P-202H Plus v2

ISDN Internet Access Router

User's Guide

Version 3.40
Edition 1
8/2006

ZyXEL

Copyright

Disclaimer

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

Trademarks

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

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

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 B digital apparatus complies with Canadian ICES-003.

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

Viewing Certifications

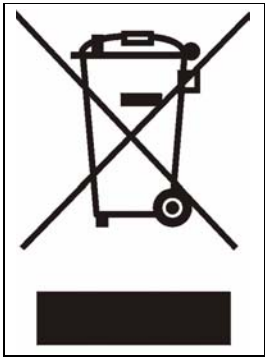
1. Go to http://www.zyxel.com.
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

Safety Warnings

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

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

This product is recyclable. Dispose of it properly.



ZyXEL Limited Warranty

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

Note

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

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

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

- 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.

METHOD	SUPPORT E-MAIL	TELEPHONE	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
COSTA RICA	soporte@zyxel.co.cr	+506-2017878	www.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso San José, Costa Rica
	sales@zyxel.co.cr	+506-2015098	ftp.zyxel.co.cr	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave.,Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	

METHOD LOCATION	SUPPORT E-MAIL	TELEPHONE	WEB SITE	REGULAR MAIL
	SALES E-MAIL	FAX	FTP SITE	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		
POLAND	info@pl.zyxel.com	+48 (22) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
		+48 (22) 333 8251		
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
SPAIN	support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 Madrid Spain
	sales@zyxel.es	+34-913-005-345		
SWEDEN	support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46-31-744-7701		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.uk	

+” is the (prefix) number you enter to make an international telephone call.

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the P-202H Plus v2 ISDN Internet access router.

Note: Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

About This User's Guide

This manual is designed to guide you through the configuration of your ZyXEL Device for its various applications. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator.

Note: Use the web configurator or System Management Terminal (SMT) to configure your ZyXEL Device. Not all features can be configured through all interfaces.

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choice.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a right angle bracket (>). For example, "In Windows, click **Start** > **Settings** > **Control Panel**" means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".
- The P-202H Plus v2 may be referred to as the "ZyXEL Device" in this User's Guide.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.
- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains connection information and instructions on getting started.
- Web Configurator Online Help

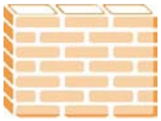
  Embedded web help for descriptions of individual screens and supplementary information.
- ZyXEL Web Site

Please go to http://www.zyxel.com for product news, firmware, updated documents, and other support materials.

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Graphics Icons Key

ZyXEL Device 	Computer 	Notebook computer
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router

CHAPTER 1 Getting To Know Your ZyXEL Device

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

1.1 Introducing the ZyXEL Device

The ZyXEL Device is a high-performance ISDN router that offers a complete Internet access solution.

By integrating NAT, firewall, VPN capability and a four-port switch, the ZyXEL Device is a complete security solution that protects your Intranet and efficiently manages data traffic on your network.

The embedded web configurator is easy to operate and totally independent of your operating system. You can also manage the ZyXEL Device via the SMT (System Management Terminal), a menu-driven interface that you can access from either a console port or telnet.

1.2 Features

This section describes the ZyXEL Device's key features.

IPSec VPN Capability

Establish Virtual Private Network (VPN) tunnels to connect (home) office computers to your company network using data encryption and the Internet; thus providing secure communications without the expense of leased site-to-site lines. The ZyXEL Device's VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

Firewall

The ZyXEL Device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The ZyXEL Device firewall supports TCP/UDP inspection, DoS detection and protection, real time alerts, reports and logs.

4-Port Switch

A combination of switch and router makes your ZyXEL Device a cost-effective and viable network solution. You can connect up to four computers to the ZyXEL Device without the cost of a hub. Use a hub to add more than four computers to your LAN.

Auto-negotiating 10/100 Mbps Ethernet LAN

The LAN interface automatically detects if they are on a 10 or a 100 Mbps Ethernet.

Auto-crossover 10/100 Mbps Ethernet LAN

The LAN interface automatically adjusts to either a crossover or straight-through Ethernet cable.

Call Scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of multiple IP addresses used within one network to different IP addresses known within another network.

SNMP (Simple Network Management Protocol - Versions 1 and 2)

SNMP, a member of the TCP/IP protocol suite, allows you to exchange management information between network devices. Your ZyXEL Device supports SNMP agent functionality that allows a manager station to manage and monitor the ZyXEL Device through the network.

IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

ISDN Data Link Connections

The ZyXEL Device supports two types of ISDN Data Link Connections: point-to-point and point-to-multipoint.

ISDN Basic Rate Interface (BRI) Support

The ZyXEL Device supports a single BRI. A BRI offers two 64 Kbps channels, which can be used independently for two destinations or be bundled to speed up data transfer.

Extensive Analog Phone Support

The ZyXEL Device is equipped with two standard phone jacks for you to connect analog devices such as telephones and FAX machines. It also supports supplementary services such as call waiting and 3-way calling.

Incoming Call Support

In addition to making outgoing calls, you can configure the ZyXEL Device to act as a remote access server for telecommuting employees.

Outgoing Data Call Bumping Support

Call bumping is a feature that allows the ZyXEL Device to manage an MP (Multilink Protocol) bundle dynamically, dropping or reconnecting a channel in a bundle when necessary. Previously, the router did this for voice calls only, but now with this new feature, the ZyXEL Device can drop a channel in an MP bundle if there is a data packet to another remote node.

CLID Callback Support For Dial-In Users

CLID (Calling Line IDentification) is an authentication method to identify a dial-in user. CLID callback is used as an ISDN toll saving feature because a call can be disconnected immediately without picking up the phone.

TCP/IP and PPP Support

- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- PPP/MP (Point-to-Point Protocol/Multilink Protocol) link layer protocol.

Dial-on-Demand

The Dial-on-Demand feature allows the ZyXEL Device to automatically place a call to a remote gateway based on the triggering packet's destination without user intervention.

PPP Multilink

The ZyXEL Device can bundle multiple links in a single connection using PPP Multilink Protocol (MP). The number of links can be either statically configured or dynamically managed based on traffic demand.

Bandwidth-On-Demand

The ZyXEL Device dynamically allocates bandwidth by dialing and dropping connections according to traffic demand.

Full Network Management

You can access the SMT (System Management Terminal) through a telnet connection or console port.

- The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyXEL Device's management interface.

Logging and Tracing

- CDR (Call Detail Record) to help analyze and manage the telephone bill.
- Built-in message logging and packet tracing.
- UNIX syslog facility support.

PAP and CHAP Security

The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyXEL Device has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client. The ZyXEL Device can also act as a surrogate DHCP server (DHCP relay) where it relays IP address assignment from another DHCP server to the clients.

Call Control

Your ZyXEL Device provides budget management for outgoing calls and maintains a blacklist for unreachable phone numbers in order to save you the expense of unnecessary charges.

Data Compression

Your ZyXEL Device incorporates Stac data compression to speed up data transfer. Stac is the de facto standard of data compression over PPP links.

Upgrade Firmware via LAN

The ZyXEL Device supports the up/downloading of firmware and configuration file over the LAN.

Supplementary Voice Features

The ZyXEL Device supports the following supplementary voice features on both of its analog or POTS (Plain Old Telephone Service) phone ports:

- Call Waiting
- Three Way Calling (Conference Calling)
- Call Transfer
- Call Forwarding
- Reminder Ring

To take full advantage of the Supplementary Voice Services available though the ZyXEL Device's phone ports, you will need to subscribe to the services from your local telephone company.

Caller ID Display Services on Analog PSTN Lines

The ZyXEL Device supports Caller ID information on both phone ports. To use Caller ID Display you need a special telephone or display unit that can show and store incoming telephone numbers.

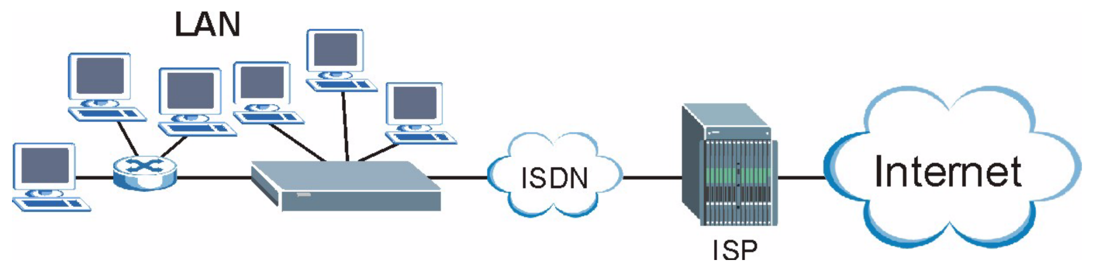
1.3 Applications for the ZyXEL Device

Here are some example uses for which the ZyXEL Device is well suited.

1.3.1 Internet Access

The ZyXEL Device is the ideal high-speed Internet access solution. Your ZyXEL Device supports the TCP/IP protocol, which the Internet uses exclusively. It is also compatible with access servers manufactured by major vendors such as Cisco and Ascend. A typical Internet access application is shown below.

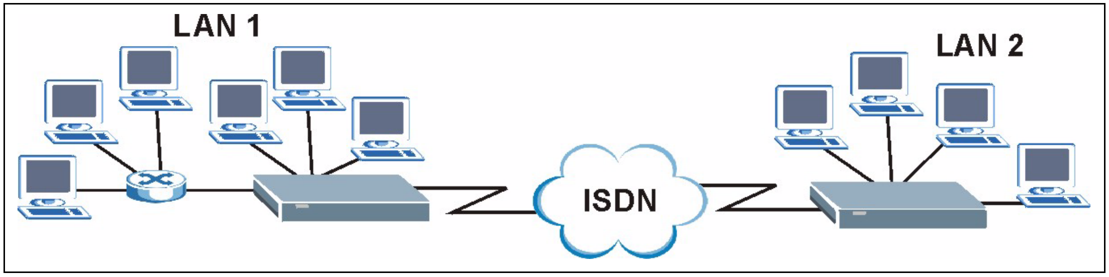
Figure 1 Internet Access Application



1.3.2 LAN-to-LAN Connection

You can use the ZyXEL Device to connect two geographically dispersed networks over the ISDN line. A typical LAN-to-LAN application for your ZyXEL Device is shown as follows.

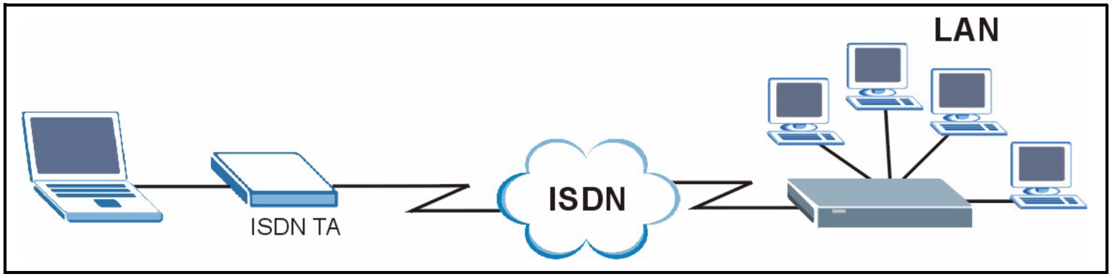
Figure 2 LAN-to-LAN Application Example



1.3.3 Remote Access Server

Your ZyXEL Device allows remote users to dial-in and gain access to your LAN. This feature enables individuals that have computers with remote access capabilities to dial in to access the network resources without being physically in the office. Either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) authentication can be used to control remote access. You can also use callback for security and/or accounting purposes.

Figure 3 Remote Access

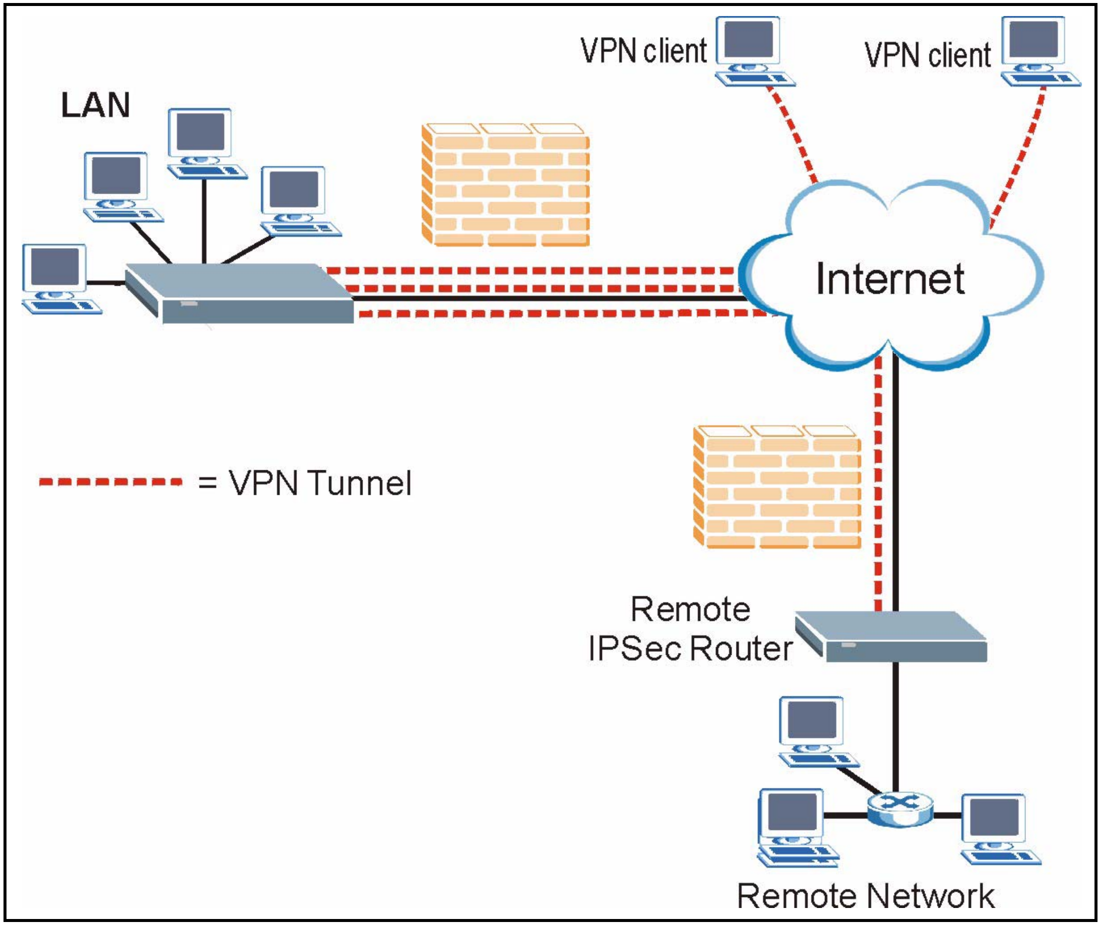


1.3.4 Secure Broadband Internet Access and VPN

The ZyXEL Device provides IP address sharing and a firewall-protected local network with traffic management.

The ZyXEL Device VPN feature is an ideal cost-effective way to connect branch offices and business partners over the Internet without the need (and expense) of leased lines between sites. The LAN computers can use VPN tunnels for secure connections to remote computers.

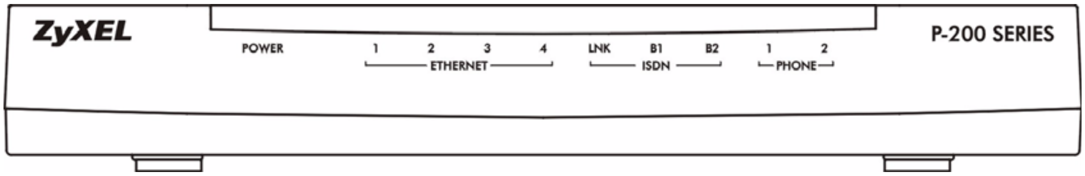
Figure 4 Secure Internet Access and VPN Application



1.4 Front Panel LEDs

The following figure shows the front panel LEDs.

Figure 5 Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is rebooting or performing diagnostics.
	Red	On	Power to the ZyXEL Device is too low.
		Off	The system is not ready or has malfunctioned.
ETHERNET 1-4	Green	On	The ZyXEL Device has a successful Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
		Off	The LAN is not connected.
ISDN LNK	Green	On	The ISDN link is connected to an ISDN switch and ready to send or receive data.
		Off	The ISDN link is not connected to an ISDN switch or has not yet initialized.
ISDN B1, B2	Green	On	The ISDN B1(B2) line is sending or receiving data.
		Off	The ISDN B1(B2) line is not sending or receiving data.
PHONE 1-2	Green	On	The telephone(s) connected to this port is (are) in use.
		Blinking	The telephone(s) connected to this port is (are) ringing.
		Off	The telephone(s) connected to this port is (are) not in use.

1.5 Hardware Connection

Refer to the Quick Start Guide for information on hardware connection.

CHAPTER 2 Introducing the Web Configurator

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

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyXEL Device setup and management via Internet browser. Use Internet Explorer 6.0 and later 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 if you need to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

Note: Even though you can connect to the ZyXEL Device wirelessly, it is recommended that you connect your computer to a LAN port for initial configuration.

1 Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).

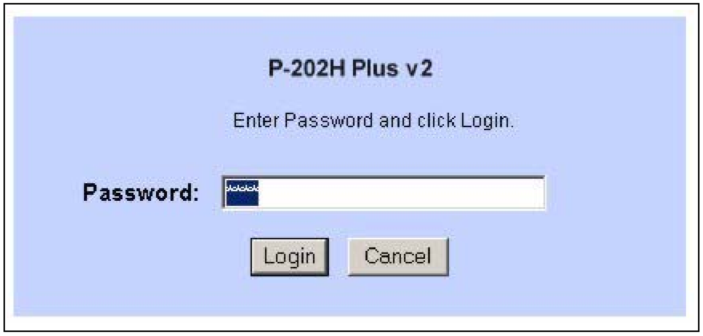
2 Prepare your computer/computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).

3 Launch your web browser.

4 Type "192.168.1.1" as the URL.

5 A window displays as shown. Type the password ("1234" is the default), then click **Login** to proceed to the next screen. In some versions, the default password appears automatically - if this is the case, click **Login**.

Figure 6 Password Screen



P-202H Plus v2

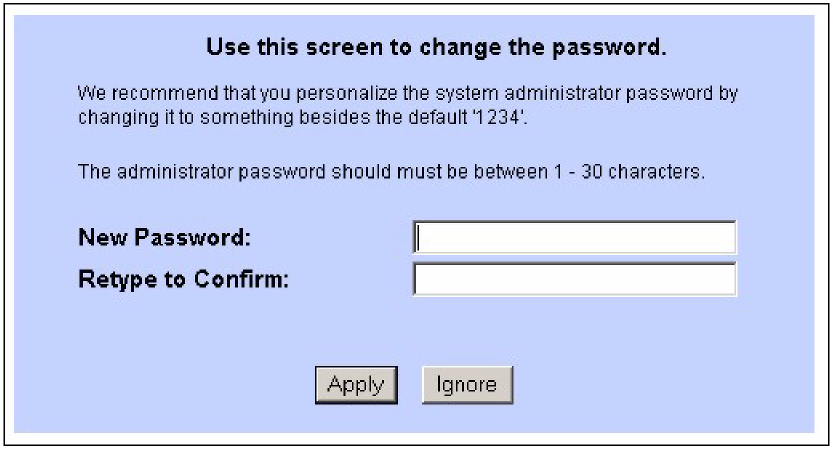
Enter Password and click Login.

Password: ****

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

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

Figure 7 Change Password at Login



Use this screen to change the password.

We recommend that you personalize the system administrator password by changing it to something besides the default '1234'.

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

New Password:

Retype to Confirm:

7 You should now see the **Site Map** screen .

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

2.3 Resetting the ZyXEL Device

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

2.3.1 Using the Reset Button

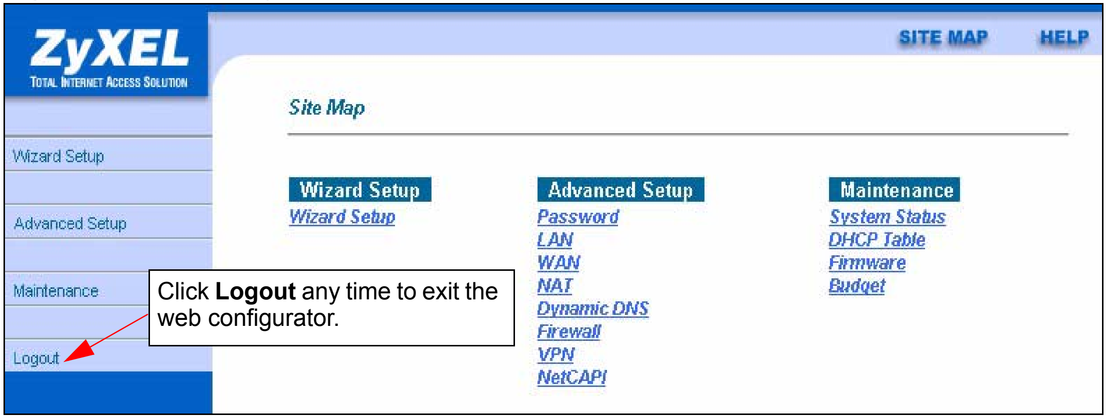
1 Make sure the **POWER** LED is on (not blinking).

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

2.4 Navigating the Web Configurator

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

Figure 8 Web Configurator: Main Screen



Click **Logout** any time to exit the web configurator.

Note: Click the HELP icon (located in the top right corner of most screens) to view embedded help.

The following table describes the sub-menus.

Table 2 Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
Wizard Setup		Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
Advanced Setup		
Password		Use this screen to change your password.
LAN	LAN Setup	Use this screen to configure LAN DHCP and TCP/IP settings.
WAN	Internet Access Setup	Use this screen to configure Internet Service Provider parameters.
NAT	NAT Mode	Use this screen to enable NAT.
	SUA Server	Use this screen to configure servers behind the ZyXEL Device.
	Address Mapping	Use this screen to configure network address translation mapping rules.
Dynamic DNS		Use this screen to allow the ZyXEL Device to use dynamic host name resolution.
Firewall	Config	Use this screen to enable the firewall.
	Email	Use this screen to send logs and alert messages to an email account.

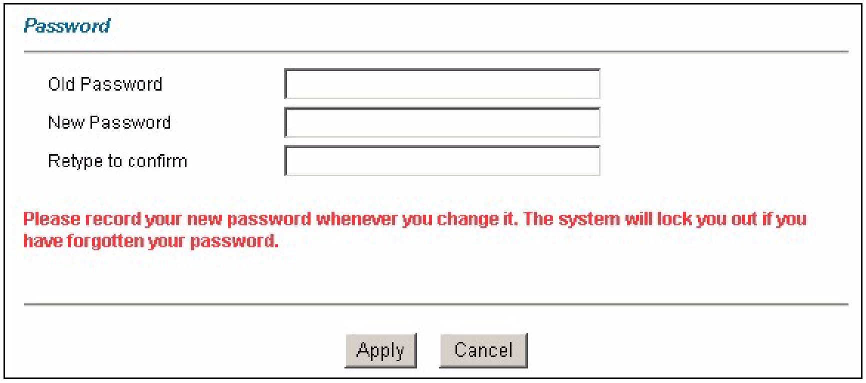
Table 2 Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
	Alert	Use this screen to configure the threshold for DoS attacks.
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add firewall rules.
	Timeout	Use this screen to configure connection timeouts.
	Logs	This screen displays firewall logs.
VPN	Setup	Use this screen to configure VPN connections and view the rule summary.
	Monitor	Use this screen to display and manage active VPN connections.
	Global Setting	Use this screen to allow NetBIOS packets through the VPN connections.
	Logs	This screen displays VPN logs.
NetCAPI		Use this screen to allow applications to access services over ISDN.
Maintenance		
System Status		This screen contains administrative and system-related information. Use this screen to access statistics.
DHCP Table		This screen shows current DHCP client information of all network clients using theZyXEL Device's DHCP server.
Firmware		Use this screen to upload firmware to your ZyXEL Device, backup and restore the configuration or reset the factory defaults to your ZyXEL Device.
Budget		This screen displays remote nodes their connected time and the time allocated for that connection.
Logout		Click **Logout** to exit the web configurator.

2.4.1 Changing 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 **Advanced Setup > Password** to display the screen as shown next.

Figure 9 Password



Password

Old Password

New Password

Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

The following table describes the labels in this screen.

Table 3 Password

LABEL	DESCRIPTION
Old Password	Type the default password (**1234**) or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 3 Wizard Setup

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

3.1 Introduction

Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP. Your ISP may have already configured some of the fields in the wizard screens for you.

Note: See the advanced menu chapters for background information on these fields.

3.1.1 MSN (Multiple Subscriber Number) and Subaddress

Depending on your location, you may have Multiple Subscriber Number (MSN) where the telephone company gives you more than one number for your ISDN line. You can assign each number to a different port, e.g., the first number to data calls, the second to A/B adapter 1 and so on. Or (DSS1) the telephone company may give you only one number, but allow you to assign your own subaddresses to different ports, e.g., subaddress 1 to data calls and 2 to A/B adapter 1.

3.1.2 PABX Outside Line Prefix

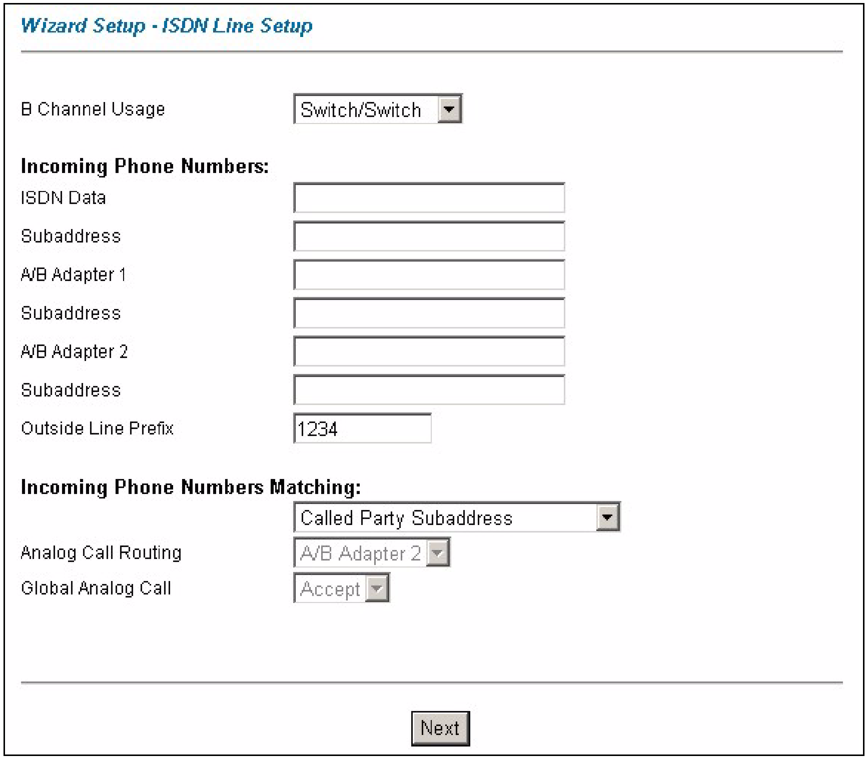
A PABX (Private Automatic Branch eXchange) generally requires you to dial a number (a single digit in most cases) when you need an outside line. If your ZyXEL Device is connected to a PABX, enter this number in the **Outside Line Prefix** field. Otherwise, leave it blank.

Please note that the PABX prefix is for calls initiated by the ZyXEL Device only. If you place a call from a device on either A/B adapter, you must dial the prefix by hand.

3.2 Wizard Setup

1 After you enter the password to access the web configurator, click **Wizard Setup** to display the first wizard screen.

Figure 10 Wizard 1: ISDN Line Set Up



Wizard Setup - ISDN Line Setup

B Channel Usage	Switch/Switch
Incoming Phone Numbers:	
ISDN Data	
Subaddress	
A/B Adapter 1	
Subaddress	
A/B Adapter 2	
Subaddress	
Outside Line Prefix	1234
Incoming Phone Numbers Matching:	Called Party Subaddress
Analog Call Routing	A/B Adapter 2
Global Analog Call	Accept

The following table describes the fields in this screen.

Table 4 Wizard 1: ISDN Line Set Up

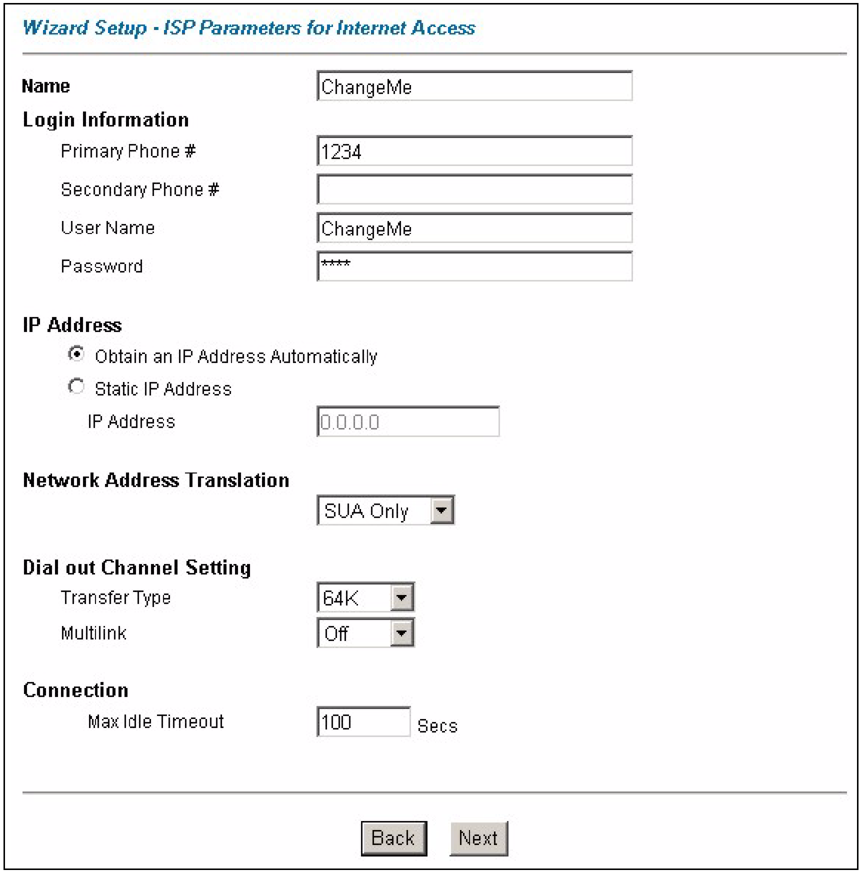
LABEL	DESCRIPTION
B Channel Usage	This is the bearer channel in an ISDN connection. B channel is a 64 Kbps full-duplex channel in both primary and basic rate ISDN. If you are using both B channels, select **Switch/Switch** (default). If you are only using one B channel (for example, your ZyXEL Device is sharing the ISDN line with another device), then select **Switch/Unused**. If your second B channel is a leased line, select **Switch/Leased**.
Incoming Phone Numbers:	
ISDN Data	Type the phone number assigned to you by your telephone company. The maximum number of digits is 25 for the telephone number.
Subaddress	Enter the subaddress assigned to **A/B Adapter 1** (**PHONE1**). The maximum number of digits is 25 for the subaddress.
A/B Adapter1	Enter the telephone number assigned to **A/B Adapter 1** (**PHONE1**).
Subaddress	Enter the subaddress assigned to **A/B Adapter 2** (**PHONE2**). The maximum number of digits is 25 for the subaddress.
A/B Adapter2	Enter the telephone number assigned to **A/B Adapter 2** (**PHONE2**).
Outside Line Prefix	If it's necessary to dial an additional number to reach an outside line, type in your prefix in this field. The maximum number of digits is 4.

Table 4 Wizard 1: ISDN Line Set Up

LABEL	DESCRIPTION
Incoming Phone Numbers Matching:	The **Incoming Phone Number Matching** setting governs how incoming calls are routed. If you **select Multiple Subscriber Number (MSN)** or **Called Party Subaddress**, a call (either ISDN data or analog) is routed to the port that matches the dialed number; if no match is found, the call is dropped. If you select **Don't Care**, then all data calls are routed to the ZyXEL Device itself. Analog calls, however, are routed to either A/B adapter 1 or 2, or simply ignored, depending on the **Analog Call Routing** field.
Analog Call Routing	Select the destination for analog calls. The choices are **A/B Adapter 2**, **A/B Adapter 1**, **Both** or **Ignore**. This field is only applicable when **Incoming Phone Number Matching** is **Don't Care**.
Global Analog Call	A global call is an incoming analog call where the switch did not send the dialed number. This happens most often when the call originates from an analog telephone line. If you specify explicit matching, i.e., **Incoming Phone Number Matching** is either **MSN** or **Called Party Subaddress**, then global calls are always ignored. If it is **Don't Care** and **Analog Call Routing** is either **A/B Adapter 1**, **A/B Adapter 2** or **Both**, then the ZyXEL Device uses **Global Analog Call** to decide how to handle global calls. If you set **Global Analog Call** to **Accept**, then global calls are routed to the port according to the **Analog Call Routing** setting; if you set **Global Analog Call** to **Ignore**, then the ZyXEL Device ignores all global calls. If **Analog Call Routing** is **Ignore** to begin with, then all analog calls, including global calls, are ignored.
Next	Click this button to set up your ZyXEL Device for Internet access.

2 The second wizard screen helps you set up your ZyXEL Device for Internet access. Click **Next** to continue.

Figure 11 Wizard 2: ISP Parameters For Internet Access



Wizard Setup - ISP Parameters for Internet Access

Name	ChangeMe
Login Information	
Primary Phone #	1234
Secondary Phone #	
User Name	ChangeMe
Password	****
IP Address	
● Obtain an IP Address Automatically	
○ Static IP Address	
IP Address	0.0.0.0
Network Address Translation	SUA Only
Dial out Channel Setting	
Transfer Type	64K
Multilink	Off
Connection	
Max Idle Timeout	100 Secs

The following table describes the fields in this screen.

Table 5 Wizard 2: ISP Parameters For Internet Access

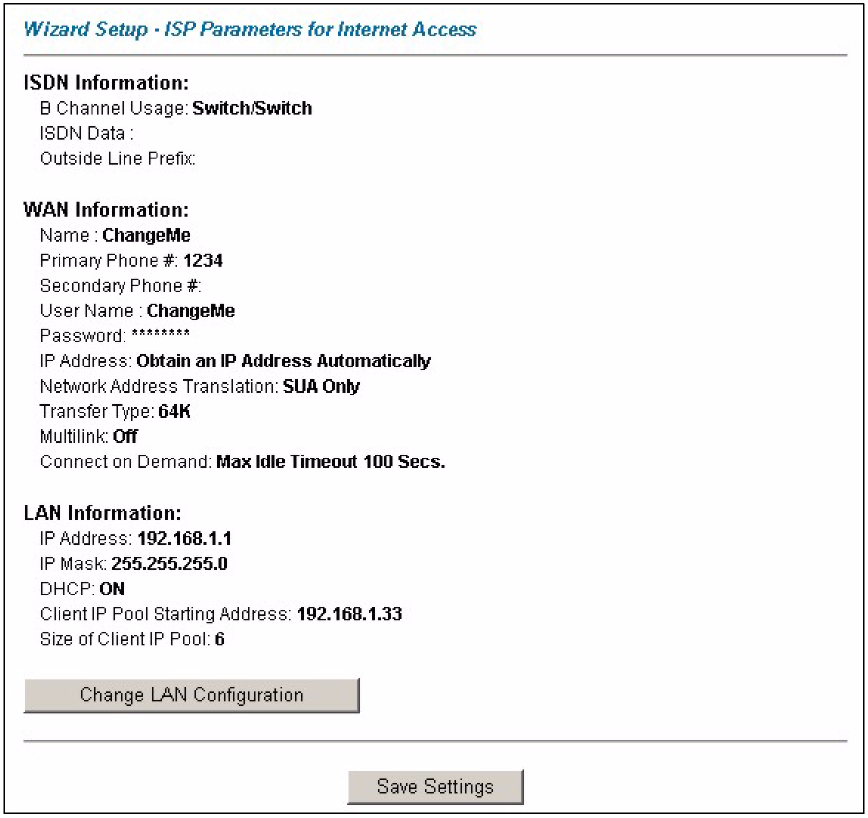
LABEL	DESCRIPTION
Name	Type the name of your service provider.
Login Information	
Primary Phone #	Your ZyXEL Device always calls your ISP using the primary phone number first. Type the number exactly as your ISP gave you.
Secondary Phone #	If the primary phone number is busy or does not answer, your ZyXEL Device will dial the secondary phone number if available. Some areas require dialing the pound sign (#) before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.
User name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
IP Address	
Obtain an IP Address Automatically	Select this option to have the ZyXEL Device obtain an IP address from a DHCP server.
Static IP Address	Select this option to manually configure your ZyXEL Device IP address.

Table 5 Wizard 2: ISP Parameters For Internet Access

LABEL	DESCRIPTION
IP Address	Type an IP address to identify your ZyXEL Device on the LAN.
Network Address Translation	Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that maps one public IP address to many private IP addresses. Choose **Full Feature** if you have multiple public IP addresses. When you select **Full Feature**, you must use the NAT address mapping rules screen to configure at least one address mapping set! Full Feature mapping types include: **One-to-One**, **Many-to-One (SUA)**, **Many-to-Many Overload**, **Many-to-Many No Overload** and **Server**. Choose **None** to disable NAT. Refer to the NAT chapter for more details.
Dial Out Channel Setting	
Transfer Type	This field specifies the type of connection between the ZyXEL Device and your ISP. Select **64K** or **Leased**.
Multilink	The ZyXEL Device uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is **64K**. If you set the transfer type to **64K**, select the way you use the PPP Multilink protocol. You can either select not to (**Off**) or always (**Always**) to bundle multiple links in a single connection to boost the effective throughput between two nodes. Otherwise, select **BOD** (Bandwidth on Demand) to add or subtract links dynamically according to traffic demand.
Connection	
Max Idle Timeout	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your ZyXEL Device. Administrative packets such as RIP are not counted as data.
Back	Click this button to reconfigure your ISDN line settings.
Next	Click this button to display a summary of all your settings.

