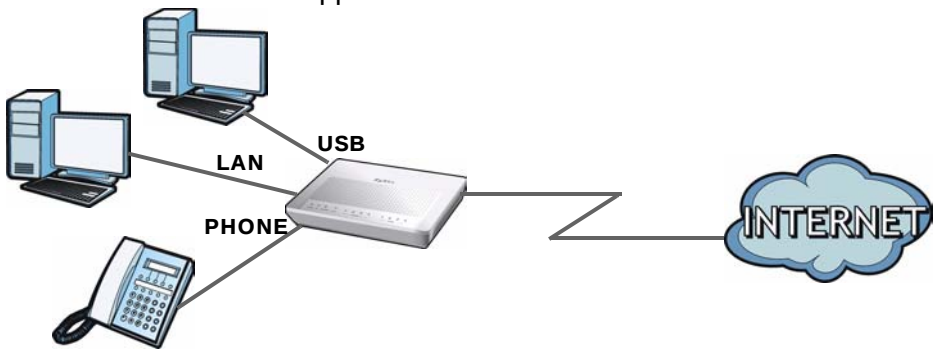
This chapter describes the key features and applications of your ZyXEL Device.

1.1 Overview

The ZyXEL Device is an embedded Multimedia Terminal Adapter (eMTA) device built with two components: a DOCSIS 2.0 cable modem component for data transfer and a PacketCable 1.5 MTA component for voice traffic. This means it can provide high-speed Internet access as well as cost-effective, standard telephone voice and fax/modem services through your cable service provider.

You can connect your computer to the ZyXEL Device either through a **LAN** or the **USB** port. Connect your telephones to the **PHONE** ports if your VoIP company gave you phone numbers.

Figure 1 Internet Access Application



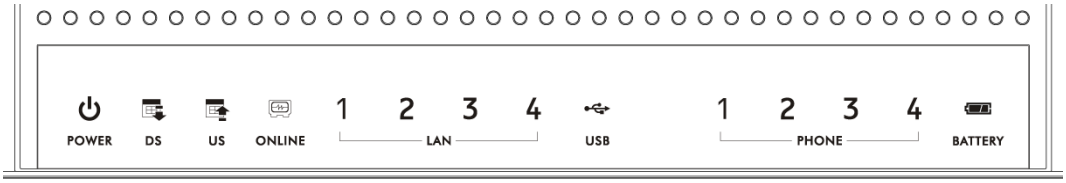
1.2 Hardware Connection and Installation

Refer to the Quick Start Guide for information about hardware connections and USB driver installation.

1.3 LEDs (Lights)

The following figure displays the labels of the LED.

Figure 2 Front Panel LEDs



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The ZyXEL Device is receiving AC power.
		Blinking	The ZyXEL Device is receiving sufficient power from the battery.
		Off	The ZyXEL Device is not receiving power or it is starting up.
DS	Green	On	The ZyXEL Device has successfully found a downstream channel.
		Blinking	The ZyXEL Device is trying to search for a downstream channel.
		Off	The downstream channel is not found.
US	Green	On	The ZyXEL Device has successfully found an upstream channel.
		Blinking	The ZyXEL Device is trying to search for an upstream channel.
		Off	The upstream channel is not found.
ONLINE	Green	On	The ZyXEL Device has successfully established a connection to the cable operator's network.
		Blinking	Slowly: The ZyXEL Device is trying to initiate a connection with the cable operator's network. Fast: The ZyXEL Device is sending/receiving data on the WAN.
		Off	The coaxial cable is not connected or the cable link is down.
LAN 1-4	Green	On	The ZyXEL Device has a successful 10/100Mb Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
		Off	The LAN is not connected.

Table 1 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
USB	Green	On	A computeris connected to the USB port on the ZyXEL Device. See Section 1.4 on page 19 for more information about the USB port.
		Blinking	The ZyXEL Device is sending/receiving data via the USB port.
		Off	The USB port is not connected.
PHONE 1-4	Green	On	The ZyXEL Device has successfully registered to an IP telephone network.
		Blinking	The phone port is in use or is getting VoIP settings from the MTA auto-provisioning server.
		Off	The phone port is not connected or has not yet connected to the MTA auto-provisioning server.
BATTERY	Green	On	• The ZyXEL Device is starting up. • The battery has sufficient power and the ZyXEL Device is using AC power. The LED turns off if the ZyXEL Device uses battery power.
		Blinking	The battery power is low.
		Off	• The ZyXEL Device is receiving sufficient power from the battery if the **PWR** LED is blinking at the same time. • The ZyXEL Device is not receiving power from the battery nor AC power. Note: The device cannot function when there is a power outage.

1.4 USB Port

The USB port is useful if you have an USB-enabled computer that does not have a network interface card available for attaching to the ZyXEL Device's LAN network. See the Quick Start Guide for details about USB driver installation procedures.

1.5 Battery Packs

You can install up to two optional battery packs in the ZyXEL Device's battery bay. This will ensure that any phones attached to the device during a power outage will continue to function for a time. See the Quick Start Guide for details about battery packs intallation procedures.

The standby time for a single battery is approximately 8 hours while the usage time is approximately 5 hours.

Note: When the battery is in use, you can only make VoIP calls. Ethernet connections will not function.

Note: Battery packs are sold separately.

2

Introducing the Web Configurator

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

2.1 Overview

The web configurator is an HTML-based management interface that allows easy setup and management via an 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).

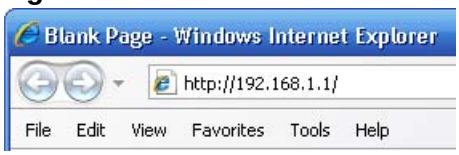
See the chapter on troubleshooting to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

Follow the steps below to log into the Web Configurator.

1 Launch your web browser. Enter “192.168.1.1” as the web site address.

Figure 3 Web browser URL screen.



2 A login screen displays. Enter the password (“1234” by default) and click **Login**.

Figure 4 Web Configurator login screen

3 It is highly recommended you change the default password! Enter a new password between 1 and 30 characters, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

If you do not change the password at least once, the following screen appears every time you log in.

Figure 5 Change Password at Login

4 You should now see the main **Site Map** screen (refer to Figure 6 on page 23).

2.2.1 Resetting the ZyXEL Device

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

2.2.1.1 Using the RESET Button

1. Make sure the **PWR** LED is on (not blinking).
2. Press and hold the **RESET** button for about 15 seconds. All LEDs should turn on. When you release the **RESET** button, the defaults have been restored and the ZyXEL Device restarts.

   You can also use the **RESET** button to restart the ZyXEL Device (without restoring the defaults) by pressing down for 2 to 14 seconds.

2.3 Navigating the Web Configurator

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

Figure 6 Status

Following table lists the menu screens.

Table 2 Web Configurator Screens Summary

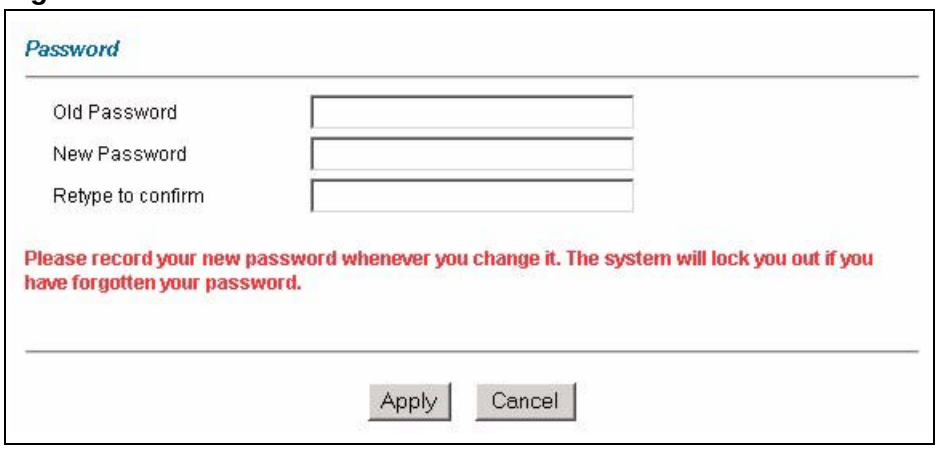
LINK	SUB-LINK	FUNCTION
Status	System Status	Use this screen to view firmware and system related information.
	CableModem Status	Use this screen to view information about the cable modem, upstream and downstream channels.
	MTA Status	Use this screen to view information about MTA and status about the VoIP ports.
Advanced Setup		
Password		Use this screen to change your password.
LAN	LAN Setup	Use this screen to configure LAN DHCP and TCP/IP settings.
	Static DHCP	Use this screen to configure static DHCP settings.
NAT		Use this screen to enable or disable Network Address Translation (NAT). You can also use this screen to configure rules the ZyXEL Device uses to convert between private to public IP addresses.
Dynamic DNS		Use this screen to set up dynamic DNS.
Static IP		Use this screen to configure up to three static WAN IP addresses and RIP settings. Configure a static IP address only if your cable service provider gave you the information. See Section 4.3 on page 41 for a configuration example.
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web to manage the ZyXEL Device.
Logs	Log Settings	Use this screen to change your ZyXEL Device's log settings.
	View Log	Use this screen to view the logs for the categories that you selected.
Maintenance	DHCP Table	This screen lists the DHCP clients connected to the ZyXEL Device.
	Diagnostic	These screen displays information to help you identify problems with the ZyXEL Device general connection.
Logout		Click this to exit the Web Configurator.

2.4 Change Login Password

It is highly recommended that you periodically change the password for accessing the ZyXEL Device. If you didn't change the default one after you logged in or you

want to change to a new password again, then click **Password** in the **Site Map** screen to display the screen as shown next.

Figure 7 Password



The following table describes the fields in this screen.

Table 3 Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

3

Status

3.1 Overview

This chapter describes the status screens you can display the ZyXEL Device's firmware and system information.

3.2 What You Can Do in the Status Screens

- Use the **System Status** screen (see Section 3.3 on page 30) to view firmware, LAN and WAN information.
- Use the **Cable Modem Status** screen (see Section 3.4 on page 32) to view status information about the cable modem, upstream and downstream channels.
- Use the **MTA Status** screen (see Section 3.5 on page 36) to view status information about the VoIP module and the phone ports.

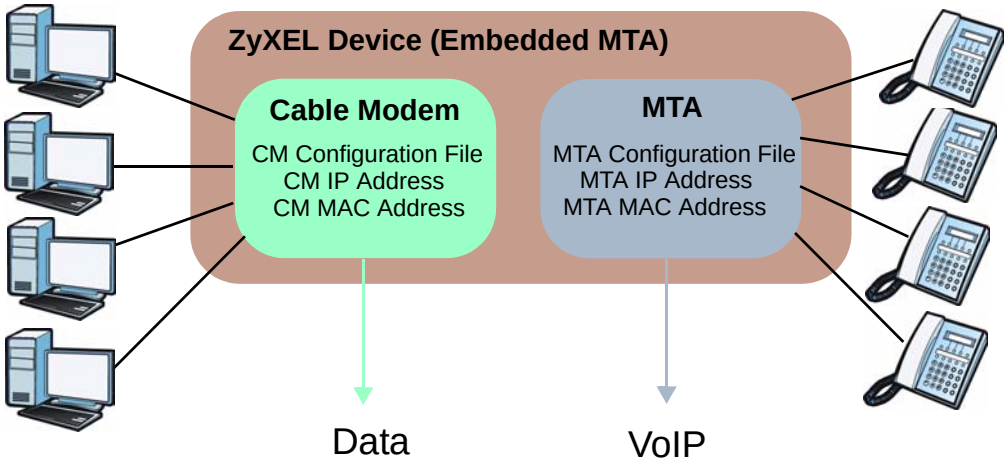
3.2.1 What You Need to Know About Status

CM and MTA

The ZyXEL Device functions as two independent units: the cable modem part and the Multimedia Terminal Adapter (MTA) part. Each part goes through the auto-provisioning stage to obtain its own configuration file, IP and MAC addresses. The

cable modem part is used for data traffic, and the MTA part is used for VoIP traffic. The following figure illustrates how it works.

Figure 8 CM and MTA



Management IP Addresses

The ZyXEL Device automatically gets one CM and one MTA management IP addresses from the cable service provider when the cable connection is established. They are private IP addresses. The ZyXEL Device uses these to communicate with the service provider's network. When the cable connection is not ready, you can access the Web Configurator using its LAN IP address (default is 192.168.1.1). When the cable connection is up, you can access the Web Configurator either using its LAN or WAN static IP address.

WAN IP Address(es)

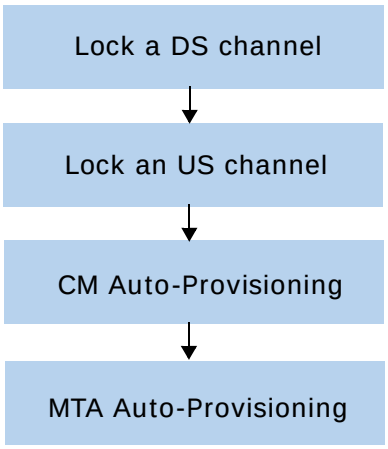
If your computers/devices need to access the Internet or provide services to Internet users, you must apply for one or multiple public IP addresses from your cable service provider. The WAN interface can have up to three public IP addresses. Configure them in the **Advanced Setup** > **Static IP** screen. See Section 4.3 on page 41 for a configuration example.

Cable Network Initiation Process

The ZyXEL Device has to communicate with your cable operator's Cable Modem Terminal Service (CMTS) in order to establish a cable network connection. As

illustrated in the following figure, it requires several steps to complete the initiation process.