3 Verify the settings in the screen shown next. To change the LAN information on the ZyXEL Device, click **Change LAN Configurations**. Otherwise click **Save Settings** to save the configuration.

Figure 12 Wizard 3: Summary



Wizard Setup - ISP Parameters for Internet Access

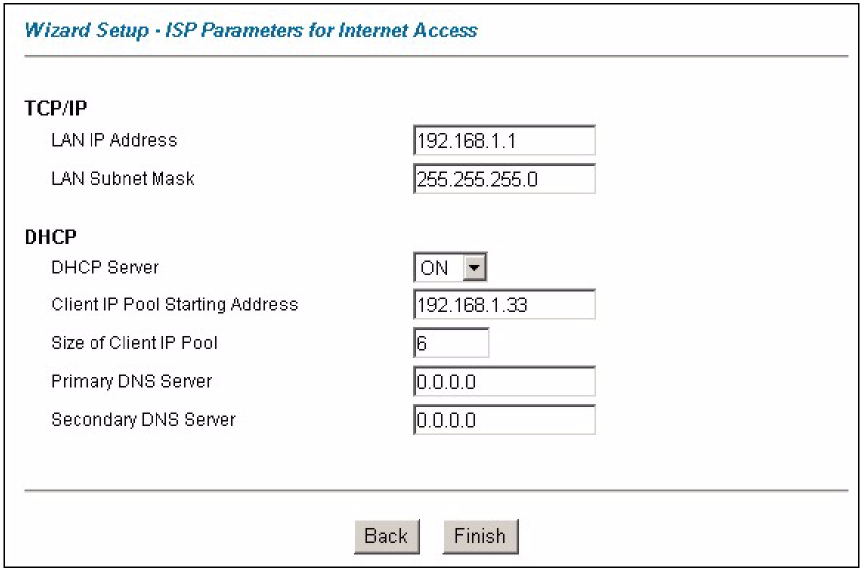
ISDN Information:
B Channel Usage: **Switch/Switch**
ISDN Data :
Outside Line Prefix:

WAN Information:
Name : **ChangeMe**
Primary Phone #: **1234**
Secondary Phone #:
User Name : **ChangeMe**
Password: ********
IP Address: **Obtain an IP Address Automatically**
Network Address Translation: **SUA Only**
Transfer Type: **64K**
Multilink: **Off**
Connect on Demand: **Max Idle Timeout 100 Secs.**

LAN Information:
IP Address: **192.168.1.1**
IP Mask: **255.255.255.0**
DHCP: **ON**
Client IP Pool Starting Address: **192.168.1.33**
Size of Client IP Pool: **6**

4 If you click **Change LAN Configuration** to change your ZyXEL Device LAN settings, the screen displays as shown below.

Figure 13 Wizard: LAN Configuration



Wizard Setup - ISP Parameters for Internet Access

TCP/IP
LAN IP Address: 192.168.1.1
LAN Subnet Mask: 255.255.255.0

DHCP
DHCP Server: ON
Client IP Pool Starting Address: 192.168.1.33
Size of Client IP Pool: 6
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0

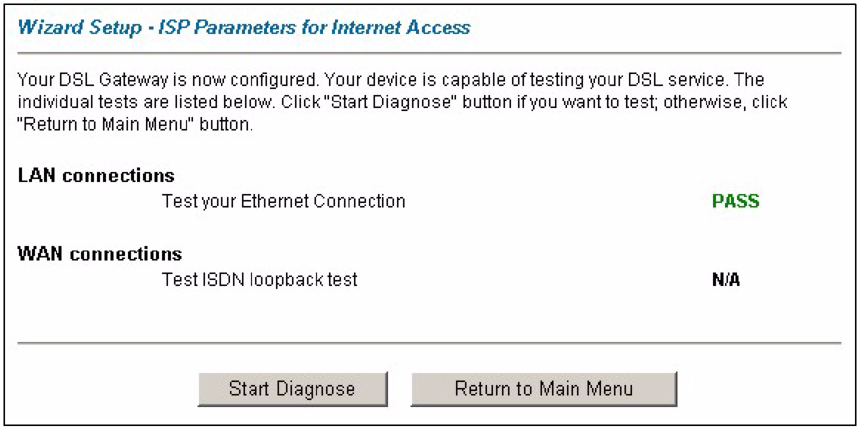
The following table describes the fields in this screen.

Table 6 Wizard: LAN Configuration

LABEL	DESCRIPTION
TCP/IP	
LAN IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default). **Note:** If you changed the ZyXEL Device's LAN IP address, you must use the new IP address if you want to access the web configurator again.
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
DHCP	
DHCP Server	From the **DHCP Server** drop-down list box, select **On** to allow your ZyXEL Device to assign IP addresses, a default gateway and DNS servers to computer systems that support the DHCP client feature. Select **Off** to disable DHCP server. When DHCP server is used, set the following items:
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.
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.
Back	Click **Back** to go back to the previous screen.
Finish	Click **Finish** to save the settings and begin testing your connection.

5 The ZyXEL Device automatically tests the connection to the computer(s) connected to the LAN ports. To test the connection from the ZyXEL Device to the ISP, click **Start Diagnose**. Otherwise click **Return to Main Menu** to go back to the **Site Map** screen.

Figure 14 Wizard 4



Wizard Setup - ISP Parameters for Internet Access

Your DSL Gateway is now configured. Your device is capable of testing your DSL service. The individual tests are listed below. Click "Start Diagnose" button if you want to test; otherwise, click "Return to Main Menu" button.

LAN connections

Test your Ethernet Connection PASS

WAN connections

Test ISDN loopback test N/A

3.2.1 Test Your Internet Connection

Launch your web browser and navigate to http://www.zyxel.com. Internet access is just the beginning. Refer to the rest of this User's Guide for more detailed information on the complete range of ZyXEL Device features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the Wizard Setup are correct.

CHAPTER 4 LAN Setup

This chapter describes how to configure LAN settings.

4.1 LAN Overview

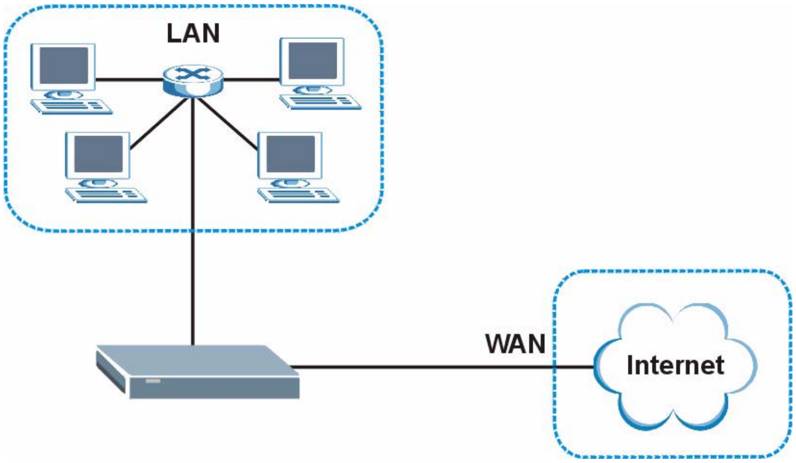
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See Section 4.3 on page 56 to configure the **LAN** screens.

4.1.1 LANs, WANs and the ZyXEL Device

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

Figure 15 LAN and WAN IP Addresses



4.1.2 DHCP Setup

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

4.1.2.1 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.

4.1.3 DNS Server Address Assignment

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

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

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in the **LAN Setup** screen.
- If the ISP did not give you DNS server information, leave the **DNS Server** fields in the **LAN Setup** screen set to **0.0.0.0** for the ISP to dynamically assign the DNS server IP addresses

4.2 LAN TCP/IP

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

4.2.1 IP Address and Subnet Mask

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

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

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

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

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

4.2.1.1 Private IP Addresses

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

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

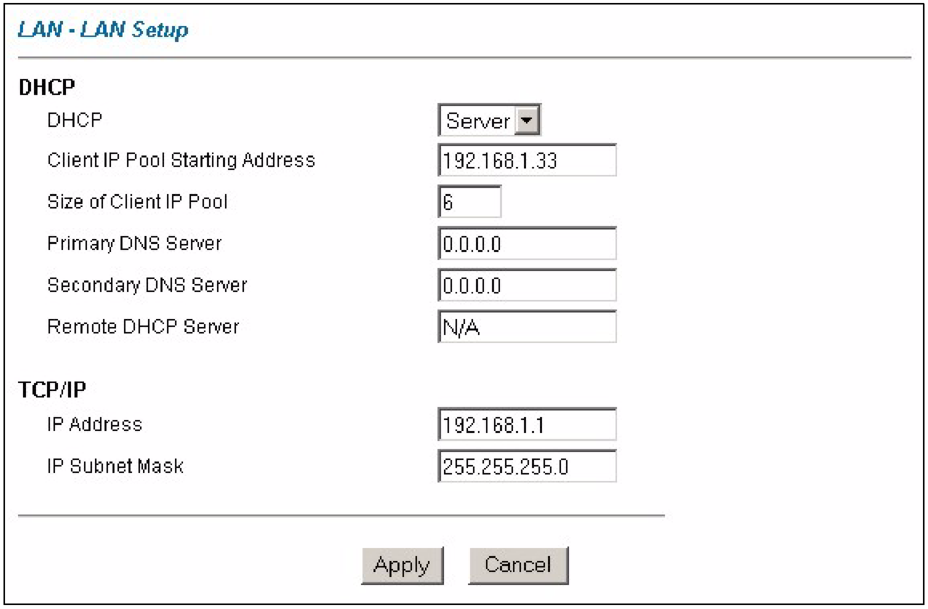
You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of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

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

4.3 Configuring LAN Setup

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

Figure 16 LAN Setup



LAN - LAN Setup

DHCP

DHCP	Server
Client IP Pool Starting Address	192.168.1.33
Size of Client IP Pool	6
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Remote DHCP Server	N/A

TCP/IP

IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0

The following table describes the fields in this screen.

Table 7 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.
Primary DNS Server Secondary DNS Server	This field is not available when you set **DHCP** to **None** or **Relay**. Type 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. Leave these entries at **0.0.0.0** if they are provided by a WAN DHCP server.
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, 192.168.1.1 (factory default).

Table 7 LAN Setup (continued)

LABEL	DESCRIPTION
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device automatically selects the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 5
WAN Setup

This chapter describes how to configure WAN settings.

5.1 WAN Overview

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

5.1.1 PPP Multilink

The ZyXEL Device uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes.

Due to the fragmentation/reconstruction overhead associated with MP, you may not get a linear increase in throughput when a link is added.

The number of links in an MP bundle can be statically configured, or dynamically determined at runtime, as explained in the following section.

5.1.2 Bandwidth on Demand

The Bandwidth on Demand (BOD) feature adds or subtracts links dynamically according to traffic demand. After the initial call, the ZyXEL Device uses BAP (Bandwidth Allocation Protocol) to ask the peer for additional telephone number if BACP (Bandwidth Allocation Control Protocol) is negotiated. Otherwise, the ZyXEL Device uses the statically configured (primary and secondary) telephone numbers of the remote node.

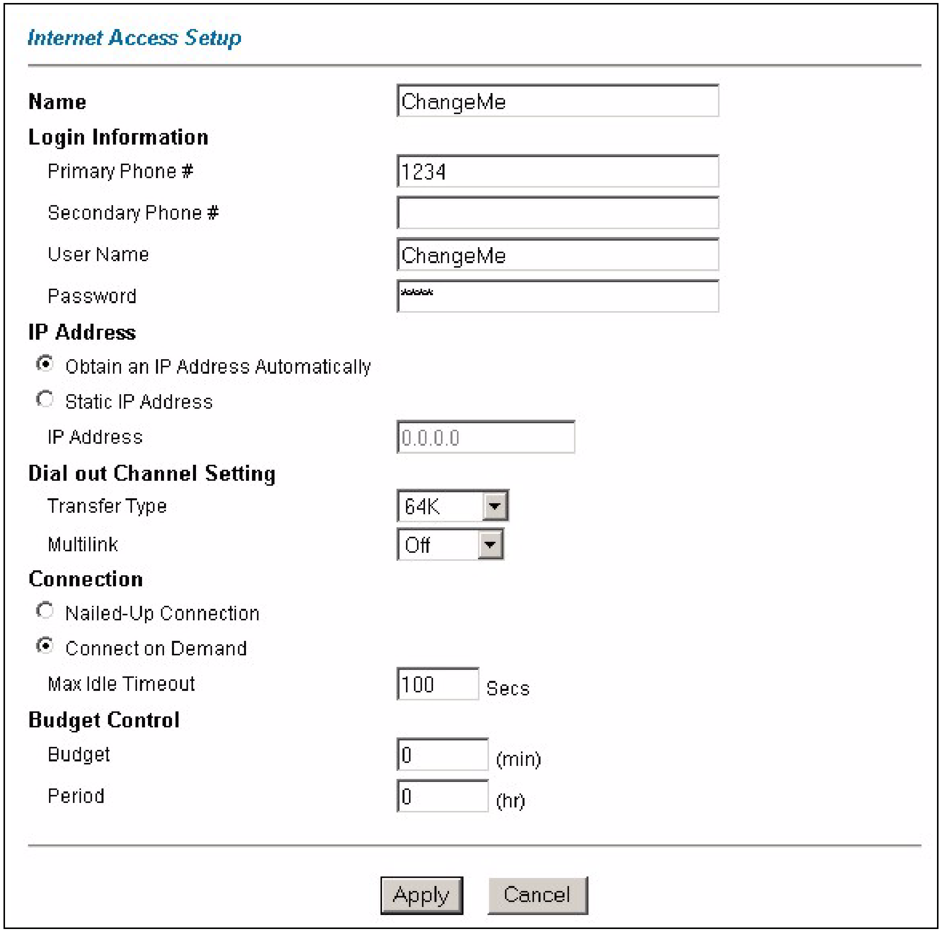
5.1.3 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP.

5.2 Internet Access Setup

To change your ZyXEL Device's WAN Internet access settings, click **WAN**.

Figure 17 WAN Setup



Internet Access Setup

Name	ChangeMe
Login Information	
Primary Phone #	1234
Secondary Phone #	
User Name	ChangeMe
Password	****
IP Address	
● Obtain an IP Address Automatically	
○ Static IP Address	
IP Address	0.0.0.0
Dial out Channel Setting	
Transfer Type	64K
Multilink	Off
Connection	
○ Nailed-Up Connection	
● Connect on Demand	
Max Idle Timeout	100 Secs
Budget Control	
Budget	0 (min)
Period	0 (hr)

The following table describes the labels in this screen.

Table 8 WAN Setup

LABEL	DESCRIPTION
Name	Type the name of your service provider.
Login Information	
Primary Phone #	Your ZyXEL Device always calls your ISP using the primary phone number first. Type the number exactly as your ISP gave you.
Secondary Phone #	If the primary phone number is busy or does not answer, your ZyXEL Device will dial the secondary phone number if available. Some areas require dialing the pound sign (#) before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.
User name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
IP Address	
Obtain an IP Address Automatically	Select this option to have the ZyXEL Device obtain an IP address from a DHCP server.

Table 8 WAN Setup (continued)

LABEL	DESCRIPTION
Static IP Address	Select this option to manually configure your ZyXEL Device IP address.
IP Address	Type an IP address to identify your ZyXEL Device on the LAN.
Dial Out Channel Setting	
Transfer Type	This field specifies the type of connection between the ZyXEL Device and your ISP. Select **64K** or **Leased**.
Multilink	The ZyXEL Device uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is **64K**. If you set the transfer type to **64K**, select the way you use the PPP Multilink protocol. You can either select not to (**Off**) or always (**Always**) to bundle multiple links in a single connection to boost the effective throughput between two nodes. Otherwise, select **BOD** (Bandwidth on Demand) to add or subtract links dynamically according to traffic demand.
Connection	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your ZyXEL Device. Administrative packets such as RIP are not counted as data.
Budget Control	
Budget	This field sets the budget callback time for all the remote dial-in users. The default for this field is 0 for no budget control.
Period	This field sets the time interval to reset the above callback budget control.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 6 Network Address Translation (NAT) Screens

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

6.1 NAT Overview

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

6.1.1 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 9 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.

6.1.2 What NAT Does

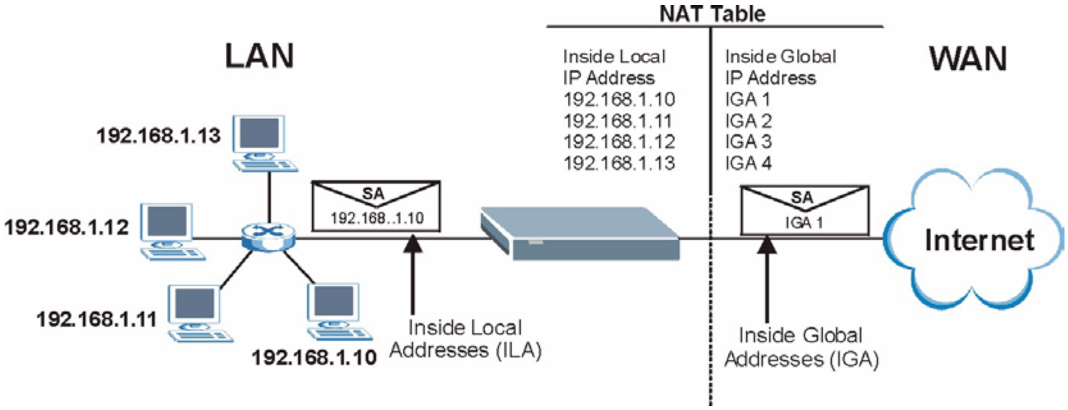
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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 and Many-to-Many Overload mapping – see Table 10 on page 67), 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)*.

6.1.3 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 and Many-to-Many Overload NAT mapping) 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 18   How NAT Works



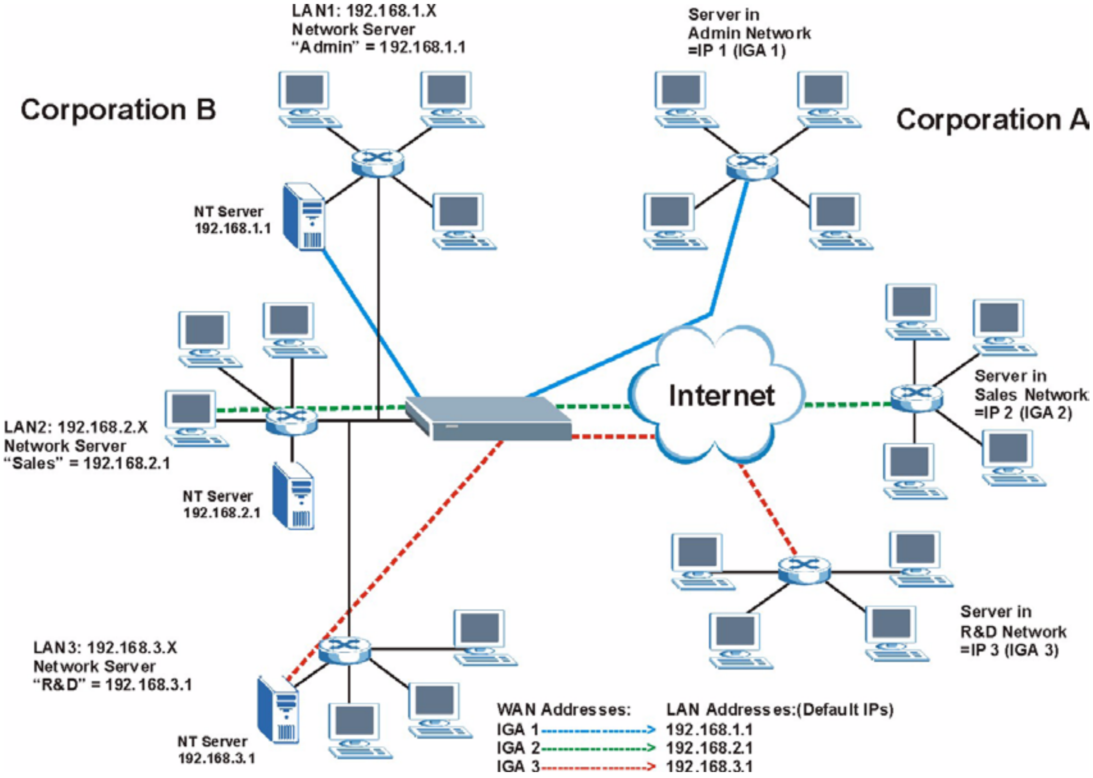
NAT Table

Inside Local IP Address	Inside Global IP Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

6.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the ZyXEL Device can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 19 NAT Application With IP Alias



6.1.5 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. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyXEL Device maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the ZyXEL Device maps each local IP address to a unique 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** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

Table 10 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1:1

Many-to-One (SUA/PAT)	ILA1←→ IGA1
	ILA2←→ IGA1
	…
		M:1

Many-to-Many Overload	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA1
	ILA4←→ IGA2
	…
		M:M Ov

Many-to-Many No Overload	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA3
	…
		M:M No OV

Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

6.2 SUA (Single User Account) Versus NAT

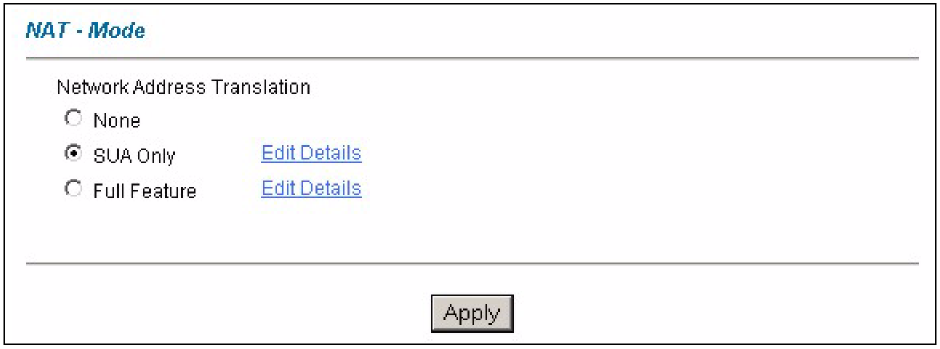
SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in Table 10 on page 67.

- Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device.

6.3 Selecting the NAT Mode

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

Figure 20 NAT Mode



NAT - Mode

Network Address Translation

○ None

● SUA Only Edit Details

○ Full Feature Edit Details

The following table describes the labels in this screen.

Table 11 NAT Mode

LABEL	DESCRIPTION
None	Select this radio button to disable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device. The ZyXEL Device uses **Server Set 1** in the **NAT - Edit SUA/NAT Server Set** screen.
Edit Details	Click this link to go to the **NAT - Edit SUA/NAT Server Set** screen.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.
Edit Details	Click this link to go to the **NAT - Address Mapping Rules** screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

6.4 SUA Server

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

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

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

6.4.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

Note: If you do not assign an IP address in **Server Set 1** (default server), the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

6.4.2 Port Forwarding: Services and Port Numbers

Use the **NAT - Edit SUA/NAT Server Set** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers.

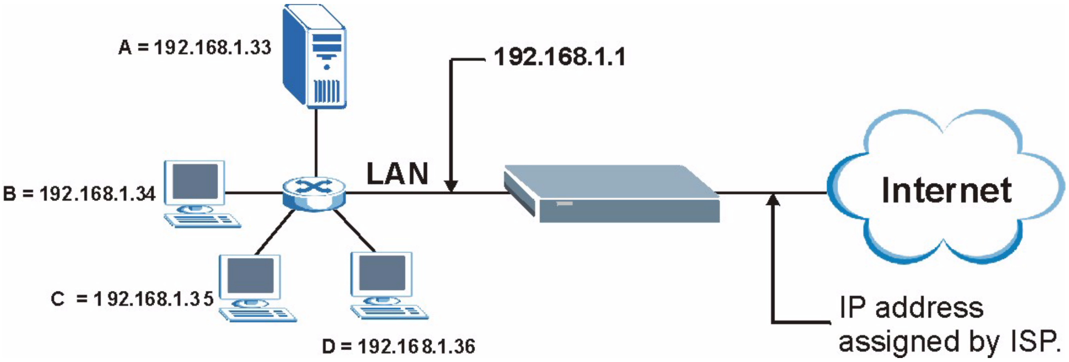
Table 12 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

6.4.3 Configuring Servers Behind NAT (Example)

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

Figure 21 Multiple Servers Behind NAT Example



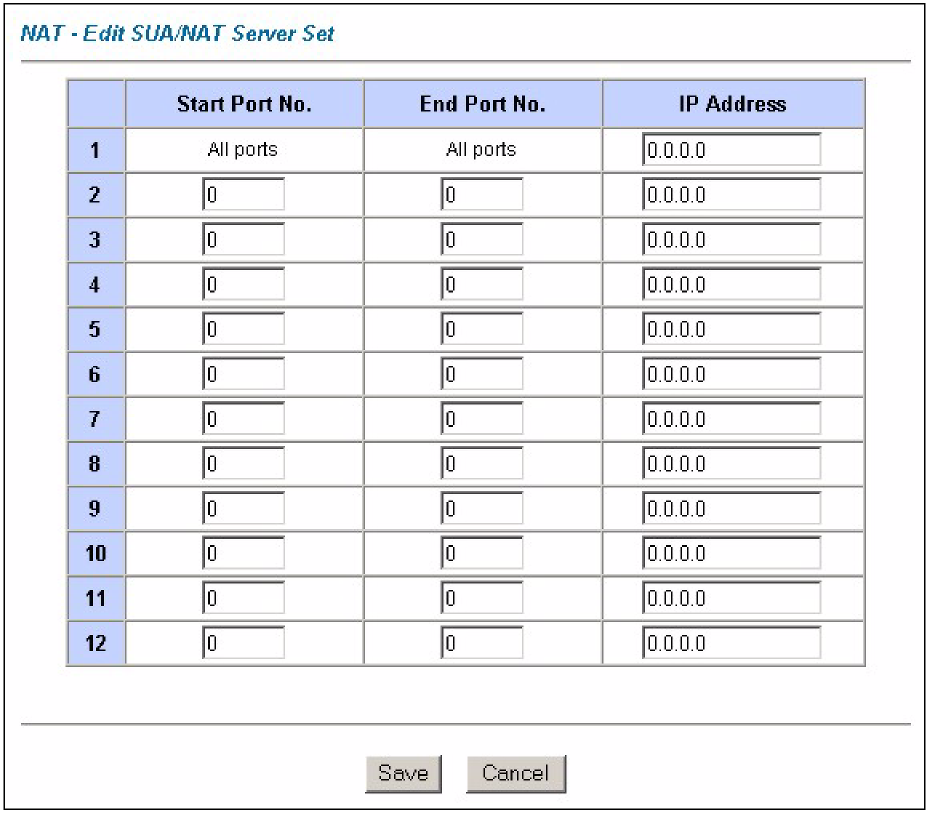
6.5 Configuring SUA Server

Note: If you do not assign an IP address in **Server Set 1** (default server), the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Click **NAT**, select **SUA Only** and click **Edit Details** to open the following screen.

See Table 12 on page 69 for port numbers commonly used for particular services.

Figure 22 Edit SUA/NAT Server Set



NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

The following table describes the fields in this screen.

Table 13 Edit SUA/NAT Server Set

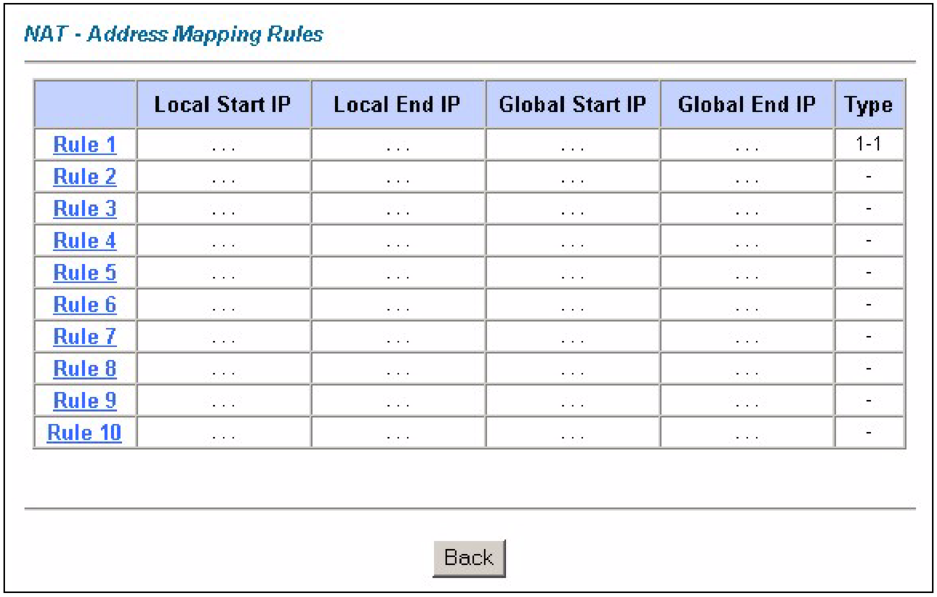
LABEL	DESCRIPTION
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port No.** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port No.** field.
End Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port No.** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port No.** field above.
IP Address	Enter the inside IP address of the server here.
Save	Click **Save** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previous configuration.

6.6 Configuring Address Mapping

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.

To change your ZyXEL Device's address mapping settings, click **NAT**, select **Full Feature** and click **Edit Details** to open the following screen.

Figure 23 Address Mapping Rules



NAT - Address Mapping Rules

	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
Rule 1	...	...	...	...	1-1
Rule 2	...	...	...	...	-
Rule 3	...	...	...	...	-
Rule 4	...	...	...	...	-
Rule 5	...	...	...	...	-
Rule 6	...	...	...	...	-
Rule 7	...	...	...	...	-
Rule 8	...	...	...	...	-
Rule 9	...	...	...	...	-
Rule 10	...	...	...	...	-

The following table describes the fields in this screen.

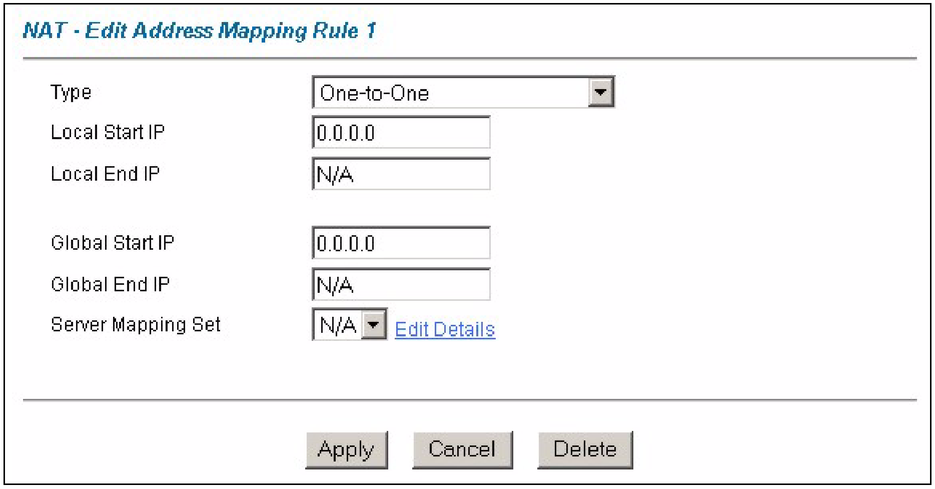
Table 14 Address Mapping Rules

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. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **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.

6.6.1 Address Mapping Rule Edit

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 24 Edit Address Mapping Rule



NAT - Edit Address Mapping Rule 1

Type	One-to-One
Local Start IP	0.0.0.0
Local End IP	N/A
Global Start IP	0.0.0.0
Global End IP	N/A
Server Mapping Set	N/A

The following table describes the fields in this screen.

Table 15 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. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. • **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. • **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. • **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 mapping set.
Edit Details	Click this link to go to the **NAT - Edit SUA/NAT Server Set** screen to edit a server set that you have selected in the **Server Mapping Set** field.
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 return to the previously saved settings.
Delete	Click **Delete** to exit this screen without saving.

CHAPTER 7 Dynamic DNS

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

7.1 Dynamic DNS Overview

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

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

7.1.1 DYNDNS Wildcard

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

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

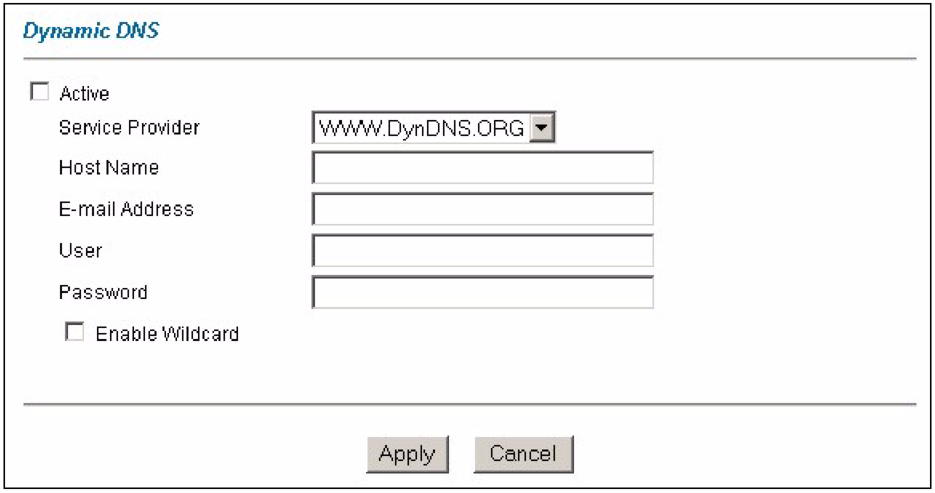
See Section 7.2 on page 74 for configuration instruction.

7.2 Configuring Dynamic DNS

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

See Section 7.1 on page 74 for more information.

Figure 25 Dynamic DNS



Dynamic DNS

□ Active

Service Provider: WWW.DynDNS.ORG

Host Name

E-mail Address

User

Password

□ Enable Wildcard

The following table describes the fields in this screen.

Table 16 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 Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
E-mail Address	Enter 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.

CHAPTER 8 Firewalls

This chapter gives some background information on firewalls and introduces the ZyXEL Device firewall.

8.1 Firewall Overview

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

8.2 Types of Firewalls

There are three main types of firewalls:

- Packet Filtering Firewalls
- Application-level Firewalls
- Stateful Inspection Firewalls

8.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

8.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

- Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.
- Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

8.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See Section 8.5 on page 82 for more information on stateful inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

8.3 Introduction to ZyXEL's Firewall

The ZyXEL Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The ZyXEL Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyXEL Device also has packet filtering capabilities.

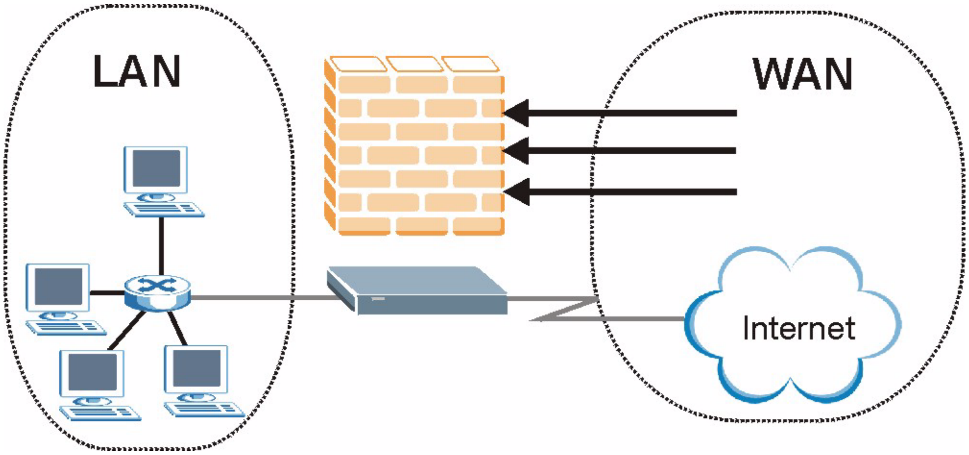
The ZyXEL Device is installed between the LAN and the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The ZyXEL Device has one ISDN port and four Ethernet LAN ports, which physically separate the network into two areas.

- The ISDN port connects to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, "inbound access" will not be allowed unless you configure remote management or create a firewall rule to allow a remote host to use a specific service.

8.3.1 Denial of Service Attacks

Figure 26 Firewall Application



8.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

8.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An "extension number", called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 17 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

8.4.2 Types of DoS Attacks

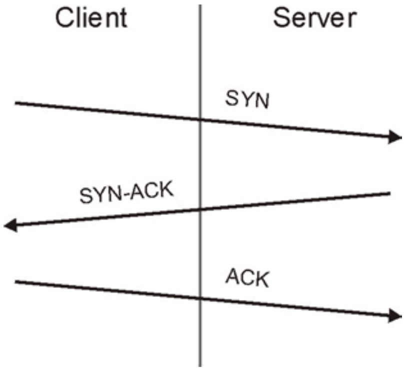
There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.
5. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

- Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.
- Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

6. Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

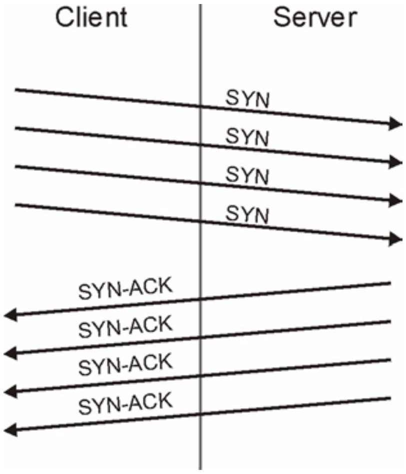
Figure 27 Three-Way Handshake



Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

- **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

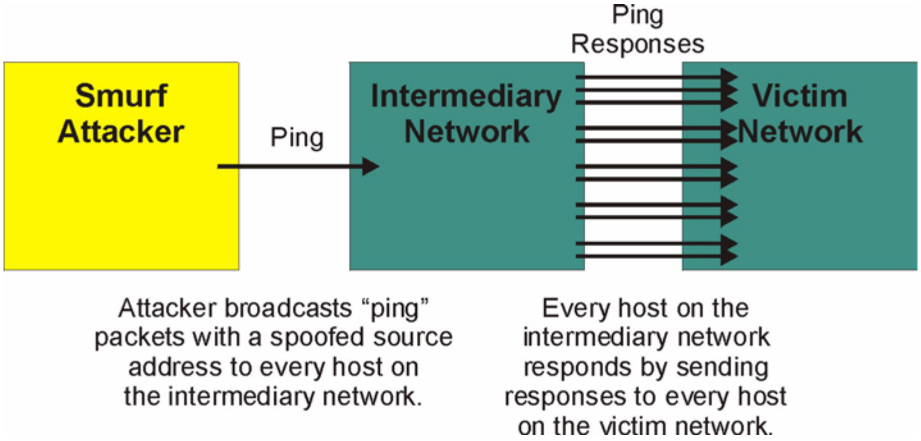
Figure 28 SYN Flood



- In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

7 A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

Figure 29 Smurf Attack


Ping
Responses
Smurf
Attacker
Ping
Intermediary
Network
Victim
Network
Attacker broadcasts "ping" packets with a spoofed source address to every host on the intermediary network.
Every host on the intermediary network responds by sending responses to every host on the victim network.

8.4.2.1 ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 18 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

8.4.2.2 Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 19 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
VE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 20 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

8.4.2.3 Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

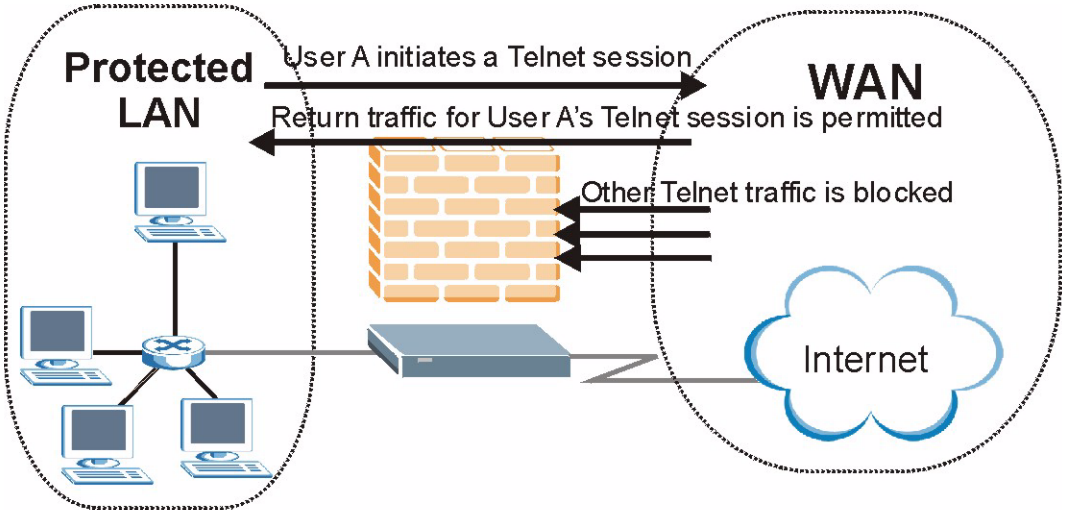
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyXEL Device blocks all IP Spoofing attempts.

8.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This “remembering” is called *saving the state.* When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The ZyXEL Device uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyXEL Device’s stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

Figure 30 Stateful Inspection


Protected LAN
User A initiates a Telnet session
WAN
Return traffic for User A’s Telnet session is permitted
Other Telnet traffic is blocked
Internet

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

8.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **The default action for packets not matching following rules** field (see Figure 34 on page 96) determine the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

8.5.2 Stateful Inspection and the ZyXEL Device

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

- Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.

- Allow certain types of traffic from the Internet to specific hosts on the LAN.
- Allow access to a Web server to everyone but competitors.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

Note: The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the ZyXEL Device itself (as with the "virtual connections" created for UDP and ICMP).

8.5.3 TCP Security

The ZyXEL Device uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the ZyXEL Device receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

8.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the ZyXEL Device is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

8.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the ZyXEL Device inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these, it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator’s Custom Ports feature to do this.

8.6 Guidelines for Enhancing Security with Your Firewall

- Change the default password via CLI (Command Line Interpreter) or web configurator.
- Limit who can telnet into your router.
- Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- Protect against IP spoofing by making sure the firewall is active.
- Keep the firewall in a secured (locked) room.

8.6.1 Security In General

You can never be too careful! Factors outside your firewall, filtering or NAT can cause security breaches. Below are some generalizations about what you can do to minimize them.

- Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
- DSL or cable modem connections are “always-on” connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.
- Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
- Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
- Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small “key” icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.
- Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
- Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.
- Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
- If you use “chat rooms” or IRC sessions, be careful with any information you reveal to strangers.
- If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.
- Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

8.7 Packet Filtering Vs Firewall

Below are some comparisons between the ZyXEL Device’s filtering and firewall functions.

8.7.1 Packet Filtering:

- The router filters packets as they pass through the router’s interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

8.7.1.1 When To Use Filtering

- To block/allow LAN packets by their MAC addresses.
- To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
- To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- To block/allow IP trace route.

8.7.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

8.7.2.1 When To Use The Firewall

- To prevent DoS attacks and prevent hackers cracking your network.
- A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
- To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- The firewall performs better than filtering if you need to check many rules.
- Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
- The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

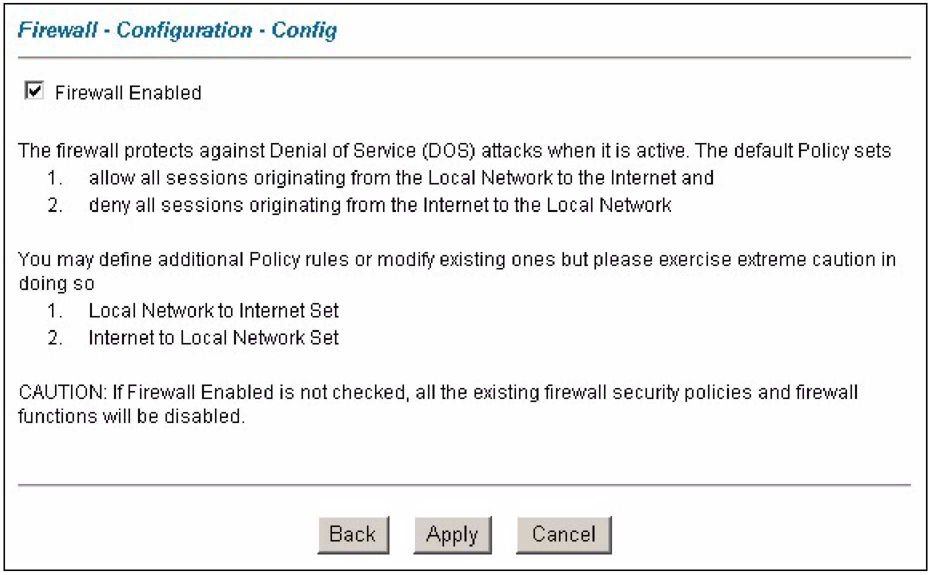
CHAPTER 9 Firewall Configuration

This chapter shows you how to enable and configure the ZyXEL Device firewall.

9.1 Enabling the Firewall

Click **Firewall** and then **Config** to display the following screen. Select the **Firewall Enabled** check box and click **Apply** to enable (or activate) the firewall.

Figure 31 Enabling the Firewall



Firewall - Configuration - Config

☑ Firewall Enabled

The firewall protects against Denial of Service (DOS) attacks when it is active. The default Policy sets

1. allow all sessions originating from the Local Network to the Internet and
2. deny all sessions originating from the Internet to the Local Network

You may define additional Policy rules or modify existing ones but please exercise extreme caution in doing so

1. Local Network to Internet Set
2. Internet to Local Network Set

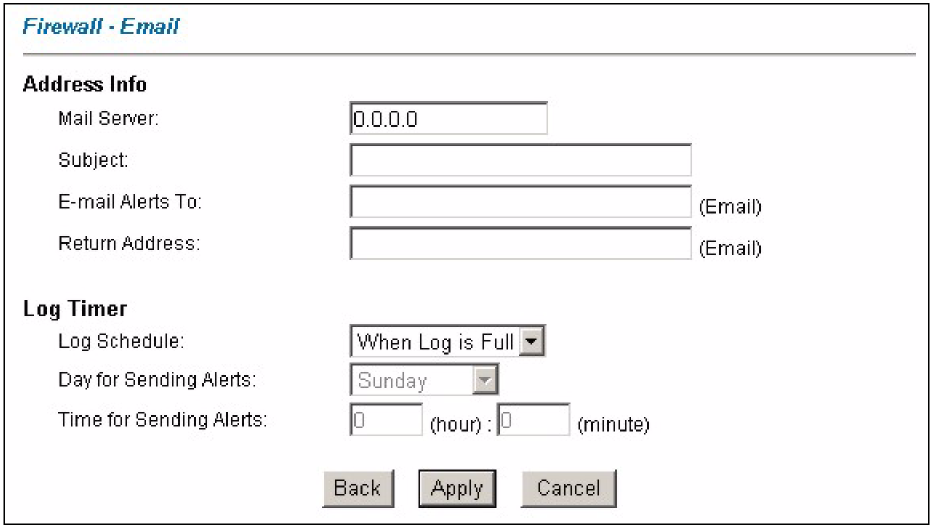
CAUTION: If Firewall Enabled is not checked, all the existing firewall security policies and firewall functions will be disabled.

9.2 E-Mail

To change your ZyXEL Device's E-mail log settings, click **Firewall**, and then **E-mail**. The screen appears as shown.

Use the **E-Mail** 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 send. An "End of Log" message displays for each mail in which a complete log has been sent

Figure 32 Firewall > E-mail



Firewall - Email

Address Info

Mail Server: 0.0.0.0

Subject:

E-mail Alerts To: (Email)

Return Address: (Email)

Log Timer

Log Schedule: When Log is Full

Day for Sending Alerts: Sunday

Time for Sending Alerts: 0 (hour) : 0 (minute)

The following table describes the labels in this screen.

Table 21 Firewall > E-mail

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.
Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends.
E-mail 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.
Return Address	Type an E-mail address to identify the ZyXEL Device as the sender of the e-mail messages i.e., a "return-to-sender" address for backup purposes.
Log Timer	
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 Alerts	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Alerts	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Back	Click **Back** to return to the previous screen.

Table 21 Firewall > E-mail (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.

9.3 Attack Alert

Attack alerts are real-time reports of DoS attacks. In the **Alert** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the ZyXEL Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

9.3.1 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Alert** screen (Figure 33 on page 92 - select the **Generate alert when attack detected** checkbox) or when a rule is matched in the **Edit Rule** screen (see Figure 35 on page 98). When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **E-mail** screen (see the chapter on E-mail).

9.3.2 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for most small offices. Factors influencing choices for threshold values are:

- The maximum number of opened sessions.
- The minimum capacity of server backlog in your LAN network.
- The CPU power of servers in your LAN network.
- Network bandwidth.
- Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.

You should make any changes to the threshold values before you continue configuring firewall rules.

9.3.3 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see Figure 27 on page 79). For UDP, "half-open" means that the firewall has detected no return traffic.

The ZyXEL Device measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the ZyXEL Device starts deleting half-open sessions as required to accommodate new connection requests. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the ZyXEL Device starts deleting half-open sessions as required to accommodate new connection requests. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

9.3.3.1 TCP Maximum Incomplete and Blocking Time

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

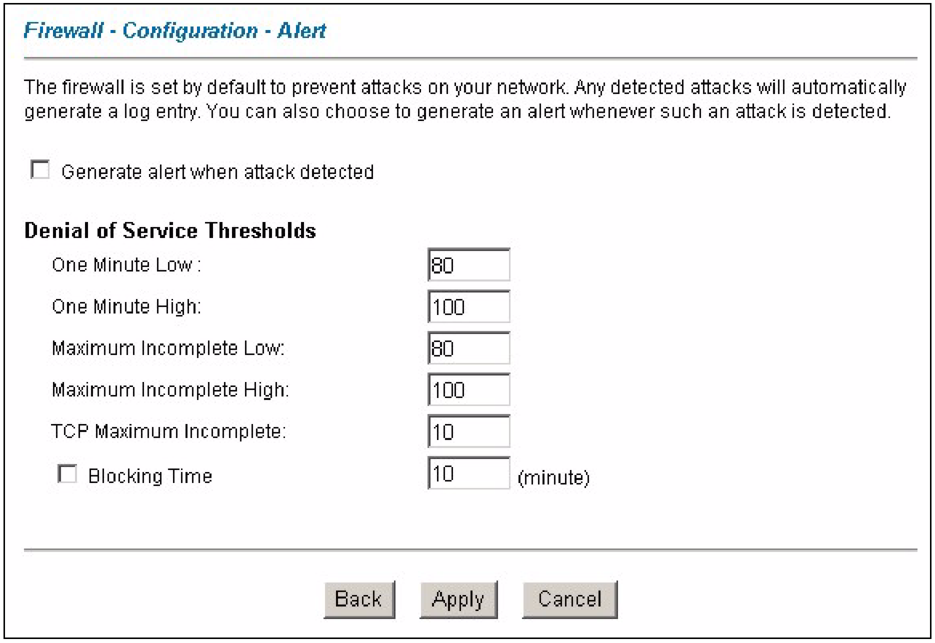
Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the ZyXEL Device starts deleting half-open sessions according to one of the following methods:

- If the **Blocking Time** timeout is 0 (the default), then the ZyXEL Device deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **Blocking Time** timeout is greater than 0, then the ZyXEL Device blocks all new connection requests to the host giving the server time to handle the present connections. The ZyXEL Device continues to block all new connection requests until the **Blocking Time** expires.

9.3.4 Configuring Firewall Alert

The ZyXEL Device also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall**, and **Alert** to bring up the next screen.



Firewall - Configuration - Alert

The firewall is set by default to prevent attacks on your network. Any detected attacks will automatically generate a log entry. You can also choose to generate an alert whenever such an attack is detected.

□ Generate alert when attack detected

Denial of Service Thresholds

One Minute Low :	80
One Minute High:	100
Maximum Incomplete Low:	80
Maximum Incomplete High:	100
TCP Maximum Incomplete:	10
□ Blocking Time	10 (minute)

Figure 33 Firewall > Alert

The following table describes the labels in this screen.

Table 22 Firewall > Alert

LABEL	DESCRIPTION
Generate alert when attack detected	Select this check box to generate an alert whenever an attack is detected.
Denial of Service Thresholds	
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection attempts.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.

Table 22 Firewall > Alert (continued)

LABEL	DESCRIPTION
Blocking Time	When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you select **Blocking Time**, any new sessions will be blocked for the length of time you specify in the next field **(minute)** and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.
(minute)	Type the length of **Blocking Time** in minutes (1-256). The default is "0".
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.

9.4 Rules Overview

Firewall rules are subdivided into "Local Network" and "Internet". By default, the ZyXEL Device's stateful packet inspection allows all communications to the Internet that originate from the local network, and blocks all traffic to the LAN that originates from the Internet. You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

Note: If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyXEL Device’s default rules.

9.5 Rule Logic Overview

Note: Study these points carefully before configuring rules.

9.5.1 Rule Checklist

State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."

1. Is the intent of the rule to forward or block traffic?
2. What direction of traffic does the rule apply to?
3. What IP services will be affected?
4. What computers on the LAN are to be affected (if any)?
5. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

9.5.2 Security Ramifications

1. Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:
2. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
3. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
4. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
5. Does this rule conflict with any existing rules?
6. Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

9.5.3 Key Fields For Configuring Rules

9.5.3.1 Action

Should the action be to **Block** or **Forward**?

Note: "Block" means the firewall silently discards the packet.

9.5.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See Section 9.11 on page 107 for more information on predefined services.

9.5.3.3 Source Address

What is the connection's source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

9.5.3.4 Destination Address

What is the connection's destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

9.6 Connection Direction

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

9.6.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. WAN to LAN Rules

9.6.2 WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

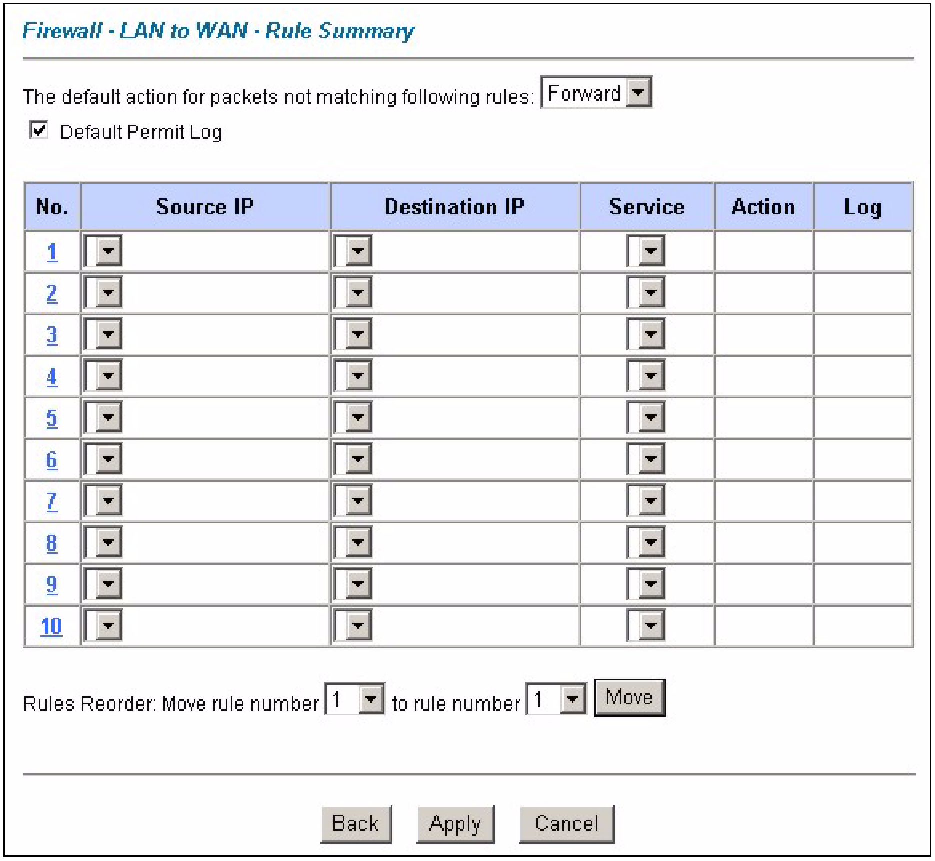
9.7 Firewall Rules Summary

Note: The fields in the **Rule Summary** screens are the same for **Local Network to Internet Set** and **Internet to Local Network Set**, so the discussion below refers to both.

Click on **Firewall**, then **Rule Summary** to bring up the following screen. This screen is a summary of the existing rules. Note the order in which the rules are listed.

Note: The ordering of your rules is very important as rules are applied in turn.

Figure 34 Firewall > Rule Summary



Firewall - LAN to WAN - Rule Summary

The default action for packets not matching following rules: Forward

☑ Default Permit Log

No.	Source IP	Destination IP	Service	Action	Log
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Rules Reorder: Move rule number 1 to rule number 1

The following table describes the labels in this screen.

Table 23 Firewall > Rule Summary

LABEL	DESCRIPTION
The default action for packets not matching following rules	Use the drop-down list box to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that do not match the following rules.
Default Permit Log	Select this check box to log all matched rules in the default set.
The following fields summarize the rules you have created. Note that these fields are read only.	
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The Move field below allows you to reorder your rules. Click a rule's number to edit the rule.
Source IP	This is the source address of the packet. Please note that a blank source or destination address is equivalent to **Any**.
Destination IP	This is the destination address of the packet. Please note that a blank source or destination address is equivalent to **Any**.
Service	This is the service to which the rule applies. See Figure 30 on page 107 for more information.
Action	This is the specified action for that rule, whether to **Block** (discard) or **Forward** (allow the passage of) packets.

Table 23 Firewall > Rule Summary (continued)

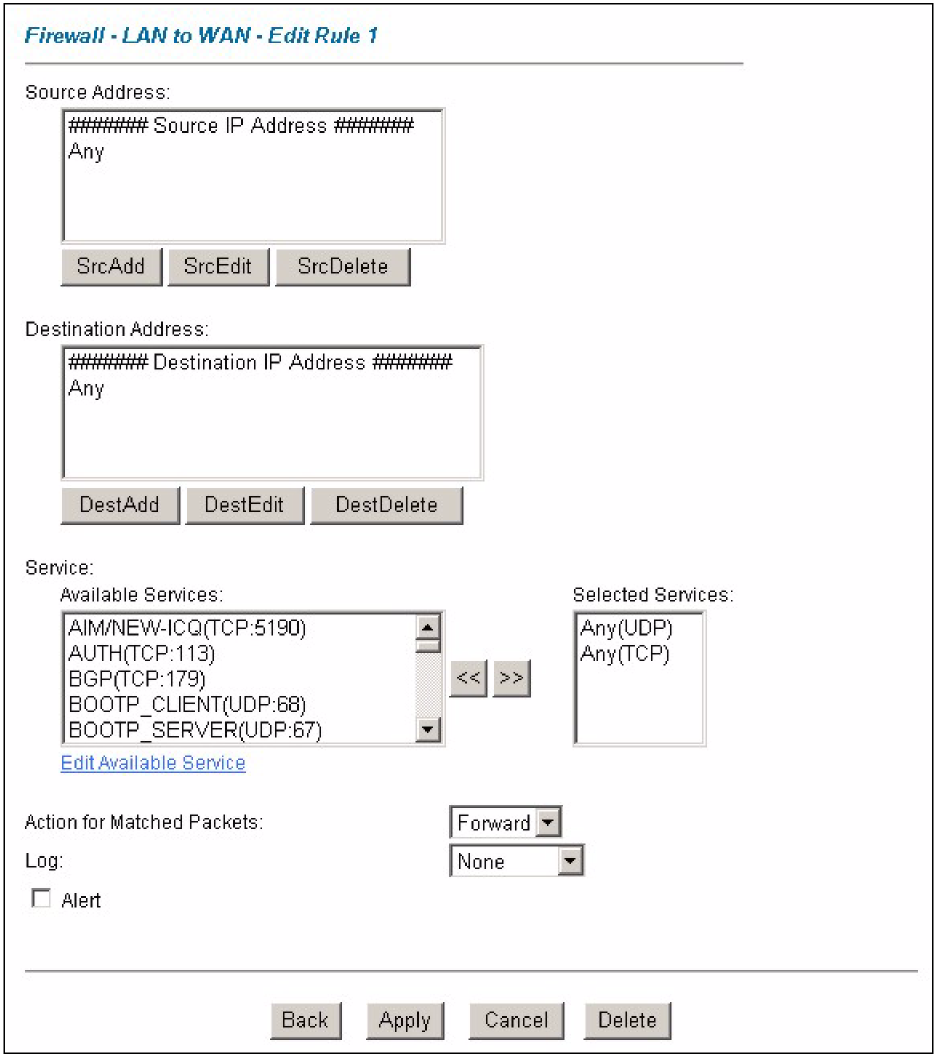
LABEL	DESCRIPTION
Log	This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**).
Rules Reorder	You may reorder your rules using this function. Use the drop-down list box to select the number of the rule you want to move. The ordering of your rules is important as rules are applied in turn.
To Rule Number	Use the drop-down list box to select to where you want to move the rule.
Move	Click **Move** to move the rule.
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.

9.7.1 Configuring Firewall Rules

Refer to Section 8.1 on page 76 for more information.

To create a new rule or edit an existing rule, click a number (**No.**) in the last screen shown to display the following screen.

Figure 35 Firewall > Edit a Rule



Firewall - LAN to WAN - Edit Rule 1

Source Address:

######## Source IP Address ########
Any

Destination Address:

######## Destination IP Address ########
Any

Service:

Available Services:

AIM/NEW-ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)
BOOTP_CLIENT(UDP:68)
BOOTP_SERVER(UDP:67)

Selected Services:

Any(UDP)
Any(TCP)

Action for Matched Packets: Forward

Log: None

□ Alert

The following table describes the labels in this screen.

Table 24 Firewall > Edit a Rule

LABEL	DESCRIPTION
Source Address	Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one. Refer to Section 9.7.2 on page 99 for more information.
Destination Address	Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one. Refer to Section 9.7.2 on page 99 for more information.
Services	Select a service in the **Available Services** box on the left, then click **>>** to select. The selected service shows up on the **Selected Services** box on the right. To remove a service, click on it in the **Selected Services** box on the right, then click **<<**.
Edit Available Service	Click this button to go to the **Customized Services** screen. Refer to Section 9.7.3 on page 100 for more information.
Edit Customized Service	Click the **Edit Customized Services** link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.

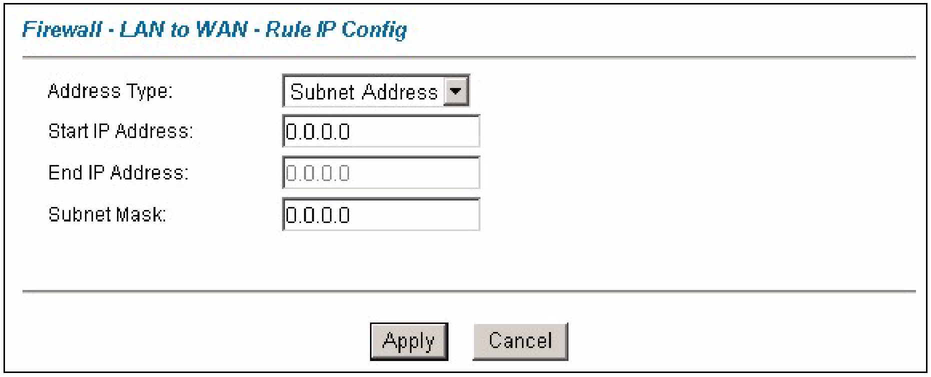
Table 24 Firewall > Edit a Rule (continued)

LABEL	DESCRIPTION
Action for Matched Packet	Use the drop down list box to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that match this rule.
Log	This field determines if a log is created for packets that match the rule (**Match**), don't match the rule (**Not-Match**), match either rule (**Both**) or no log is created (**None**).
Alert	Select the **Alert** check box to determine that this rule generates an alert when the rule is matched.
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.
Delete	Click **Delete** to exit this screen without saving.

9.7.2 Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen. Either action displays the following screen.

Figure 36 Firewall > Source and Destination Addresses



Firewall - LAN to WAN - Rule IP Config

Address Type: Subnet Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

The following table describes the labels in this screen.

Table 25 Firewall > Source and Destination Addresses

LABEL	DESCRIPTION
Address Type	Do you want your rule to apply to packets with a particular (single) IP address, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Type the single IP address or the starting IP address in a range here.
End IP Address	Type the ending IP address in a range here.
Subnet Mask	Type the subnet mask here, if applicable.

Table 25 Firewall > Source and Destination Addresses

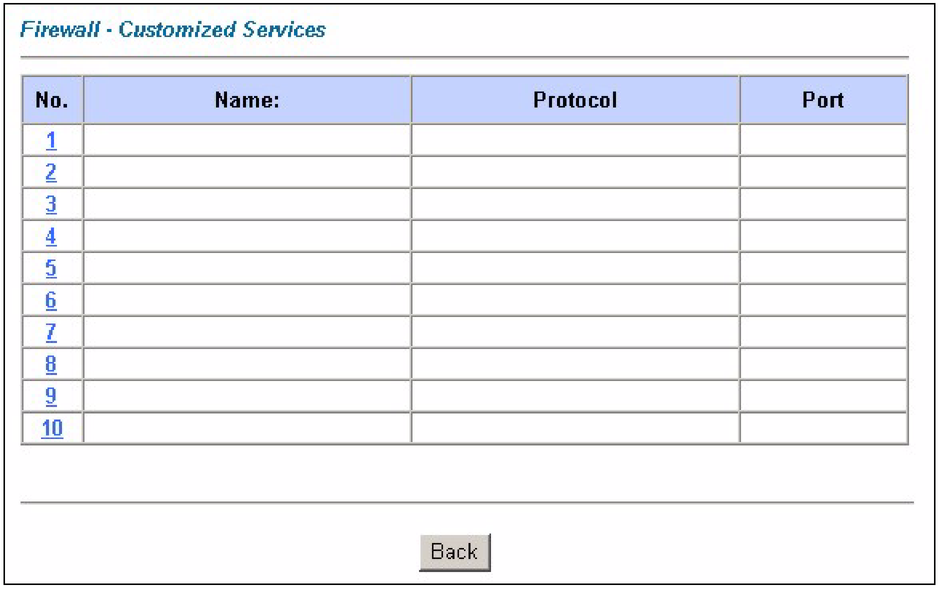
LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

9.7.3 Customized Services

Configure customized services and port numbers not predefined by the ZyXEL Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read Section 9.11 on page 107. Click the **Edit Available Service** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Refer to Section 8.1 on page 76 for more information.

Figure 37 Firewall > Customized Services



Firewall - Customized Services

No.	Name:	Protocol	Port
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

The following table describes the labels in this screen.

Table 26 Firewall > Customized Services

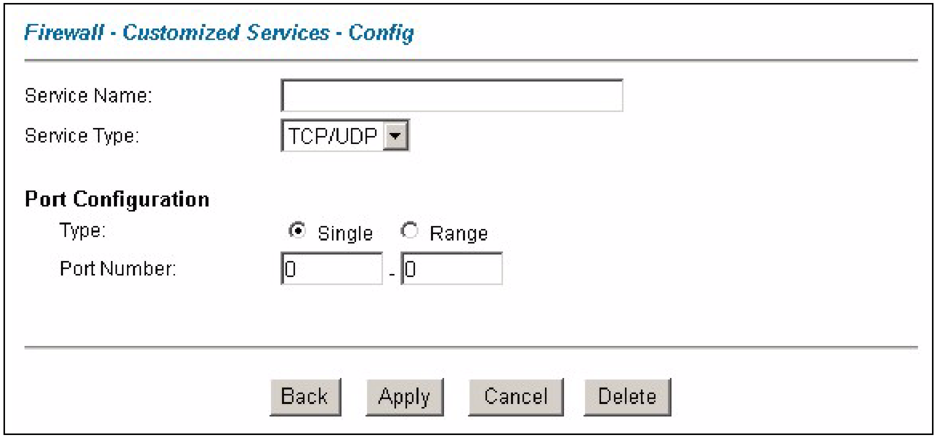
LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to a screen where you can configure or edit a customized service. See Section 9.7.4 on page 101 for more information.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (**TCP**, **UDP** or **TCP/UDP**) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click **Back** to return to the **Firewall Edit Rule** screen.

9.7.4 Configuring A Customized Service

Click a rule number in the **Firewall Customized Services** screen to create a new custom port or edit an existing one. This action displays the following screen.

Refer to Section 8.1 on page 76 for more information.

Figure 38 Firewall > Configure Customized Services



Firewall - Customized Services - Config

Service Name:

Service Type: TCP/UDP

Port Configuration

Type: ● Single ○ Range

Port Number: 0 - 0

The following table describes the labels in this screen.

Table 27 Firewall > Configure Customized Services

LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (**TCP**, **UDP** or **TCP/UDP**) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
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.
Delete	Click **Delete** to exit this screen without saving.

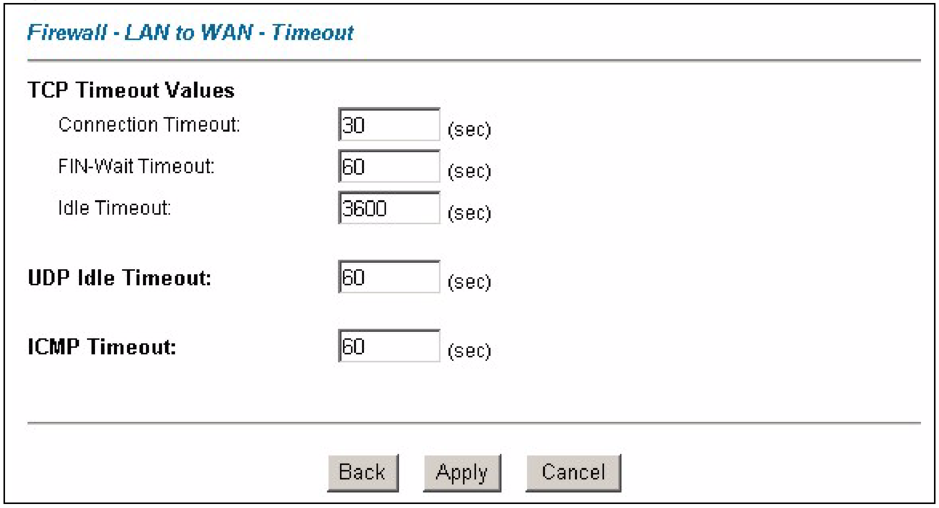
9.8 Timeout

The fields in the **Timeout** screens are the same for **Local Network to Internet Set** and **Internet to Local Network Set**, so the discussion below refers to both.

9.8.1 Factors Influencing Choices for Timeout Values

The factors influencing choices for timeout values are the same as the factors influencing choices for threshold values - see Section 9.3.2 on page 90. Click **Timeout** for either **Local Network to Internet Set** or **Internet to Local Network Set**.

Figure 39 Firewall > Timeout



Firewall - LAN to WAN - Timeout

TCP Timeout Values

Connection Timeout: 30 (sec)

FIN-Wait Timeout: 60 (sec)

Idle Timeout: 3600 (sec)

UDP Idle Timeout: 60 (sec)

ICMP Timeout: 60 (sec)

The following table describes the labels in this screen.

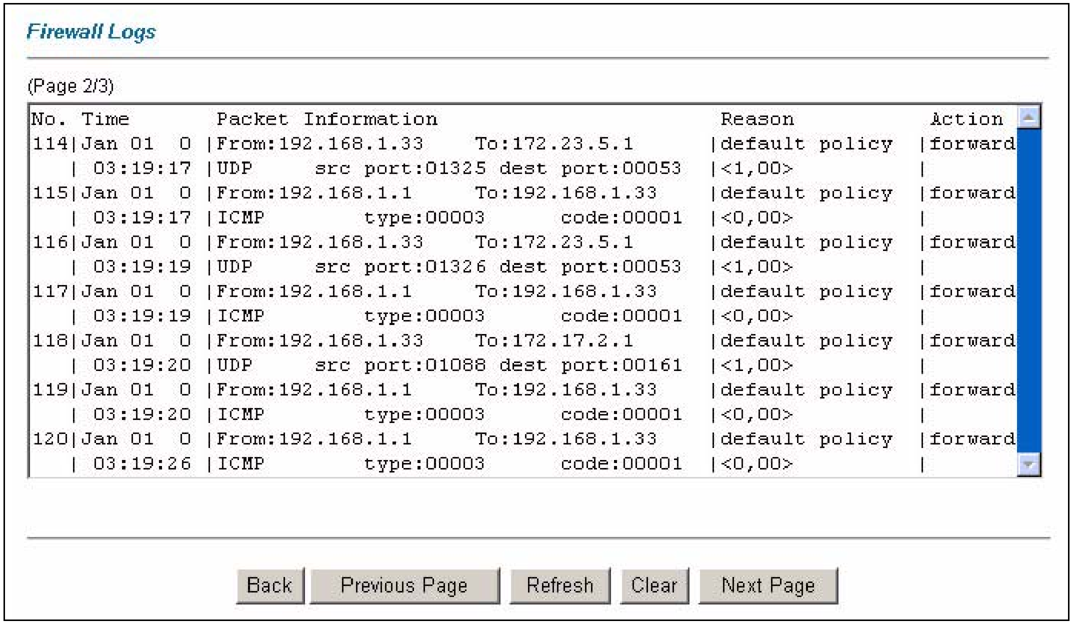
Table 28 Firewall > Timeout

LABEL	DESCRIPTION
TCP Timeout Values	
Connection Timeout	Type the number of seconds (default 30) for the ZyXEL Device to wait for a TCP session to reach the established state before dropping the session.
FIN-Wait Timeout	Type the number of seconds (default 60) for a TCP session to remain open after the firewall detects a FIN-exchange (indicating the end of the TCP session)
Idle Timeout	Type the number of seconds (default 3600) for an inactive TCP connection to remain open before the ZyXEL Device considers the connection closed.
UDP Idle Timeout	Type the number of seconds (default 60) for an inactive UDP connection to remain open before the ZyXEL Device considers the connection closed.
ICMP Timeout	Type the number of seconds (default 60) for an ICMP session to wait for the ICMP response.
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.

9.9 Logs Screen

When you configure a new rule you also have the option to log events that match, don't match (or both) this rule. Click **Logs** to bring up the next screen. Firewall logs may also be viewed in SMT Menu 21.3 or via syslog (SMT **Menu 24.3.2 - System Maintenance - UNIX Syslog**). Syslog is an industry standard protocol used for capturing log information for devices on a network. 128 entries are available numbered from 0 to 127. Once they are all used, the log wraps around and the old logs are lost.