Figure 9 Cable Network Initiation Process



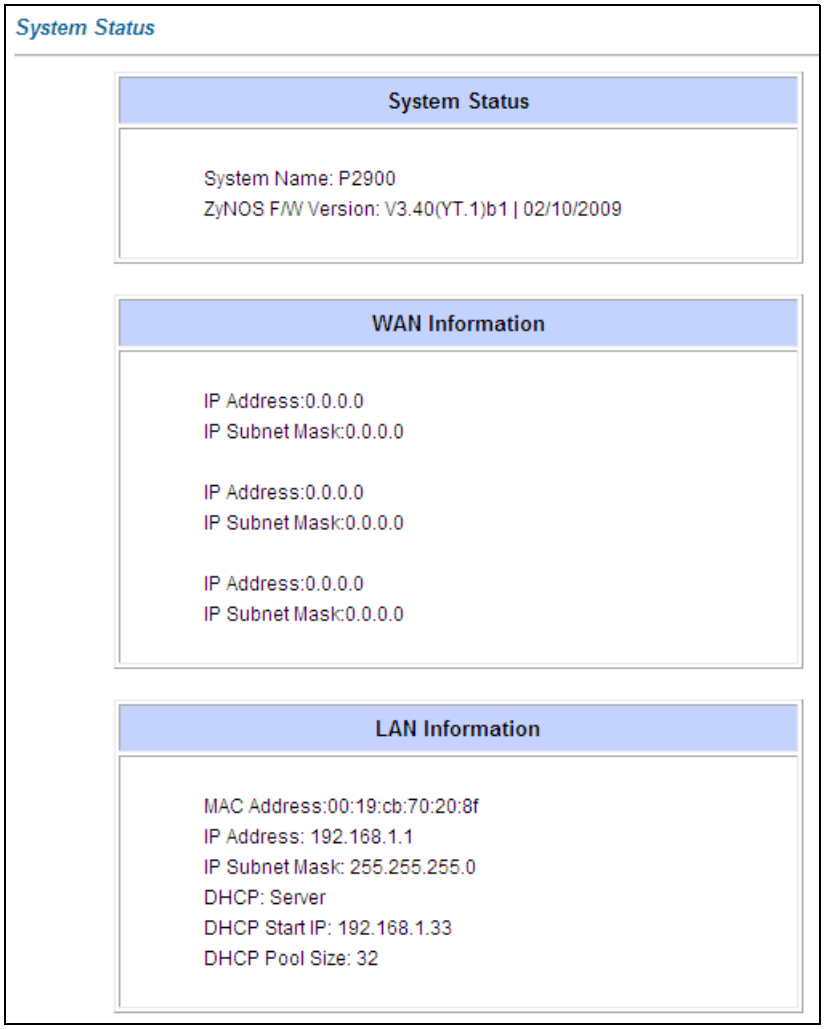
- Search and lock a downstream channel.
- Search and lock an upstream channel.
- Auto-provisioning of the cable modem settings.
- Auto-provisioning of the MTA settings.

See Section on page 32 for more details about the provisioning process.

3.3 The System Status Screen

Click **Status > System Status** to open the following screen. Check these fields when there is a problem with the network connection.

Figure 10 Status > System Status



The following table describes the labels in this screen.

Table 4 Status > System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the ZyXEL Device's name. It is for identification purpose.
ZyNOS F/W Version	This is the current version of the firmware the device uses. It also shows the date the firmware was created.
WAN Information	

Table 4 Status > System Status (continued)

LABEL	DESCRIPTION
IP Address	This is the static IP address you configured in the **Advanced Setup** > **Static IP** screen. Normally, this is a public IP address used to communicate with the Internet. The IP address appears as **0.0.0.0** if you did not configure a static IP address.
IP Subnet Mask	This is the subnet mask of the static IP address.
LAN Information	
MAC Address	This is the Media Access Control (MAC) or Ethernet address unique to your ZyXEL Device.
IP Address	This is the LAN IP address.
IP Subnet Mask	This is the subnet mask of the LAN.
DHCP	This field displays the DHCP mode the ZyXEL Device is providing to the LAN. Choices are: **Server** - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to DHCP clients in the LAN. **Relay** - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote DHCP server and the clients. **None** - The ZyXEL Device is not providing any DHCP services to the LAN. Select this to **None** and turn the NAT off if you want your computers to get DHCP IP addresses from your service provider's DHCP server, rather than the ZyXEL Device.
DHCP Start IP	This is the first address of the contiguous addresses in the DHCP IP address pool that the ZyXEL Device assigns to DHCP clients on your LAN.
DHCP Pool Size	This is the size or count of the DHCP IP address pool. This indicates the number of DHCP clients that can receive IP addresses from the ZyXEL Device.

3.4 The Cable Modem Status Screen

This section describes the information in the **Cable Modem Status** screen.

3.4.1 What You Need to Know About Cable Modem Status

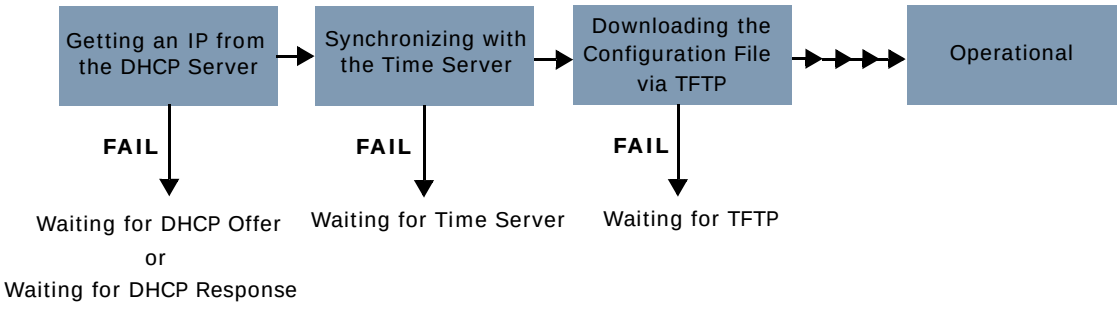
Downstream/Upstream Channels

In order to establish a successful connection with the cable provider's network, the ZyXEL Device must first find and lock onto two frequencies for communication with the cable operator's network. A frequency is also called a channel. Communication with the cable operator's network cannot proceed until the ZyXEL Device locks specific channels for sending and receiving data.

Auto-Provisioning

During the provisioning step, your ZyXEL Device passes through several negotiation stages with the CMTS, as illustrated in the following figure. The ZyXEL Device has to obtain an IP address, set the system's time/date and download the configuration file. If any step fails, the "**Waiting for...**" message will appear in the **CM Status** screen.

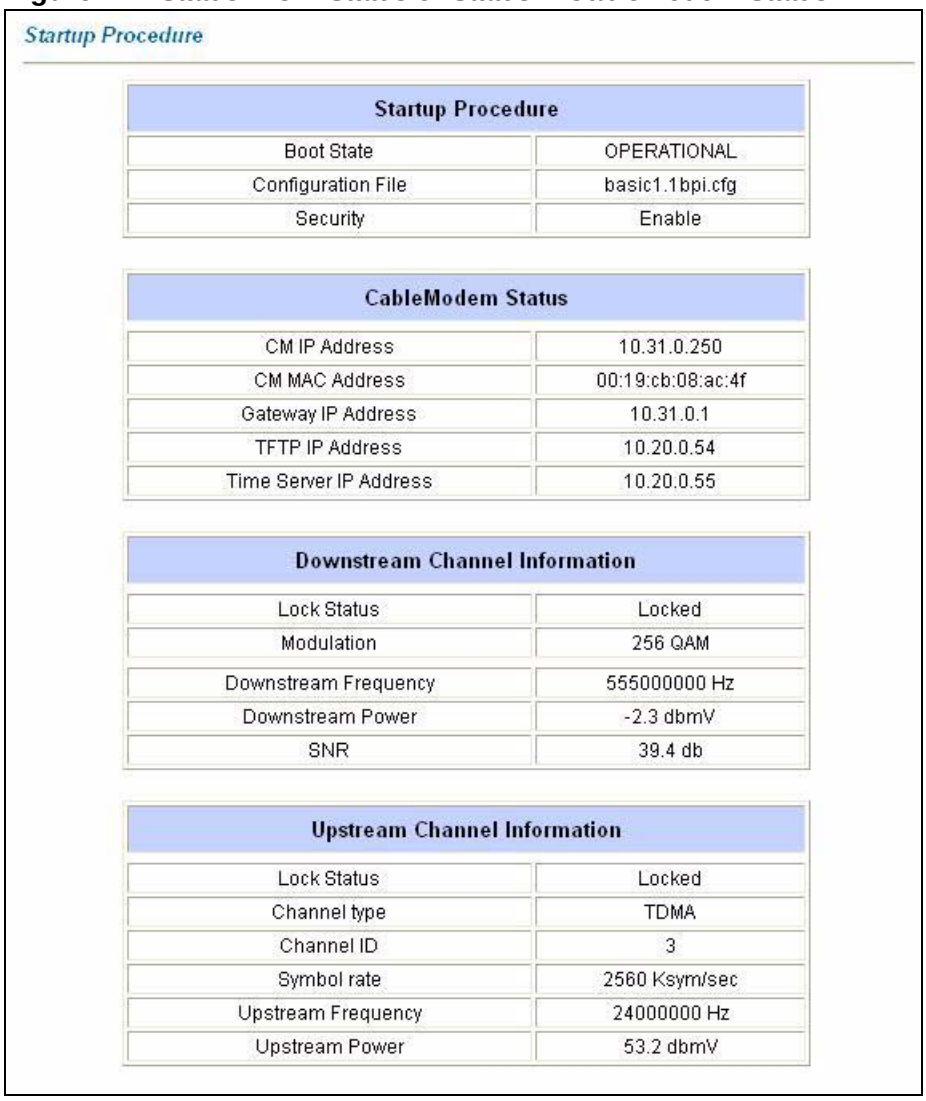
Figure 11 Negotiation Stages with the CMTS



3.4.2 Viewing the Cable Modem Status Screen

Click **Status > CM Status** or **Status** > **CableModem Status** to open the following screen.

Figure 12 Status > CM Status or Status > CableModem Status



The following table describes the labels in this screen.

Table 5 Status > CM Status or Status > CableModem Status

LABEL	DESCRIPTION
Startup Procedure	To establish a successful connection to the cable provider's network, the ZyXEL Device must go through a series of well-defined initialization steps.
Boot State	This is the provision status of the cable modem. • **In Progress** - The ZyXEL Device is in the negotiation process with the CMTS. • **OK** - The ZyXEL Device completed configuration. • **Disabled** - The ZyXEL Device's WAN connection has been disabled. • **Waiting for DHCP Offer** - The ZyXEL Device is waiting for a DHCP server to offer it an IP address. • **Waiting for DHCP Response** - The ZyXEL Device is waiting for a response from the DHCP server. • **Waiting for Time Server** - The ZyXEL Device is waiting for a response from the time server. • **Waiting for TFTP** - The ZyXEL Device is waiting for a response from the TFTP server. • **Operational** - The ZyXEL Device has successfully gone through the boot up process. • **Refused by CMTS** - The ZyXEL Device could not complete one of the initialization steps.
Configuration File	This is the name of the configuration file on the ZyXEL Device. This is a binary format file which must be DOCSIS 2.0 compliant (see RFC 2132 for additional information). The field is blank if there was a problem in obtaining or installing the configuration file. • **OK** - The ZyXEL Device obtains a configuration file from the CMTS, and installs it. • **In Progress** - The ZyXEL Device is trying to obtain a configuration file from the CMTS.
Security	This shows whether an encryption method is enabled or disabled to protect data flow over the Internet. DOCSIS uses Baseline Privacy Interface (BPI) and BPI+ as the encryption methods.
CableModem Status	
CM IP Address	This is the IP address negotiated with your cable operator, after a successful DHCP negotiation (for example, 10.21.0.11) and download of the modem configuration file. This field may also be blanked out with a series of dashed lines (--- --- --- ---) indicating that the modem configuration failed or is in progress; no IP address has been set.
CM MAC Address	This is the MAC address unique to your ZyXEL Device.
Gateway IP Address	This is the IP address of the default gateway, if applicable.
TFTP IP Address	This is the IP address of the TFTP.
Time Server IP Address	This is the IP address of the time server.
Downstream Channel Information	This is the data path used by the CMTS for sending information to your ZyXEL Device.

Table 5 Status > CM Status or Status > CableModem Status (continued)

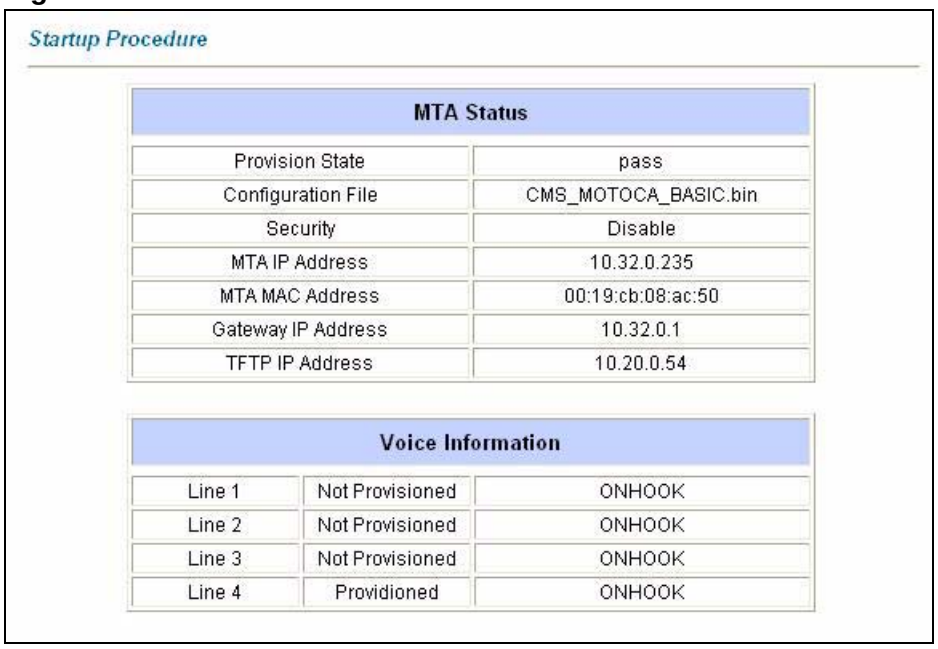
LABEL	DESCRIPTION
Lock Status	This indicates whether ZyXEL Device has found a downstream channel. The ZyXEL Device is either **Locked** or **Not Locked** on to the channel advertised by the CMTS.
Modulation	This is the method used to encode transmission information, similar to FM or AM on your radio. The ZyXEL Device supports **256 QAM** or **64 QAM** (Quadrature Amplitude Modulation) for the downstream channel.
Downstream Frequency	This is a standard channel frequency (in hertz) from the DOCSIS 2.0 specification.
Downstream Power	The is the power level in decibels/mili-volt (dbmV). This value is set by the CMTS.
SNR	The SNR (Signal to Noise Ratio), in decibels/mili-volt, is the ratio of signal power to channel noise power. This value is set by the CMTS.
Upstream Channel Information	This is the data path used by the CMTS for receiving information from your ZyXEL Device.
Lock Status	This indicates whether ZyXEL Device has found an upstream channel. The ZyXEL Device is either **Locked** or **Not Locked** on to the channel advertised by the CMTS.
Modulation	This is the method used to encode transmission information, similar to FM or AM on your radio. The ZyXEL Device supports **TDMA**, **ATDMA**, **SCDMA**, **Mixed** or **Unknown** for the upstream channel.
Channel ID	This is a standard channel number from the DOCSIS 2.0 specification. Channel numbers and channel frequencies are specified in pairs in DOCSIS 2.0.
Symbol Rate	This is the symbol rate (in Kilo symbols/second) for communication between the CMTS and the ZyXEL Device. This is set during initial configuration with a value supplied by the CMTS. Typical values for QAM64 and QAM256 are 5.05 Mega-symbols/second and 5.36 Mega-symbols/second.
Upstream Frequency	This is a standard channel frequency (in hertz) from the DOCSIS 2.0 specification.
Upstream Power	The is the power level in decibels/mili-volt (dbmV). This value is set by the CMTS.