Figure 40 Firewall > Logs



Firewall Logs

(Page 2/3)

```
No. Time        Packet Information                                   Reason            Action
114|Jan 01   0 |From:192.168.1.33     To:172.23.5.1        |default policy  |forward
   | 03:19:17 |UDP      src port:01325 dest port:00053    |<1,00>           |
115|Jan 01   0 |From:192.168.1.1      To:192.168.1.33      |default policy  |forward
   | 03:19:17 |ICMP          type:00003       code:00001  |<0,00>           |
116|Jan 01   0 |From:192.168.1.33     To:172.23.5.1        |default policy  |forward
   | 03:19:19 |UDP      src port:01326 dest port:00053    |<1,00>           |
117|Jan 01   0 |From:192.168.1.1      To:192.168.1.33      |default policy  |forward
   | 03:19:19 |ICMP          type:00003       code:00001  |<0,00>           |
118|Jan 01   0 |From:192.168.1.33     To:172.17.2.1        |default policy  |forward
   | 03:19:20 |UDP      src port:01088 dest port:00161    |<1,00>           |
119|Jan 01   0 |From:192.168.1.1      To:192.168.1.33      |default policy  |forward
   | 03:19:20 |ICMP          type:00003       code:00001  |<0,00>           |
120|Jan 01   0 |From:192.168.1.1      To:192.168.1.33      |default policy  |forward
   | 03:19:26 |ICMP          type:00003       code:00001  |<0,00>           |
```

The following table describes the labels in this screen.

Table 29 Firewall > Logs

LABEL	DESCRIPTION	EXAMPLE
No.	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real-time; otherwise the time shown in these examples is displayed.	dd:mm:yy: For example, Jan 01 0 hh:mm:ss: For example, 03:19:17
Packet Information	This field lists packet information such as:	From and To IP addresses or protocol and port numbers.

Table 29 Firewall > Logs (continued)

LABEL	DESCRIPTION	EXAMPLE
Reason	This field states the reason for the log; i.e., was the rule matched, not matched, or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol.
	This is a log for a DoS attack.	attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop, or syn flood.
Action	This field displays whether the packet was blocked (i.e., silently discarded), forwarded or neither (Block, Forward or None). "None" means that no action is dictated by this rule.	Block, Forward or None
Back	Click **Back** to return to the previous screen.	
Previous Page/ Next Page	Click **Previous Page** or **Next Page** to view other pages in your log.	
Refresh	Click **Refresh** to renew the log screen.	
Clear	Click **Clear** to clear all the logs.	

9.10 Example Firewall Rule

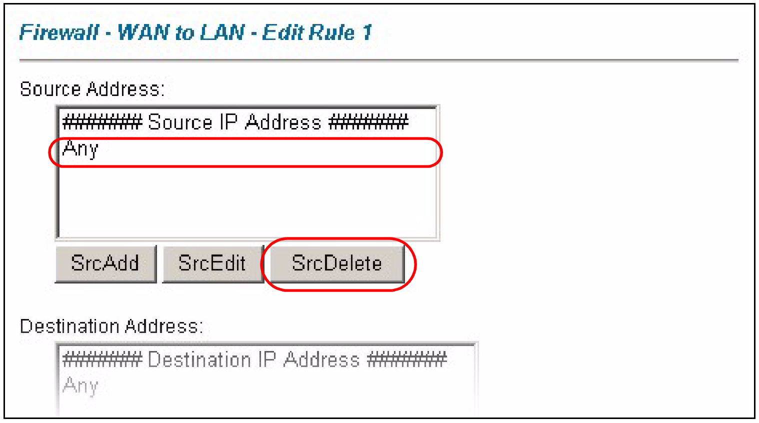
The following Internet firewall rule example allows a hypothetical "MyService" connection from the Internet.

1 Click **Firewall**, then **Rule Summary** under **Internet to Local Network Set**.

2 Click a rule number to open the **Edit Rule** screen.

3 Click **Any** in the **Source Address** box and then click **SrcDelete**.

Figure 41 Firewall Example: Edit Rule



Firewall - WAN to LAN - Edit Rule 1

Source Address:

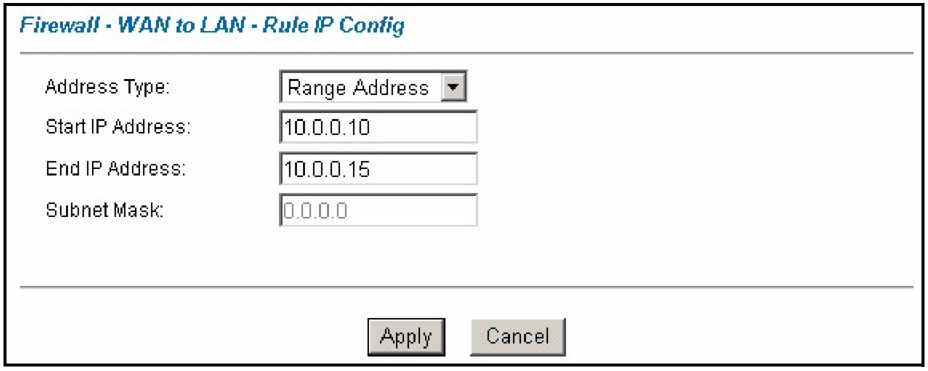
####### Source IP Address #######
Any

Destination Address:

####### Destination IP Address #######
Any

4 Click **SrcAdd** to open the **Rule IP Config** screen. Configure it as follows and click **Apply**.

Figure 42 Firewall Example: Configure Source IP



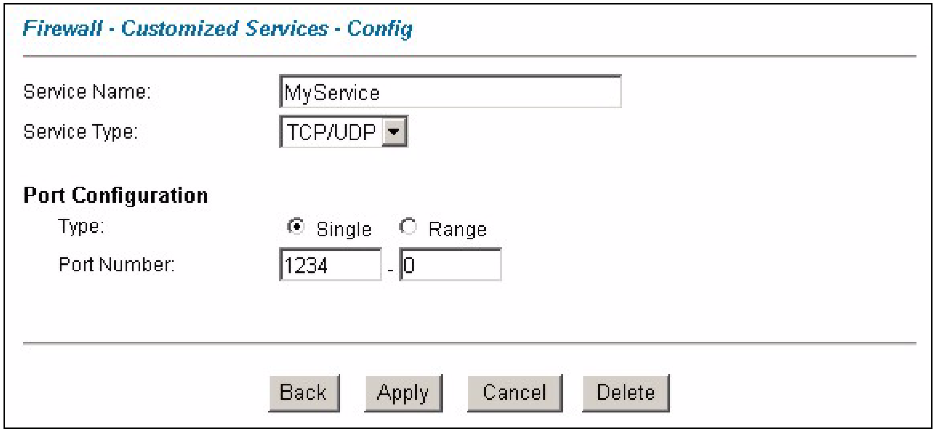
Firewall - WAN to LAN - Rule IP Config

Address Type:	Range Address
Start IP Address:	10.0.0.10
End IP Address:	10.0.0.15
Subnet Mask:	0.0.0.0

5 Click **Edit Available Service** in the **Edit Rule** screen and then click a rule number to bring up the **Firewall Customized Services Config** screen. Configure as follows.

Note: Customized services show up with an "*" before their names in the **Services** list box and the **Rule Summary** list box. Click **Apply** after you've created your customized service.

Figure 43 Firewall Example: Customized Service



Firewall - Customized Services - Config

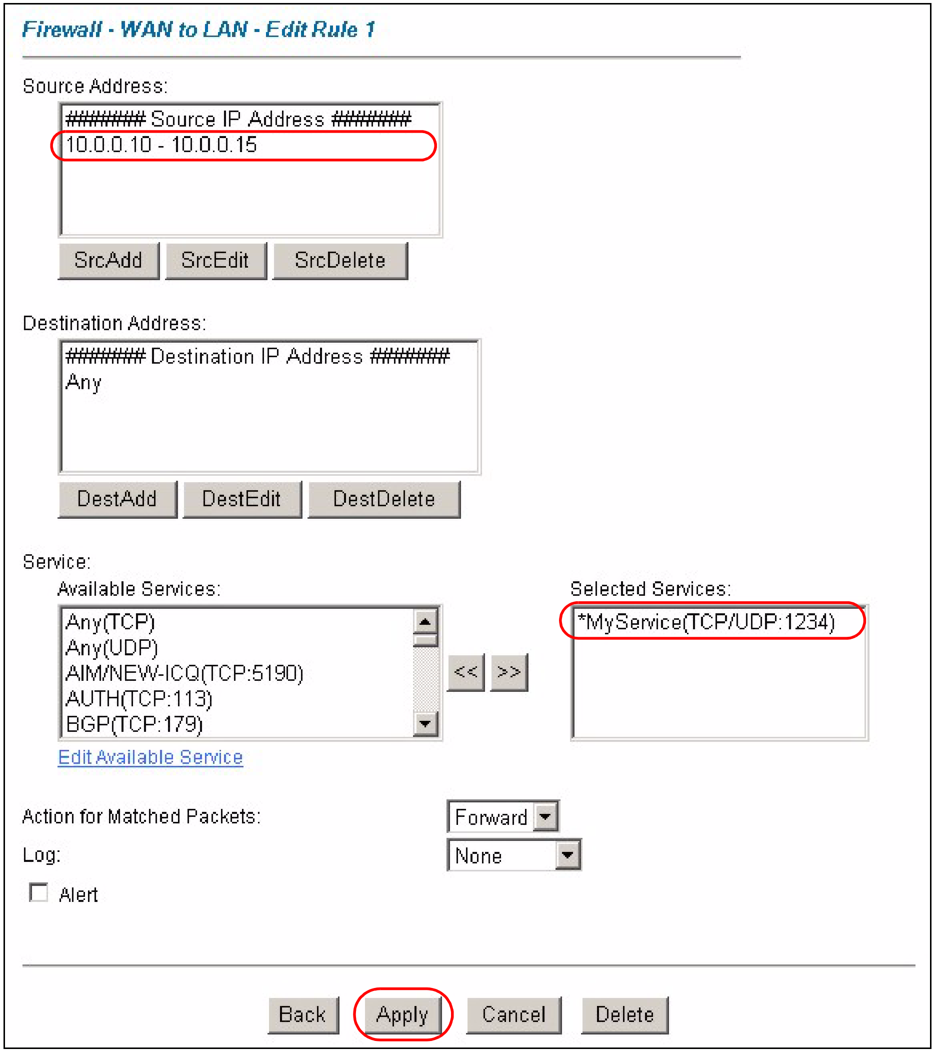
Service Name:	MyService
Service Type:	TCP/UDP

Port Configuration

Type:	● Single ○ Range
Port Number:	1234 - 0

6 Follow the procedures outlined earlier in this chapter to configure all your rules. Configure the rule configuration screen like the one below and apply it.

Figure 44 Firewall Example: Edit Rule: Select Customized Services



Firewall - WAN to LAN - Edit Rule 1

Source Address:
####### Source IP Address #######
10.0.0.10 - 10.0.0.15

Destination Address:
####### Destination IP Address #######
Any

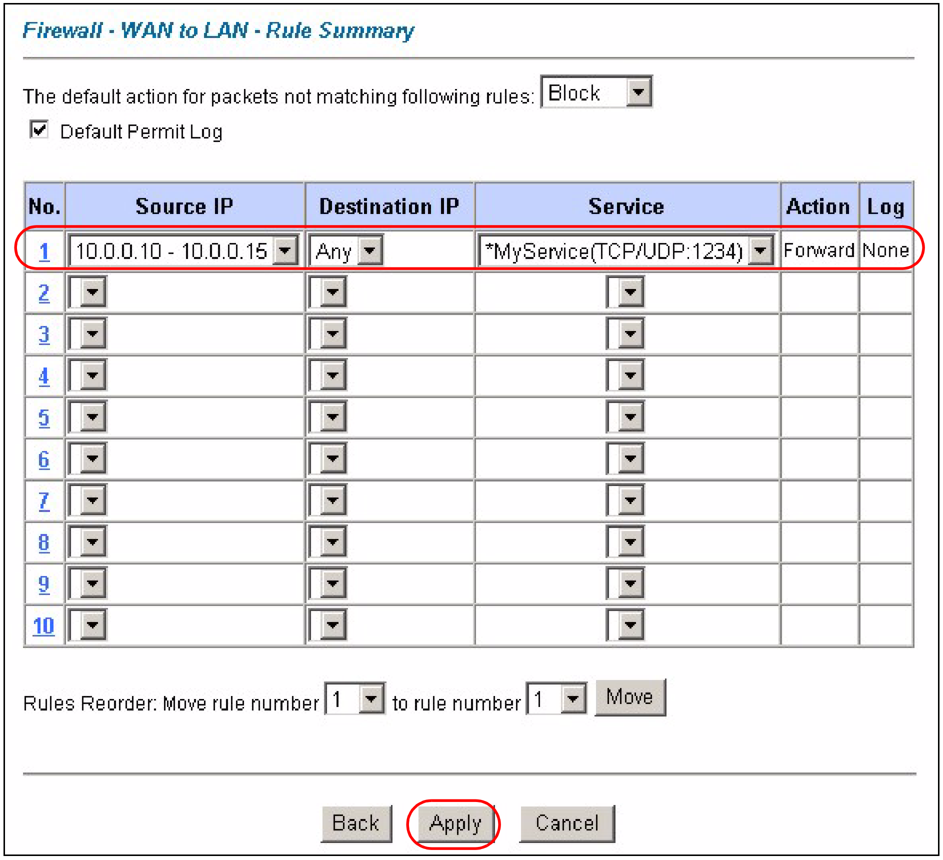
Service:
Available Services:
Any(TCP)
Any(UDP)
AIM/NEW-ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)

Selected Services:
*MyService(TCP/UDP:1234)

Action for Matched Packets: Forward
Log: None
□ Alert

7 On completing the configuration procedure for these Internet firewall rules, the **Rule Summary** screen should look like the following. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the ZyXEL Device.

Figure 45 Firewall Example: Rule Summary



Firewall - WAN to LAN - Rule Summary

The default action for packets not matching following rules: Block

☑ Default Permit Log

No.	Source IP	Destination IP	Service	Action	Log
1	10.0.0.10 - 10.0.0.15	Any	*MyService(TCP/UDP:1234)	Forward	None
2					
3					
4					
5					
6					
7					
8					
9					
10					

Rules Reorder: Move rule number 1 to rule number 1

9.11 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see Section 9.7.1 on page 97) displays all predefined services that the ZyXEL Device already supports. 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 default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom service ports may also be configured using the **Edit Available Service** function discussed previously.

Table 30 Predefined 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.

Table 30 Predefined Services (continued)

SERVICE	DESCRIPTION
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	Net Meeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IPSEC_TRANSPORT/ TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks’ messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.

Table 30 Predefined Services (continued)

SERVICE	DESCRIPTION
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS (TCP/ UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP(UDP:1900)	Simole Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using DUDP port 1900.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRMWORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

CHAPTER 10 Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

10.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

10.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

10.1.2 Security

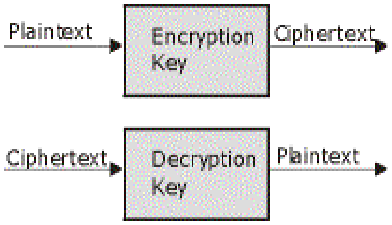
A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

10.1.3 Other Terminology

10.1.3.1 Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms “ciphertext” to plaintext. Decryption also requires a key.

Figure 46 Encryption and Decryption



10.1.3.2 Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

10.1.3.3 Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

10.1.3.4 Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

10.1.4 VPN Applications

The ZyXEL Device supports the following VPN applications.

- Linking Two or More Private Networks Together

  Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- Accessing Network Resources When NAT Is Enabled

  When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

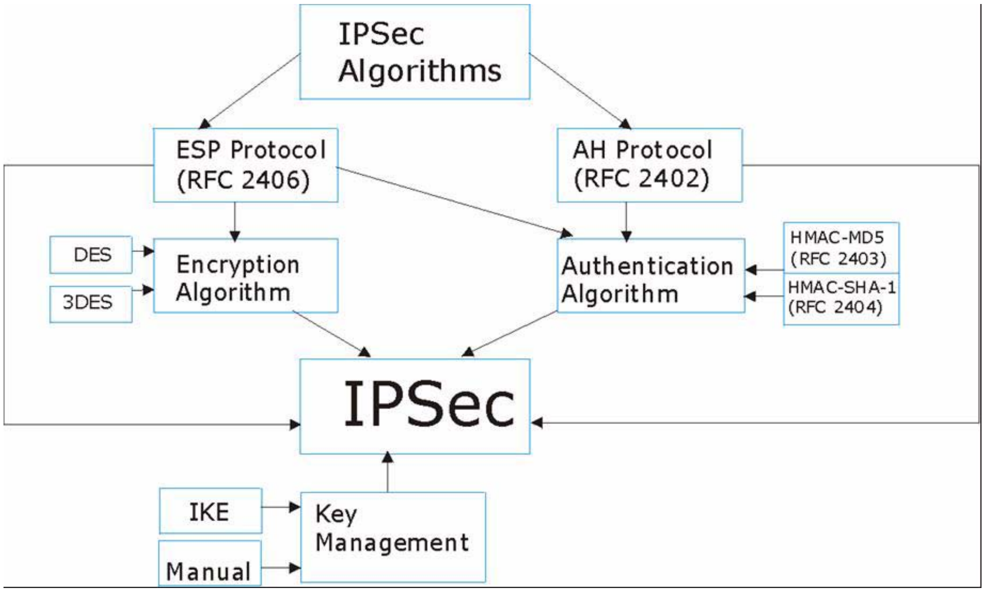
- Unsupported IP Applications

  A VPN tunnel may be created to add support for unsupported emerging IP applications. See Chapter 1 on page 32 for an example of a VPN application.

10.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 47 IPSec Architecture



10.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Please see Section 11.2 on page 116 for more information.

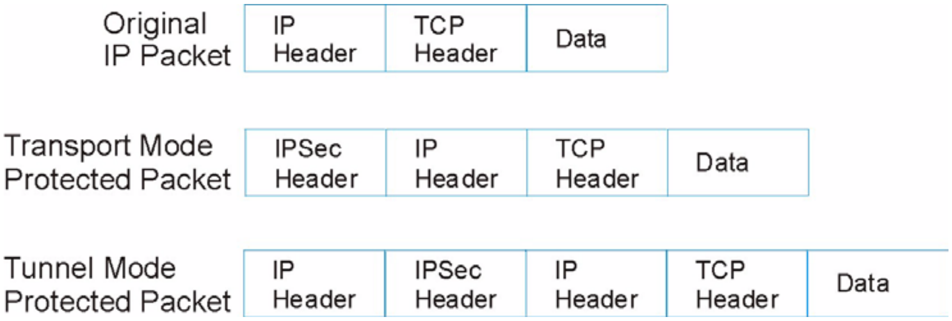
10.2.2 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

10.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 48 Transport and Tunnel Mode IPSec Encapsulation



10.3.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

10.3.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

10.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyXEL Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints.

Table 31 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

CHAPTER 11 VPN Screens

This chapter introduces the VPN web configurator. See the section on logs for information on viewing logs and the appendices for IPSec log descriptions.

11.1 VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

11.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

11.2.1 AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

11.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as the services offered by **AH**. **ESP** authenticating properties are limited compared to the AH due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

.

Table 32 AH and ESP

	ESP	AH
Encryption	**DES** (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	
	Select **NULL** to set up a phase 2 tunnel without encryption.	
Authentication	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select **MD5** for minimal security and **SHA-1** for maximum security.	

11.3 My IP Address

My IP Address is the WAN IP address of the ZyXEL Device. If this field is configured as 0.0.0.0, then the ZyXEL Device will use the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel. The ZyXEL Device has to rebuild the VPN tunnel if the **My IP Address** changes after setup.

11.4 Secure Gateway IP Address

Secure Gateway IP Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway IP Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway IP Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway IP Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyXEL Device has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

11.4.1 Dynamic Secure Gateway Address

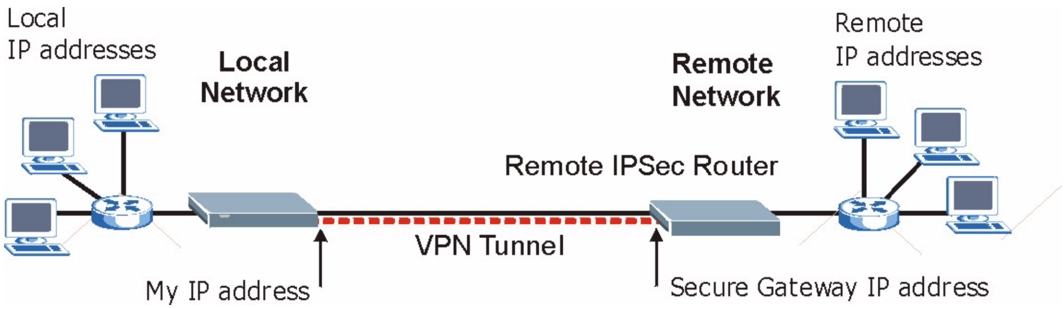
If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network.

Note: The Secure Gateway IP Address may be configured as 0.0.0.0 only when using **IKE** key management and not **Manual** key management.

11.5 VPN Summary Screen

The following figure helps explain the main fields in the web configurator.

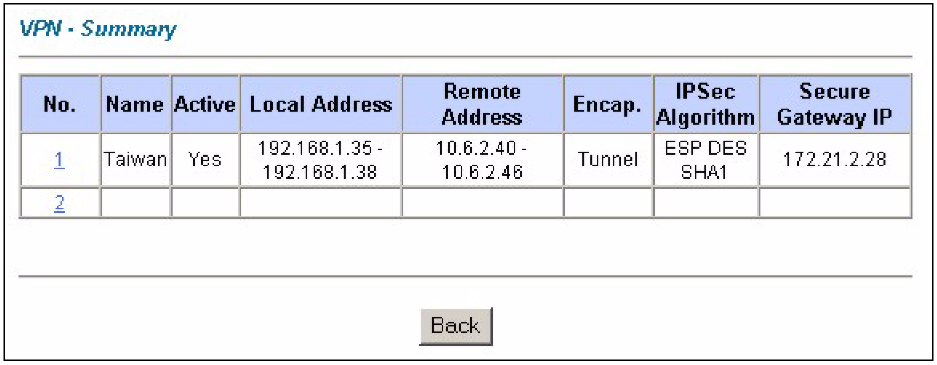
Figure 49 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **VPN** and **Setup** to open the **Summary** screen. This is a read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by clicking an index number to configure the associated submenus.

Figure 50 VPN Summary



VPN - Summary

No.	Name	Active	Local Address	Remote Address	Encap.	IPSec Algorithm	Secure Gateway IP
1	Taiwan	Yes	192.168.1.35 - 192.168.1.38	10.6.2.40 - 10.6.2.46	Tunnel	ESP DES SHA1	172.21.2.28
2							

The following table describes the labels in this screen.

Table 33 VPN Summary

LABEL	DESCRIPTION
No.	This is the VPN policy index number. Click a number to edit VPN policies.
Name	This field displays the identification name for this VPN policy.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.
Local Address	This is the IP address of the computer on your local network behind your ZyXEL Device. The same (static) IP address is displayed twice when the **Local Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Address Type** field in the **VPN-IKE** (or V**PN-Manual Key**) screen is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Local Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Subnet**.
Remote Address	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays **N/A** when the **Secure Gateway IP Address** field is set to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the **Remote Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Remote Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Subnet**.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).
Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase ZyXEL Device processing requirements and communications latency (delay).
Secure Gateway IP	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway IP Address** field in the **VPN-IKE** screen to **0.0.0.0.**
Back	Click this button to return to the previous screen.

11.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the ZyXEL Device automatically renegotiates the tunnel when the IPSec SA lifetime period expires (Section 11.10 on page 126 for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an "always on" connection after you initiate it. Both IPSec routers must have a ZyXEL Device-compatible keep alive feature enabled in order for this feature to work.

If the ZyXEL Device has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the ZyXEL Device because the ZyXEL Device never drops the tunnels that are already connected.

Note: When there is outbound traffic with no inbound traffic, the ZyXEL Device automatically drops the tunnel after two minutes.

11.7 ID Type and Content

With aggressive negotiation mode (see Section 11.10.1 on page 127), the ZyXEL Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyXEL Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyXEL Device from IPSec routers with dynamic IP addresses (see Section 11.16 on page 136 for a telecommuter configuration example).

Note: Regardless of the ID type and content configuration, the ZyXEL Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 11.10.1 on page 127), the ID type and content are encrypted to provide identity protection. In this case the ZyXEL Device can only distinguish between up to eight different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyXEL Device can distinguish up to eight incoming SAs because you can select between three encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see Section 11.11 on page 128). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 34 Local ID Type and Content Fields

LOCAL ID TYPE	CONTENT
IP	Type the IP address of your computer or leave the field blank to have the ZyXEL Device automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyXEL Device.

Table 34 Local ID Type and Content Fields

LOCAL ID TYPE	CONTENT
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyXEL Device.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

Table 35 Peer ID Type and Content Fields

PEER ID TYPE	CONTENT
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL Device automatically use the address in the **Secure Gateway Address** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router’s IP address or what you configure in the **Secure Gateway IP Address** field below.	

11.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two ZyXEL Devices in this example can complete negotiation and establish a VPN tunnel

Table 36 Matching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two ZyXEL Devices in this example cannot complete their negotiation because ZyXEL Device **B**’s **Local ID type** is **IP**, but ZyXEL Device **A**’s **Peer ID type** is set to **E-mail**. An “ID mismatched” message displays in the IPSEC LOG.

Figure 51 Mismatching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10

Figure 51 Mismatching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

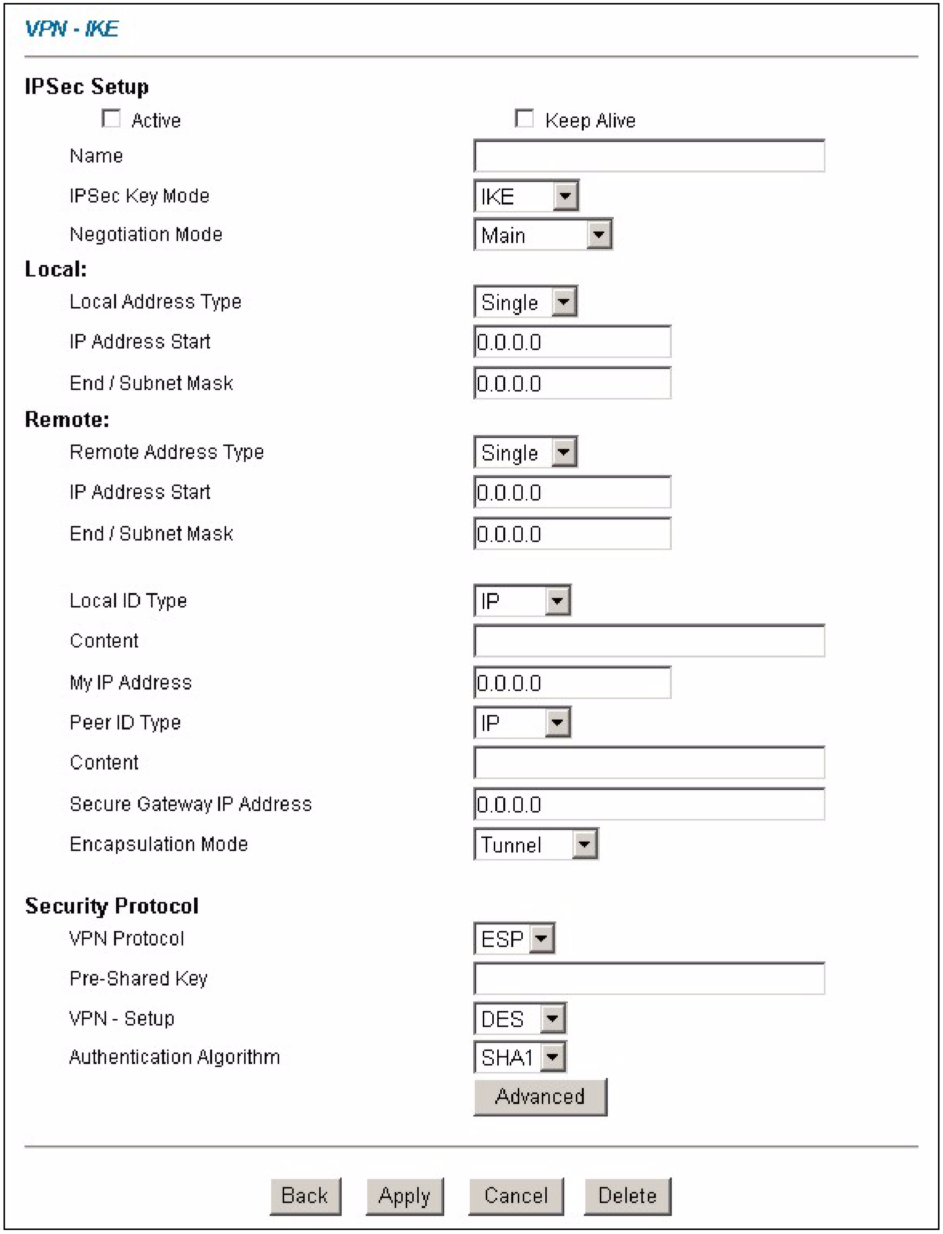
11.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 11.10 on page 126 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

11.9 VPN Rules

Click a number (**No.**) on the **Summary** screen to edit VPN rules.

Figure 52 VPN Rule Setup



VPN - IKE

IPSec Setup

□ Active □ Keep Alive

Name

IPSec Key Mode: IKE

Negotiation Mode: Main

Local:

Local Address Type: Single

IP Address Start: 0.0.0.0

End / Subnet Mask: 0.0.0.0

Remote:

Remote Address Type: Single

IP Address Start: 0.0.0.0

End / Subnet Mask: 0.0.0.0

Local ID Type: IP

Content

My IP Address: 0.0.0.0

Peer ID Type: IP

Content

Secure Gateway IP Address: 0.0.0.0

Encapsulation Mode: Tunnel

Security Protocol

VPN Protocol: ESP

Pre-Shared Key

VPN - Setup: DES

Authentication Algorithm: SHA1

The following table describes the labels in this screen.

Table 37 VPN Rule Setup

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select this check box to have the ZyXEL Device automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
IPSec Key Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.

Table 37 VPN Rule Setup (continued)

LABEL	DESCRIPTION
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. The ZyXEL Device's negotiation mode should be identical to that on the remote secure gateway.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Secure Gateway IP Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway IP Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway IP Address** field set to **0.0.0.0**.
Local Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** for a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Local Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your ZyXEL Device.
End/Subnet Mask	When the **Local Address Type** field is configured to **Single**, enter the IP address in the **IP Address Start** field again here. When the **Local Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind your ZyXEL Device.
	Remote Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** with a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Remote Address Type** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.
End/ Subnet Mask	When the **Remote Address Type** field is configured to **Single**, enter the IP address in the **IP Address Start** field again here. When the **Remote Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.

Table 37 VPN Rule Setup (continued)

LABEL	DESCRIPTION
Local ID Type	Select **IP** to identify this ZyXEL Device by its IP address. Select **DNS** to identify this ZyXEL Device by a domain name. Select **E-mail** to identify this ZyXEL Device by an e-mail address.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The ZyXEL Device automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyXEL Device in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
My IP Address	Enter the WAN IP address of your ZyXEL Device. The ZyXEL Device uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. The VPN tunnel has to be rebuilt if this IP address changes.
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	The configuration of the peer content depends on the peer ID type. • For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyXEL Device will use the address in the **Secure Gateway IP Address** field (refer to the **Secure Gateway IP Address** field description). • For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the ZyXEL Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
Secure Gateway IP Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **IPSec Keying Mode** field must be set to **IKE**). In this case only the remote IPSec router can initiate the VPN. In order to have more than one active rule with the **Secure Gateway IP Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway IP Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway IP Address** field set to **0.0.0.0**.

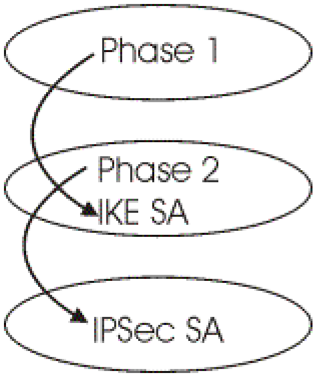
Table 37 VPN Rule Setup (continued)

LABEL	DESCRIPTION
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Security Protocol	
VPN Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **VPN - Setup** and **Authentication Algorithm** fields (described next). Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described later).
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x” (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
VPN - Setup	Select **DES**, **3DES** or **NULL** from the drop-down list box. The ZyXEL Device’s encryption algorithm should be identical to the secure remote gateway. When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Advanced	Click **Advanced** to configure more detailed settings of your IKE key management.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to begin configuring this screen afresh.

11.10 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 53 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).

Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see Section 11.10.3 on page 128. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyXEL Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyXEL Device also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

11.10.1 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

11.10.2 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

11.10.3 Perfect Forward Secrecy (PFS)

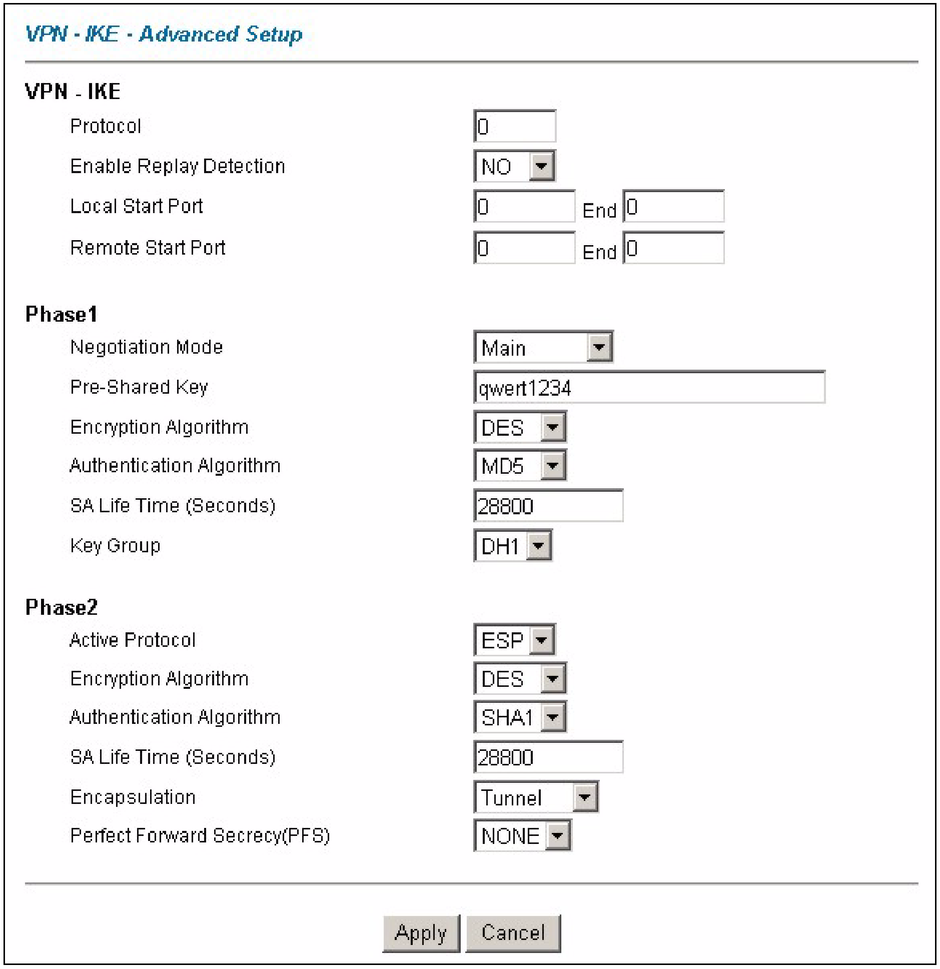
Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the ZyXEL Device. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

11.11 Advanced IKE Settings

Select **Advanced** at the bottom of the **VPN-IKE** screen. The following screen displays.

Figure 54 Advanced Rule Setup



VPN - IKE - Advanced Setup

VPN - IKE

Protocol	0
Enable Replay Detection	NO
Local Start Port	0 End 0
Remote Start Port	0 End 0

Phase1

Negotiation Mode	Main
Pre-Shared Key	qwert1234
Encryption Algorithm	DES
Authentication Algorithm	MD5
SA Life Time (Seconds)	28800
Key Group	DH1

Phase2

Active Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA Life Time (Seconds)	28800
Encapsulation	Tunnel
Perfect Forward Secrecy(PFS)	NONE

The following table describes the labels in this screen.

Table 38 Advanced Rule Setup

LABEL	DESCRIPTION
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **YES** to enable replay detection, or select **NO** to disable it.
Local Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field (or equal to it for configuring an individual port).
Remote Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3

Table 38 Advanced Rule Setup (continued)

LABEL	DESCRIPTION
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field (or equal to it for configuring an individual port).
Phase 1 A phase 1 exchange establishes an IKE SA (Security Association).	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. The ZyXEL Device's negotiation mode should be identical to that on the remote secure gateway.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x” (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select **DES** or **3DES** from the drop-down list box. The ZyXEL Device's encryption algorithm should be identical to the secure remote gateway. When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. The ZyXEL Device's authentication algorithm should be identical to the secure remote gateway. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate the source and integrity of packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select **SHA-1** for maximum security.
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	A phase 2 exchange uses the IKE SA established in phase 1 to negotiate the SA for IPSec.
Active Protocol	Select **ESP** or **AH** from the drop-down list box. The ZyXEL Device's IPSec Protocol should be identical to the secure remote gateway. The ESP (Encapsulation Security Payload) protocol (RFC 2406) provides encryption as well as the authentication offered by AH. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below). The AH protocol (Authentication Header Protocol) (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field.

Table 38 Advanced Rule Setup (continued)

LABEL	DESCRIPTION
Encryption Algorithm	The encryption algorithm for the ZyXEL Device and the secure remote gateway should be identical. When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop down list-box. The ZyXEL Device's encapsulation mode should be identical to the secure remote gateway.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (None) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose from **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1, a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2, a 1024 bit (1Kb) random number (more secure, yet slower).
Apply	Click **Apply** to save your changes back to the ZyXEL Device and return to the **VPN-IKE** screen.
Cancel	Click **Cancel** to return to the **VPN-IKE** screen without saving your ZyXEL Device.

11.12 Manual Key

Manual key management is useful if you have problems with **IKE** key management.

11.12.1 Security Parameter Index (SPI)

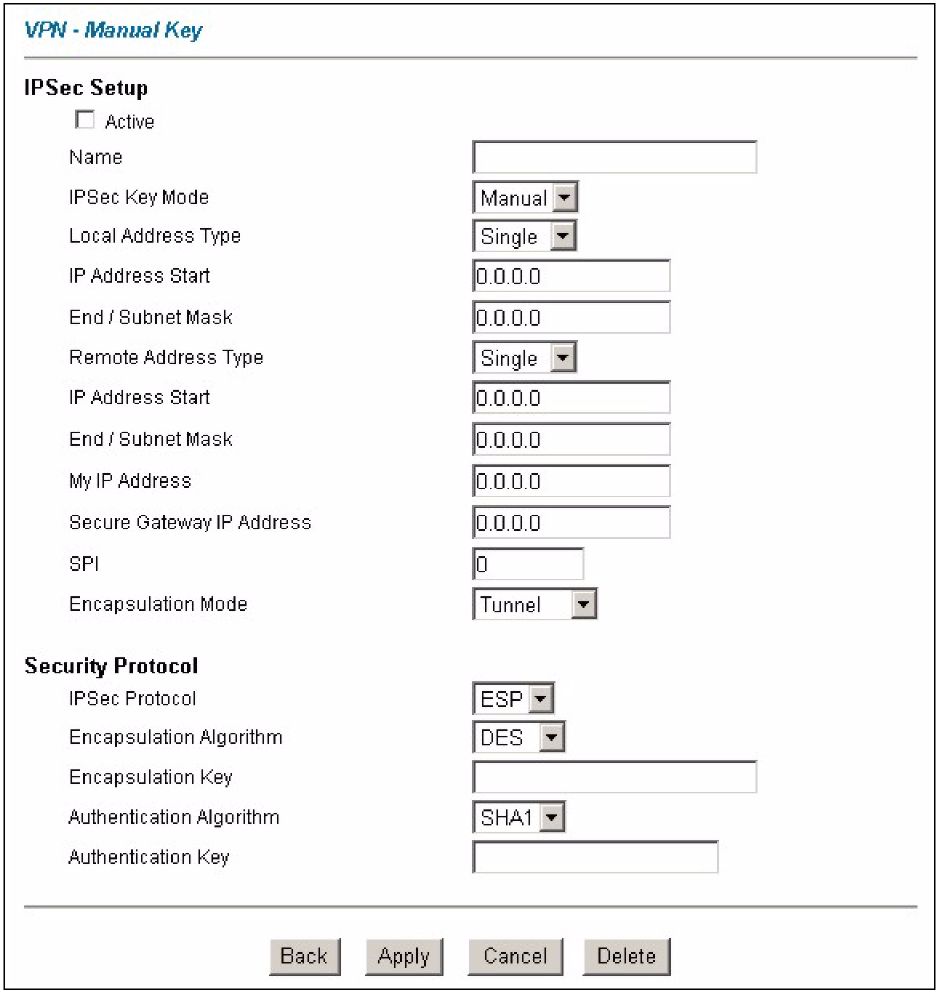
An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association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

Note: Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

11.13 Manual Key Screen

You only configure **VPN Manual Key** when you select **Manual** in the **IPSec Key Mode** field on the **VPN-IKE** screen. The **VPN-Manual Key** screen as shown next.

Figure 55 Rule Setup with Manual Key



VPN - Manual Key

IPSec Setup

□ Active

Name	
IPSec Key Mode	Manual
Local Address Type	Single
IP Address Start	0.0.0.0
End / Subnet Mask	0.0.0.0
Remote Address Type	Single
IP Address Start	0.0.0.0
End / Subnet Mask	0.0.0.0
My IP Address	0.0.0.0
Secure Gateway IP Address	0.0.0.0
SPI	0
Encapsulation Mode	Tunnel

Security Protocol

IPSec Protocol	ESP
Encapsulation Algorithm	DES
Encapsulation Key	
Authentication Algorithm	SHA1
Authentication Key	

The following table describes the labels in this screen.

Table 39 Rule Setup with Manual Key

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN policy.
IPSec Key Mode	Select **IKE** or **Manual** from the drop-down list box. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
Local Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** for a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.

Table 39 Rule Setup with Manual Key

LABEL	DESCRIPTION
IP Address Start	When the **Local Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your ZyXEL Device.
End/Subnet Mask	When the **Local Address Type** field is configured to **Single**, enter the IP address in the **IP Address Start** field again here. When the **Local Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind your ZyXEL Device.
Remote Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** with a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Remote Address Type** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.
End/ Subnet Mask	When the **Remote Address Type** field is configured to **Single**, enter the IP address in the **IP Address Start** field again here. When the **Remote Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
My IP Address	Enter the WAN IP address of your ZyXEL Device. The ZyXEL Device uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. The VPN tunnel has to be rebuilt if this IP address changes.
Secure Gateway IP Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
IPSec Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next). Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described later).

Table 39 Rule Setup with Manual Key

LABEL	DESCRIPTION
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. The ZyXEL Device's encryption algorithm should be identical to the secure remote gateway. When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Encryption Key (Only with ESP)	With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
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.
Delete	Click **Delete** to remove the current rule.

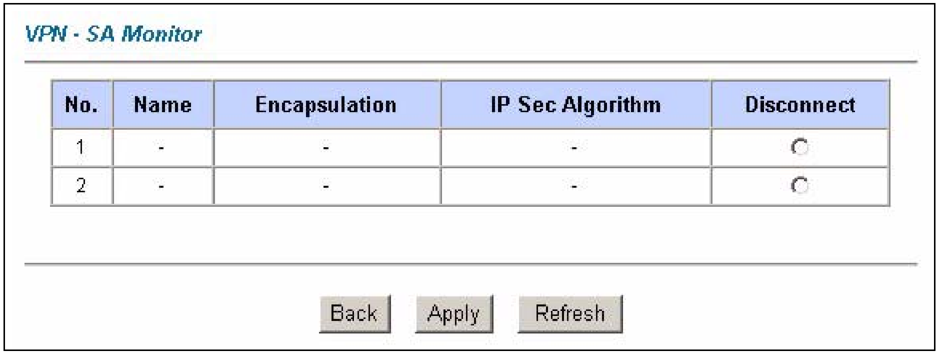
11.14 SA Monitor Screen

In the web configurator, click **VPN** and the **Monitor** link. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the labels in this tab.

Note: When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the Keep Alive section to have the ZyXEL Device renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 56 SA Monitor


VPN - SA Monitor

No.	Name	Encapsulation	IP Sec Algorithm	Disconnect
1	-	-	-	○
2	-	-	-	○

The following table describes the labels in this screen.

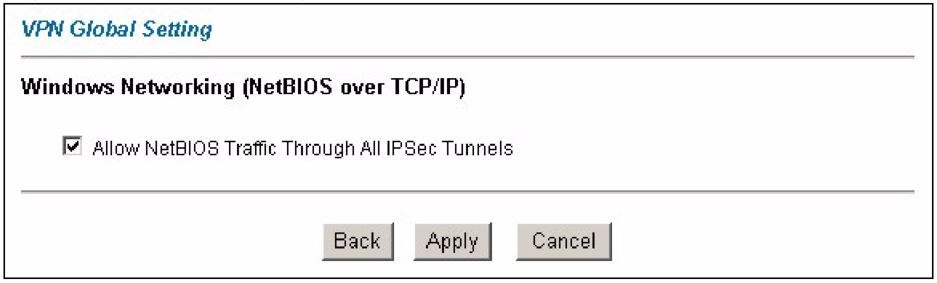
Table 40 SA Monitor

LABEL	DESCRIPTION
No.	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyXEL Device processing requirements and communications latency (delay).
Disconnect	Click the radio button next to a security association and then **Apply** to stop that security association.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Refresh	Click **Refresh** to display the current active VPN connection(s).

11.15 Global Setting Screen

To change your ZyXEL Device's global settings, click the **VPN**, then the **Global Setting** link. The screen appears as shown.

Figure 57 Global Setting


VPN Global Setting

Windows Networking (NetBIOS over TCP/IP)

☑ Allow NetBIOS Traffic Through All IPSec Tunnels

The following table describes the labels in this screen.

Table 41 Global Setting

LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow NetBIOS Traffic Through All IPSec Tunnels	Select this check box to send NetBIOS packets through the VPN connection.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to begin configuring this screen afresh.

11.16 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyXEL Device at headquarters from remote IPSec routers that use dynamic WAN IP addresses.

11.16.1 Telecommuters Sharing One VPN Rule Example

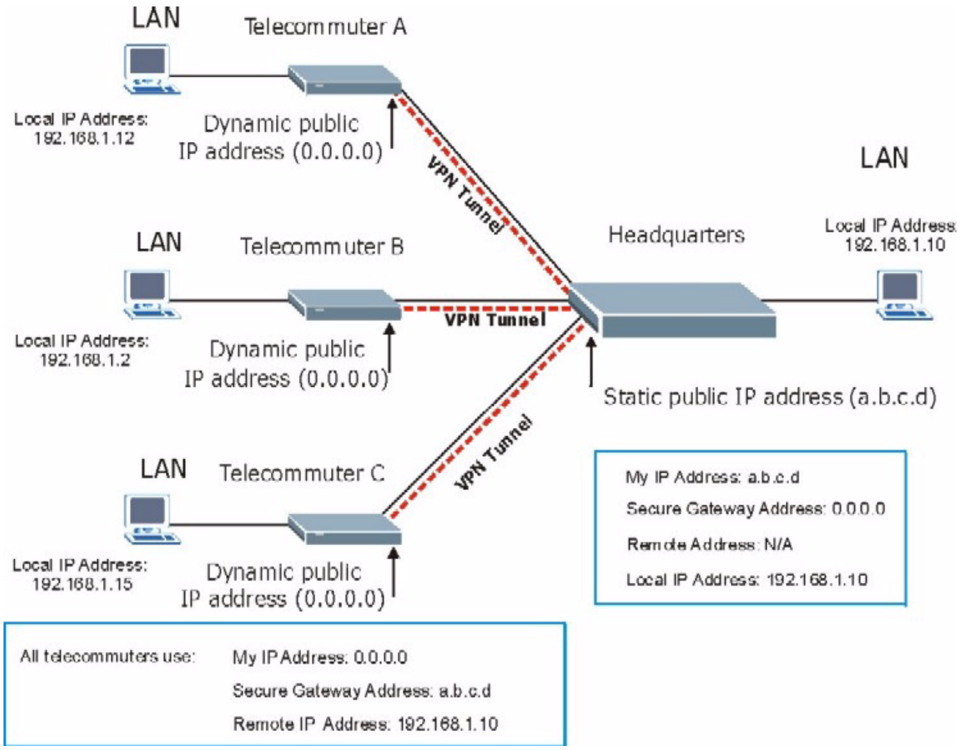
Multiple telecommuters can use one VPN rule to simultaneously access a ZyXEL Device at headquarters. They must all use the same IPSec parameters (including the pre-shared key) but the local IP addresses (or ranges of addresses) cannot overlap. See the following table and figure for an example.

Having everyone use the same pre-shared key may create a vulnerability. If the pre-shared key is compromised, all of the VPN connections using that VPN rule are at risk. A recommended alternative is to use a different VPN rule for each telecommuter and identify them by unique IDs (see Section 11.16.2 on page 137)..

Table 42 Telecommuter and Headquarters Configuration Example

	TELECOMMUTER	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address or domain name.	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.

Figure 58 Telecommuters Sharing One VPN Rule Example

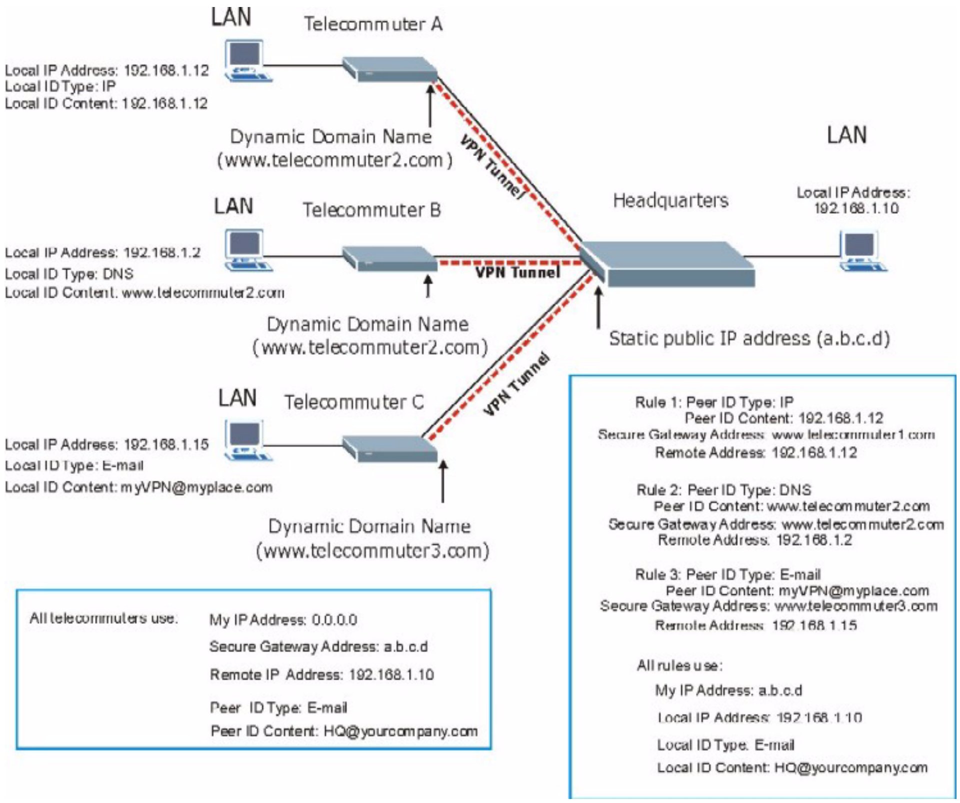

LAN
Telecommuter A
Local IP Address: 192.168.1.12
Dynamic public IP address (0.0.0.0)
VPN Tunnel
LAN
Telecommuter B
Local IP Address: 192.168.1.2
Dynamic public IP address (0.0.0.0)
VPN Tunnel
LAN
Telecommuter C
Local IP Address: 192.168.1.15
Dynamic public IP address (0.0.0.0)
VPN Tunnel
Headquarters
LAN
Local IP Address 192.168.1.10
Static public IP address (a.b.c.d)
My IP Address: a.b.c.d
Secure Gateway Address: 0.0.0.0
Remote Address: N/A
Local IP Address: 192.168.1.10
All telecommuters use:
My IP Address: 0.0.0.0
Secure Gateway Address: a.b.c.d
Remote IP Address: 192.168.1.10

11.16.2 Telecommuters Using Unique VPN Rules Example

With aggressive negotiation mode (see Section 11.10.1 on page 127), the ZyXEL Device can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyXEL Device at headquarters. They can use different IPSec parameters (including the pre-shared key) and the local IP addresses (or ranges of addresses) can overlap.

See the following graphic for an example where three telecommuters each use a different VPN rule to initiate a VPN connection to a ZyXEL Device located at headquarters. The ZyXEL Device at headquarters identifies each by its secure gateway address (a dynamic domain name) and uses the appropriate VPN rule to establish the VPN connection.

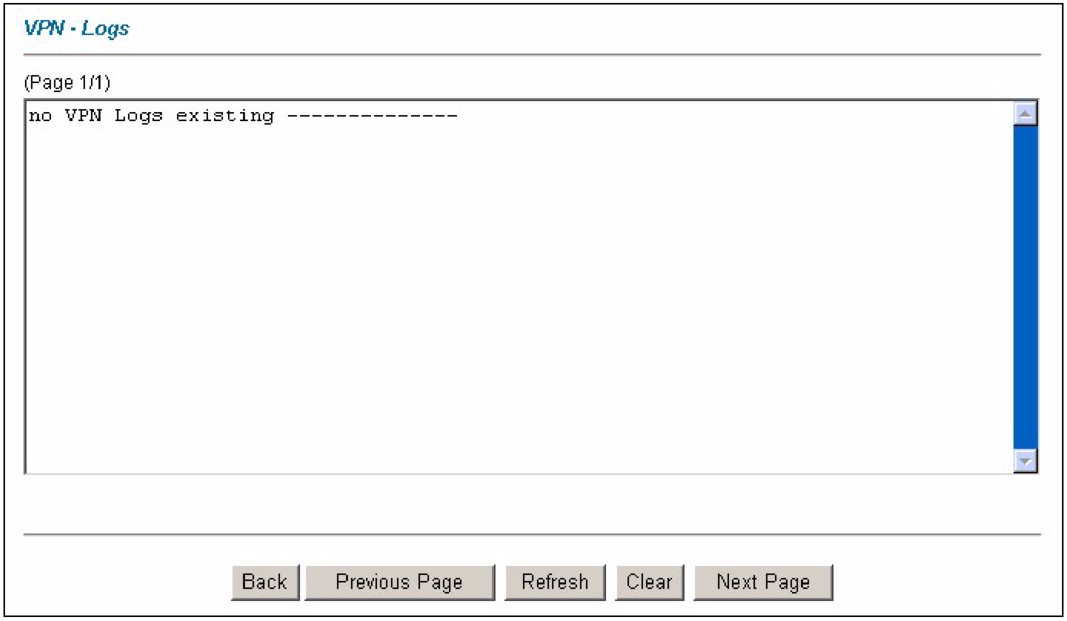
Figure 59 Telecommuters Using Unique VPN Rules Example


LAN
Telecommuter A
Local IP Address: 192.168.1.12
Local ID Type: IP
Local ID Content: 192.168.1.12
Dynamic Domain Name
(www.telecommuter2.com)
VPN Tunnel
LAN
Headquarters
Local IP Address:
192.168.1.10
LAN
Telecommuter B
Local IP Address: 192.168.1.2
Local ID Type: DNS
Local ID Content: www.telecommuter2.com
VPN Tunnel
Dynamic Domain Name
(www.telecommuter2.com)
Static public IP address (a.b.c.d)
VPN Tunnel
LAN
Telecommuter C
Local IP Address: 192.168.1.15
Local ID Type: E-mail
Local ID Content: myVPN@myplace.com
Dynamic Domain Name
(www.telecommuter3.com)
All telecommuters use:
My IP Address: 0.0.0.0
Secure Gateway Address: a.b.c.d
Remote IP Address: 192.168.1.10
Peer ID Type: E-mail
Peer ID Content: HQ@yourcompany.com
Rule 1: Peer ID Type: IP
Peer ID Content: 192.168.1.12
Secure Gateway Address: www.telecommuter1.com
Remote Address: 192.168.1.12
Rule 2: Peer ID Type: DNS
Peer ID Content: www.telecommuter2.com
Secure Gateway Address: www.telecommuter2.com
Remote Address: 192.168.1.2
Rule 3: Peer ID Type: E-mail
Peer ID Content: myVPN@myplace.com
Secure Gateway Address: www.telecommuter3.com
Remote Address: 192.168.1.15
All rules use:
My IP Address: a.b.c.d
Local IP Address: 192.168.1.10
Local ID Type: E-mail
Local ID Content: HQ@yourcompany.com

11.17 Logs

This screen displays the logs for all VPNs. The VPN log includes log index numbers, the date and time of the log records, and log messages. Refer to the Log appendix for descriptions and examples of VPN logs.

Figure 60 VPN Logs



```
no VPN Logs existing --------------
```

The following table describes the labels in this screen.

Table 43 VPN Logs

LABEL	DESCRIPTION
Log	This field lists a message that gives information about the reason for the log.
Back	Click this button to return to the previous screen.
Previous Page	Click this button to view the previous page.
Refresh	Click this button to update the current log archive.
Clear	Click this button to remove recorded information from this menu.
Next Page	Click this button to view more items in the summary (if you have a summary list that exceeds this page).

CHAPTER 12 NetCAPI

This chapter covers the NetCAPI screen.

12.1 NetCAPI Overview

Your ZyXEL Device supports NetCAPI. NetCAPI is ZyXEL's implementation of CAPI (Common ISDN Application Program Interface) capabilities over a network. It runs over DCP (Device Control Protocol) developed by RVS-COM.

NetCAPI can be used for applications such as Eurofile transfer, file transfer, G3/G4 Fax, Autoanswer host mode, telephony, etc. on Windows 95/98/NT platforms.

12.2 CAPI

CAPI is an interface standard that allows applications to access ISDN services. Several applications can share one or more ISDN lines. When an application wants to communicate with an ISDN terminal it sends a series of standard commands to the terminal. The CAPI standard defines the commands and allows you to use a well-defined mechanism for communications using ISDN lines.

CAPI also simplifies the development of ISDN applications through many default values that do not need to be programmed. It provides a unified interface for applications to access the different ISDN services such as data, voice, fax, telephony, etc.

12.2.1 ISDN-DCP

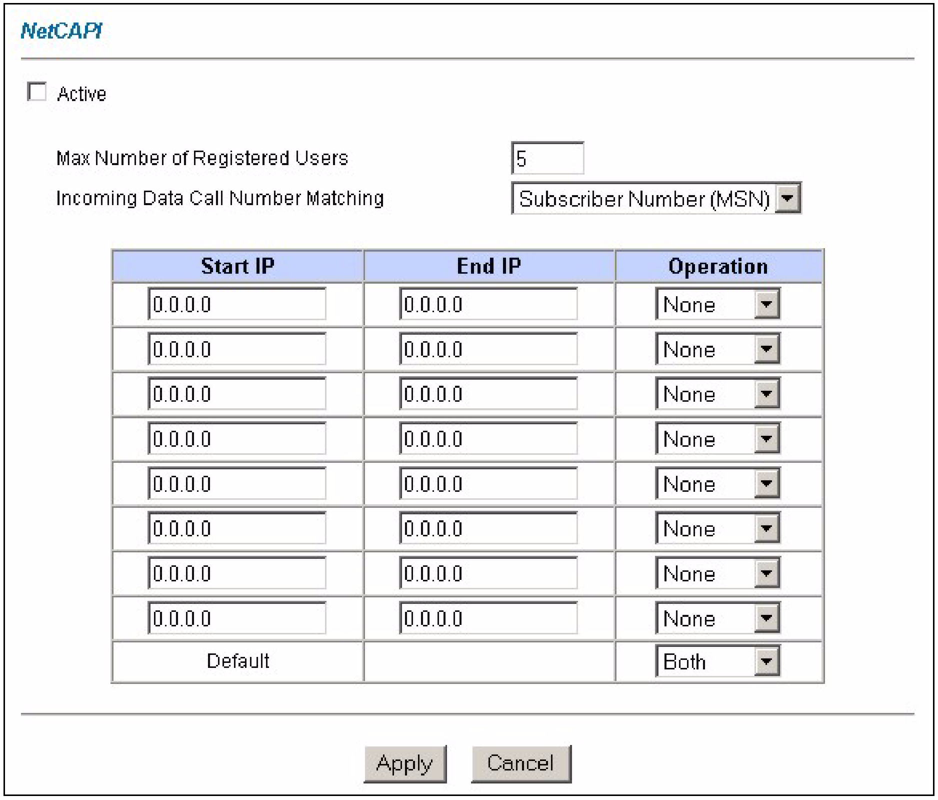
ISDN-DCP allows a computer on the LAN to use services such as transmitting and receiving faxes as well as placing and receiving phone calls.

Using ISDN-DCP, the ZyXEL Device acts as a DCP server. By default, the ZyXEL Device listens for DCP messages on TCP port number 2578 (the Internet-assigned number for RVS-COM DCP). When the ZyXEL Device receives a DCP message from a DCP client i.e., a computer, the ZyXEL Device processes the message and acts on it. Your ZyXEL Device supports all the DCP messages specified in the ISDN-DCP specification.

12.3 Configuring NetCAPI

To edit your ZyXEL Device's NetCAPI settings, click **Advanced > NetCAPI**. The screen appears as shown.

Figure 61 NetCAPI



NetCAPI

□ Active

Max Number of Registered Users	5
Incoming Data Call Number Matching	Subscriber Number (MSN)

Start IP	End IP	Operation
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
Default		Both

The following table describes the fields in this screen.

Table 44 NetCAPI

LABEL	DESCRIPTION
Active	Select this check box to enable NetCAPI.
Max Number of Registered Users	When you want to use NetCAPI to place outgoing calls or to listen to incoming calls, you must start RVSCOM on your computer, and RVSCOM registers itself to the ZyXEL Device. Enter the maximum number of clients (no more than 5) for which you want the ZyXEL Device to allow connections at the same time.
Incoming Data Call Number Matching	This field determines how incoming calls are routed. Select **NetCAPI** if you want to direct all incoming data calls to NetCAPI. Select **Subscriber Number (MSN)** if you want to direct all incoming call to the ZyXEL Device only when the incoming phone number matches the ISDN DATA number. If the incoming phone number does not match the ISDN DATA number, then the call will be routed to NetCAPI. Select **Called Party Subaddress** if you want to direct all incoming calls to the ZyXEL Device only when the incoming call matches the subaddress of ISDN DATA. If the incoming call does not match the subaddress of ISDN DATA, then the call will be routed to NetCAPI.
Start IP	Enter the first IP address of a group of NetCAPI clients. Each group contains contiguous IP addresses.

Table 44 NetCAPI

LABEL	DESCRIPTION
End IP	Enter the last IP address in a NetCAPI client group.
Operation	Select **Incoming** if you wish to grant incoming calls permission. Select **Outgoing** if you wish to grant outgoing calls permission. Select **Both** if you wish to grant both incoming calls and outgoing calls permissions. Select **None** if you wish to deny all calls.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

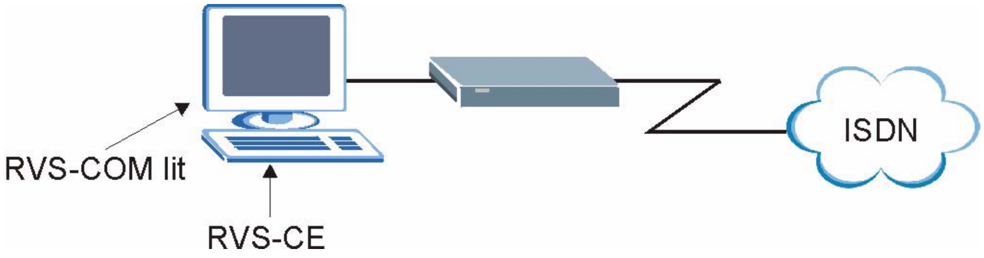
12.3.1 Configuring the ZyXEL Device as a NetCAPI Server

This section describes how to configure your ZyXEL Device to be a NetCAPI server.

By default, NetCAPI is enabled on your ZyXEL Device. When NetCAPI is enabled, the ZyXEL Device listens for incoming DCP messages from the computers. By default, the ZyXEL Device listens for DCP messages on TCP port 2578.

The following figure illustrates the configuration used in this example.

Figure 62 Configuration Example



Before entering any configurations, you must install the CAPI driver (RVS-CE) and communication program such as RVS-COM Lite on your computer.

12.3.2 RVS-COM

RVS-COM includes an ISDN CAPI driver with its communication program. RVS-CE (Core Engine) is an ISDN-CAPI 2.0 driver for Windows 95/98/NT that can be used by different ISDN communication programs (such as AVM Fritz or RVS-COM) to access the ISDN on the ZyXEL Device.

NetCAPI can carry out CAPI applications only if the CAPI driver is installed on your computer. In addition to the CAPI driver, you will need a communication software program such as RVS-COM Lite, Fritz etc., for users to access CAPI.

The ISDN router is a shared device and can be used by several different client workstations at the same time: e.g. one computer sending a fax, another computer doing a file transfer. RVS-COM has to be installed on each client workstation in order to share the ISDN lines.

12.3.3 Example of Installing a CAPI driver and Communication Software

Please uninstall previous versions of "RVS-CAPI" and "RVS-COM lite" before you install the new versions. In Windows, use the **Add/Remove Programs** window (click **Start**, **Settings**, **Control Panel** and **Add/Remove Programs**) to uninstall RVS-CAPI and RVS-COM.

To install the CAPI driver and the communication software, enter one of the license keys of your RVS-COM Lite CD-ROM and follow the instructions on the configuration wizard. When you install RVS-Lite, RVS-COM AUTOMATICALLY installs CAPI driver before installing RVS-Lite.

If you did not install RVS-Lite and want to use other programs such as AVM Fritz to access the ISDN router, you must first install the CAPI driver - RVS-CE using the English version installation wizard (in \DISKs\CEPE\DISK1\) and start the SETUP.EXE.

CHAPTER 13 Supplementary Phone Services

This chapter discusses the European ISDN supplemental services.

13.1 Overview

The ZyXEL Device supports a comprehensive set of advanced calling features known as Supplemental Services. European ISDN Supplemental Services may vary and have different naming conventions that can be generalized as follows. Please check with your telephone company for the services they offer.

Table 45 Supplemental Services In Europe

Call Waiting Call Hold Call Retrieve
Three Party Conference
Call Forwarding Call Forwarding Busy (CFB) Call Forwarding Unconditional (CFU) Call Forwarding No Reply (CFNR)
Multiple Subscriber Number (MSN) / Subaddress
Terminal Portability: Suspend Resume

These features vary slightly between different Central Office switch types. You need to check with your telephone company to confirm if these services are available to you and if so, are there any additional charges for them.

In some cases, your telephone company may only enable these features on your first directory (phone) number. In this case, you may want to request that the features be enabled on your second directory number as well.

13.2 Setting Up Supplemental Phone Service

All Supplemental Phone Services are enabled by default except for Call Waiting, which is disabled by default but can be enabled in SMT **Menu 2.1 - ISDN Advanced Setup**. The **Calling Line Indication**, or Caller ID, also in this menu decides whether the other party can see your number when you call. If set to **Enable** (default), the ZyXEL Device sends the caller ID and the party you call can see your number, otherwise if set to Disable, the caller ID is blocked.

13.3 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the ZyXEL Device.

13.4 Call Waiting

ISDN Call Waiting allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

By default call waiting is enabled on both telephone ports (except France where the default is disabled), but can be toggled on either port from **Menu 2.1**.

13.4.1 How to Use Call Waiting

The Call Waiting feature on your ISDN line works in exactly the same way as it does on a regular analog line (which almost everyone is familiar with).

13.4.1.1 Placing the Current Call on Hold

To place the current call on hold and answer the incoming call, press the flash key after hearing a call waiting indicator tone.

13.4.1.2 Dropping the Current Call to Switch to an Incoming/Holding Call

After hearing a Call Waiting indicator tone, simply hang up the telephone and wait for it to ring before answering the incoming/holding call.

An incoming caller receives a busy signal if

- You have two calls active (one active and one on hold, or both active using Three-Way Calling) already.

- You are dialing a number on the B-channel the incoming caller is attempting to reach, but have not yet established a connection.

13.5 Three Way Calling

Three Way Calling allows you to add a third party to an existing call. This service must be subscribed from your telephone company.

13.5.1 How to Use Three-Way Calling

If you wish to call someone and conference him/her in with an existing call:

- Press the flash key to put the existing call on hold and receive a dial tone.
- Dial the third party's telephone number.
- When you are ready to conference the calls together, press the flash key again to establish a three-way conference call.

Note: If you wish to cancel your attempt to establish the conference call because the third party's line is busy or if they do not answer, simply hang-up the telephone and pick it back up after it starts ringing to return to the first caller.

13.5.1.1 To drop the last call added to the three-way call:

Simply press the flash key. The last call that was added to the conference is dropped.

13.5.1.2 To drop yourself from the conference call:

If you hang up your telephone during a three-way call and the two other callers remain on the line, the ISDN network will do an implicit transfer to directly connect the two remaining callers together.

13.6 Call Transfer

Call Transfer allows you to transfer an active call to a third party. This service must be subscribed from your telephone company.

13.6.1 How to Use Call Transfer

Transferring an active call to a third party:

1. Once you have an active call (Caller A), press the flash key to put Caller A on hold and receive a dial tone.
2. Dial the third party's telephone number (Caller B).

3 When you are ready to conference the two calls together, press the flash key to establish a three-way-conference call.

4 Hang up the telephone. The ISDN network does an implicit transfer to directly connect Caller A with Caller B.

13.6.2 To Do a Blind Transfer:

1 Once you have an active call (Caller A), press the flash key to put the existing call on hold and receive a dial tone.

2 Dial the third party's telephone number (Caller B).

3 Before Caller B picks up the call, you can transfer the call by pressing the flash key. The call is automatically transferred.

13.7 Call Forwarding

Call forwarding means the switch will ring another number at a place where you will be when someone dials your directory number.

There are two methods of activating call forwarding. The first is exactly the same as on an analog line, i.e., you pick up the handset and dial the access code assigned by your telephone company and the number that you want the calls forwarded. Check with your telephone company for this access code.

The second is with the "phone flash" commands where you pick up the handset and press the flash key before dialing the following:

Table 46 Phone Flash Commands

COMMAND	DESCRIPTION
*20*forward-number#	Activate CFB (Call Forwarding Busy)
*21*forward-number#	Activate CFU (Call Forwarding Unconditional)
*22*forward-number#	Activate CFNR (Call Forwarding No Reply)
#20#	Deactivate CFB
#21#	Deactivate CFU
#22#	Deactivate CFNR

Either method should work fine, and you can use whichever one you are most comfortable with.

13.8 Reminder Ring

The ZyXEL Device sends a single short ring to your telephone every time a call has been forwarded (US switches only).

13.9 Multiple Subscriber Number (MSN)

In Europe you can subscribe (for a fee) more than one number for your ISDN line from your telephone company. You can then assign each number to a different port, e.g., the first number to data calls, the second to A/B adapter 1 and so on. On the other hand, the telephone company may give you only one number, but allow you to assign your own sub-addresses to different ports, e.g., sub-address 1 to data calls and 2 to A/B adapter 1.

If you choose **Multiple Subscriber Number (MSN)** to determine routing for all incoming calls, the ZyXEL Device will compare the incoming call's **Called Party Number** or **Subaddress** to the number you set and route the incoming call to the destination that matches the number set. This feature is useful for those who connect a fax machine to one analog port while connecting a telephone set to the other analog port.

13.10 Using MSN

Go to **Wizard Setup**, **Advanced Setup > NetCAPI** or SMT **Menu 2 - ISDN Setup**. Select **Multiple Subscriber Number (MSN)** or **Called Party Subaddress** in the **Incoming Data Call Number Matching** or **Incoming Phone Number Matching** field. Assign MSN/ Subaddress numbers to the data/POTS ports. Then the data port or POTS port will answer incoming calls if and only if the called numbers match the MSN/Subaddress numbers assigned.

13.11 Terminal Portability (Suspend/Resume)

The Terminal Portability service allows you to suspend a phone call temporarily. You can then resume this call later, at another location if you so wish.

13.11.1 How to Suspend/Resume a Phone Call:

13.11.1.1 To suspend an active phone call

1 Press the flash key twice.

2 Dial *3n*#, where n is any number from 1 to 9.

13.11.1.2 To resume your phone call

1 Reconnect at a(n) (ISDN) telephone that is linked to the same S/T interface (Network Terminator-1, NT1) where you suspended the call.

2 ick up the handset and press the flash key.

3 Dial #3n#, where n is any number from 1 to 9, but should be identical to that used above.

CHAPTER 14
Maintenance

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

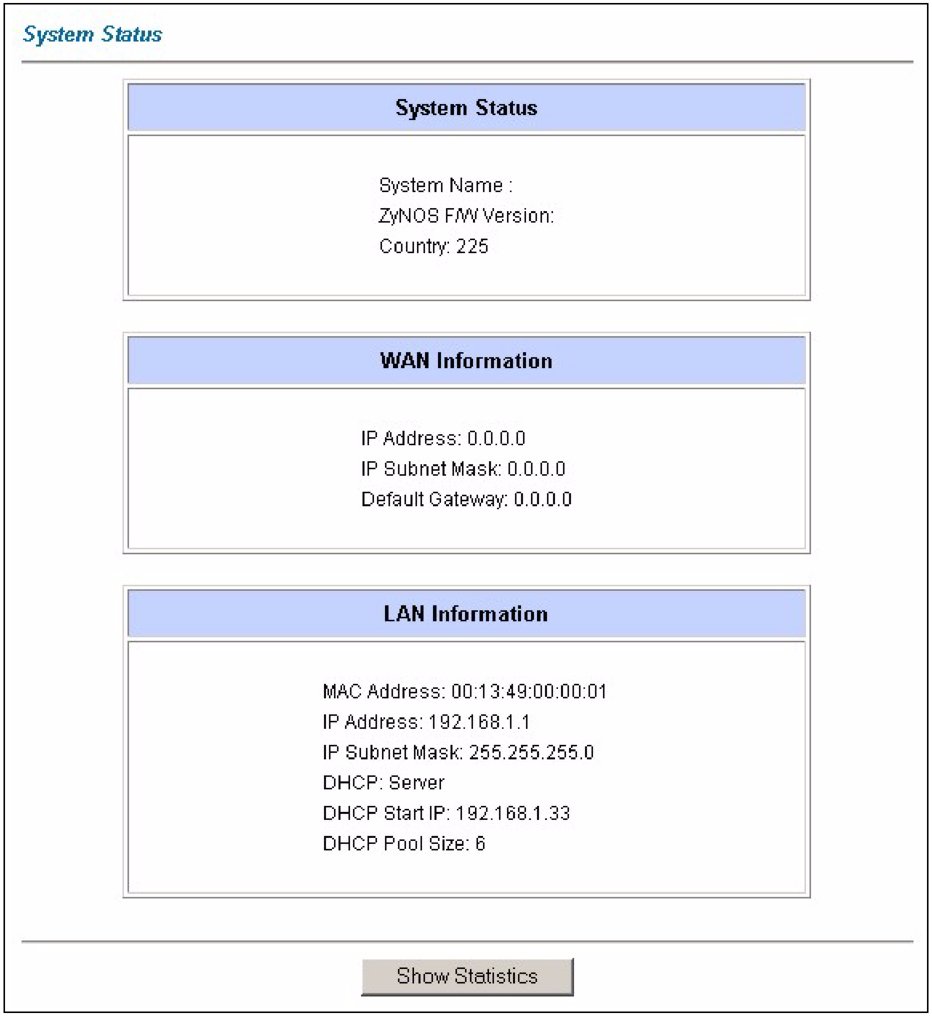
14.1 Maintenance Overview

The maintenance screens can help you view system information and DHCP client information, upload new firmware and configure budget management.