3.5 The MTA Status Screen

The Multimedia Terminal Adapter (MTA) supports conversion between analog telephone signals and IP data packets, providing Voice over IP (VoIP) interfaces for analog telephones.

Use the **MTA Status** screen to view information about the MTA. Click **Status** > **MTA Status** to display the screen as shown.

Figure 13 Status > MTA Status



The following table describes the labels in this screen.

Table 6 Status > MTA Status

LABEL	DESCRIPTION
MTA Status	
Provision State	This is the provision state of the MTA.
Configuration File	This is the name of the configuration file downloaded for the MTA.
Security	This shows whether the ZyXEL Device encrypts voice traffic (using 3DES or AES).
MTA IP Address	This is the IP address negotiated for the MTA, after a successful DHCP negotiation (e.g.10.21.0.11) and download of the configuration file. This field may also be blanked out with a series of dashed lines (--- --- --- ---) indicating that the modem configuration failed or is in progress; no IP address has been set.
MTA MAC Address	This is the MAC address unique for the MTA.

Table 6 Status > MTA Status (continued)

LABEL	DESCRIPTION
Gateway IP Address	This is the IP address of the default gateway, if applicable.
TFTP IP Address	This is the IP address of TFTP.
Voice Information	
Line 1-4	This field shows the status information about the VoIP ports.

4

Tutorials

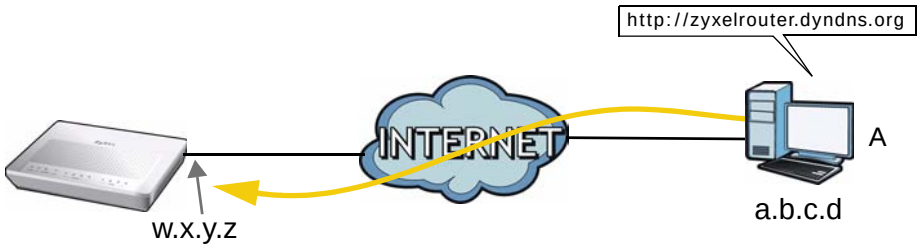
4.1 Overview

This chapter shows you how to use the ZyXEL Device's various features.

- Access the ZyXEL Device Using DDNS, see page 39
- Multiple WAN Configuration, see page 41

4.2 Access the ZyXEL Device Using DDNS

If you connect your ZyXEL Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The ZyXEL Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the ZyXEL Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial shows you how to:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your ZyXEL Device
- Testing the DDNS Setting

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

4.2.1 Registering a DDNS Account on www.dyndns.org

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

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

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

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

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

Then you will need to configure the same account and host name on the ZyXEL Device later.

4.2.2 Configuring DDNS on Your ZyXEL Device

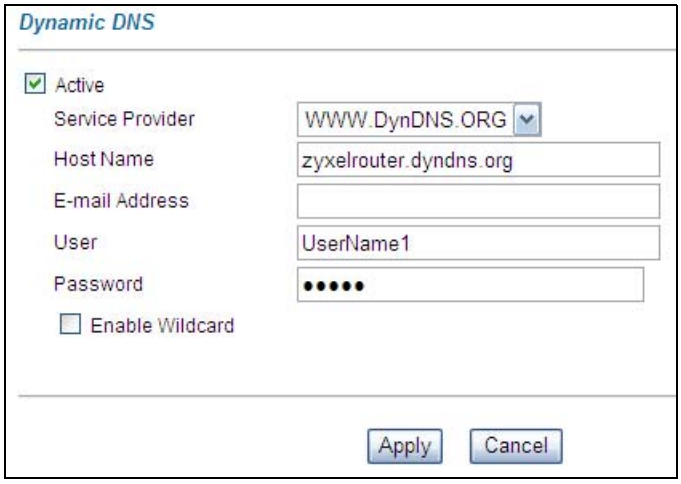
1 Log into the ZyXEL Device's advanced mode.

2 Configure the following settings in the **Advanced Setup** > **Dynamic DNS** screen.

2a Select **Active**.

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

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



2d Click **Apply**.

4.2.3 Testing the DDNS Setting

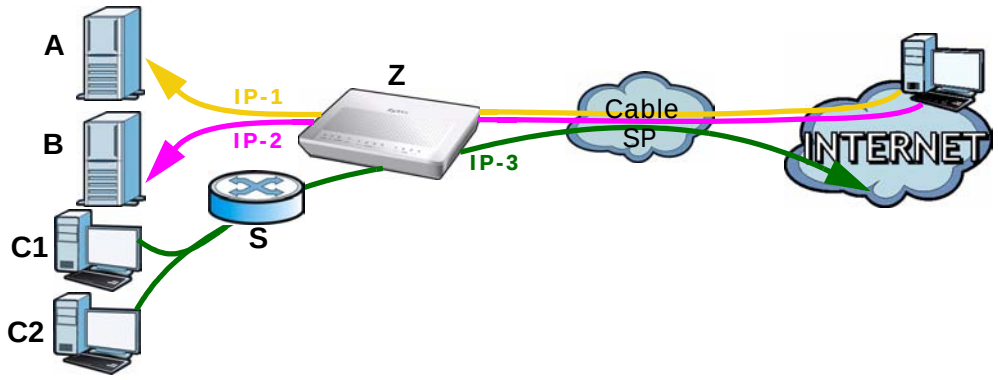
Now you should be able to access the ZyXEL Device from the Internet. To test this:

1. Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
2. Type **http://zyxelrouter.dyndns.org** and press [Enter].
3. The ZyXEL Device's login page should appear. You can then log into the ZyXEL Device and manage it.

4.3 Multiple WAN Configuration

A company uses the ZyXEL Device (**Z**) to connect to a cable network. They apply for three public IP addresses from the service provider (**Cable SP**) in order to provide web (**A**) and FTP (**B**) services to public users and Internet access for company users (**C1** and **C2**). A computer from the Internet can access server **A** through **IP-1** and server **B** through **IP-2**. **C1** and **C2** connect to the ZyXEL Device's LAN through a switch (**S**). The ZyXEL Device uses NAT to convert private LAN IP addresses to **IP-3** for outgoing Internet packets.The following figure shows you an example.

Figure 14 Multiple WAN Application



This tutorial uses the following example settings:

Table 7 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
Static IP 1	1.1.1.1/24
Static IP 2	2.2.2.1/24
Static IP 3	3.3.3.1/24
LAN IPs	Management IP: 192.168.1.1/24 DHCP Type: Server DHCP IP Range: 192.168.1.33~192.168.1.64
A's IP	1.1.1.5/24 (**IP-1**), gateway: 1.1.1.1
B's IP	2.2.2.5/24 (**IP-2**), gateway: 2.2.2.1
NAT	On, Many-to-One

Note: You have to apply for a public IP address if you need one and configure it as a static IP address on the Web Configurator.

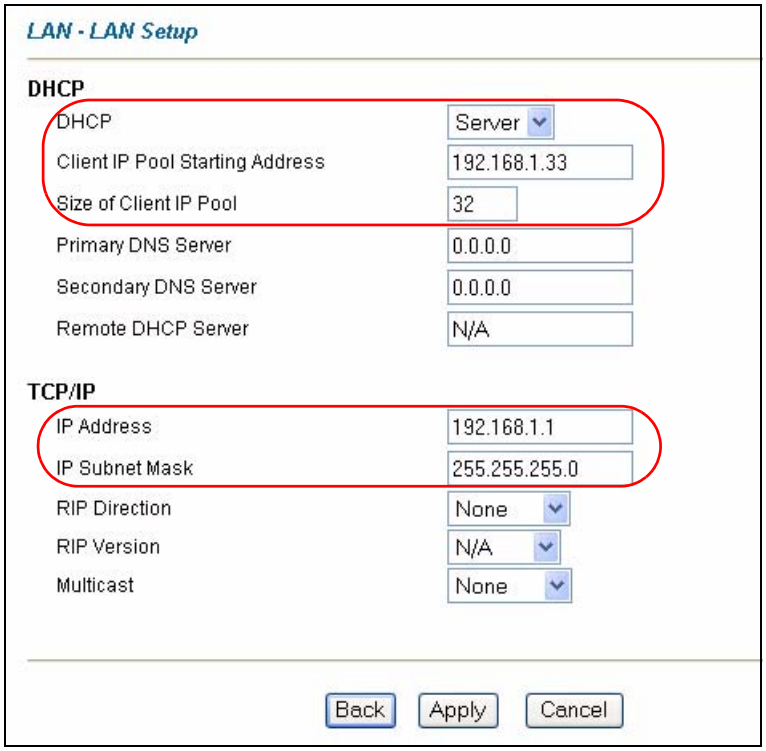
4.3.1 Network Setup and IP Settings

Use this section to set up the network and configure the IP settings on servers **A** and **B**. This section also shows how to enable DHCP for LAN computers IP assignments.

1. This tutorial assumes your ZyXEL Device has successfully connected to the cable network. You should see the **ONLINE** LED is on from the ZyXEL Device's front panel.

2. Configure the IP addresses on **A** and **B** (see Table 7). Connect them to the ZyXEL Device's LAN. Turn on the Web and FTP services on **A** and **B** respectively.

3 Log into the ZyXEL Device's Web Configurator. Configure the **Advanced Setup** > **LAN** screen as shown next. Click **Apply**.

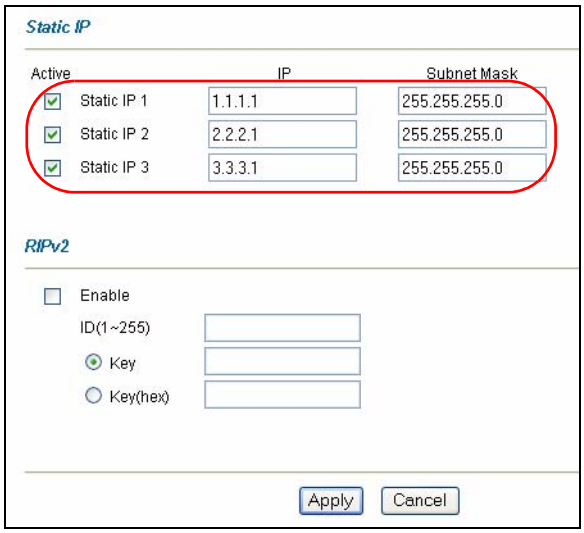


4 Enable DHCP client on computers **C1** and **C2** by selecting **Obtain an IP address automatically** in the network settings. Connect them to the ZyXEL Device's LAN through a switch. Each of them should get an IP address respectively.

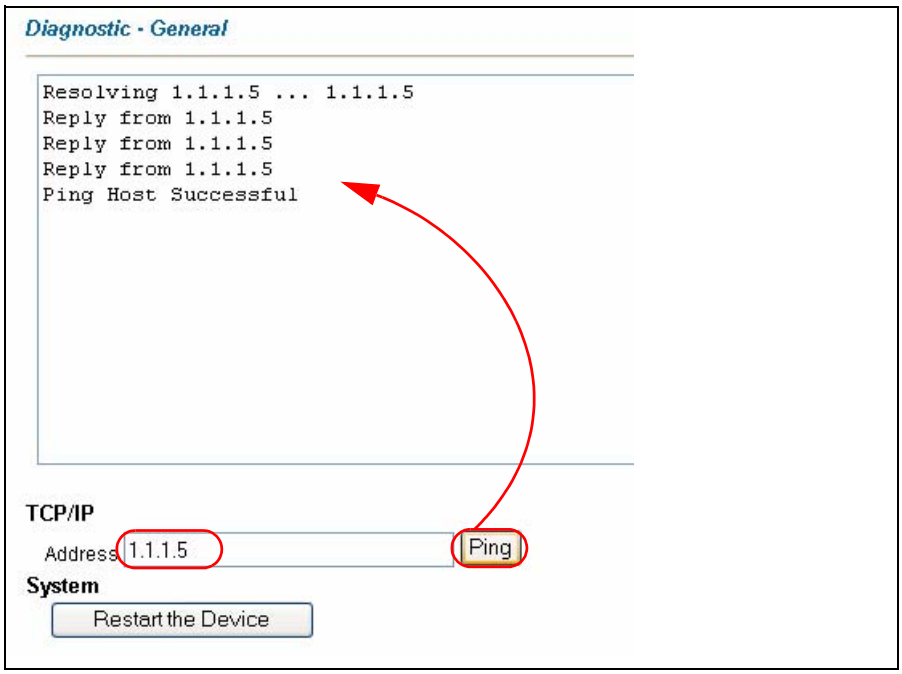
4.3.2 Configuring Static IP Addresses

Use this section to configure two static IP addresses for servers **A** and **B**. Computers (**C1**~**C2**) also use one static IP address to access the Internet.

1 Configure the **Advanced** > **Static IP** screen as shown. Click **Apply**.



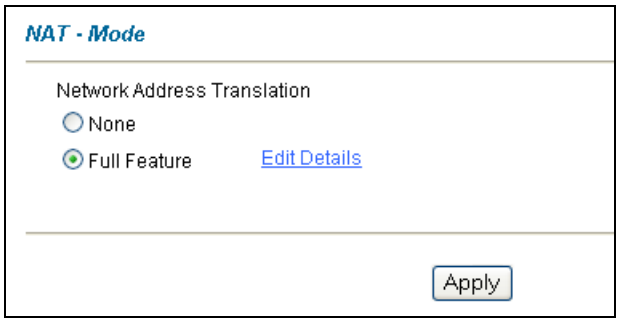
2 Ping **A** and **B** in the **Maintenance** > **Diagnostic** screen to test the connectivity. You should get **A**'s and **B**'s responses. If they fail, make sure the network is correctly connected and if each server has a firewall that they allow ping packets from the ZyXEL Device. An example is shown next.



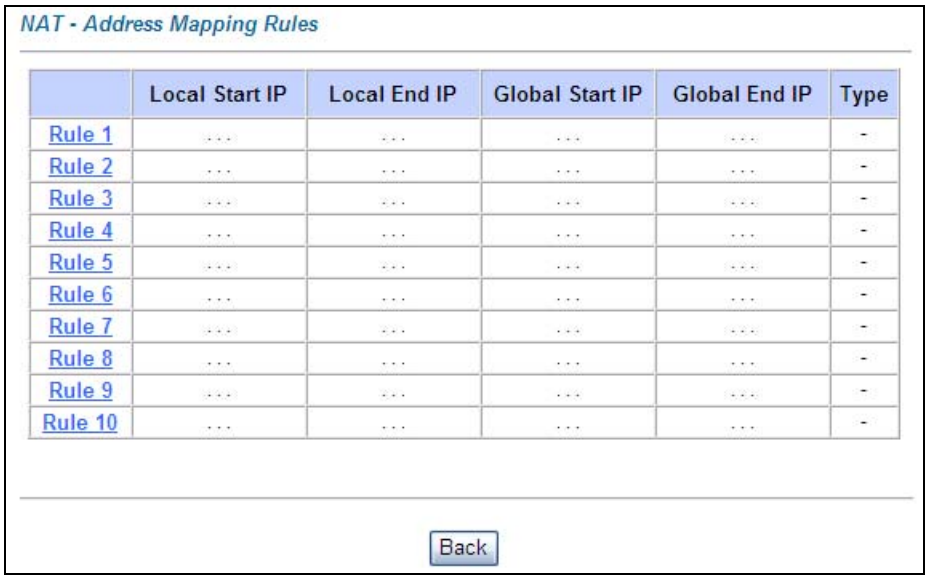
4.3.3 Configuring NAT

You must enable NAT on the ZyXEL Device if you want your LAN computers to access the Internet using private IP addresses.

1 Select **Full Feature** and click **Apply** in the **Advanced Setup** > **NAT** screen.

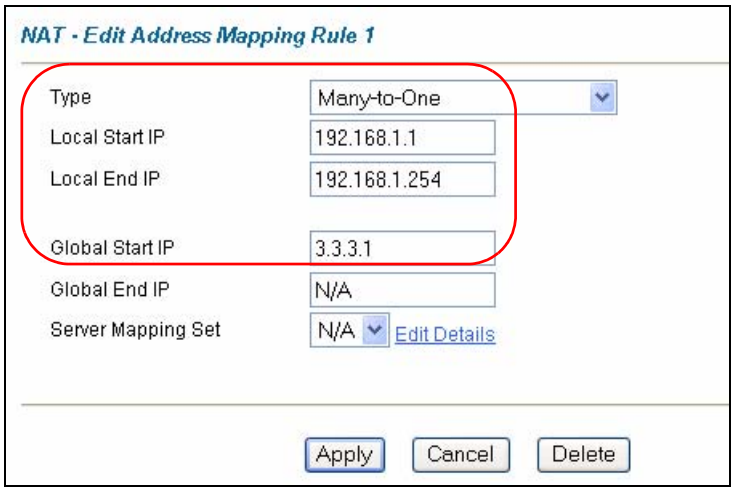


2 Click the **Edit Details** link in the **NAT-Mode** screen above. The **NAT - Address Mapping Rules** screen appears as shown next.



3 Click the **Rule 1** link.

4 Configure the settings as shown next. Then click **Apply**.



5 Computer **C1** should be able to connect to the Internet.

4.3.4 Access the Web/FTP Services from the Internet

Use a computer on the Internet to access http://1.1.1.5 and ftp://2.2.2.5. You should be able to access a web page on **A** and the FTP login screen on **B**.

PART II
Advanced Setup

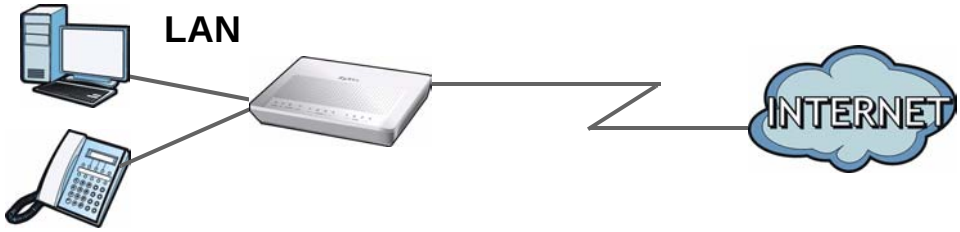
5

LAN Setup

5.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is limited to the immediate area, usually the same building or floor of a building.

Use the **LAN** screens to help you configure a LAN DHCP server and manage IP addresses.



5.1.1 What You Can Do in the LAN Screens

- Use the **LAN Setup** screen (Section 5.2 on page 51) to configure the DHCP settings, and set the LAN IP address and subnet mask of your ZyXEL Device. You can also edit your ZyXEL Device's RIP, Multicast and Any IP from this screen.
- Use the **Static DHCP** screen (Section 5.2 on page 51) to configure the static DHCP settings of your ZyXEL Device.

5.1.2 What You Need To Know About LAN

IP Address

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 Mask

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.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your ZyXEL Device an IP address, subnet mask, DNS and other routing information when it's turned on.

RIP

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

Multicast

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

IGMP

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

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

Finding Out More

See Section 5.4 on page 54 for technical background information on LANs.

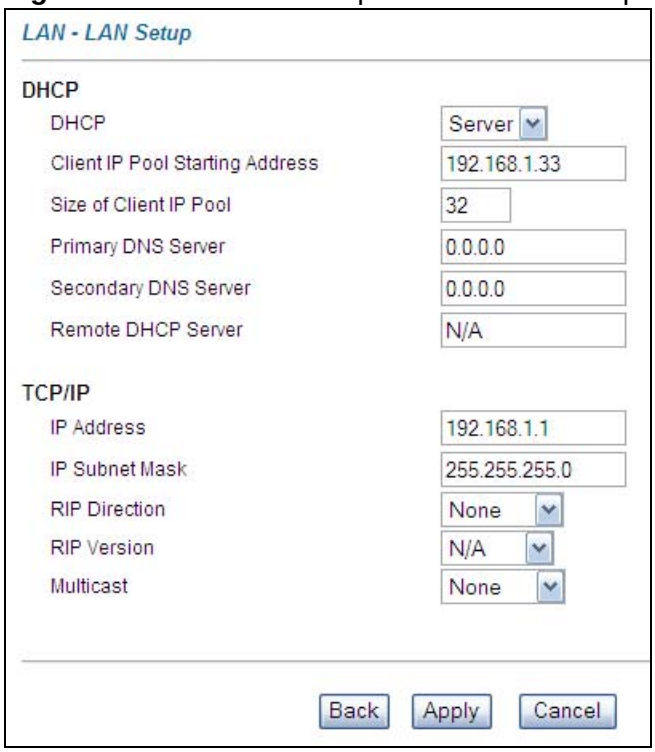
5.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

5.2 The LAN Setup Screen

Click **Advanced Setup** > **LAN** > **LAN Setup** to open the **LAN Setup** screen.

Figure 15 Advanced Setup > LAN > LAN Setup



The following table describes the fields in this screen.

Table 8 Advanced Setup > LAN > LAN Setup

LABEL	DESCRIPTION
DHCP	
DHCP	If set to **Server**, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case. When DHCP is used, the following items need to be set.
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.

Table 8 Advanced Setup > LAN > LAN Setup (continued)

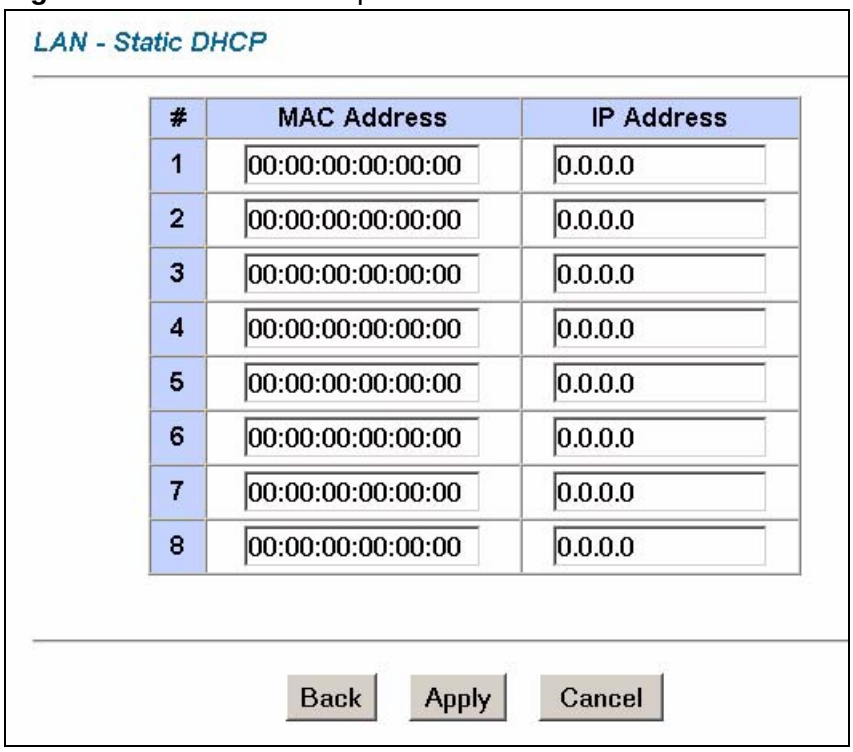
LABEL	DESCRIPTION
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.
TCP/IP	
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.100.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**. The **RIP Direction** field controls the sending and receiving of RIP packets.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**. The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving).
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP versions 1 (**IGMP-v1**) and 2 (**IGMP-v2**). Select **None** to disable it.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.3 The Static DHCP Screen

Click **Advanced Setup** > **LAN** > **Static DHCP** to open the **Static DHCP** screen. A DHCP server may assign a different IP address to a computer when its DHCP

lease expires. If you want the computer to always receive the same IP address from the DHCP server, then configure a static DHCP IP address here.

Figure 16 Advanced Setup > LAN > Static DHCP



The following table describes the fields in this screen.

Table 9 Advanced Setup > LAN > Static DHCP

LABEL	DESCRIPTION
#	This is the index number for the entries in this table.
MAC Address	Type the MAC address of the computer to which you want to assign a specific DHCP IP address. Use hexadecimal characters in the following format: “0A:A0:00:BB:CC:DD”
IP Address	Type the IP address you want to dedicate to the computer in dotted decimal notation, for example, “150.222.0.1”.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.4 LAN Technical Reference

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

5.4.1 DHCP Setup

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

IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

5.4.2 DNS Server Address

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

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you the DNS server addresses, enter them in the DNS Server fields in the **LAN Setup** screen.
- The ZyXEL Device acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left blank in the **LAN Setup** screen.

5.4.3 LAN TCP/IP

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

IP Address and Subnet Mask

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 were the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

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

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

Private IP Addresses

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

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

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

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

5.4.4 RIP Setup

RIP Directions

The sending and receiving of RIP packets can occur in the following ways:

- Both - the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- In Only - the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- Out Only - the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- None - the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

RIP Versions

RIP-1 is universally supported, but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

5.4.5 Multicast

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

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

The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks

to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

6

Network Address Translation (NAT) Screens

6.1 Overview

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

6.1.1 What You Can Do in the NAT Screen

Use the **NAT Mode** screen (Section 6.2 on page 60) to disable NAT, or enable and configure NAT mapping rules.

6.1.2 What You Need to Know About NAT

Inside/Outside

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back,

NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Finding Out More

See Section 6.3 on page 63 for technical background information on NAT.

6.2 The NAT Mode Screen

You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device. Click **Advanced Setup** > **NAT** to open the following screen.

Figure 17 Advanced Setup > NAT

The following table describes the labels in this screen.

Table 10 Advanced Setup > NAT

LABEL	DESCRIPTION
None	Select this to disable NAT.
Full Feature	Select this to enable NAT.
Edit Details	Click this link to take you to a screen where you can configure public and private IP mapping rules.
Apply	Click **Apply** to save your configuration.

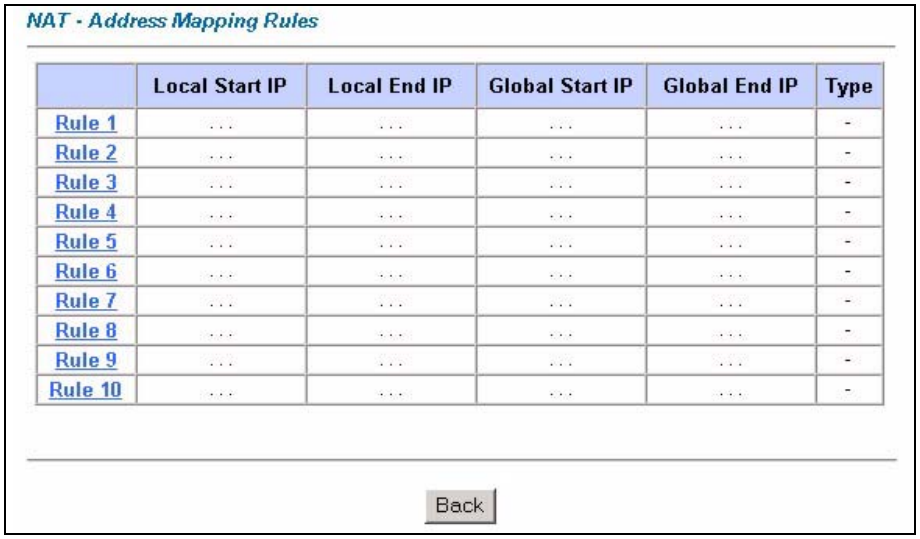
6.2.1 Configuring Address Mapping Rules

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete

rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

Click **Advanced Setup** > **NAT**, select **Full Feature** and click **Edit Details** to open the following screen. Use this screen to change your ZyXEL Device's address mapping settings.