14.2 System Status

Click **System Status** to open the following screen, where you can use to monitor your ZyXEL Device. Note that these fields are READ-ONLY and only for diagnostic purposes.

Figure 63 System Status



System Status

System Status

System Name :
ZyNOS F/W Version:
Country: 225

WAN Information

IP Address: 0.0.0.0
IP Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0

LAN Information

MAC Address: 00:13:49:00:00:01
IP Address: 192.168.1.1
IP Subnet Mask: 255.255.255.0
DHCP: Server
DHCP Start IP: 192.168.1.33
DHCP Pool Size: 6

The following table describes the labels in this screen.

Table 47 System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your ZyXEL Device. It is for identification purposes.
ZyNOS Firmware Version	This is the ZyNOS firmware version and the date the firmware was created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Country	This is the country code value (in decimal notation).
WAN Information	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
LAN Information	

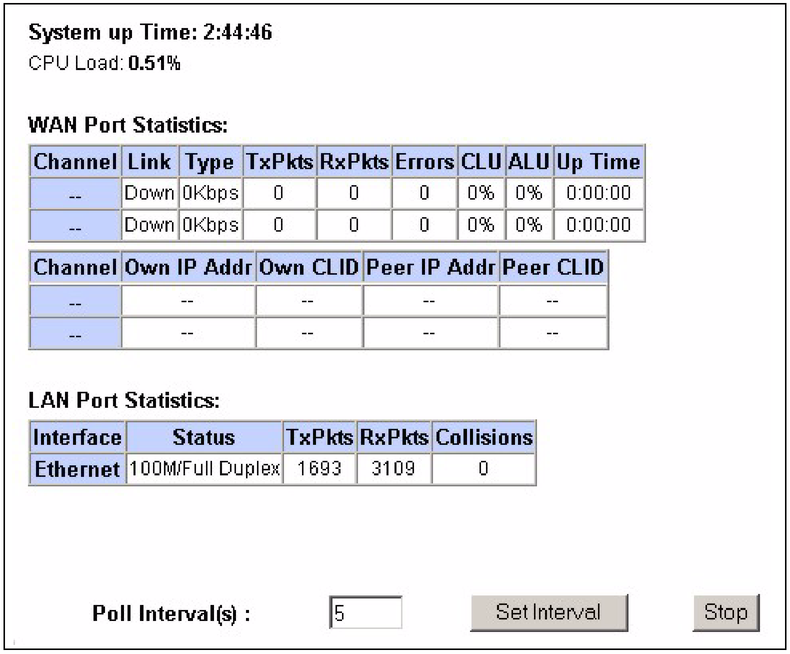
Table 47 System Status

LABEL	DESCRIPTION
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the LAN port DHCP role - **Server**, **Relay** or **None**.
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
Show Statistics	Click **Show Statistics** to see the performance statistics such as number of packets sent and number of packets received for each port.

14.2.1 System Statistics

Click **Show Statistics** in the **System Status** screen to open the following screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 64 System Status > Show Statistics



System up Time: 2:44:46

CPU Load: **0.51%**

WAN Port Statistics:

Channel	Link	Type	TxPkts	RxPkts	Errors	CLU	ALU	Up Time
--	Down	0Kbps	0	0	0	0%	0%	0:00:00
--	Down	0Kbps	0	0	0	0%	0%	0:00:00

Channel	Own IP Addr	Own CLID	Peer IP Addr	Peer CLID
--	--	--	--	--
--	--	--	--	--

LAN Port Statistics:

Interface	Status	TxPkts	RxPkts	Collisions
Ethernet	100M/Full Duplex	1693	3109	0

Poll Interval(s) : 5

The following table describes the fields in this screen.

Table 48 System Status > Show Statistics

LABEL	DESCRIPTION
System up Time	This is the elapsed time the system has been up.
CPU Load	This specifies the percentage of CPU utilization.

Table 48 System Status > Show Statistics (continued)

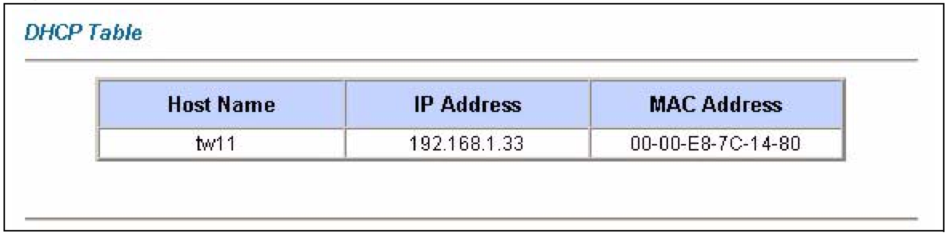
LABEL	DESCRIPTION
WAN Port Statistics	
Channel	This shows statistics for **B1** and **B2** channels respectively. This is the information displayed for each channel.
Link	This shows the name of the remote node or the user the channel is currently connected to or the status of the channel (e.g., Down, Idle, Calling, Answering, NetCAPI, etc.).
Type	This is the current connecting speed.
TxPkts	This is the number of transmitted packets on this channel.
RxPkts	This is the number of received packets on this channel.
Errors	This displays the number of error packets on this channel.
CLU	The CLU (Current Line Utilization) is the percentage of current bandwidth used on this channel.
ALU	The ALU (Average Line Utilization) is a 5-second moving average of usage for this channel.
Up Time	Time this channel has been connected to the current remote node.
Channel	This shows statistics for **B1** and **B2** channels respectively. This is the information displayed for each channel.
Own IP Addr	This refers to the IP address of the ZyXEL Device.
Own CLID	This shows your Caller ID.
Peer IP Addr	This refers to the IP address of the peer.
Peer CLID	This refers to the Caller ID of the peer.
LAN Port Statistics	
Interface	This shows the type of LAN interface connection.
Status	This displays the port speed and duplex setting.
TxPkts	This is the number of transmitted packets to the LAN.
RxPkts	This is the number of received packets from the LAN.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

14.3 DHCP Table Screen

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 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.

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 Host Name, IP Address, and MAC Address) of all network clients using the DHCP server.

Figure 65 DHCP Table



DHCP Table

Host Name	IP Address	MAC Address
tw11	192.168.1.33	00-00-E8-7C-14-80

The following table describes the fields in this screen.

Table 49 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.

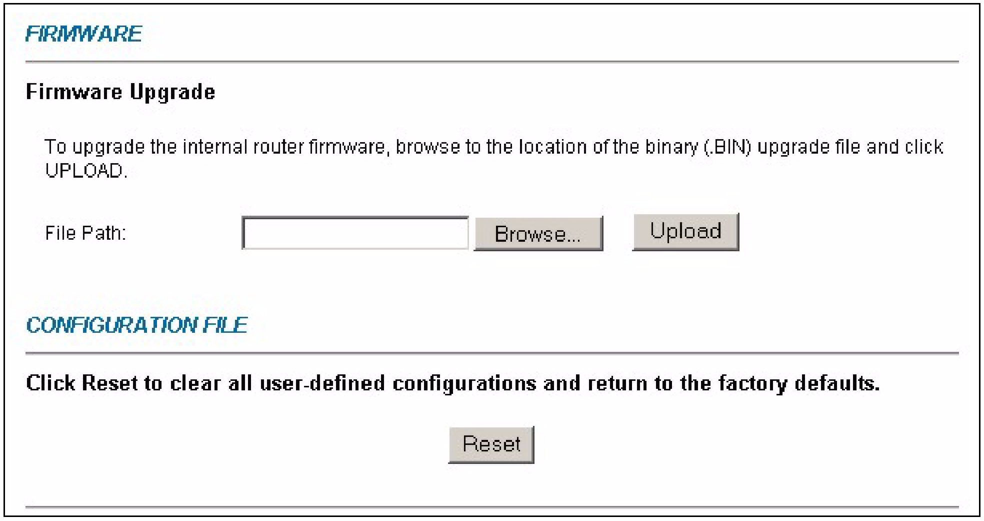
14.4 Firmware Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a.bin extension, for example, "ZyXEL Device.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

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

Click **Firmware** to open the following screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 66 Firmware Upgrade



FIRMWARE

Firmware Upgrade

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click UPLOAD.

File Path:

CONFIGURATION FILE

Click Reset to clear all user-defined configurations and return to the factory defaults.

The following table describes the labels in this screen.

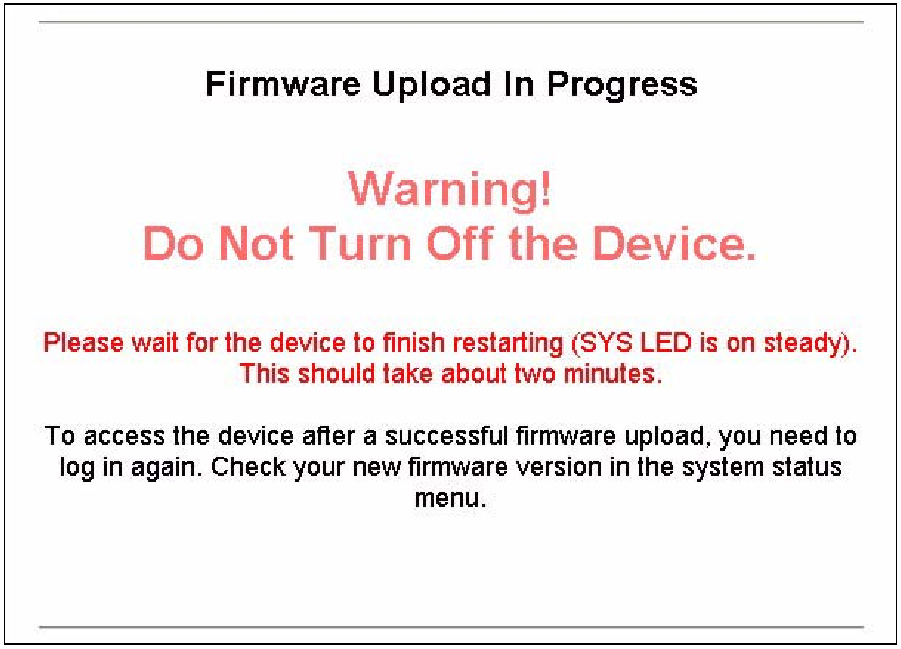
Table 50 Firmware Upgrade

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Reset	Click this button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL device. Refer to the chapter about introducing the web configurator for more information on the **RESET** button.

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

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

Figure 67 Firmware Upload In Progress



Firmware Upload In Progress

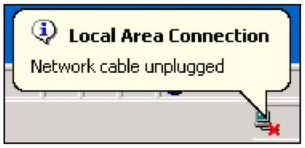
Warning!
Do Not Turn Off the Device.

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

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

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

Figure 68 Network Temporarily Disconnected

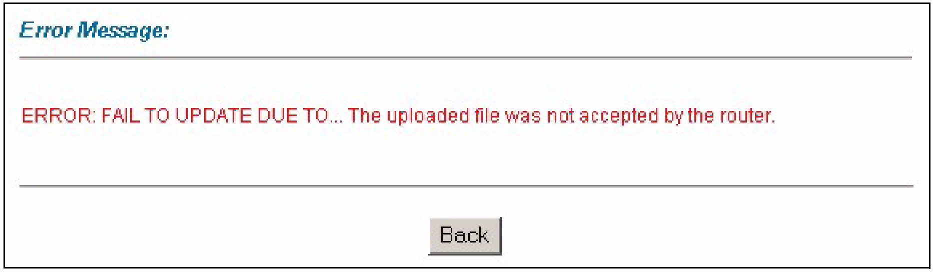


Local Area Connection
Network cable unplugged

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

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

Figure 69 Error Message



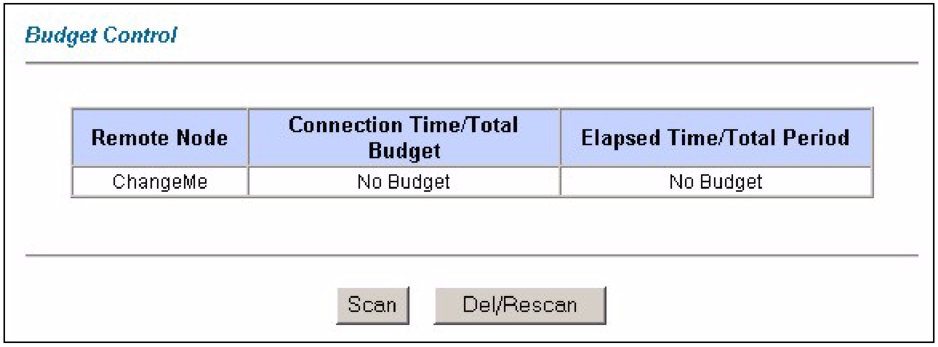
Error Message:

ERROR: FAIL TO UPDATE DUE TO... The uploaded file was not accepted by the router.

14.5 Budget Control

Budget management allows you to set a limit on the total outgoing call time of the ZyXEL Device over a period of time. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Figure 70 Budget Control



Budget Control

Remote Node	Connection Time/Total Budget	Elapsed Time/Total Period
ChangeMe	No Budget	No Budget

The following table describes the labels in this screen.

Table 51 Budget Control

LABEL	DESCRIPTION
Remote Node	This is the name of the remote node.
Connection Time/ Total Budget	This is the total connection time that has gone by. For example, 5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/ Total Period	The period is the time cycle in hours that the allocation budget is reset. The elapsed time is the time used up within this period. For example, 0.5/1 means that 30 minutes out of the 1-hour time period has elapsed.
Scan	Click this to scan the remote nodes and update status.
Del/Rescan	Click this to begin the scan afresh.

CHAPTER 15 Introducing the SMT

This chapter explains how to access and navigate the System Management Terminal and gives an overview of its menus.

15.1 SMT Introduction

The ZyXEL Device’s SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

15.2 Accessing the ZyXEL Device via Console Port

Follow the steps below to access your ZyXEL Device via the console port.

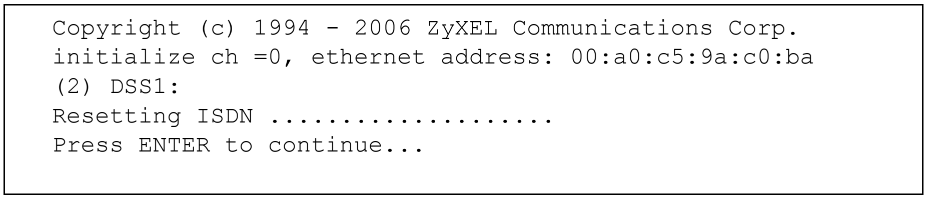
Configure a terminal emulation communications program as follows: VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, data flow set to none, 9600 bps port speed.

15.2.1 Initial Screen

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

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

Figure 71 Initial Screen



```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:9a:c0:ba
(2) DSS1:
Resetting ISDN ....................
Press ENTER to continue...
```

15.2.2 Entering Password

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

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

Please note that if there is no activity for longer than five minutes after you log in, your ZyXEL Device will automatically log you out and displays a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

Figure 72 Login Screen

```
              Enter Password : ****
```

15.3 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your ZyXEL Device.

1. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**.
2. Enter "1234" in the **Password** field.
3. After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your ZyXEL Device will automatically log you out. You will then have to telnet into the ZyXEL Device again.

15.4 SMT Menu Overview

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

Table 52 SMT Menus Overview

MENUS	SUB MENUS		
1 General Setup	1.1 Configure Dynamic DNS		
2 ISDN Setup	2.1 ISDN Advanced Setup		
	2.2 NetCAPI Setup		
3 Ethernet Setup	3.1 General Ethernet Setup		
	3.2 TCP/IP and DHCP Setup	3.2.1 IP Alias Setup	
4 Internet Access Setup			
11 Remote Node Setup	11.1 Remote Node Profile		
	11.2 Remote Node PPP Options		
	11.3 Remote Node Network Layer Options		
	11.5 Remote Node Filter		

Table 52 SMT Menus Overview (continued)

MENUS	SUB MENUS		
12 Static Routing Setup	12.1 Edit IP Static Route		
13 Default Dial-in Setup	13.1 Default Dial-in Filter		
14 Dial-in User Setup	14.1 Edit Dial-in User		
15 NAT Setup	15.1 Address Mapping Sets	15.1.x Address Mapping Rules	15.1.x.x Address Mapping Rule
	15.2 NAT Server Sets		
21 Filter and Firewall Rule Setup	21.1 Filter Setup	21.1.x Filter Rules Summary	21.1.x.1 Generic Filter Rule
			21.1.x.1 TCP/IP Filter Rule
	21.1 Firewall Setup		
	21.3 View Firewall Log		
22 SNMP Configuration			
23 System Security	23.1 Change Password		
	23.2 External Server		
24 System Maintenance	24.1 System Status		
	24.2 System Information and Console Port Speed	24.2.1 System Information	
		24.2.2 Console Port Speed	
	24.3 Log and Trace	24.3.1 View Error Log	
		24.3.2 UNIX Syslog and Accounting	
		24.3.3 Accounting Server	
		24.3.4 Call-Triggering Packet	
	24.4 Diagnostic		
	24.5 Backup Configuration		
	24.6 Restore Configuration		
	24.7 Upload Firmware	24.7.1 Upload Router Firmware	
		24.7.2 Upload Router Configuration File	
	24.8 Command Interpreter Mode		
	24.9 Call Control	24.9.1 Call Control Parameters	
		24.9.2 Blacklist	
		24.9.3 Budget Management	
		24.9.4 Call History	
	24.10 Time and Date Setting		
	24.11 Remote Management		
26 Schedule Setup	26.1 Schedule Set Setup		

Table 52 SMT Menus Overview (continued)

MENUS	SUB MENUS		
27 VPN/IPSec Setup	27.1 IPSec Summary	27.1.1 IPSec Setup	27.1.1.1 IKE Setup
			27.1.1.2 Manual Setup
	27.2 SA Monitor		
	27.3 View IPSec Log		

15.5 Navigating the SMT Interface

The SMT(System Management Terminal) is the interface that you use to configure your ZyXEL Device.

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

Table 53 Main Menu Commands

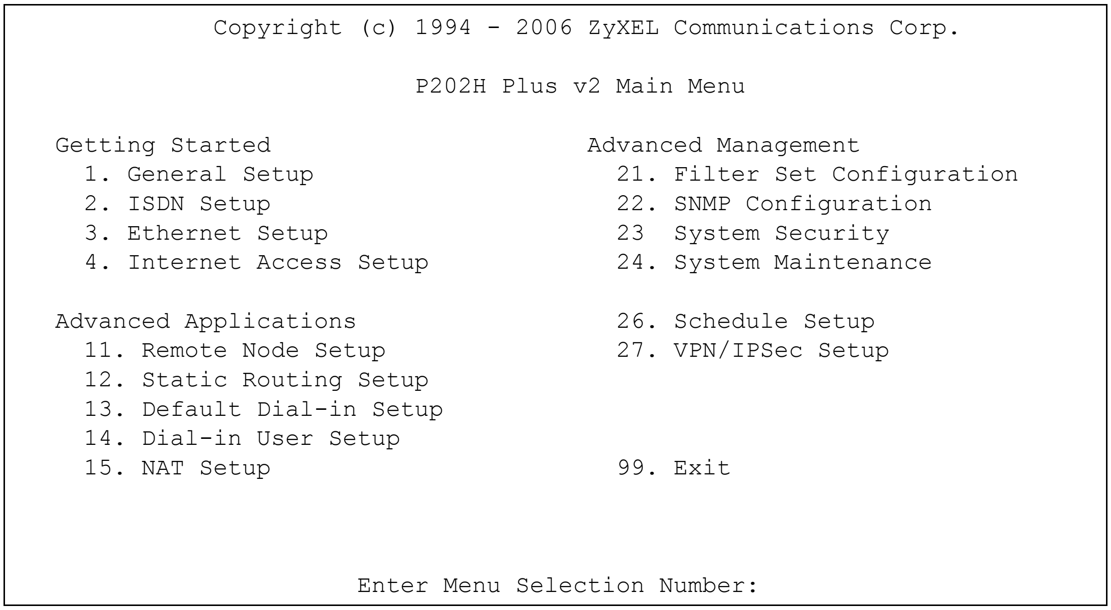
OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change **No** to **Yes**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

Table 53 Main Menu Commands

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

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

Figure 73 SMT Main Menu



```
              Copyright (c) 1994 - 2006 ZyXEL Communications Corp.

                            P202H Plus v2 Main Menu

   Getting Started                      Advanced Management
     1. General Setup                     21. Filter Set Configuration
     2. ISDN Setup                        22. SNMP Configuration
     3. Ethernet Setup                    23  System Security
     4. Internet Access Setup             24. System Maintenance

   Advanced Applications                  26. Schedule Setup
     11. Remote Node Setup                27. VPN/IPSec Setup
     12. Static Routing Setup
     13. Default Dial-in Setup
     14. Dial-in User Setup
     15. NAT Setup                        99. Exit



                        Enter Menu Selection Number:
```

15.5.1 System Management Terminal Interface Summary

The following table describes the fields in the previous screen.

Table 54 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	ISDN Setup	Use this menu to set up the ISDN.
3	Ethernet Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.

Table 54 Main Menu Summary

#	MENU TITLE	DESCRIPTION
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Use this menu to set up static routes.
13	Default Dial-in Setup	Use this menu to set up default dial-in parameters so that your ZyXEL Device can be used as a dial-in server.
14	Dial-in User Setup	Use this menu to configure settings for remote dial-in users.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Use this menu to configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to change your password and set up an authentication server.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN/ IPSec Setup	Use this menu to configure VPN connections.
99	Exit	Use this to exit from SMT (necessary for remote configuration).

15.6 Changing the System Password

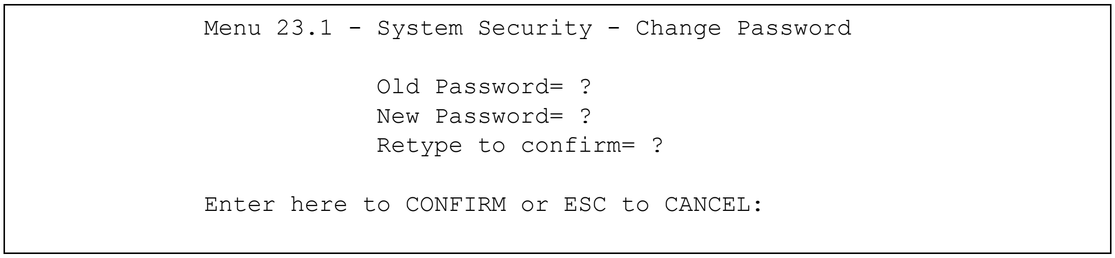
Change the system password by following the steps shown next.

1 Enter 23 in the main menu to open **Menu 23 - System Security**.

2 Enter 1 in menu 23 to display **Menu 23.1 - System Security - Change Password**.

3 Type your existing system password in the **Old Password** field, for example “1234”, and press [ENTER]

Figure 74 Menu 23 System Password



```
              Menu 23.1 - System Security - Change Password

                          Old Password= ?
                          New Password= ?
                          Retype to confirm= ?

              Enter here to CONFIRM or ESC to CANCEL:
```

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

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

Note: When you type in a password, the screen displays an "*" for each character you type.

CHAPTER 16 Menu 1 General Setup

Menu 1 - General Setup contains administrative and system-related information.

16.1 General Setup

Menu 1 - General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

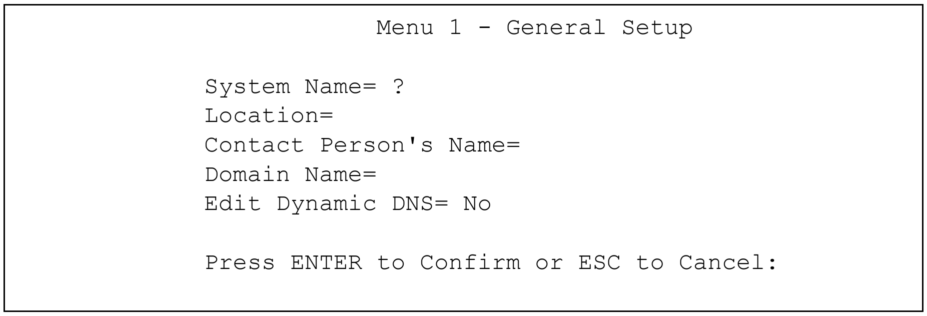
- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the ZyXEL Device **System Name**.
- In Windows 2000 click **Start**, **Settings**, **Control Panel** and then double-click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

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

16.2 Procedure To Configure Menu 1

1 Enter 1 in the main menu to open **Menu 1 - General Setup** (shown next)

Figure 75 Menu 1 General Setup.



```
                     Menu 1 - General Setup

        System Name= ?
        Location=
        Contact Person's Name=
        Domain Name=
        Edit Dynamic DNS= No

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

2 Fill in the required fields. Refer to the table shown next for more information about these fields.

Table 55 Menu 1 General Setup

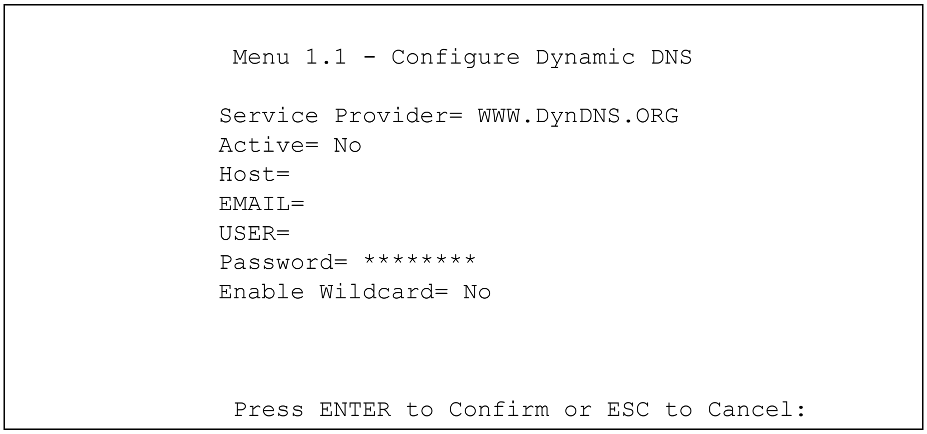
FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Location	Enter the geographic location (up to 31 characters) of your ZyXEL Device.
Contact Person's Name	Enter the name (up to 30 characters) of the person in charge of this ZyXEL Device.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your router. The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

16.2.1 Procedure to Configure Dynamic DNS

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

To configure Dynamic DNS, go to **Menu 1 - General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS** as shown next.

Figure 76 Menu 1.1 Configure Dynamic DNS



```
                 Menu 1.1 - Configure Dynamic DNS

                Service Provider= WWW.DynDNS.ORG
                Active= No
                Host=
                EMAIL=
                USER=
                Password= ********
                Enable Wildcard= No



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

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 56 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.
Host	Enter the domain name assigned to your ZyXEL Device by your Dynamic DNS provider.
EMAIL	Enter your e-mail address.
Username	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Your ZyXEL Device supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. This field is **N/A** when you choose DDNS client as your service provider.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

Note: The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

CHAPTER 17 Menu 2 ISDN Setup

This chapter tells you how to configure the ISDN Setup menus for your Internet connection.

17.1 ISDN Setup Overview

Menu 2 - ISDN Setup allows you to enter the information about your ISDN line. Different telephone companies deploy different types of switches for ISDN service. Depending on the switch for your particular installation, you will have a different number of telephone numbers You need to pass the ISDN setup before your system can make an outgoing call or answer an incoming call.

17.1.1 Supplementary Voice Services

To take full advantage of the Supplementary Voice Services available though the ZyXEL Device's phone ports, you will need to subscribe to the service from your telephone company. The Supplementary Voice Services available on the ZyXEL Device series include:

- Call Waiting
- Three Way Calling (conference)
- Call Transfer
- Call Forwarding.

The Advanced Phone Services chapter in this manual describes these services in more detail. There may be an additional charge for each of these services, so just choose the services you need. The phone company representative will ask you for the Feature Keys (buttons) for any Voice Features that you have chosen to activate.

17.1.2 ISDN Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number. By default call waiting is enabled on both telephone ports (except for France), but can be disabled on either port from **Menu 2.1**.

17.1.3 PABX Outside Line Prefix

A PABX (Private Automatic Branch eXchange) generally requires you to dial a number (a single digit in most cases) when you need an outside line. If your ZyXEL Device is connected to a PABX, enter this number in **PABX Outside Line Prefix**, otherwise, leave it blank.

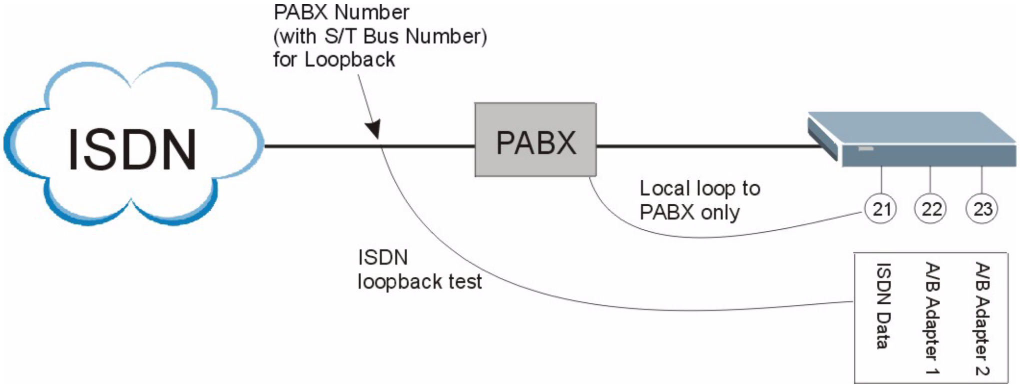
Please note that the PABX prefix is for calls initiated by the ZyXEL Device only. If you place a call from a device on either A/B adapter, you must dial the prefix by hand.

17.1.4 Outgoing Calling Party Number

If these fields are not blank, the ZyXEL Device will use these values as the calling party number for "ISDN Data", "A/B Adapter 1" and "A/B Adapter 2" outgoing calls. Otherwise, the individual entries for "ISDN Data", "A/B Adapter 1" and "A/B Adapter 2" will be used as the calling party number. You only need to fill in these fields if your switch or PABX requires a specific calling party number for outgoing calls, otherwise, leave them blank.

The following diagram illustrates the **PABX Number (with S/T Bus Number) for Loopback** and **Outgoing Calling Party Number** fields for a ZyXEL Device behind an ISDN PABX.

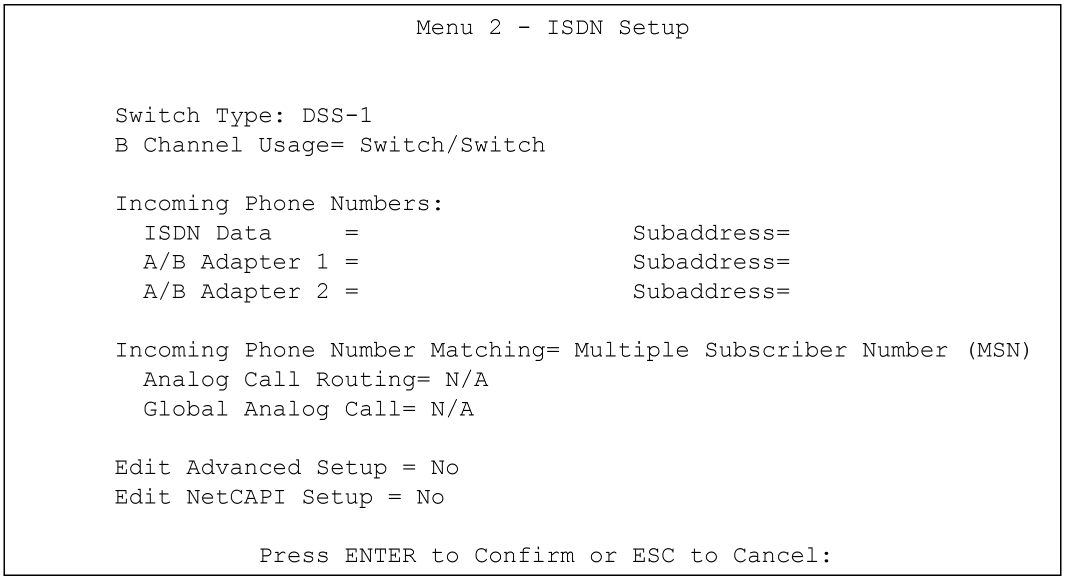
Figure 77 ZyXEL Device Behind a PABX



17.2 ISDN Setup

From the main menu, enter 2 to open menu 2.

Figure 78 Menu 2 ISDN Setup



```
                             Menu 2 - ISDN Setup


       Switch Type: DSS-1
       B Channel Usage= Switch/Switch

       Incoming Phone Numbers:
         ISDN Data     =                   Subaddress=
         A/B Adapter 1 =                   Subaddress=
         A/B Adapter 2 =                   Subaddress=

       Incoming Phone Number Matching= Multiple Subscriber Number (MSN)
         Analog Call Routing= N/A
         Global Analog Call= N/A

       Edit Advanced Setup = No
       Edit NetCAPI Setup = No

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

The following table describes the fields in this menu.

Table 57 Menu 2 ISDN Setup

FIELD	DESCRIPTION
Switch Type	This read only field displays your switch type, **DSS-1**.
B Channel Usage	In general, this will be **Switch/Switch** (default). If you are only using one B channel (e.g., your ZyXEL Device is sharing the ISDN BRI line with another device), then select **Switch/Unused**. If your second B channel is a leased line, select **Switch/Leased.** Press [SPACE BAR] to toggle through all the options. The options are below. • Switch/Unused • Switch/Switch • Switch/Leased • Leased/Switch • Leased/Unused • Unused/Leased • Leased/Leased
Incoming Phone Numbers:	
ISDN Data & Subaddress	Enter the telephone number and the subaddress assigned to ISDN data calls for the ZyXEL Device. The maximum number of digits is 25 for the telephone number and 5 for the subaddress.
A/B Adapter 1 & Subaddress	Enter the telephone number and the subaddress assigned to A/B Adapter 1 (PHONE1).
A/B Adapter 2 & Subaddress	Same as above for A/B Adapter 2 (PHONE2).
Incoming Phone Number Matching	Determines how incoming calls are routed. The choices for this field are **Multiple Subscriber Number (MSN)**, **Called Party Subaddress** and **Don't Care**.

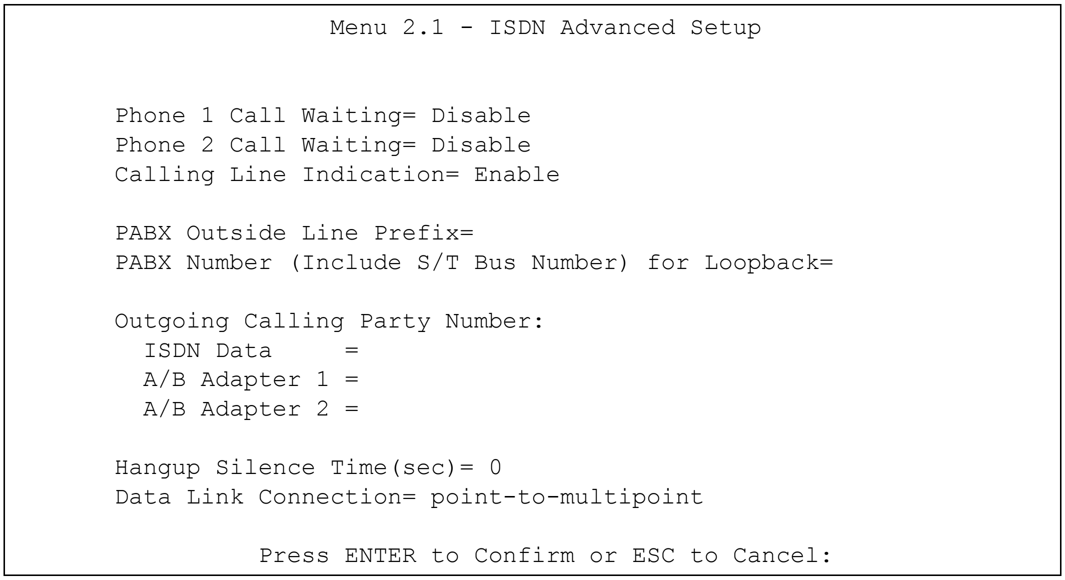
Table 57 Menu 2 ISDN Setup

FIELD	DESCRIPTION
Analog Call Routing	Select the destination for analog calls. The choices are **A/B Adapter 1**, **A/B Adapter 2** and **Ignore**. This field is only applicable when **Incoming Phone Number Matching** is **Don't Care**.
Global Analog Call	Select how to handle global analog calls. The choices are **Accept** and **Ignore**. This field is not applicable when the **Analog Call Routing** is **Ignore**.
Edit Advanced Setup	Advanced setup features are configured when you select **Yes** to enter **Menu 2.1 - ISDN Advanced Setup**.
Edit NetCAPI Setup	Press the [SPACE BAR] to select **Yes** or **No**. Select **Yes** to configure **Menu 2.2 - NetCAPI Setup** (discussed next).
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

17.2.1 ISDN Advanced Setup

Select **Yes** in the **Edit Advanced Setup** field of **Menu 2 - ISDN Setup** to display menu 2.1 as shown later.

Figure 79 Menu 2.1 ISDN Advanced Setup



```
                      Menu 2.1 - ISDN Advanced Setup


       Phone 1 Call Waiting= Disable
       Phone 2 Call Waiting= Disable
       Calling Line Indication= Enable

       PABX Outside Line Prefix=
       PABX Number (Include S/T Bus Number) for Loopback=

       Outgoing Calling Party Number:
         ISDN Data     =
         A/B Adapter 1 =
         A/B Adapter 2 =

       Hangup Silence Time(sec)= 0
       Data Link Connection= point-to-multipoint

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

The following table describes the fields in this menu.