Figure 18 Address Mapping Rules



The following table describes the fields in this screen.

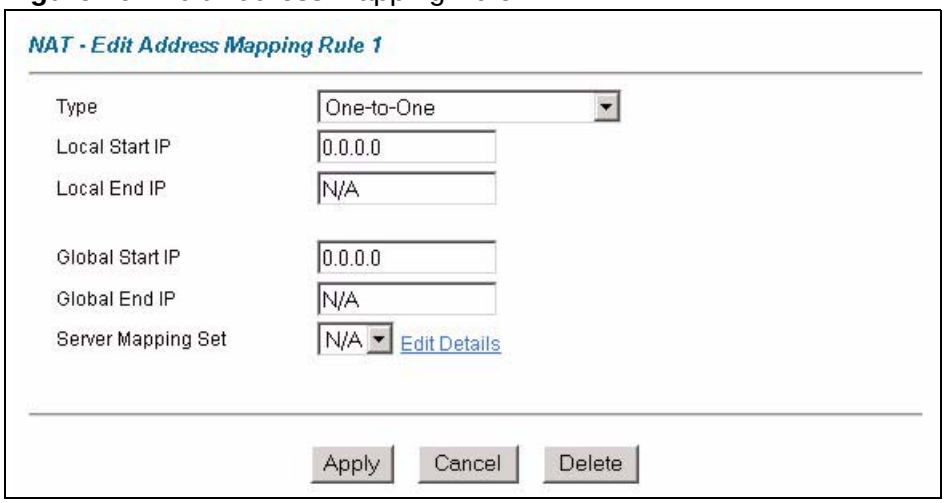
Table 11 Address Mapping Rules

LABEL	DESCRIPTION
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.
Type	**1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Back	Click **Back** to return to the **NAT Mode** screen.

6.2.2 Editing an Address Mapping Rule

Use this screen to edit an address mapping rule. Click the rule's link in the **NAT Address Mapping Rules** screen to display the screen shown next.

Figure 19 Edit Address Mapping Rule



The following table describes the fields in this screen.

Table 12 Edit Address Mapping Rule

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. • **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. • **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. • **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	Only available when **Type** is set to **Server**. Select a number from the drop-down menu to choose a server set from the **NAT - Address Mapping Rules** screen.
Edit Details	Click this link to go to the **NAT - Edit NAT Server Set** screen to edit a server set that you have selected in the **Server Mapping Set** field.

Table 12 Edit Address Mapping Rule (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previously saved settings.
Delete	Click **Delete** to exit this screen without saving.

6.3 NAT Technical Reference

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

6.3.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 13 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

6.3.2 What NAT Does

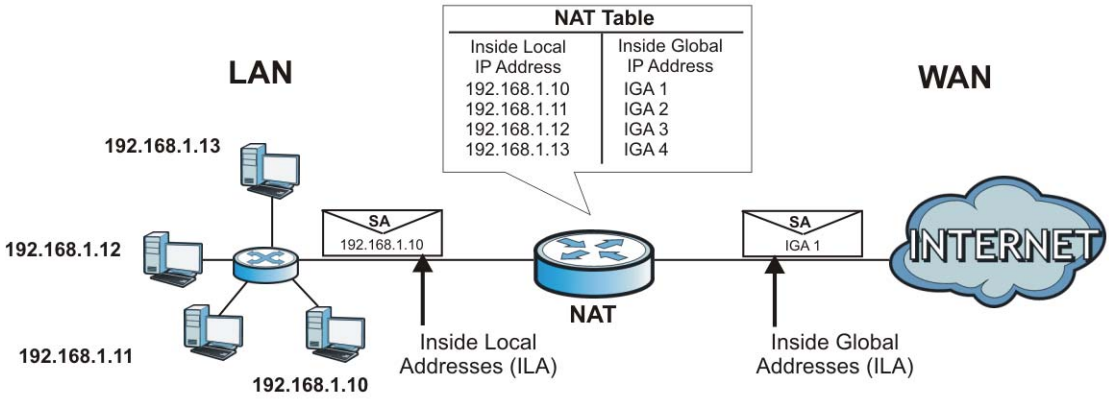
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One – see Table 14 on page 65), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

6.3.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 20 How NAT Works



6.3.4 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyXEL Device maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyXEL Device maps multiple local IP addresses to one global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** NAT mapping type.

The following table summarizes these types.

Table 14 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1←→ IGA1
Many-to-One	ILA1←→ IGA1 ILA2←→ IGA1 ...
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1

7

Dynamic DNS Setup

7.1 Overview

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

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

7.1.1 What You Can Do in the Dynamic DNS Screen

Use the **Dynamic DNS** screen (Section 7.2 on page 68) to enable DDNS and configure the DDNS settings on the ZyXEL Device.

7.1.2 What You Need to Know About Dynamic DNS

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

7.2 The Dynamic DNS Screen

To change your ZyXEL Device's DDNS, click **Advanced Setup** > **Dynamic DNS**. The screen appears as shown.

Figure 21 Advanced Setup > Dynamic DNS

The following table describes the fields in this screen.

Table 15 Advanced Setup > Dynamic DNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Host Names	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider.
E-mail Address	Type your e-mail address.
User	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8

Static IP

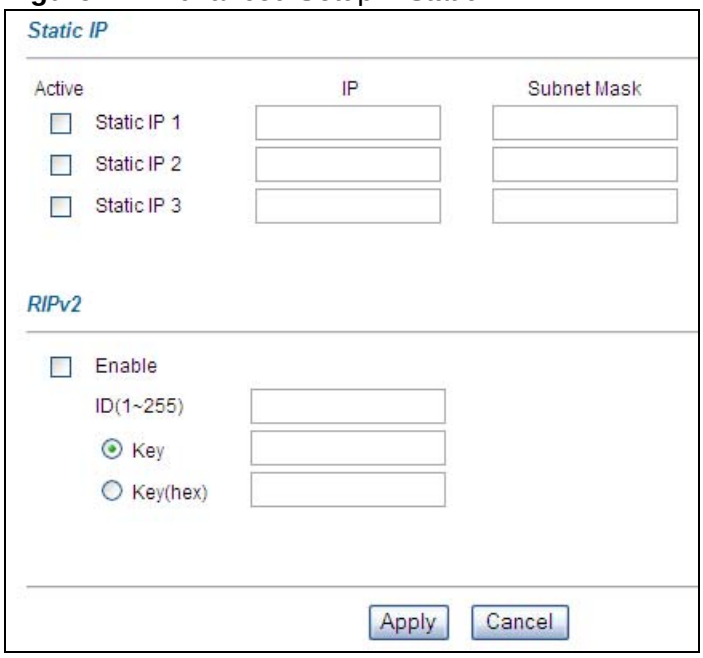
8.1 Overview

Use the **Static IP** screen (see Section 8.2 on page 69) to assign static IP addresses and configure the RIPv2 settings. See the Section 4.3 on page 41 for an application example of how you can use static IP addresses.

8.2 The Static IP Screen

Click **Advanced Setup** > **Static IP** to open the following screen. Use this screen to configure the static WAN IP addresses.

Figure 22 Advanced Setup > Static IP



The following table describes the fields in this screen.

Table 16 Advanced Setup > Static IP

LABEL	DESCRIPTION
Static IP	
Active Static IP 1-3	Select this to activate the static IP feature.
IP	Enter the IP address in this field.
Subnet Mask	Enter the subnet mask in this field.
RIPv2	
Enable	Select this to activate RIP.
ID (1-255)	Enter the ID number obtained from the router you want to exchange information.
Key	Enter the key obtained from the router you want to exchange information.
Key (hex)	Enter the key obtained from the router you want to exchange information.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9

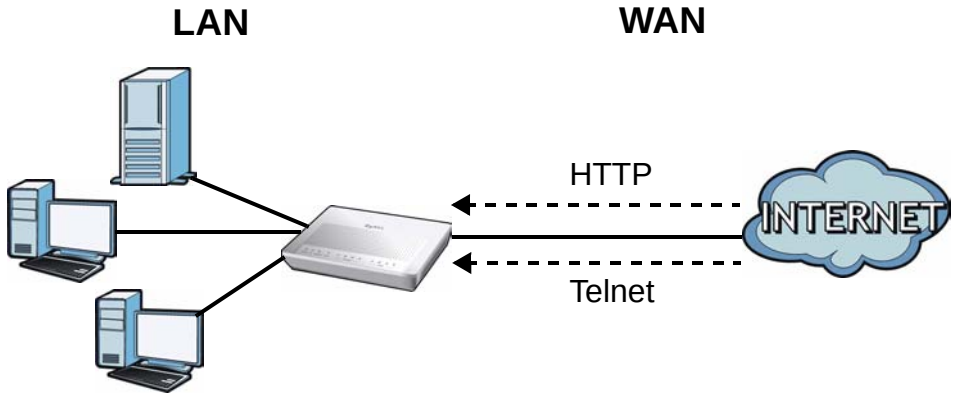
Remote Management Configuration

9.1 Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

The following figure shows remote management of the ZyXEL Device coming in from the WAN.

Figure 23 Remote Management From the WAN



Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

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

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

To disable remote management of a service, select **Disable** in the corresponding **Access Status** field.

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

1 Telnet

2 HTTP

Finding Out More

See Section 9.3 on page 74 for technical background information on remote management configuration.

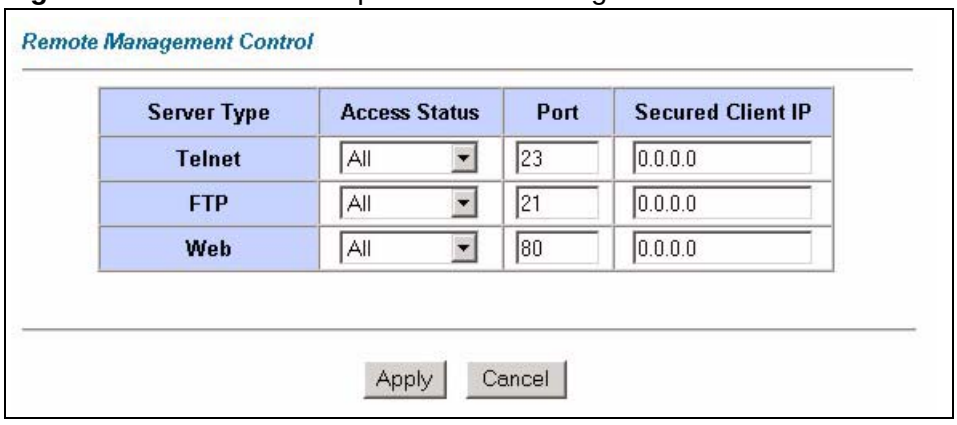
9.1.1 What You Can Do in the Remote Management Screen

Use the **Remote Management** screen (Section 9.2 on page 72) to configure through which interface and from which IP address users can use Telnet, FTP or HTTP to manage the ZyXEL Device.

9.2 The Remote Management Screen

Click **Advanced Setup** > **Remote Management** to open the following screen.

Figure 24 Advanced Setup > Remote Management



The following table describes the fields in this screen.

Table 17 Advanced Setup > Remote Management

LABEL	DESCRIPTION
Server Type	Each of these labels denotes a service that you may use to remotely manage the ZyXEL Device.
Access Status	Select the access interface. Choices are **All**, **LAN Only**, **WAN Only** and **Disable**.
Port	This field shows the port number for the remote management service. You may change the port number for a service in this field, but you must use the same port number to use that service for remote management.
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyXEL Device. Type an IP address to restrict access to a client with a matching IP address.
Apply	Click **Apply** to save your settings back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Note: You can upload and download the ZyXEL Device configuration files using FTP. To use this feature, your computer must have an FTP client.

Note: You can use the ZyXEL Device's embedded web configurator for configuration and file management.

9.2.1 Firmware Upgrade Example

The OS (Operating System) firmware (sometimes referred to as the "ras" file) has a "bin" filename extension. This example shows how to access the ZyXEL Device from LAN using FTP, type the user name and password and then use the `put xxx.bin ras` command to replace the current firmware (named `ras`) with the firmware file `firmware.bin`. Wait until the uploading is completed, type `quit` to exit FTP.

Figure 25 FTP Firmware Upgrade Example

```
D:\Firmware\P-29004HB>ftp 192.168.1.1
Connected to 192.168.1.1.
220 P2900 FTP version 1.0 ready at Mon Jan 03 08:08:45 2000
User (192.168.1.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 3648378 bytes sent in 140.79Seconds 25.91Kbytes/sec.
ftp> quit
```

9.3 Remote Management Technical Reference

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

9.3.1 Remote Management Limitations

Remote management does not work when:

- You have not enabled that service on the interface in the corresponding remote management screen.
- You have disabled that service in one of the remote management screens.
- 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.
- 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.

9.3.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

9.3.3 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.

10 Logs

10.1 Overview

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.

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

10.1.1 What You Can Do in the Log Screens

- Use the **Log Settings** screen (Section 10.2 on page 76) to configure the mail server, the syslog server, when to send logs, and what logs to send.
- Use the **View Logs** screen (Section 10.3 on page 78) to see the logs for the categories that you selected in the **Log Settings** screen.

10.1.2 What You Need to Know About Logs

Alerts

An alert is a message that is enabled as soon as the event occurs. They include system errors, attacks (access control) and attempted access to blocked web sites. 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 display in red and logs display in black.

Logs

A log is a message about an event that occurred on your ZyXEL Device. For example, when someone logs in to the ZyXEL Device, you can set a schedule for how often logs should be enabled, or sent to a syslog server.

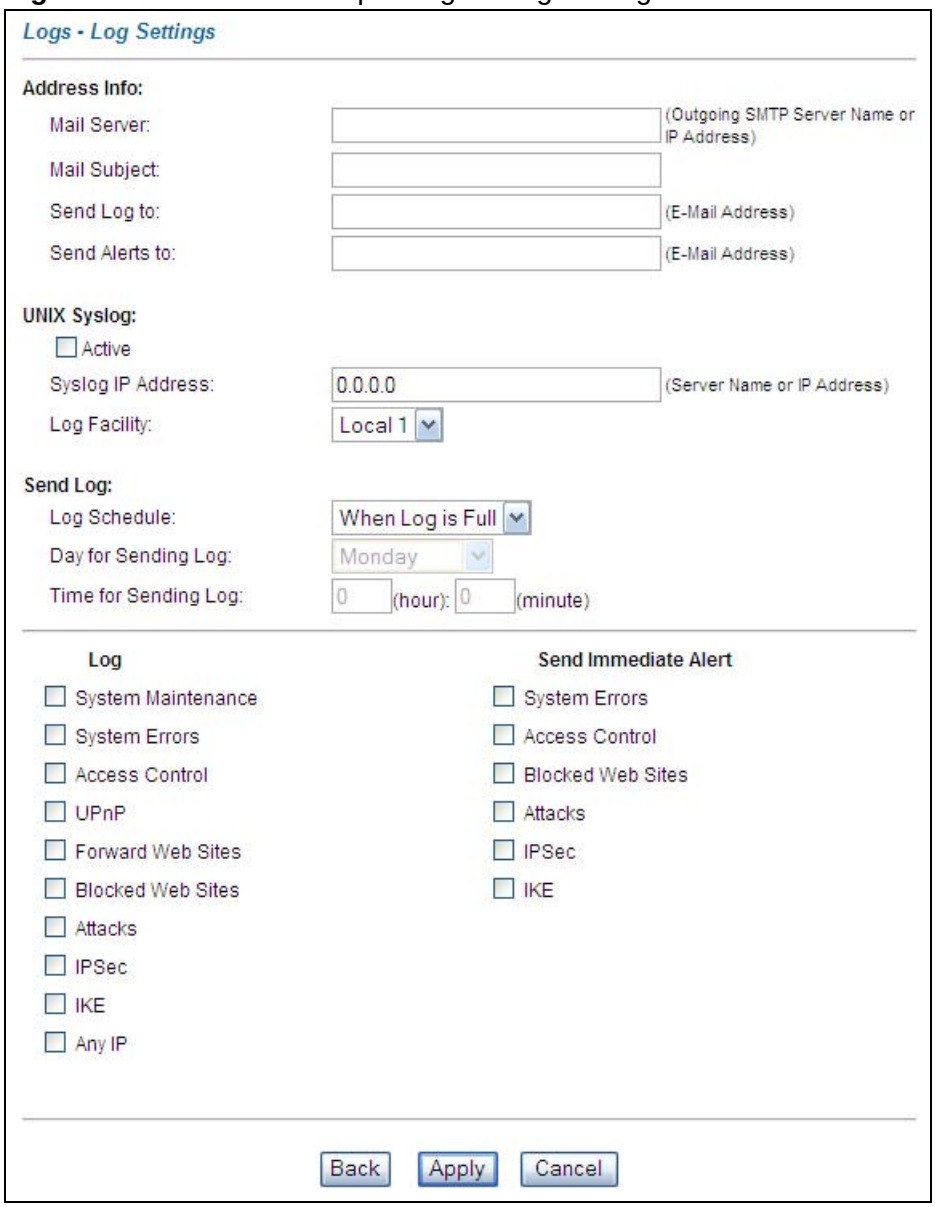
10.2 The Log Settings Screen

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

To change your ZyXEL Device's log settings, click **Advanced Setup** > **Logs** > **Log Settings** to open the following screen.

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

Figure 26 Advanced Setup > Logs > Log Settings



The following table describes the fields in this screen.

Table 18 Advanced Setup > Logs > Log Settings

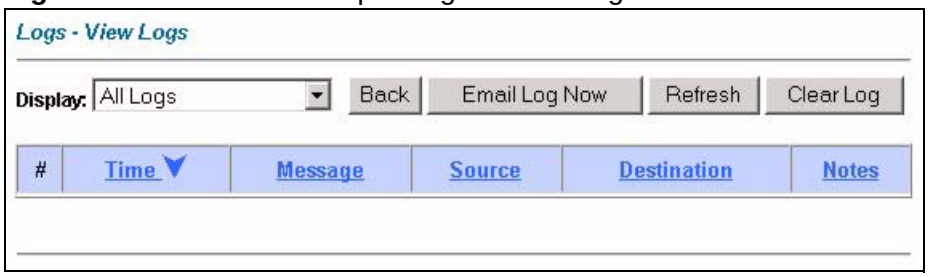
LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log 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	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
UNIX Syslog	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog 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 you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent
Day for Sending Log	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.
Log	Select the categories of logs that you want to record. Logs include alerts.
Send Immediate Alert	Select the categories of alerts for which you want the ZyXEL Device to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

10.3 The View Logs Screen

Click **Advanced Setup** > **Logs** > **View Logs** to open the screen. Use the **View Logs** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 10.2 on page 76).

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

Figure 27 Advanced Setup > Logs > View Logs



The following table describes the fields in this screen.

Table 19 Advanced Setup > Logs > View Logs

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected 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.
Back	Click **Back** to return to the previous screen
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

10.3.1 Email Log Example

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- "End of Log" message shows that a complete log has been sent.