Table 58 Menu 2.1 ISDN Advanced Setup

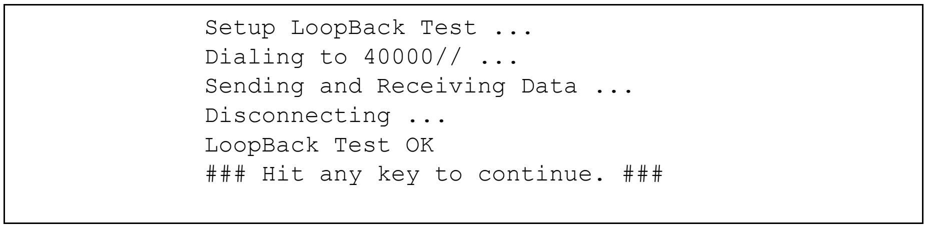
FIELD	DESCRIPTION
Phone 1/2 Call Waiting	The Call Waiting feature on your ISDN line works in exactly the same way as it does on a regular analog line. After hearing a call waiting indicator tone, press and immediately release the flash button on your telephone. This puts your current call on hold and answers the incoming call.
Calling Line Indication	The Calling Line Indication, or Caller ID, governs whether the other party can see your number when you call. If set to Enable, the ZyXEL Device sends the caller ID and the party you call can see your number; if it is set to Disable, the caller ID is blocked.
PABX Outside Line Prefix	Enter the number for outside line access if the ZyXEL Device is connected to a PABX; otherwise, leave it blank. The maximum number of digits is 4.
PABX Number (Include S/T Bus Number) for Loopback	Enter the S/T bus number if the ZyXEL Device is connected to an ISDN PABX. If this field is left as blank then the ISDN loopback test will be skipped.
Outgoing Calling Party Number	You only need to fill in this field if your switch requires a specific Outgoing Calling Party Number; otherwise, leave it blank.
ISDN Data	Enter the telephone number(s) assigned to your ISDN line by your telephone company. Some switch types only have one telephone number. Note that the ZyXEL Device only accepts digits; please do not include '-' or spaces in this field. This field should be no longer than 25 digits.
A/B Adapter 1	Enter the telephone number assigned to A/B Adapter 1 (PHONE1).
A/B Adapter 2	Enter the telephone number assigned to A/B Adapter 2 (PHONE2).
Hangup Silence Time(sec)	Most answering machines automatically terminate a call after a predefined length of silence. Specify the time in seconds that elapses before the answering machine drops the call when the ZyXEL Device receives tones from the switch and send a silence tone to the answering machine.
Data Link Connection	There are two types of ISDN **Data Link Connection** namely: **point-to-multipoint** and **point-to-point**. When you select **point-to-multipoint**, the TE1 value will be assigned by negotiation with the switch. When you select point-to-point, the TE1 value will be assigned a unique value of 0.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

17.2.2 Configuring Advanced Setup

When you are finished, press [ENTER] at the message: 'Press ENTER to confirm or ESC to Cancel', the ZyXEL Device uses the information that you entered to initialize the ISDN line. It should be noted that whenever the switch type is changed, the ISDN initialization takes slightly longer.

At this point, the ZyXEL Device asks if you wish to test your ISDN. If you select **Yes**, the ZyXEL Device will perform a loop-back test to check the ISDN line. If the loop-back test fails, please note the error message that you receive and take the appropriate troubleshooting action.

Figure 80 Loopback Test



```
              Setup LoopBack Test ...
              Dialing to 40000// ...
              Sending and Receiving Data ...
              Disconnecting ...
              LoopBack Test OK
              ### Hit any key to continue. ###
```

17.3 NetCAPI

Your ZyXEL Device supports NetCAPI. NetCAPI is ZyXEL's implementation of CAPI (Common ISDN Application Program Interface) capabilities over a network. It runs over DCP (Device Control Protocol) developed by RVS-COM.

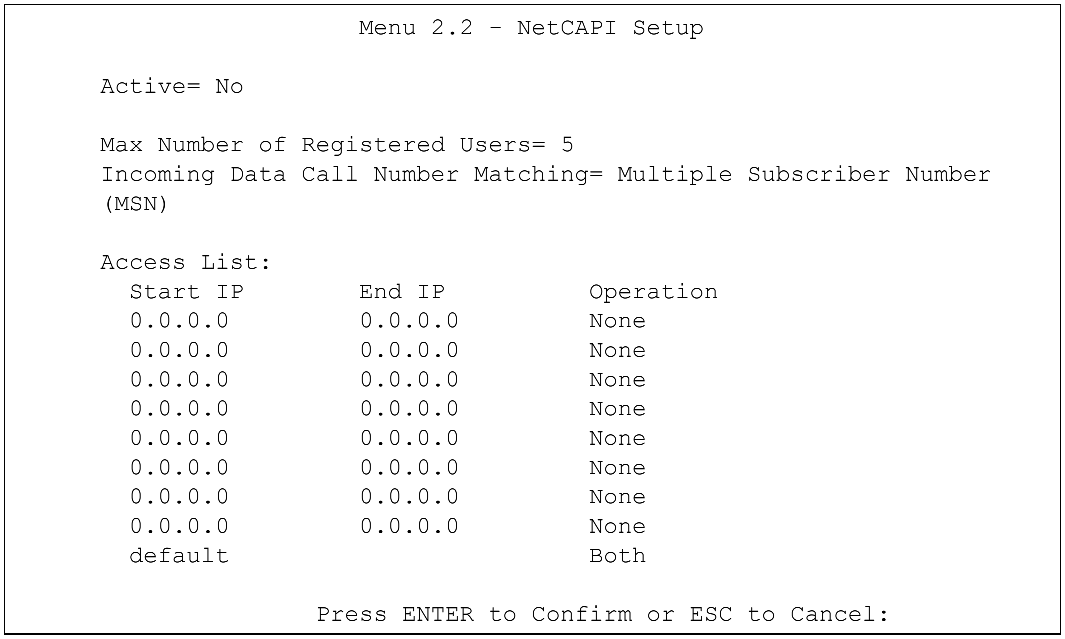
NetCAPI can be used for applications such as Eurofile transfer, file transfer, G3/G4 Fax, Autoanswer host mode, telephony, etc. on Windows 95/98/NT platforms.

See the NetCAPI chapter for more information regarding CAPI drivers.

17.3.1 Configuring NetCAPI

Press the [SACEBAR] to select **Yes** in **Edit NetCAPI Setup** field in **Menu 2** and press [ENTER] to go to **Menu 2.2 - NetCAPI Setup**.

Figure 81 Menu 2.2 NetCAPI Setup



```
                        Menu 2.2 - NetCAPI Setup

      Active= No

      Max Number of Registered Users= 5
      Incoming Data Call Number Matching= Multiple Subscriber Number
      (MSN)

      Access List:
        Start IP        End IP          Operation
        0.0.0.0         0.0.0.0         None
        0.0.0.0         0.0.0.0         None
        0.0.0.0         0.0.0.0         None
        0.0.0.0         0.0.0.0         None
        0.0.0.0         0.0.0.0         None
        0.0.0.0         0.0.0.0         None
        0.0.0.0         0.0.0.0         None
        0.0.0.0         0.0.0.0         None
        default                         Both

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

The following table describes the fields in this menu.

Table 59 Menu 2.2 NetCAPI Setup

FIELD	DESCRIPTION
Active	This field allows you to enable or disable NetCAPI. Press the [SPACEBAR] to select **Yes** or **No**.
Max Number of Registered Users	When you want to use NetCAPI to place outgoing calls or to listen to incoming calls, you must start RVSCOM on your computer, and RVSCOM will register itself to the ZyXEL Device. This option is the maximum number of clients that the ZyXEL Device supports at the same time.
Incoming Data Call Number Matching	This field determines how incoming calls are routed. Select **NetCAPI** if you want to direct all incoming data calls to NetCAPI. Select **Subscriber Number (MSN)** if you want to direct all incoming call to the ZyXEL Device only when the incoming phone number matches the ISDN DATA number. If the incoming phone number does not match the ISDN DATA number, then the call will be routed to NetCAPI. Select **Called Party Subaddress** if you want to direct all incoming calls to the ZyXEL Device only when the incoming call matches the subaddress of ISDN DATA. If the incoming call does not match the subaddress of ISDN DATA, then the call will be routed to NetCAPI.
Access List:	
Start IP	Refers to the first IP address of a group of NetCAPI clients. Each group contains contiguous IP addresses.
End IP	Refers to the last IP address in a NetCAPI client group.
Operation	Select **Incoming** if you wish to grant incoming calls permission. Select **Outgoing** if you wish to grant outgoing calls permission. Select **Both** if you wish to grant both incoming calls and outgoing calls permissions. Select **None** if you wish to deny all calls.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

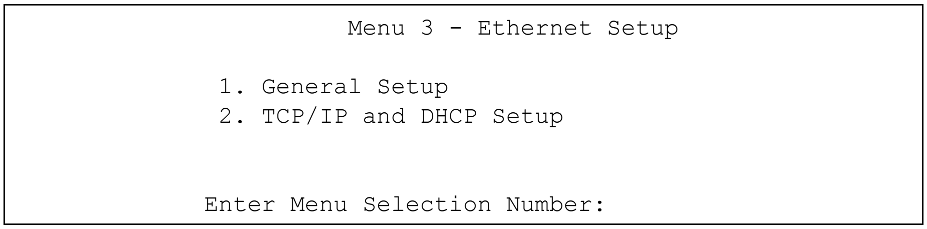
CHAPTER 18
Menu 3 Ethernet Setup

This chapter covers how to configure your wired Local Area Network (LAN) settings.

18.1 Ethernet Setup

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

Figure 82 Menu 3 Ethernet Setup

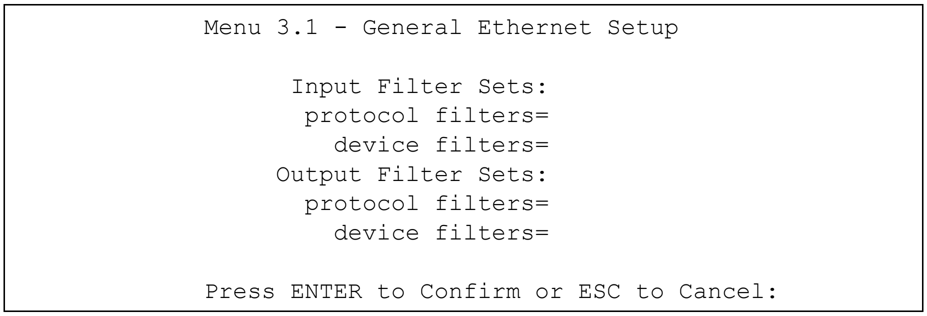


```
          Menu 3 - Ethernet Setup

 1. General Setup
 2. TCP/IP and DHCP Setup


Enter Menu Selection Number:
```

18.1.1 General Ethernet Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches

Figure 83 Menu 3.1 LAN Port Filter Setup.



```
Menu 3.1 - General Ethernet Setup

      Input Filter Sets:
       protocol filters=
         device filters=
     Output Filter Sets:
       protocol filters=
         device filters=

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

If you need to define filters, please read the Filter Set Configuration chapter first, then return to this menu to define the filter sets.

18.2 Ethernet TCP/IP and DHCP Server

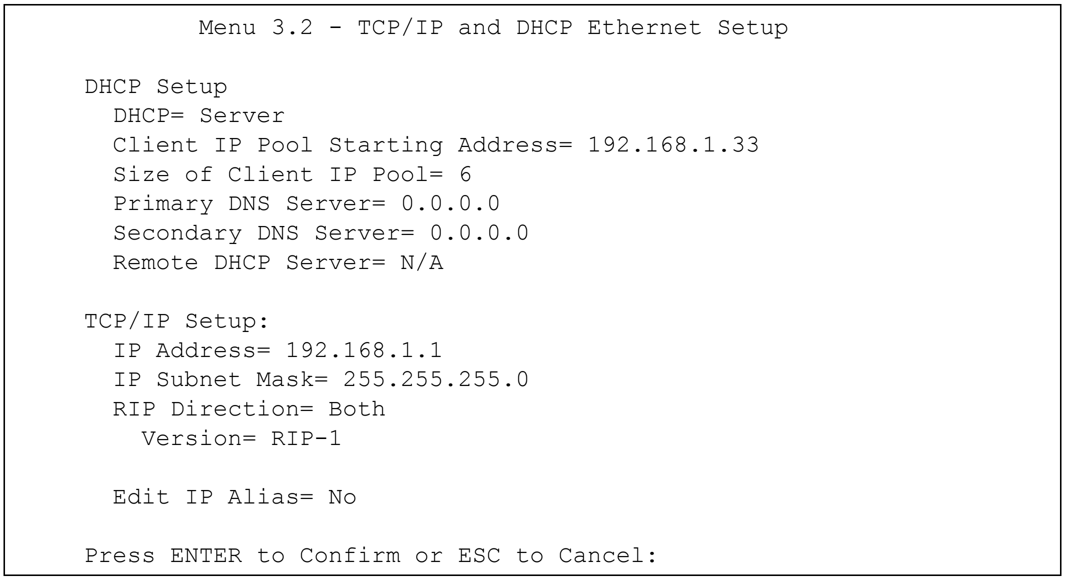
The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability. For remote node TCP/IP configuration, refer to the chapter on Remote Node Configuration.

18.3 Configuring TCP/IP Ethernet Setup and DHCP

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

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

Figure 84 Menu 3.2 TCP/IP and DHCP Ethernet Setup



```
            Menu 3.2 - TCP/IP and DHCP Ethernet Setup

    DHCP Setup
      DHCP= Server
      Client IP Pool Starting Address= 192.168.1.33
      Size of Client IP Pool= 6
      Primary DNS Server= 0.0.0.0
      Secondary DNS Server= 0.0.0.0
      Remote DHCP Server= N/A

    TCP/IP Setup:
      IP Address= 192.168.1.1
      IP Subnet Mask= 255.255.255.0
      RIP Direction= Both
        Version= RIP-1

      Edit IP Alias= No

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

Follow the instructions in the next table on how to configure the DHCP fields.

Table 60 DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
DHCP Setup	
DHCP	This field enables/disables the DHCP server. If set to **Server**, your ZyXEL Device will act as a DHCP server. 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 requests and responses between the remote server and the clients. When set to Server, the following four items need to be set:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.

Table 60 DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.
Primary DNS Server Secondary 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.
Remote DHCP Server	If Relay is selected in the DHCP field above, then enter the IP address of the actual, remote DHCP server here.

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

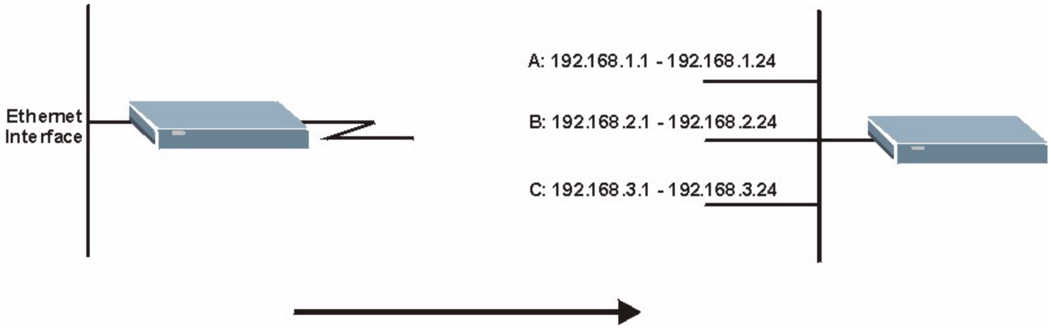
Table 61 Menu 3.2: LAN TCP/IP Setup Fields

FIELD	DESCRIPTION
TCP/IP Setup:	
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select **None** (default) to disable it.
Edit IP Alias	The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.	

18.3.1 IP Alias Setup

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

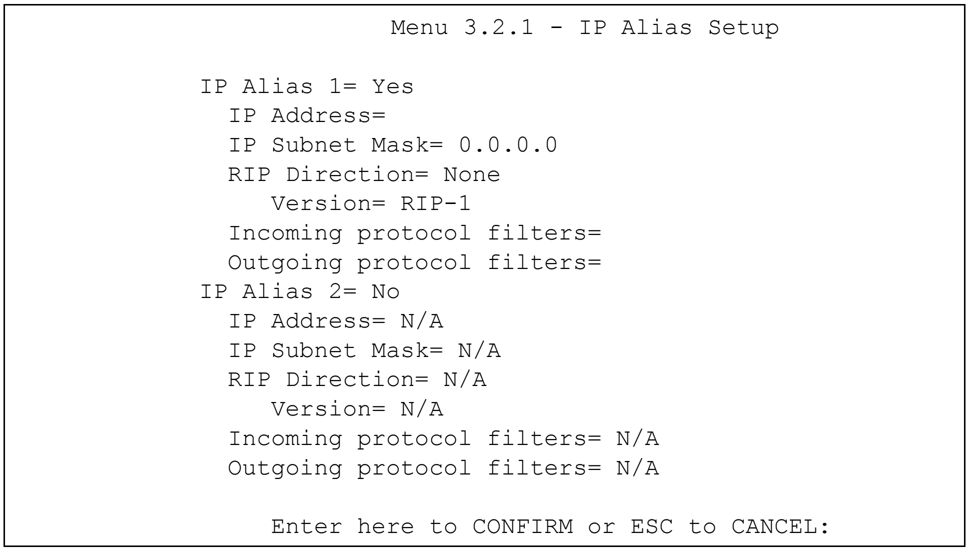
Figure 85 Physical Network & Partitioned Logical Networks


Ethernet Interface
A: 192.168.1.1 - 192.168.1.24
B: 192.168.2.1 - 192.168.2.24
C: 192.168.3.1 - 192.168.3.24

You must use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

Figure 86 Menu 3.2.1 IP Alias Setup



```
                          Menu 3.2.1 - IP Alias Setup

             IP Alias 1= Yes
               IP Address=
               IP Subnet Mask= 0.0.0.0
               RIP Direction= None
                  Version= RIP-1
               Incoming protocol filters=
               Outgoing protocol filters=
             IP Alias 2= No
               IP Address= N/A
               IP Subnet Mask= N/A
               RIP Direction= N/A
                  Version= N/A
               Incoming protocol filters= N/A
               Outgoing protocol filters= N/A

                  Enter here to CONFIRM or ESC to CANCEL:
```

Use the instructions in the following table to configure IP alias parameters.

Table 62 Menu 3.2.1 IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1, 2	Choose **Yes** to configure the LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.

Table 62 Menu 3.2.1 IP Alias Setup

FIELD	DESCRIPTION
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyXEL Device.
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyXEL Device.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 19
Internet Access Setup

This chapter shows you how to configure your ZyXEL Device for Internet access.

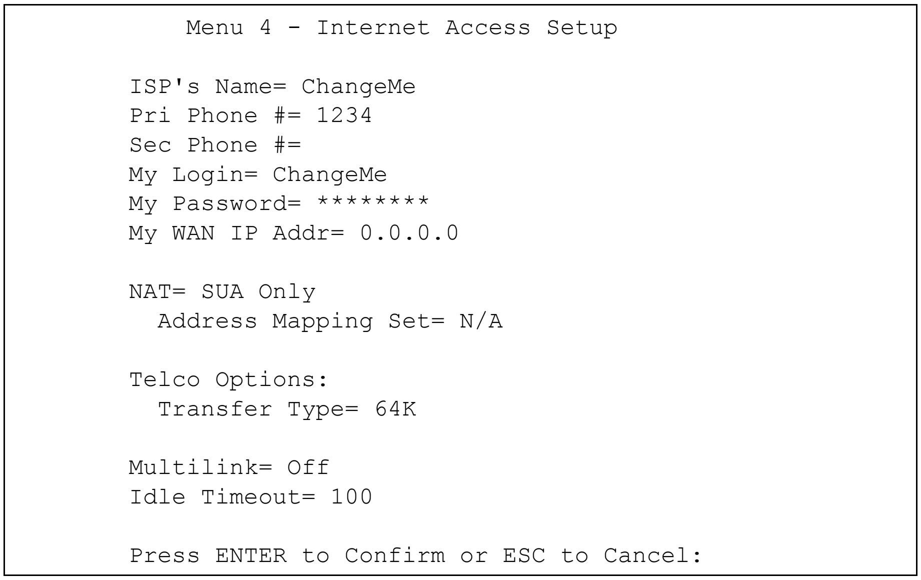
19.1 Introduction to Internet Access Setup

Menu 4 allows you to enter the Internet access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your ZyXEL Device for Internet access, you need to collect your Internet account information from your ISP.

19.2 Internet Access Setup

From the main menu, type 4 to display **Menu 4 - Internet Access Setup**.

Figure 87 Menu 4 Internet Access Setup



```
            Menu 4 - Internet Access Setup

        ISP's Name= ChangeMe
        Pri Phone #= 1234
        Sec Phone #=
        My Login= ChangeMe
        My Password= ********
        My WAN IP Addr= 0.0.0.0

        NAT= SUA Only
          Address Mapping Set= N/A

        Telco Options:
          Transfer Type= 64K

        Multilink= Off
        Idle Timeout= 100

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

The following table describes the fields in this menu.

Table 63 Internet Access Setup

FIELD	DESCRIPTION
ISP’s Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Pri/Sec Phone #	Both the Primary and the Secondary Phone number refer to the number that the ZyXEL Device dials to connect to the ISP.
My Login	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
My WAN IP Addr	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your ZyXEL Device. **Note:** This is the address assigned to your local router WAN, not the remote router. If the remote router is a router, then this entry determines the local router **Rem IP Addr** in menu 11.1.
NAT	Choose from **None**, **Full Feature** or **SUA Only**. When you select **Full Feature** you must configure at least one address mapping set. See the chapter on NAT for a full discussion of this new feature.
Address Mapping Set	A NAT address mapping set is to create the mapping table used to assign global addresses to computers on the LAN. You may enter any address mapping set number up to 8. Set 255 (read only) is used for SUA.
Telco options:	
Transfer Type	This field specifies the type of connection between the ZyXEL Device and this remote node. Select **64K**, or **Leased**.
Multilink	The ZyXEL Device uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is **64K**. Options for this field are: **Off**, **BOD** and **Always**.
Idle Timeout	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your ZyXEL Device. Administrative packets such as RIP are not counted as data. **Note:** Idle Timeout only applies when the ZyXEL Device initiates the call.
When you are finished, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration. At this point, the SMT will ask if you wish to test the Internet connection. If you select **Yes**, your ZyXEL Device will call the ISP to test the Internet connection. If the test fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.	

CHAPTER 20 Remote Node Configuration

This chapter covers remote node configuration.

20.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use Menu 4 to set up Internet access, you are actually configuring one of the remote nodes. Once a remote node is configured correctly, traffic to the remote network will trigger your ZyXEL Device to make a call automatically, i.e., Dial on Demand. The following describes how to configure **Menu 11.1 Remote Node Profile**, **Menu 11.2 - Remote Node PPP Options**, **Menu 11.3 - Remote Node Network Layer Options** and **Menu 11.5 - Remote Node Filter**.

20.1.1 Minimum Toll Period

Phone calls are normally charged per basic time unit with the time being rounded up to the nearest unit when bills are calculated. For example, the ZyXEL Device may make a call but drop the call after 10 seconds (maybe there was no reply) but the call would still be charged at a minimum time unit, let us say 3 minutes. With minimum toll period, the ZyXEL Device will try to use all the toll period. In the above case, the ZyXEL Device tries to extend the idle timeout to the nearest 3 minutes (basic charging unit of time). If there is traffic during the extended 2 minutes and 50 seconds, the idle timeout will be cleared and a second call is eliminated. Since the session time calculation by the ZyXEL Device is not always perfectly synchronized with your telephone company, the ZyXEL Device drops the channel 5 seconds before the toll period you set, to compensate for any lag. As such, you must not set the minimum toll period to less than 5 seconds.

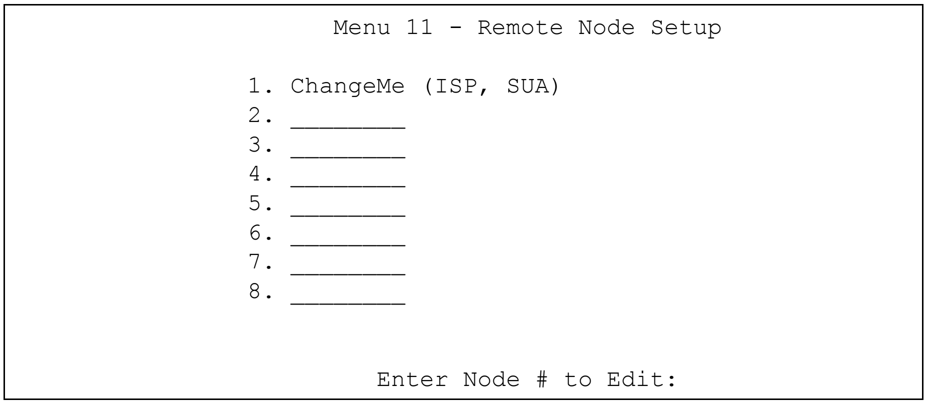
20.2 Remote Node Profile Setup

To configure a remote node, follow these steps:

1 From the main menu, select menu option 11 to open **Menu 11 Remote Node Setup**.

2 When menu 11 appears as shown in the following figure, enter the number of the remote node that you wish to configure.

Figure 88 Menu 11 Remote Node Setup

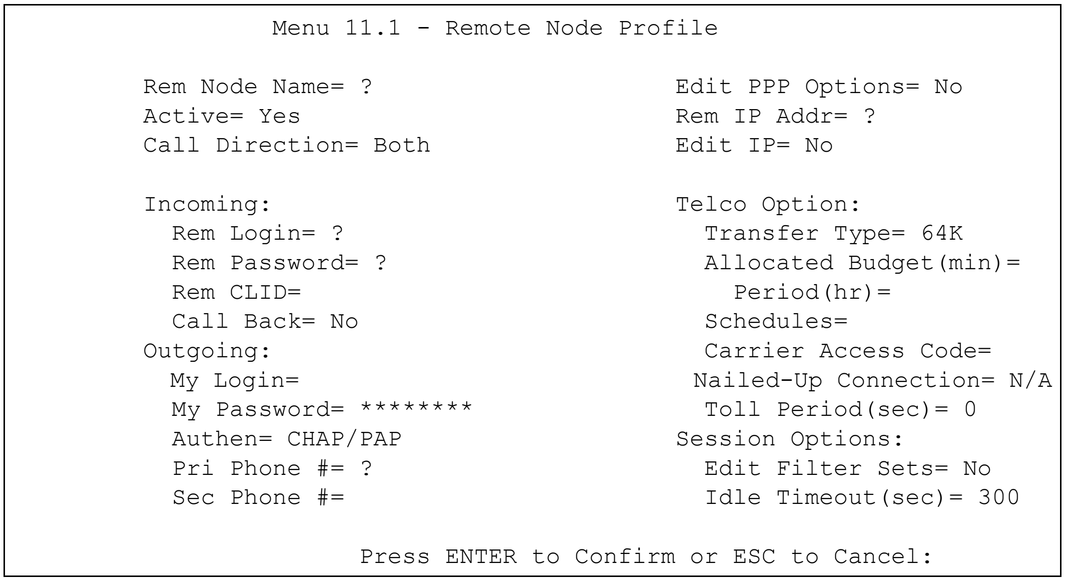


```
                       Menu 11 - Remote Node Setup

                 1. ChangeMe (ISP, SUA)
                 2. ________
                 3. ________
                 4. ________
                 5. ________
                 6. ________
                 7. ________
                 8. ________


                          Enter Node # to Edit:
```

3 When **Menu 11.1 - Remote Node Profile** appears, fill in the fields as described in the following table to define this remote profile.

The following explains how to configure the remote node profile menu.

Figure 89 Menu 11.1 Remote Node Profile



```
                  Menu 11.1 - Remote Node Profile

         Rem Node Name= ?                     Edit PPP Options= No
         Active= Yes                          Rem IP Addr= ?
         Call Direction= Both                 Edit IP= No

         Incoming:                            Telco Option:
           Rem Login= ?                         Transfer Type= 64K
           Rem Password= ?                      Allocated Budget(min)=
           Rem CLID=                              Period(hr)=
           Call Back= No                        Schedules=
         Outgoing:                              Carrier Access Code=
           My Login=                           Nailed-Up Connection= N/A
           My Password= ********                Toll Period(sec)= 0
           Authen= CHAP/PAP                   Session Options:
           Pri Phone #= ?                       Edit Filter Sets= No
           Sec Phone #=                         Idle Timeout(sec)= 300

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

The following table describes the fields in this menu.

Table 64 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION
Rem Node Name	This is a required field. Enter a descriptive name for the remote node, for example, Corp. This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node).

Table 64 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION
Call Direction	If this parameter is set to **Both**, your ZyXEL Device can both place and receive calls to/from this remote node. If set to **Incoming**, your ZyXEL Device will not place a call to this remote node. If set to **Outgoing**, your ZyXEL Device will drop any incoming calls from this remote node. Several other fields in this menu depend on this parameter. For example, in order to enable **Callback**, the **Call Direction** must be set to **Both**.
Incoming:	
Rem Login	Enter the login name that this remote node will use when it calls your ZyXEL Device. The login name in this field combined with the **Rem Password** will be used to authenticate this node.
Rem Password	Enter the password used when this remote node calls your ZyXEL Device.
Rem CLID	This field is applicable only if **Call Direction** is either set to **Both** or **Incoming**. Otherwise, a **N/A** appears in the field. This is the Calling Line ID (the telephone number of the calling party) of this remote node. If you enable the **CLID Authen** field in **Menu 13 - Default Dial-In Setup**, your ZyXEL Device will check the CLID in the incoming call against the CLIDs in the database. If no match is found and **CLID Authen** is set to **Required**, the call will be dropped.
Call Back	This field is applicable only if **Call Direction** is set to **Both**. Otherwise, a **N/A** appears in the field. This field determines whether or not your ZyXEL Device will call back after receiving a call from this remote node. If this option is enabled, your ZyXEL Device will disconnect the initial call from this node and call it back at the **Outgoing Primary Phone Number** (see Section 22.4 on page 205).
Outgoing	
My Login	This is a required field if **Call Direction** is either **Both** or **Outgoing**. Enter the login name for your ZyXEL Device when it calls this remote node.
My Password	This is a required field if **Call Direction** is either **Both** or **Outgoing**. Enter the password for your ZyXEL Device when it calls this remote node.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP/PAP** - Your ZyXEL Device will accept either CHAP or PAP when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.

Pri(mary)
Sec(ondary)
Phone #
	Your ZyXEL Device always calls this remote node using the **Primary Phone** number first for a dial-up line.
	If the **Primary Phone** number is busy or does not answer, your ZyXEL Device will dial the **Secondary Phone** number if available.
	Some areas require dialing the pound sign # before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.

Edit PPP Options	To edit the PPP options for this remote node, move the cursor to this field. Press [SPACE BAR] and then [ENTER] to select Yes and press [ENTER]. This will bring you to **Menu 11.2 - Remote Node PPP Options**. For more information on configuring PPP options, see Section 20.6 on page 191.

Table 64 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION
Rem IP Addr	This is a required field [?]. Enter the IP address of the remote gateway.
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.3 - Remote Node Network Layer Options**.
Telco Options:	
Transfer Type	This field specifies the type of connection between the ZyXEL Device and this remote node. When set to **Leased**, the **Allocated Budget** and **Period** do not apply.
Allocated Budget (min)	This field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 for no budget control.
Period (hr)	This field sets the time interval to reset the above outgoing call budget control.
Schedules	Apply up to 4 schedule sets, separated by commas to your remote node here. Please see ahead for a full discussion on schedules.
Carrier Access Code	In some European countries, you need to enter the access code number of your preferred telecommunications service provider. Your telephone company should supply you with this number.
Nailed-up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. See the following section for more details.
Toll Period	This is the basic unit of time for charging purposes, e.g., 25 cents every 3 minutes - 3 minutes is the **Toll Period**.
Session Options	
Edit Filter Sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.
Idle Timeout (sec)	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your ZyXEL Device. Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes). Idle timeout only applies when the ZyXEL Device initiates the call. 0 sec means the remote node will never be automatically disconnected.
Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

20.3 Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor’s implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

20.4 PPP Multilink

The ZyXEL Device uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes.

Due to the fragmentation/reconstruction overhead associated with MP, you may not get a linear increase in throughput when a link is added.

The number of links in an MP bundle can be statically configured, or dynamically determined at runtime, as explained in the following section.

20.5 Bandwidth on Demand

The Bandwidth on Demand (BOD) feature adds or subtracts links dynamically according to traffic demand. After the initial call, the ZyXEL Device uses BAP (Bandwidth Allocation Protocol) to ask the peer for additional telephone number if BACP (Bandwidth Allocation Control Protocol) is negotiated. Otherwise, the ZyXEL Device uses the statically configured (primary and secondary) telephone numbers of the remote node.

The configuration of bandwidth on demand focuses on the Base Transmission Rate (BTR) and the Maximum Transmission Rate (MTR). The relationship between BTR and MTR are shown in the following table:

Table 65 BTR vs MTR for BOD

BTR AND MTR SETTING	NO. OF CHANNEL(S) USED	MAX NO. OF CHANNEL(S) USED	BANDWIDTH ON DEMAND
BTR = 64, MTR = 64	1	1	Off
BTR = 64, MTR = 128	1	2	On
BTR = 128, MTR = 128	2	2	Off

When bandwidth on demand is enabled, a second channel will be brought up if traffic on the initial channel is higher than the high **Target Utility** number for longer than the specified **Add Persist** value. Similarly, the second channel will be dropped if the traffic level falls below the low **Target Utility** number for longer than the **Subtract Persist** value.

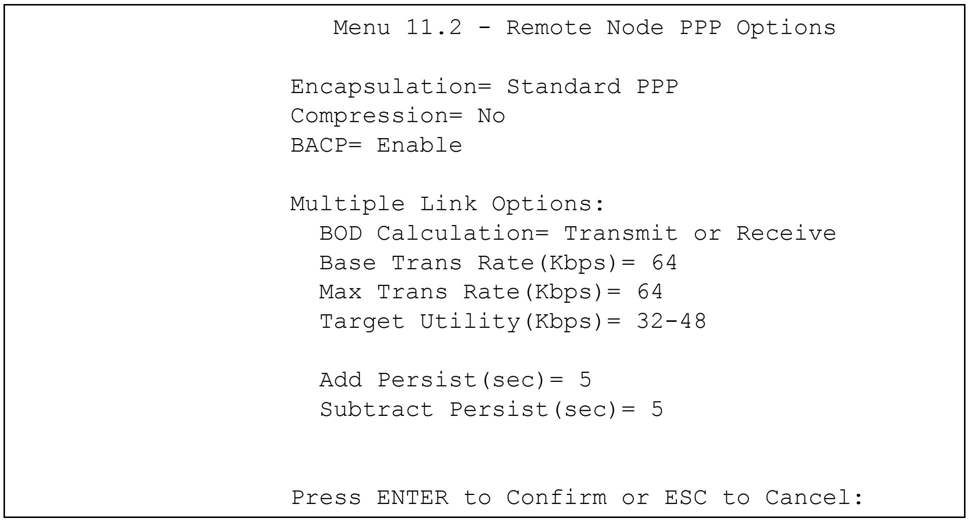
The **Target Utility** specifies the line utilization range at which you want the ZyXEL Device to add or subtract bandwidth. The range is 30 to 64 Kbps (kilobits per second). The parameters are separated by a '-'. For example, '30-60' means the add threshold is 30 Kbps and subtract threshold is 60 Kbps. The ZyXEL Device performs bandwidth on demand only if it initiates the call. Addition and subtraction are based on the value set in the **BOD Calculation** field. If this field is set to **Transmit or Receive**, then traffic in either direction will be included to determine if a link should be added or dropped. **Transmit** will only use outgoing traffic to make this determination and **Receive** will only use incoming traffic to make this determination.

If, after making the call to bring up a second channel, the second channel does not succeed in joining the Multilink Protocol bundle (because the remote device does not recognize the second call as coming from the same device), the ZyXEL Device will hang up the second call and continue with the first channel alone.

20.6 Editing PPP Options

To edit the remote node PPP options, move the cursor to the **Edit PPP Options** field in **Menu 11.1 - Remote Node Profile**, and use [SPACE BAR] to select **Yes**. Press [ENTER] to open menu 11.2, as shown next.

Figure 90 Menu 11.2 Remote Node PPP Options



```
                       Menu 11.2 - Remote Node PPP Options

                    Encapsulation= Standard PPP
                    Compression= No
                    BACP= Enable

                    Multiple Link Options:
                      BOD Calculation= Transmit or Receive
                      Base Trans Rate(Kbps)= 64
                      Max Trans Rate(Kbps)= 64
                      Target Utility(Kbps)= 32-48

                      Add Persist(sec)= 5
                      Subtract Persist(sec)= 5


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

The following table describes the fields in this menu.

Table 66 Menu 11.2 Remote Node PPP Options

FIELD	DESCRIPTION
Encapsulation	Select **CISCO PPP** only when this remote node is a Cisco machine; otherwise, select **Standard PPP**.
Compression	Turn on/off Stac Compression. The default for this field is No.
BACP	Your ZyXEL Device negotiates the secondary phone number for a dial-up line from the peer when BACP (Bandwidth Allocation Control Protocol) is enabled; otherwise it uses the secondary phone number set in menu 11.1.
Multiple Link Options:	
BOD Calculation	Select the direction of the traffic you wish to use in determining when to add or subtract a link. Options for this field are: **Transmit or Receive**, **Transmit** and **Receive**.
Base Trans Rate (Kbps)	Select the base data transfer rate for this remote node in Kbps. There are two choices for this field: **64** where only one channel is used or, **128** where two channels are used as soon as a packet triggers a call.