Figure 28 E-mail Log Example

```
Subject:
        Firewall Alert From ZyXEL Device
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
.....{snip}.....
.....{snip}.....
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

Time Format Day-Month-Year

Time Format Month-Day-Year

PART III
Maintenance and Troubleshooting

11

Maintenance

11.1 Overview

This chapter discusses how to view the DHCP client and system information.

11.2 What You Can Do in this Chapter

- Use the **DHCP Table** screen (Section 11.3 on page 83) to show current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.
- Use the **Diagnostic** screens (Section 11.4 on page 85) to display information to help you identify problems with the ZyXEL Device.

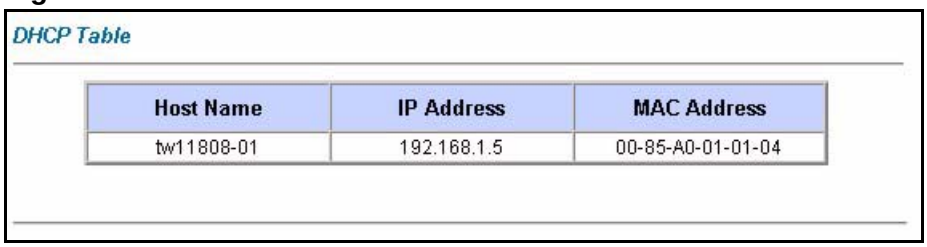
11.3 The DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows computers to obtain IP addresses, subnet masks, and other TCP/IP settings at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it (See Section 5.2 on page 51). When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured. The DHCP table shows what network computers, identified by their IP address and host name, obtained what IP addresses.

Click **Maintenance**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client

information (including **IP Address**, **Host Name** and **MAC Address**) of all network computers using the DHCP server.

Figure 29 Maintenance > DHCP Table



The following table describes the fields in this screen.

Table 20 Maintenance > DHCP Table

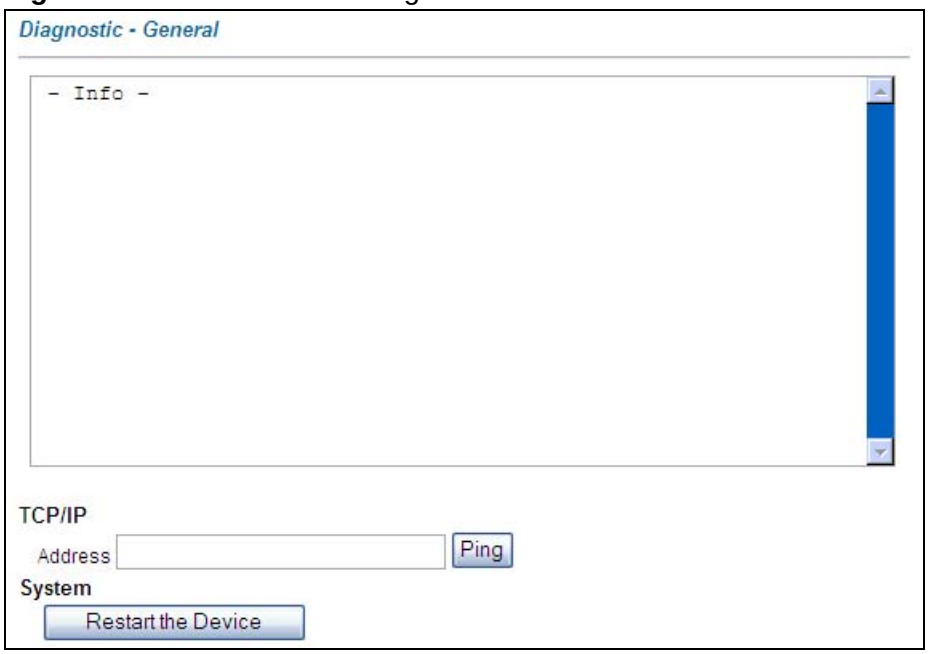
LABEL	DESCRIPTION
Host Name	This is the name of the host computer.
IP Address	This field displays the IP address relative to the **Host Name** field.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed host name. Every Ethernet device has a unique MAC 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.

11.4 The Diagnostics Screen

Use the **Diagnostics** screen to ping a device to test the connection.

Click **Maintenance > Diagnostic** to display the screen.

Figure 30 Maintenance > Diagnostic



The following table describes the labels in this screen.

Table 21 Maintenance > Diagnostic

LABEL	DESCRIPTION
Info	This read-only text box displays the ping test results.
TCP/IP	
Address	Type the IP address of a device that you want to ping in order to test a connection.
Ping	Click this button to begin the ping test.
System	
Restart the Device	Click this to restart the ZyXEL Device.
Clear Results	Click **Clear Results** to clear the **Results** text box.

PART IV
Product Specification, Appendices and Index

12

Troubleshooting

12.1 Overview

This chapter offers some suggestions for solving problems you might encounter.

None of the LEDs turn on when you turn the power on.

- Make sure that you use the included power adapter to connect to the ZyXEL Device and that it is plugged into an appropriate power source.
- Check all cable connections. If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.

Cannot access the Internet.

- Check the condition of the coaxial cable connected to the back of the cable modem. If the cable looks to be in poor condition, replace it.
- Check with your cable service provider if one of the **PWR**, **DS** and **US** LEDs is not steady on.
- Check with your cable service provider if the **ONLINE** LED is off or blinking slowly.
- Make sure your computer is configured correctly for TCP/IP networking(see Setting Up Your Computer's IP Address in the Quick Start Guide).
- Make sure your computer can communicate with the ZyXEL Device (either through the LAN or the USB port). Use ping to check the connectivity. If you cannot ping to the ZyXEL Device, do the following:
  - Use the `arp -d` command to delete the existing Address Resolution Protocol (ARP) table. Then try to ping to the ZyXEL Device again.
  - If you want your computer to use a private IP address, make sure your computer is configured as the same network as the ZyXEL Device's LAN.
  - If you want your computer to use a public IP address, make sure it is in the same network as one of the ZyXEL Device's WAN static IP.

- If you want your computer to get a dynamic IP address assigned by a DHCP server provided by your cable service provider, make sure your computer is able to receive a dynamic IP address. You have to also disable the DHCP Server function on the ZyXEL Device (select **None** in the **DHCP** field in the **Advanced Setup** > **LAN** > **LAN Setup** screen, see Section 5.2 on page 51)

The USB LED is off.

- Check the USB cable connection. Unplug and plug in the USB cable.
- Check that your computer operating system is supported by the USB driver and that it has been properly installed. Try installing the USB software again.

Cannot make a VoIP call.

- You should have applied for at least one phone number from your VoIP service provider and the number(s) should be activated.
- Make sure you connect your telephone to the right port. Each **PHONE** port maps to a unique number.
- Check the phone connection. Disconnect and connect the phone cable. The **PHONE** LED for the connected port should light. Contact your VoIP service provider if the **PHONE** LED still keeps off. If it is not, check that the phone wire is not broken, the telephone is turned on and working and that the ZyXEL Device is turned on and working.
- If the **PHONE** LED is on but you still cannot make a call, check that the **DS**, **US**, and **ONLINE** LEDs are on. If they are not, you have an Internet access problem. See Cannot access the Internet on page 89.

A

Product Specifications

See also the Introduction chapter for a general overview of the key features.

General ZyXEL Device Specifications

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

Table 22 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	243.36 mm (W) x 160.98mm (D) x 40.74 mm (H)
Power	Input: 100 - 240 VAC, 50/60 Hz Output: 18 VDC 2A CEC 4 complaint
Ethernet Ports	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Fast Ethernet ports
USB Port	One USB 1.1 B-type port for connecting to the ZyXEL Device
Cable Jack	One cable jack for connecting a 75-ohm coaxial cable
Phone Ports	Four RJ-11 FXS ports for VoIP applications
Operation Environment	Temperature: 0º C ~ 40º C Humidity: 10% ~ 95% RH
Storage Environment	Temperature: -40º C ~ 70º C Humidity: 10% ~ 95% RH
Battery	Two battery slots used for power supply backup Standby time: up to eight hours In use time: up to five hours
DOWNSTREAM CHANNEL	
Center Frequency	91 to 857 MHZ
Channel Bandwidth	6 Mhz
Input Impedance	75 ohms (nominal)
Modulation	64 QAM or 256 QAM

Table 22 Hardware Specifications

SPECIFICATION	DESCRIPTION
Maximum Data rate	30 Mbps for 64 QAM 40 Mbps for 256 QAM
Symbol Rates	5.057 Msym/s for 64 QAM 5.361 Msym/s for 256 QAM
Operating Level	-15 to +15 dBmV
UPSTREAM CHANNEL	
Frequency Range	5 to 42 Mhz
Bandwidth	200 Khz/400 Khz/800 Khz 1.6 Mhz/3.2 Mhz/6.4* Mhz
Output Impedance	75 ohms (nominal)
Modulation	8*/16/32*/64*/128* QAM or QPSK
Maximum Data Rate	30 Mbps
Symbol Rates	160, 320, 640, 1280, 2560 and 5120* Ksym/s
Operating Level	TDMA: +8 to +54 dBmV (32 QAM, 64QAM) +8 to +55 dBmV (8 QAM, 16QAM) +8 to +58 dBmV (QPSK) S-CDMA: +8 to +53 dBmV (all modulation types)

Table 23 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Administrator User Name	admin
Default Administrator Password	1234
High Speed Internet Access	The ZyXEL Device supports transmission speeds of up to 43 Mbps upstream and 30 Mbps downstream. Actual speeds attained depend on your cable operator's CMTS (Cable Modem Termination System). Note: The standard your cable operator supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained depend on the distance from the cable operator's central office, noise, and so on.

Table 23 Firmware Features

FEATURE	DESCRIPTION
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Off by default. Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients. Relay - Supports up to five (5) IP addresses from a remote DHCP server. Server - Configurable IP address pool and limits on number of DHCP clients.
Routing	Static IP only Static IP with public DHCP Static IP with NAT and private DHCP Static IP with NAT
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restore	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Logs	Use logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.

Table 23 Firmware Features

FEATURE	DESCRIPTION
Cable Modem Standards	DOCSIS 2.0 compliant DOCSIS 1.1/1.0 backward compatible Packet Cable 1.5/1.1 compliant
Device Management	Remote management through Web Configurator (HTTP), Telnet, TFTP and SNMP (v1, v2 and v3) Remote firmware upgrade Syslog and alert
External Antenna	Detachable 2 dBi antenna
Security	
DOCSIS Security Type	Baseline Privacy Interface (BPI) and BPI+
PacketCable Security Type	Support IPSec security mechanism: • Voice traffic authentication: MD5 and SHA • Voice traffic encryption: 3DES, AES and NULL Media stream encryption: SRTP
Packet filter	DOCSIS packet filter
Alerts and Logs	Logging: gateway activities, hacking attempts Alerts: Email alerts based on filtering
Operating System Compatibility	
Ethernet Connection	Windows 95, Windows 98 SE, Windows 2000, Windows ME, Windows XP, Macintosh, Linux and UNIX
USB Connection	Window 98 SE, Windows 2000, Windows ME, Windows XP

Wall-mounting Instructions

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

Note: See Table 32 on page 95 for the size of screws to use and how far apart to place them.

1 Select a position free of obstructions on a sturdy wall.

2 Drill two holes for the screws.

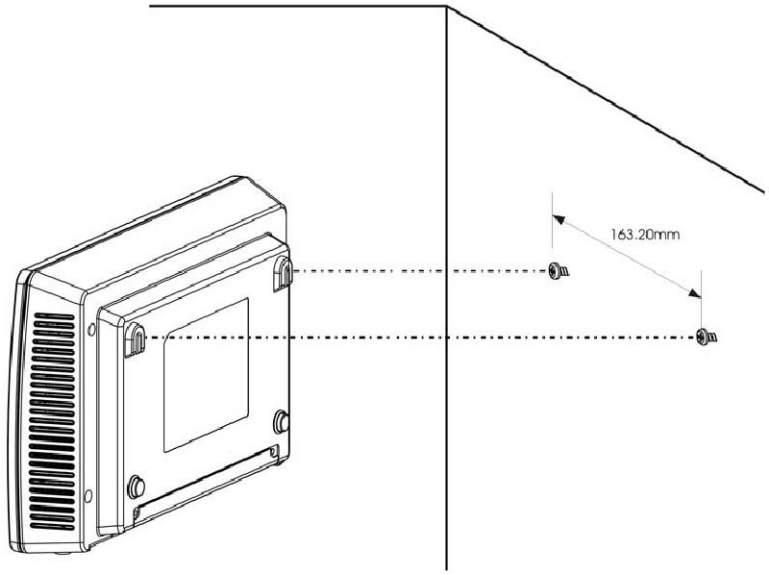
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

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

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

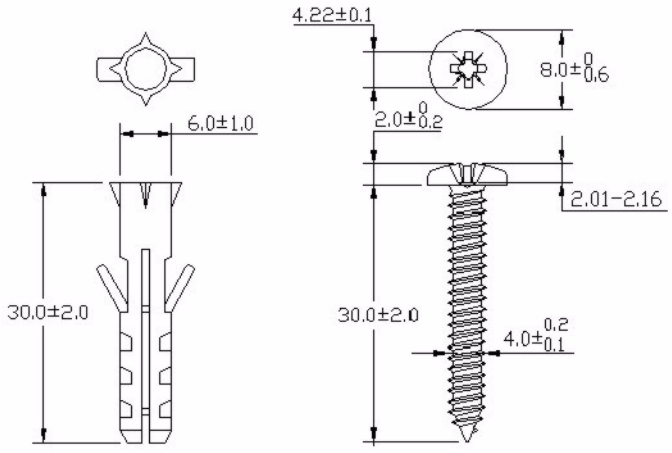
5 Align the holes on the back of the ZyXEL Device with the screws on the wall. Hang the ZyXEL Device on the screws.

Figure 31 Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 32 Masonry Plug and M4 Tap Screw



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.

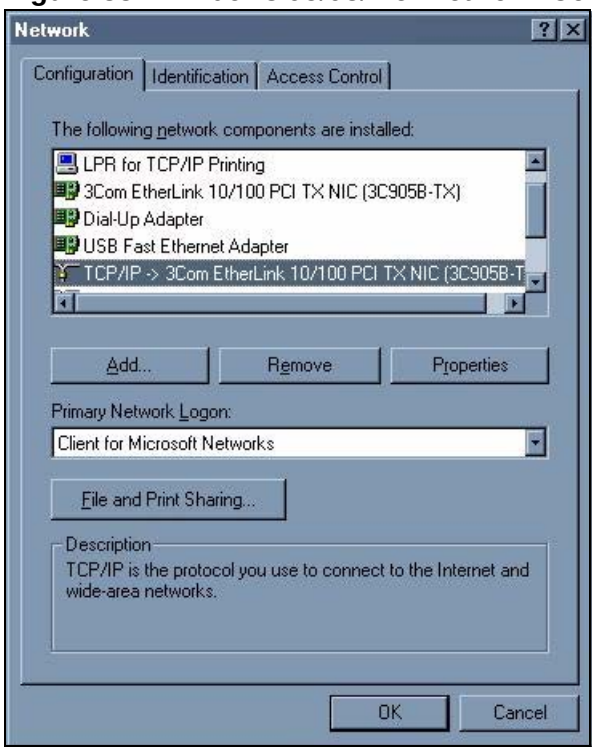
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 33 WIndows 95/98/Me: Network: Configuration



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.

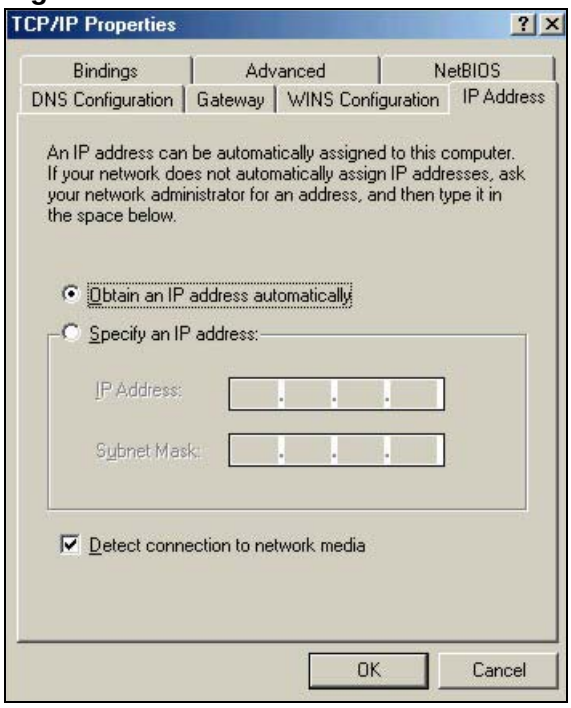
Configuring

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.

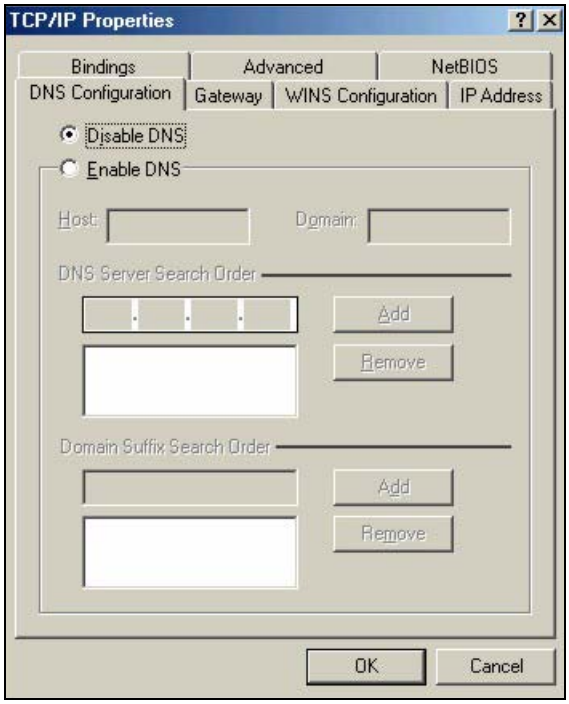
Figure 34 Windows 95/98/Me: TCP/IP Properties: IP Address



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 35 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



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.

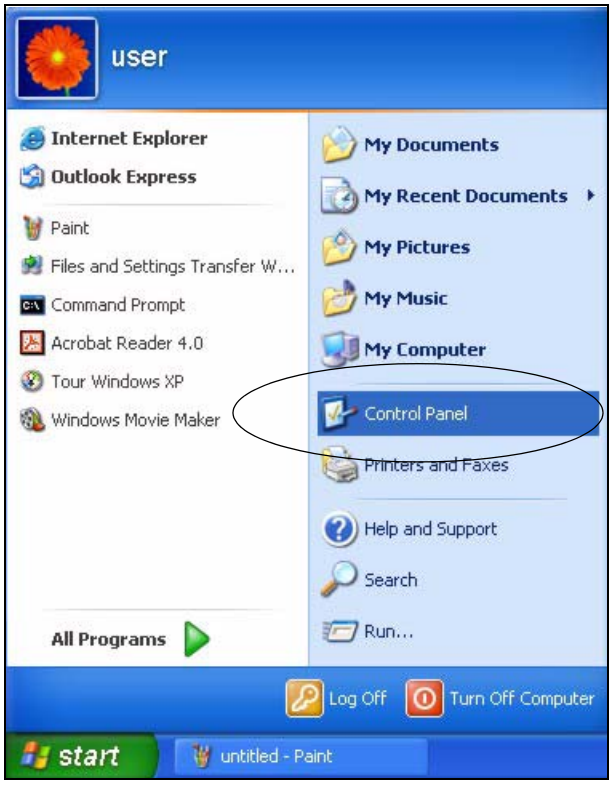
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

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 36 Windows XP: Start Menu

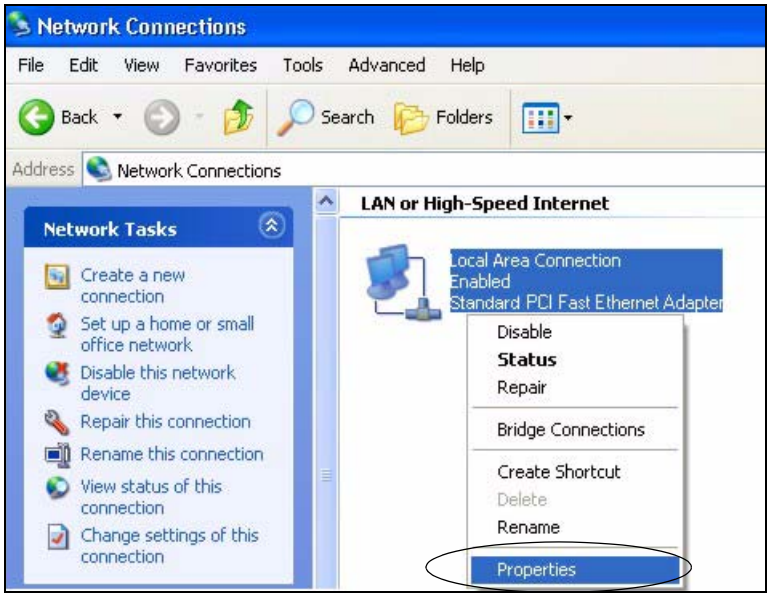


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 37 Windows XP: Control Panel

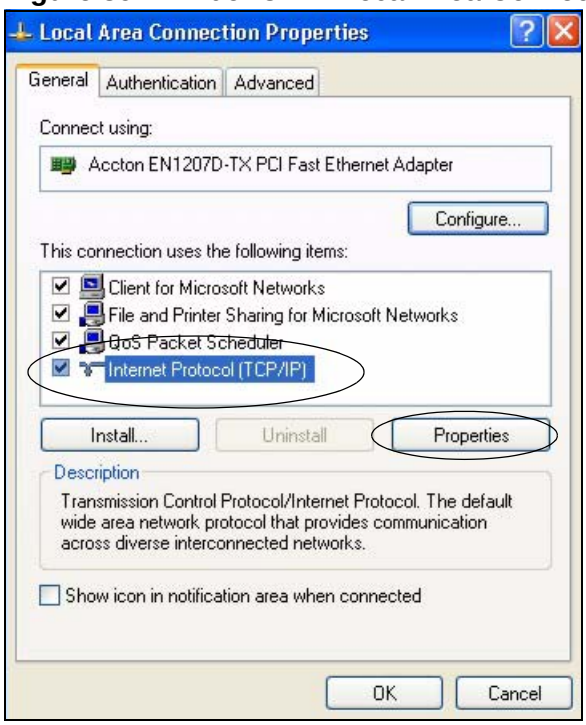
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 38 Windows XP: Control Panel: Network Connections: Properties



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

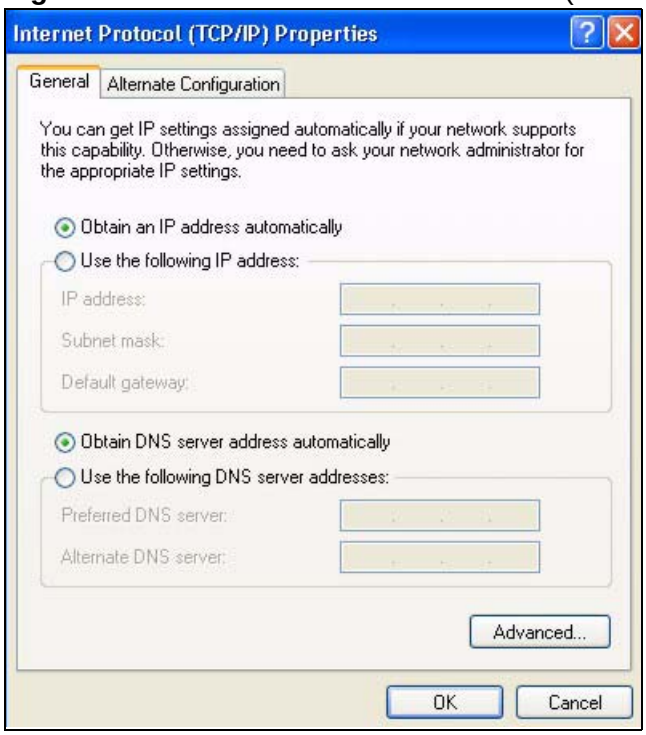
Figure 39 Windows XP: Local Area Connection Properties



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 40 Windows XP: Internet Protocol (TCP/IP) Properties



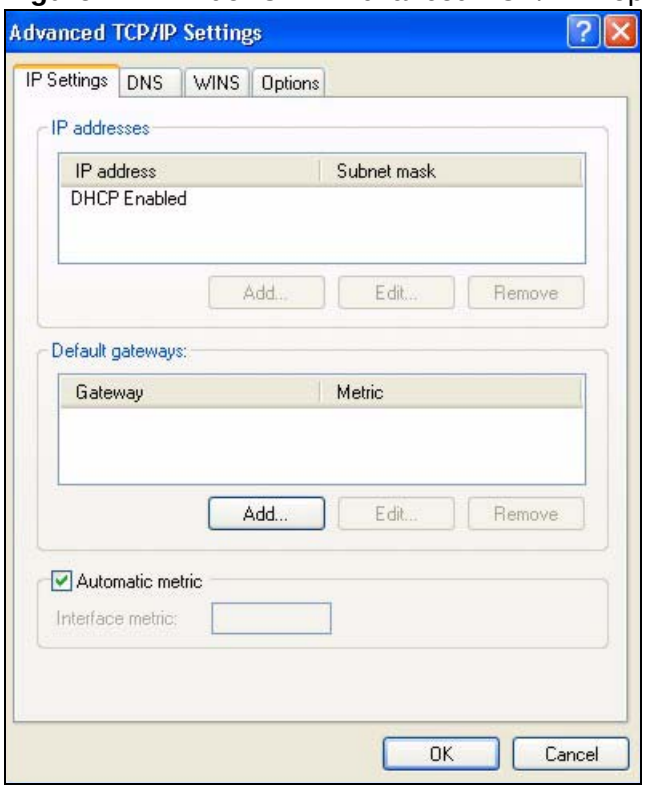
6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

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 41 Windows XP: Advanced TCP/IP Properties

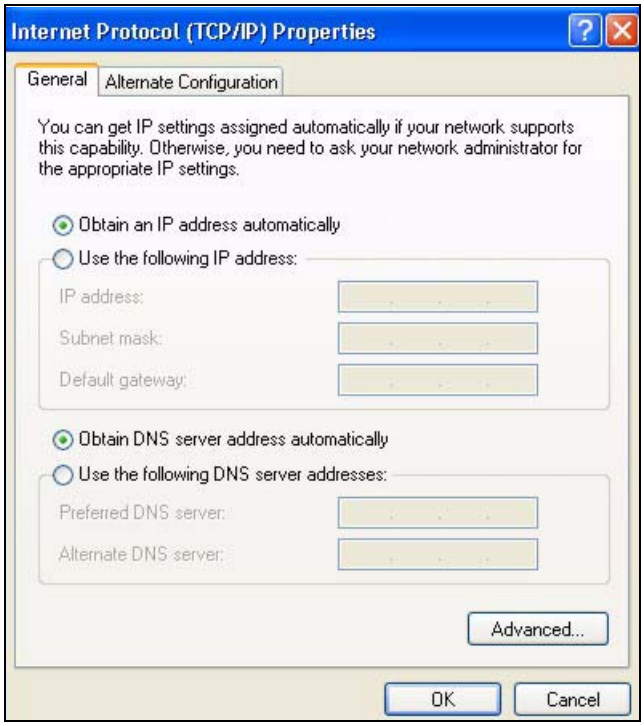


7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- 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 42 Windows XP: Internet Protocol (TCP/IP) Properties



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

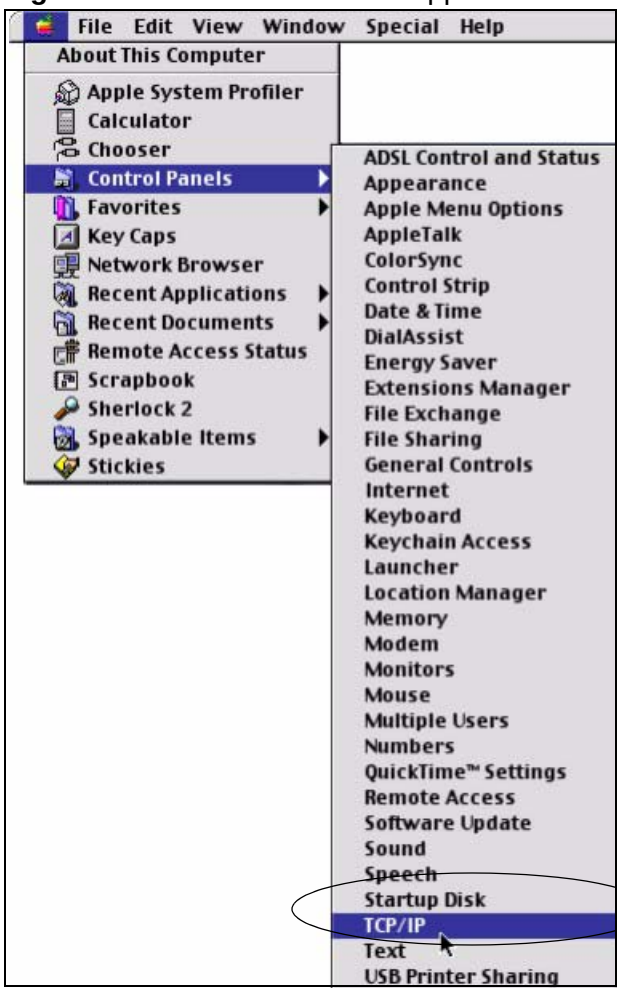
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

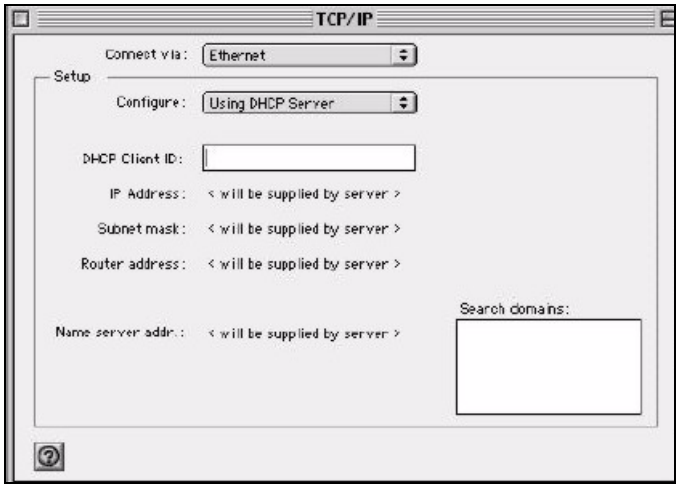
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 43 Macintosh OS 8/9: Apple Menu



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

Figure 44 Macintosh OS 8/9: TCP/IP



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).

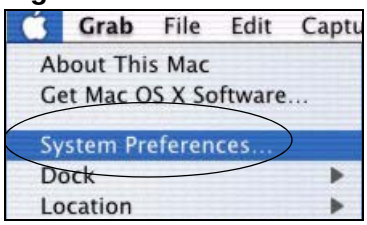
Verifying Settings

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 45 Macintosh OS X: Apple Menu

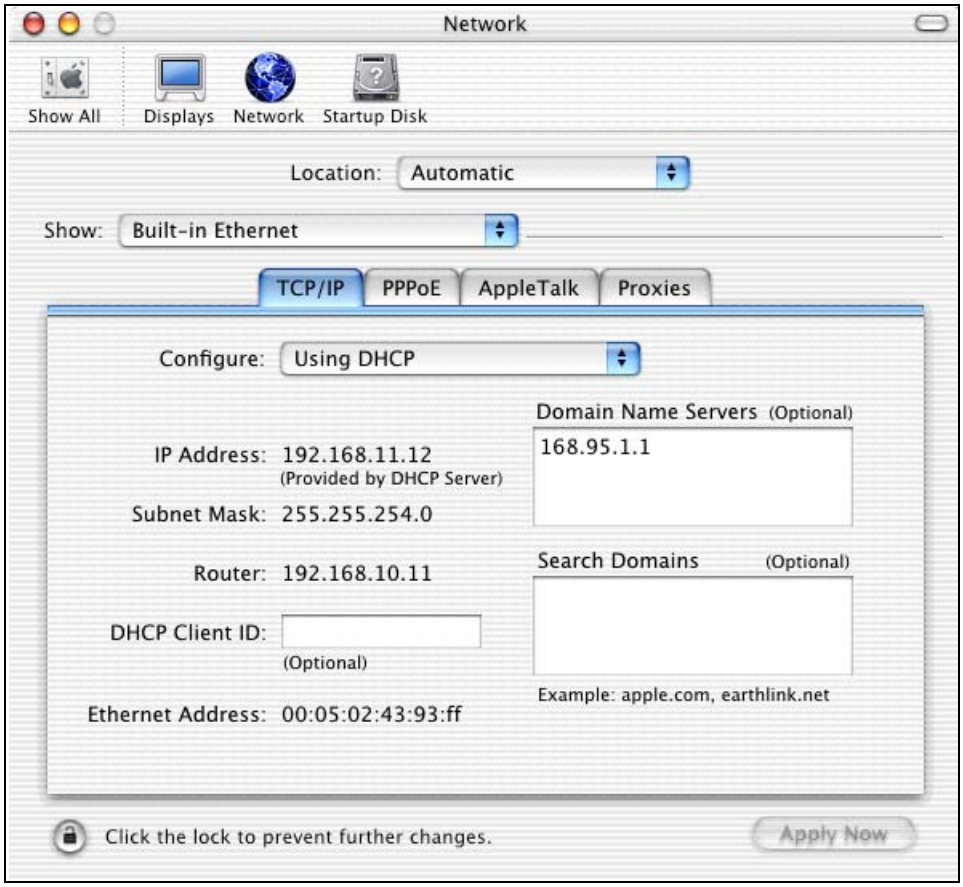


2 Click **Network** in the icon bar.

- 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 46 Macintosh OS X: Network



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.

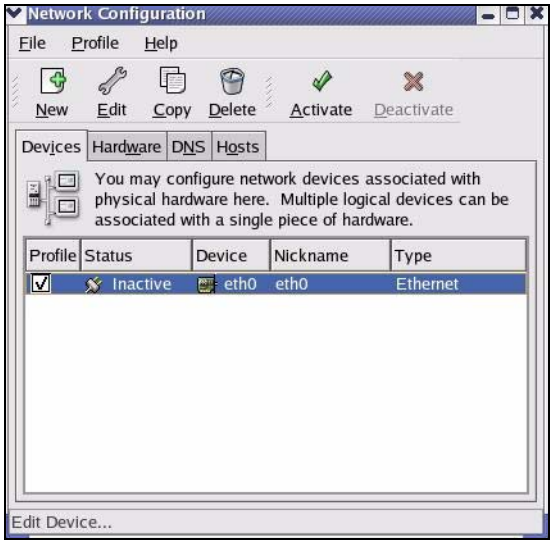
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

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

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

Figure 47 Red Hat 9.0: KDE: Network Configuration: Devices



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

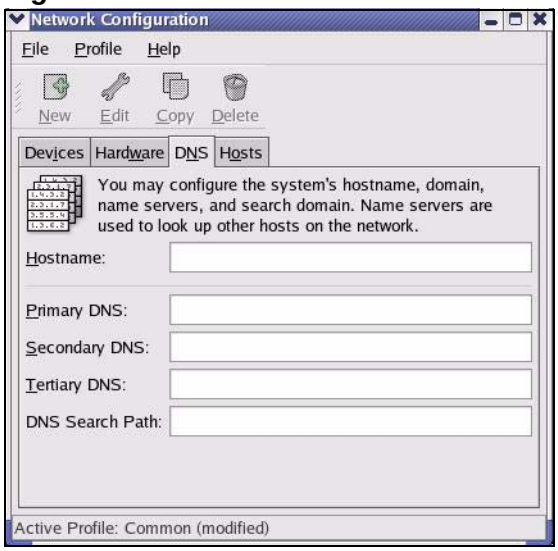
Figure 48 Red Hat 9.0: KDE: Ethernet Device: General

- 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 49 Red Hat 9.0: KDE: Network Configuration: DNS



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 50 Red Hat 9.0: KDE: Network Configuration: Activate

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 51 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 52 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 53 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 54 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 55 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

Common Services

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

Table 24 Commonly Used Services

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

Table 24 Commonly Used Services

SERVICE	DESCRIPTION
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

D

Legal Information

Copyright

Disclaimer

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

Your use of the ZyXEL Device is subject to the terms and conditions of any related service providers.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

B

C

D

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W