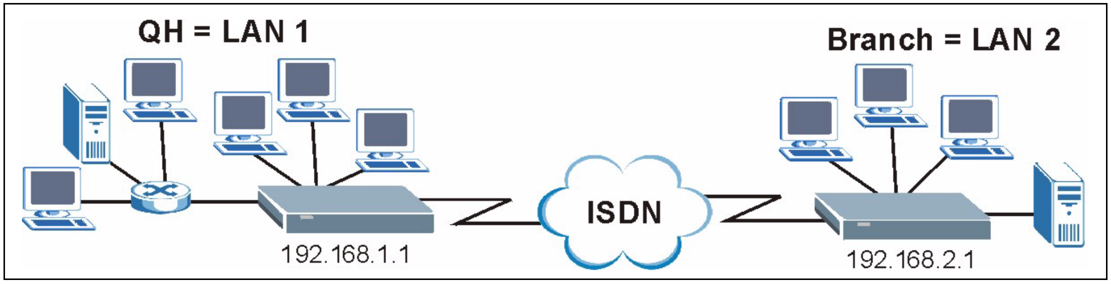
Table 66 Menu 11.2 Remote Node PPP Options

FIELD	DESCRIPTION
Max Trans Rate (Kbps)	Enter the maximum data transfer rate allowed for this remote node. This parameter is in kilobits per second.
Target Utility (Kbps)	Enter the two thresholds separated by a "-" for subtracting and adding the second port.
Add Persist	This parameter specifies the number of seconds where traffic is above the adding threshold before the ZyXEL Device will bring up the second link.
Subtract Persist	This parameter specifies the number of seconds where traffic is below the subtraction threshold before your ZyXEL Device drops the second link.
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

20.7 LAN-to-LAN Application

A typical LAN-to-LAN application is to use your ZyXEL Device to connect a branch office to the headquarters, as depicted in the following diagram.

Figure 91 TCP/IP LAN-to-LAN Application



For the branch office, you need to configure a remote node in order to dial out to headquarters.

LAN 1 Setup

```
                      Menu 11.1 - Remote Node Profile

        Rem Node Name= LAN_2                 Edit PPP Options= No
        Active= Yes                          Rem IP Addr= 192.168.2.1
        Call Direction= Both                 Edit IP= No

        Incoming:                            Telco Option:
          Rem Login= lan2                      Transfer Type= 64K
          Rem Password= ********               Allocated Budget(min)= 0
          Rem CLID=                              Period(hr)= 0
          Call Back= No                        Schedules=
        Outgoing:                              Carrier Access Code=
          My Login= lan1                       Nailed-Up Connection= N/A
           y Password= ********                Toll Period(sec)= 0
          Authen= CHAP/PAP                   Session Options:
          Pri Phone #= 035783942               Edit Filter Sets= No
          Sec Phone #=                         Idle Timeout(sec)= 300

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

LAN 2 Setup

```
                            Menu 11.1 - Remote Node Profile

        Rem Node Name= LAN_1                 Edit PPP Options= No
        Active= Yes                          Rem IP Addr= 192.168.1.1
        Call Direction= Both                 Edit IP= No

        Incoming:                            Telco Option:
          Rem Login= lan1                      Transfer Type= 64K
          Rem Password= ********               Allocated Budget(min)= 0
          Rem CLID=                              Period(hr)= 0
          Call Back= No                        Schedules=
        Outgoing:                              Carrier Access Code=
          My Login= lan2                       Nailed-Up Connection= N/A
           y Password= ********                Toll Period(sec)= 0
          Authen= CHAP/PAP                   Session Options:
          Pri Phone #= 0227176324              Edit Filter Sets= No
          Sec Phone #=                         Idle Timeout(sec)= 300

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

Additionally, you may also need to define static routes if some services reside beyond the immediate remote LAN.

20.8 Configuring Network Layer Options

Follow the steps below to edit **Menu 11.3 - Remote Node Network Layer Options** shown next.

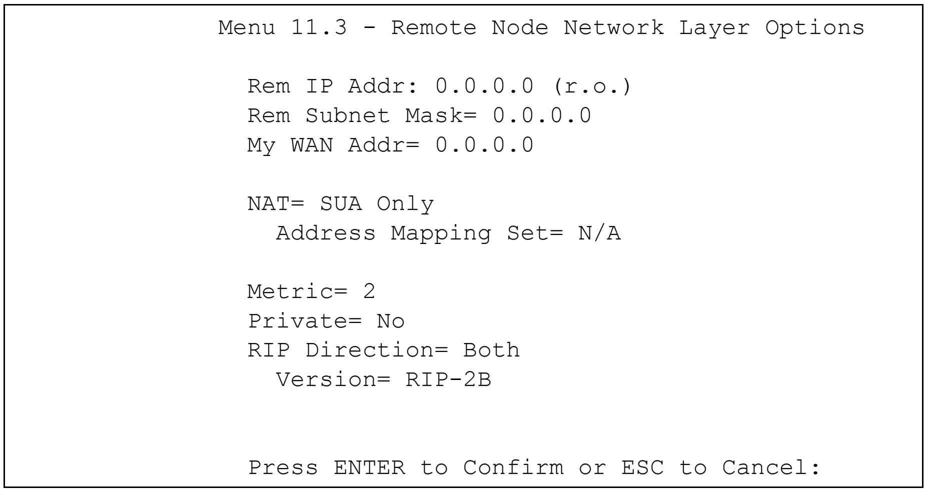
1 To configure the TCP/IP parameters of a remote node, first configure the three fields in **Menu 11.1 - Remote Node Profile**, as shown in the following table.

Table 67 TCP/IP-related Fields in Remote Node Profile

Rem IP Addr	Enter the IP address of the remote gateway in **Menu 11.1 - Remote Node Profile**. You must fill in either the remote ZyXEL Device WAN IP address or the remote ZyXEL Device LAN IP address. This depends on the remote router's WAN IP i.e., for the (remote) ZyXEL Device, the **My WAN IP Addr** settings in **Menu 4**. For example, if the remote WAN IP is set to 172.16.0.2 (the remote router's WAN IP), then you should enter 172.16.0.2 in the **Rem IP Add** field. If the remote WAN IP is 0.0.0.0, then enter 192.168.1.1(the remote router's LAN IP) in the **Rem IP Addr** field).
Edit IP	Press [SPACE BAR] and then [ENTER] to select **Yes** and press [ENTER] to go to **Menu 11.3 - Remote Node Network Layer Options**.

2 Move the cursor to the **Edit IP** field in **Menu 11 - Remote Node Profile**, and then press [SPACE BAR] to toggle and set the value to **Yes**. Press [ENTER] to open **Menu 11.3 - Remote Node Network Layer Options**.

Figure 92 Menu 11.3 Remote Node Network Layer Options



```
               Menu 11.3 - Remote Node Network Layer Options

                 Rem IP Addr: 0.0.0.0 (r.o.)
                 Rem Subnet Mask= 0.0.0.0
                 My WAN Addr= 0.0.0.0

                 NAT= SUA Only
                   Address Mapping Set= N/A

                 Metric= 2
                 Private= No
                 RIP Direction= Both
                   Version= RIP-2B


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

The following table describes the fields in this menu.

Table 68 Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION
Rem IP Addr	This will show the IP address you entered for this remote node in the previous menu.
Rem Subnet Mask	Enter the subnet mask for the remote network.

Table 68 Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION
My WAN Addr	Some implementations, especially the UNIX derivatives, require the ISDN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the ISDN port of your ZyXEL Device. **Note:** This is the address assigned to your local ZyXEL Device WAN, not the remote router. If the remote router is a ZyXEL Device, then this entry determines the local ZyXEL Device **Rem IP Addr** in menu 11.1.
NAT	Choose from **None**, **Full Feature**, or **SUA Only**. When you select **Full Feature**, you must configure at least one address mapping set. For more information about NAT and the choices listed refer to the NAT Chapter.
Address Mapping Set	A NAT address mapping set is to create the mapping table used to assign global addresses to computers on the LAN. You may enter any address mapping set number up to 8. Set 255 (read only) is used for SUA.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyXEL Device will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select from **Both**, **In Only**, **Out Only** and **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

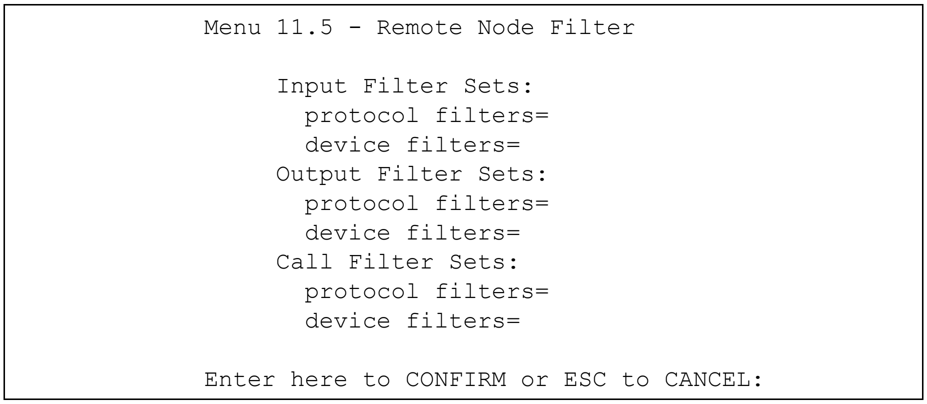
20.9 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyXEL Device to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. For more information on defining the filters, please refer to the Filters chapter. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 93 Menu 11.5 Remote Node Filter



```
              Menu 11.5 - Remote Node Filter

                   Input Filter Sets:
                     protocol filters=
                     device filters=
                   Output Filter Sets:
                     protocol filters=
                     device filters=
                   Call Filter Sets:
                     protocol filters=
                     device filters=

              Enter here to CONFIRM or ESC to CANCEL:
```

CHAPTER 21 Static Route Setup

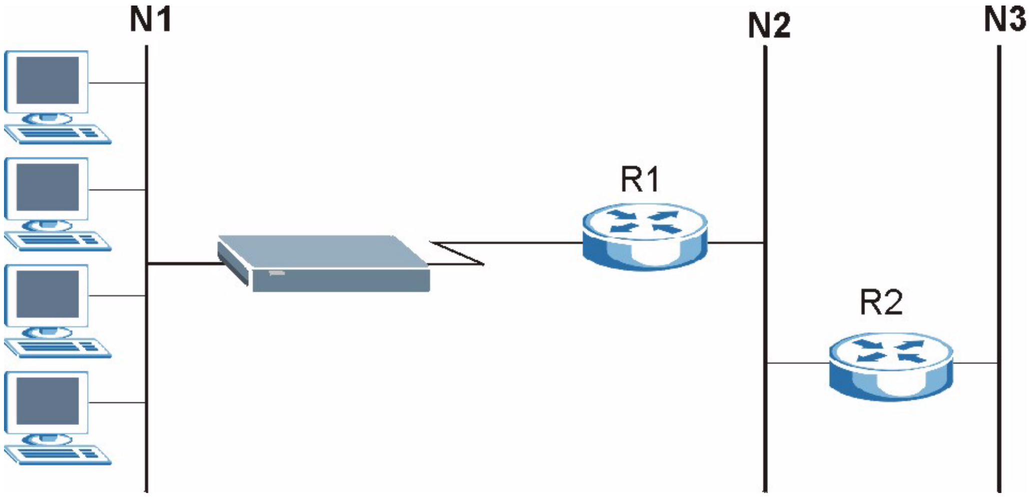
This chapter shows you how to setup IP static routes.

21.1 Static Route

Static routes tell the ZyXEL Device routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

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

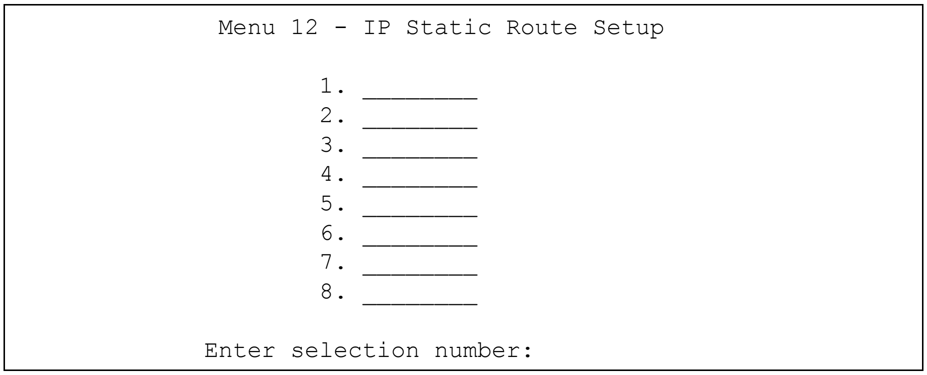
Figure 94 Example of Static Routing Topology



21.2 IP Static Route Setup

To configure an IP static route, use **Menu 12 – Static Routing Setup** (shown next).

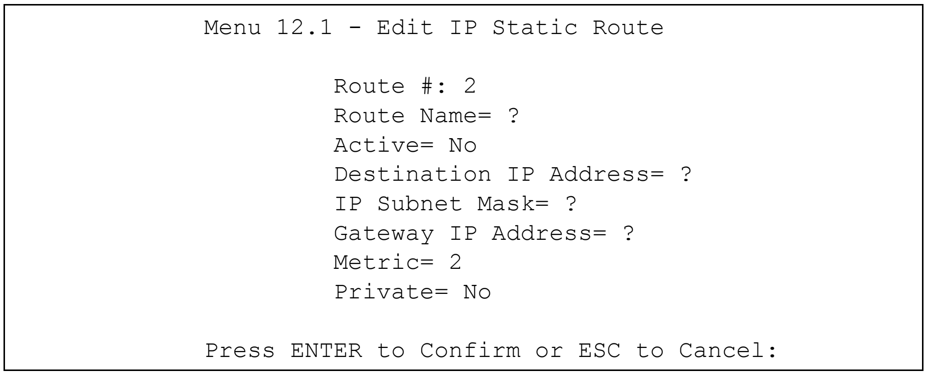
Figure 95 Menu 12 IP Static Route Setup



```
               Menu 12 - IP Static Route Setup

                      1. ________
                      2. ________
                      3. ________
                      4. ________
                      5. ________
                      6. ________
                      7. ________
                      8. ________

              Enter selection number:
```

Now, type the route number of a static route you want to configure.

Figure 96 Menu12.1 Edit IP Static Route



```
              Menu 12.1 - Edit IP Static Route

                       Route #: 2
                       Route Name= ?
                       Active= No
                       Destination IP Address= ?
                       IP Subnet Mask= ?
                       Gateway IP Address= ?
                       Metric= 2
                       Private= No

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

The following table describes the fields for **Menu 12.1 – Edit IP Static Route Setup**.

Table 69 Menu12.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on IP Subnet Mask in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over WAN, the gateway must be the IP address of one of the remote nodes.

Table 69 Menu12.1 Edit IP Static Route

FIELD	DESCRIPTION
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyXEL Device will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

CHAPTER 22
Dial-in Setup

This chapter shows you how to configure your ZyXEL Device to receive calls from remote dial-in users including telecommuters and remote nodes. This is done in SMT menus 13 and 14.

22.1 Dial-in Users Overview

There are several differences between dial-in users and remote nodes, as summarized in the next table.

Table 70 Remote Dial-in Users/Remote Nodes Comparison Chart

REMOTE DIAL-IN USERS	REMOTE NODES
Your ZyXEL Device will only answer calls from remote dial-in users; it will not make calls to them.	Your ZyXEL Device can make calls to and receive calls from the remote node.
All remote dial-in users share one common set of parameters, as defined in the **Menu 14 Default Dial-in User Setup**.	Each remote node can have its own set of parameters such as Bandwidth On Demand, Protocol, Security, etc.

22.2 Default Dial-in User Setup

This section covers the default dial-in parameters. The parameters in menu 13 affect incoming calls from both remote dial-in users and remote nodes until authentication is completed. Once authentication is completed and if it matches a remote node, your ZyXEL Device will use the parameters from that particular remote node.

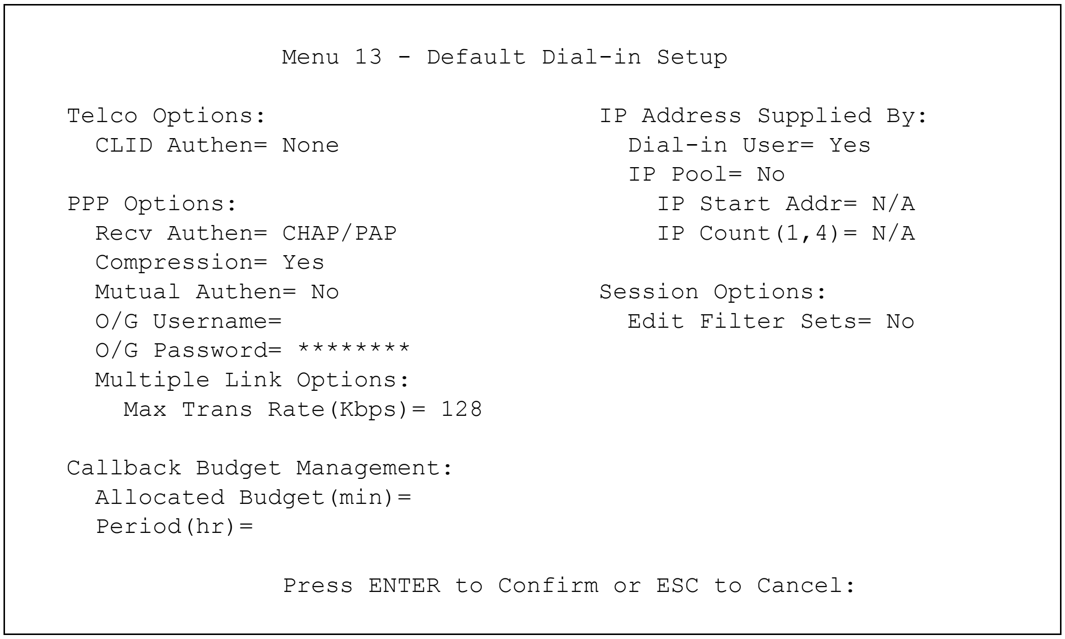
22.2.1 CLID Callback Support For Dial-In Users

CLID (Calling Line IDentification) authentication affords you the security of limiting a user to only initiate connections from a fixed location. The ZyXEL Device uses the caller ID sent by the switch to match against the CLIDs in the database. Please note that for CLID authentication to work on the ZyXEL Device, your telephone company must support caller ID. If the remote node requires mutual authentication, please fill in the **O/G Username** and **O/G Password** fields. You must also fill in these fields when a dial-in user to whom we are calling back requests authentication.

22.3 Setting Up Default Dial-in

From the Main Menu, enter 13 to go to **Menu 13 - Default Dial-in Setup**. This section describes how to configure the protocol-independent fields in this menu. For the protocol-dependent fields, refer to the appropriate chapters.

Figure 97 Menu 13 Default Dial-in Setup



```
                Menu 13 - Default Dial-in Setup

Telco Options:                       IP Address Supplied By:
  CLID Authen= None                    Dial-in User= Yes
                                       IP Pool= No
PPP Options:                             IP Start Addr= N/A
  Recv Authen= CHAP/PAP                  IP Count(1,4)= N/A
  Compression= Yes
  Mutual Authen= No                  Session Options:
  O/G Username=                        Edit Filter Sets= No
  O/G Password= ********
  Multiple Link Options:
    Max Trans Rate(Kbps)= 128

Callback Budget Management:
  Allocated Budget(min)=
  Period(hr)=

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

The following table describes the fields in this menu.

Table 71 Menu 13 Default Dial-in Setup

FIELD	DESCRIPTION
Telco Options:	
CLID Authen	This field sets the CLID authentication parameter for all incoming calls. There are three options for this field: **None** - No CLID is required. **Required** - CLID must be available, or the ZyXEL Device will not answer the call. **Preferred** - If the CLID is available then CLID will be used; otherwise, authentication is performed in PPP negotiation.
PPP Options:	
Recv Authen	This field sets the authentication protocol for incoming calls. For security reason, setting authentication to **None** is strongly discouraged. Options for this field are: **CHAP/PAP** - Your ZyXEL Device will try CHAP first, but PAP will be used if CHAP is not available. **CHAP** -Use CHAP only. **PAP** - Use PAP only. **None** - Your ZyXEL Device tries to acquire CHAP/PAP first, but no authentication is required if CHAP/PAP is not available.

Table 71 Menu 13 Default Dial-in Setup

FIELD	DESCRIPTION
Compression	Turn on/off Stac Compression. The default for this field is **No**.
Mutual Authen	Some vendors, e.g., Cisco, require mutual authentication, i.e., the node that initiates the call will request a user name and password from the far end that it is dialing to. If the remote node requires mutual authentication, set this field to **Yes**.
O/G Username	Enter the login name to be used to respond to the peer's authentication request.
O/G Password	Enter the outgoing password to be used to respond to the peer's authentication request.
Multiple Link Options:	
Max Trans Rate(Kbps)	Enter the maximum data transfer rate between your ZyXEL Device and the remote dial-in user. 64 - At most, one B channel is used. 128 - A maximum of two channels can be used. When the ZyXEL Device calls back to the remote dial-in user, the maximum data transfer rate is always 64.
Callback Budget Management:	
Allocated Budget (min)	This field sets the budget callback time for all the remote dial-in users. The default for this field is **0** for no budget control.
Period (hr)	This field sets the time interval to reset the above callback budget control.
IP Address Supplied By:	
Dial-in User	If set to **Yes**, the ZyXEL Device will allow a remote host to specify its own IP address. If set to **No**, the remote host must use the IP address assigned by your ZyXEL Device from the IP pool, configured below. This is to prevent the remote host from using an invalid IP address and potentially disrupting the whole network.
IP Pool	This field tells your ZyXEL Device to provide the remote host with an IP address from the pool. This field is required if **Dial-In IP Address Supplied By: Dial-in User** is set to **No**. You can configure this field even if **Dial-in User** is set to **Yes**, in which case your ZyXEL Device will accept the IP address if the remote peer specifies one; otherwise, an IP address is assigned from the pool.
IP Start Addr	This field is applicable only if you selected **Yes** in the **Dial-In IP Address Supplied By: IP Pool** field. The IP pool contains contiguous IP addresses and this field specifies the first one in the pool. The IP start address is the start of a series of consecutive IP addresses.
IP Count (1, 4)	In this field, enter the number (1 to 4) of addresses in the IP pool. For example, if the starting address is 192.168.135.5 and the count is 2, then the pool will have 192.68.135.5 and 192.68.135.6. The IP count is the number of consecutive IP addresses allowed.
Session Options:	

Table 71 Menu 13 Default Dial-in Setup

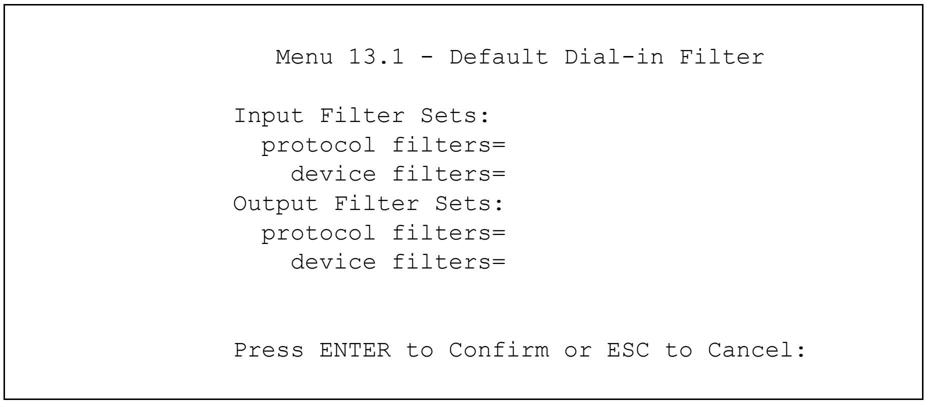
FIELD	DESCRIPTION
Edit Filter Sets	Press [SPACE BAR] and then [ENTER] to select Yes to edit the filter sets. Keep in mind that the filter set(s) will only apply to remote dial-in users but not the remote nodes. **Note:** Spaces and [-] symbol are accepted in this field. For more information on customizing your filter sets, see Chapter 25 on page 234. The default is blank, i.e., no filters.
Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

22.3.1 Default Dial-in Filter

Use **Menu 13.1 - Default Dial-in Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between all dial-in users and your ZyXEL Device. Note that the filter set(s) only applies to the dial-in users but not the remote nodes. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each filter field. The default is no filters.

Spaces are accepted in this field. For more information on defining the filters, see the filters chapter.

Figure 98 Menu 13.1 Default Dial-in Filter



```
                    Menu 13.1 - Default Dial-in Filter

                 Input Filter Sets:
                   protocol filters=
                     device filters=
                 Output Filter Sets:
                   protocol filters=
                     device filters=


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

22.4 Callback Overview

Callback serves two purposes. One is security. When set to callback to a fixed number, an intruder will not gain access to your network even if he/she stole the password from your user, because the ZyXEL Device always calls back to the pre-configured number.

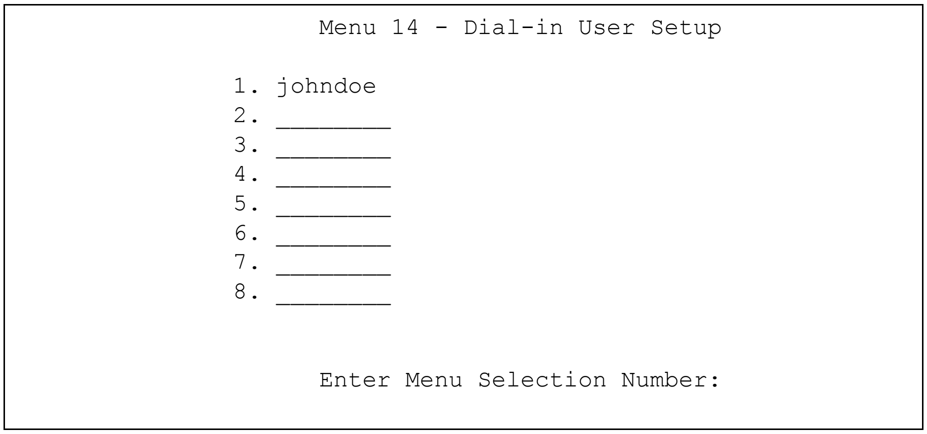
The other is ease of accounting. For instance, your company pays for the connection charges for telecommuting employees and you use your ZyXEL Device as the dial-in server. When you turn on the callback option for the dial-in users, all usage is charged to the company instead of the employees, and your accounting department can avoid the hassles of accountability and reimbursement.

22.5 Dial-In User Setup

This section provides steps on how to set up a remote dial-in user.

1 From the main menu, enter 14 to go to **Menu 14 - Dial-in User Setup**, as shown in the next figure.

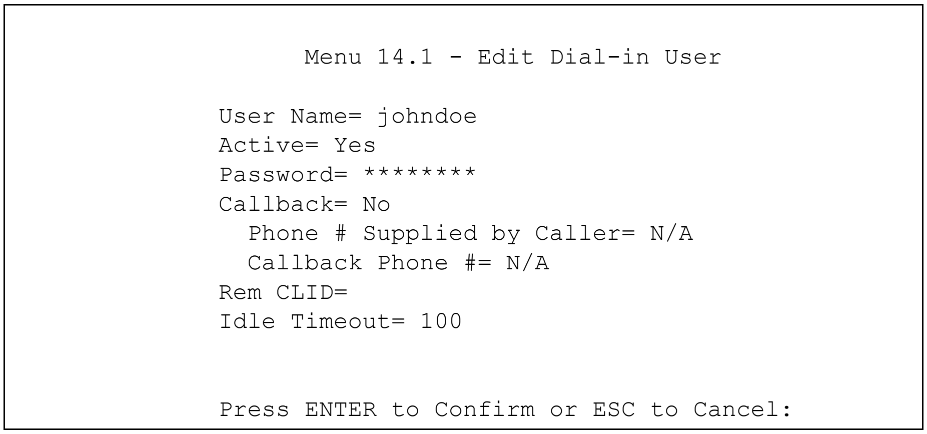
Figure 99 Menu 14 Dial-in User Setup



```
                        Menu 14 - Dial-in User Setup

                  1. johndoe
                  2. ________
                  3. ________
                  4. ________
                  5. ________
                  6. ________
                  7. ________
                  8. ________


                        Enter Menu Selection Number:
```

2 Select one of the users by number, this will bring you to **Menu 14.1 - Edit Dial-in User**, as shown next.

Figure 100 Menu 14.1 Edit Dial-in User



```
                       Menu 14.1 - Edit Dial-in User

                 User Name= johndoe
                 Active= Yes
                 Password= ********
                 Callback= No
                   Phone # Supplied by Caller= N/A
                   Callback Phone #= N/A
                 Rem CLID=
                 Idle Timeout= 100


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

The following table describes the fields in this menu.

Table 72 Menu 14.1 Edit Dial-in User

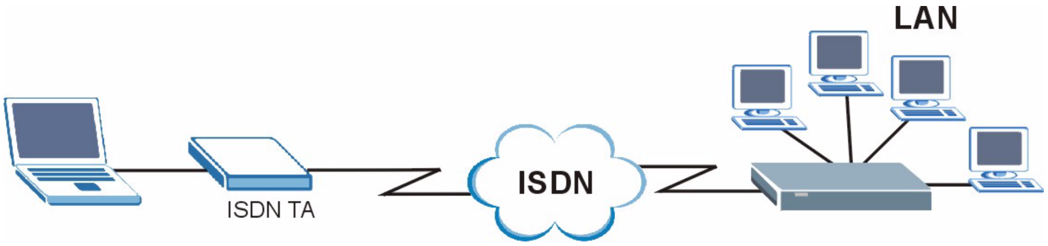
FIELD	DESCRIPTION
User Name	This is a required field. This will be used as the login name for authentication. Choose a descriptive word for login, for example, johndoe.
Active	You can disallow dial-in access to this user by setting this field to inactive. Inactive users are displayed with a [-] (minus sign) at the beginning of the name in menu 14.
Password	Enter the password for the remote dial-in user.
Callback	This field determines if your ZyXEL Device will allow call back to this user upon dial-in. If this option is enabled, your ZyXEL Device will call back to the user if requested. In such a case, your ZyXEL Device will disconnect the initial call from this user and dial back to the specified callback number (see ahead). **No** - The default is no callback. **Optional** - The user can choose to disable callback. **Mandatory** - The user cannot disable callback.
Phone # Supplied by Caller	This option allows the user to specify the call back telephone number on a call-by-call basis. This is useful when your ZyXEL Device returns a call back to a mobile user at different numbers, e.g., a sales rep. in a hotel. If the setting is **Yes**, the user can specify and send to the ZyXEL Device the callback number of his/her choice. The default is **No**, i.e., your ZyXEL Device always calls back to the fixed callback number.
Callback Phone #	If **Phone # Supplied by Caller** is **No**, then this is a required field. Otherwise, a **N/A** will appear in the field. Enter the telephone number to which your ZyXEL Device will call back.
Rem CLID	If you enable **CLID Authen** field in menu 13, then you need to specify the telephone number from which this user calls. Your ZyXEL Device will check the CLID in the incoming call against the CLIDs in the database. If they do not match and **CLID Authen** is **Required**, your ZyXEL Device will not answer the call.
Idle Time-out	Enter the idle time (in seconds). This time-out determines how long the dial-in user can be idle before your ZyXEL Device disconnects the call when the ZyXEL Device is calling back. Idle time is defined as the period of time where there is no data traffic between the dial-in user and your ZyXEL Device. The default is 100 seconds.
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

22.6 Telecommuting Application With Windows Example

Telecommuting enables people to work at remote sites and yet still have access to the resources in the business office. Typically, a telecommuter will use a client workstation with TCP/IP and dial-out capabilities, e.g., a Windows® PC or a Macintosh. For telecommuters to call in to your ZyXEL Device, you need to configure a dial-in user profile for each telecommuter. Additionally, you need to configure the Default Dial-in User Setup to set the operational parameters for all dial-in users.

An example of remote access server for telecommuters is shown next.

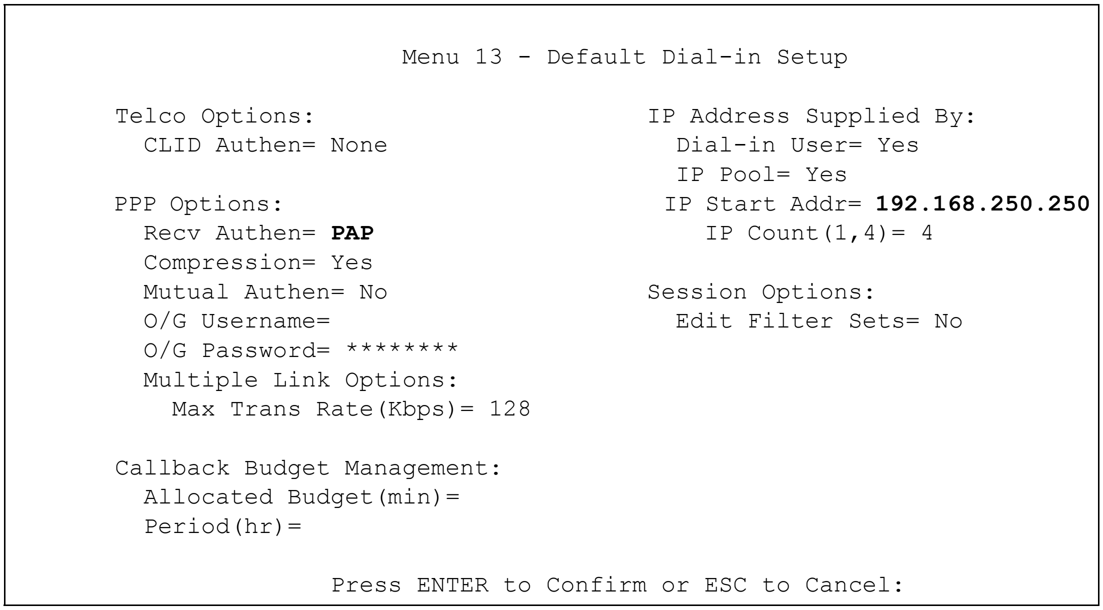
Figure 101 Example of Telecommuting



See the following screens on how to configure your ZyXEL Device if a remote user's computer is running Windows®.

Configuring Menu 13:

Figure 102 Configuring Menu 13 for Remote Access

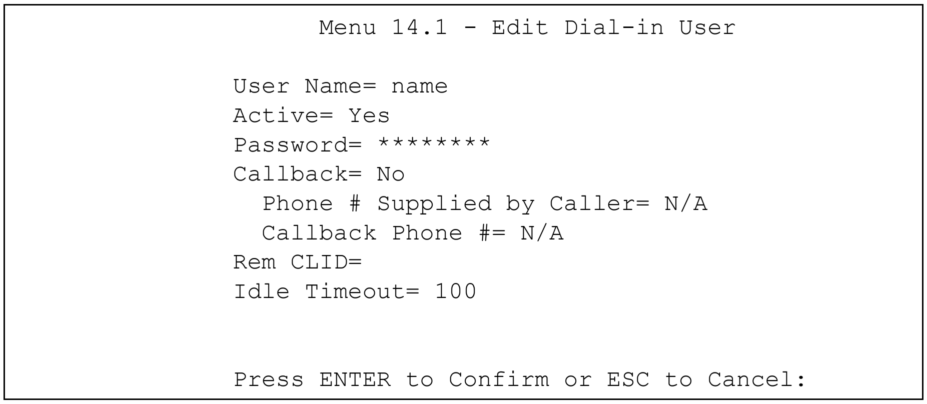


```
                      Menu 13 - Default Dial-in Setup

  Telco Options:                           IP Address Supplied By:
    CLID Authen= None                        Dial-in User= Yes
                                             IP Pool= Yes
  PPP Options:                              IP Start Addr= 192.168.250.250
    Recv Authen= PAP                           IP Count(1,4)= 4
    Compression= Yes
    Mutual Authen= No                      Session Options:
    O/G Username=                            Edit Filter Sets= No
    O/G Password= ********
    Multiple Link Options:
      Max Trans Rate(Kbps)= 128

  Callback Budget Management:
    Allocated Budget(min)=
    Period(hr)=

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

Configuring Menu 14.1

Note: The **User Name** and **Password** must be the same as in Dial-Up Networking in Windows®.

Figure 103 Edit Dial-in-User Example



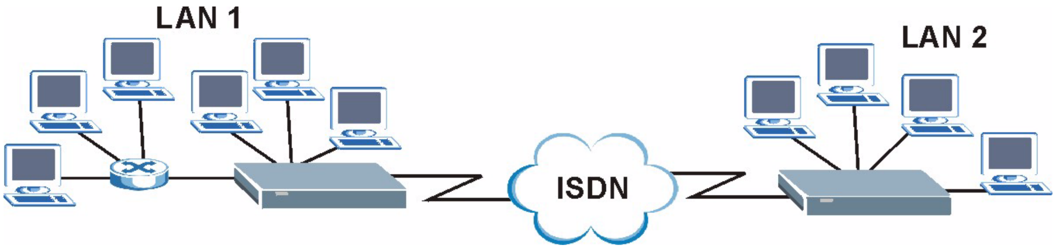
```
                      Menu 14.1 - Edit Dial-in User

                User Name= name
                Active= Yes
                Password= ********
                Callback= No
                  Phone # Supplied by Caller= N/A
                  Callback Phone #= N/A
                Rem CLID=
                Idle Timeout= 100


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

Note: The caller always controls **Idle Timeout**, so this field does not apply when there is callback.

22.7 LAN-to-LAN Server Application Example

Your ZyXEL Device can also be used as a dial-in server for LAN-to-LAN application to provide access for the workstations on a remote network. For your ZyXEL Device to be set up as a LAN-to-LAN server, you need to configure the default dial-in user setup to set the operational parameters for incoming calls. Additionally, you must create a remote node for the router on the remote network (see the chapter on remote node configuration). An example of your ZyXEL Device being used as a LAN-to-LAN server is shown as follows.

Figure 104 Example of a LAN-to-LAN Server Application

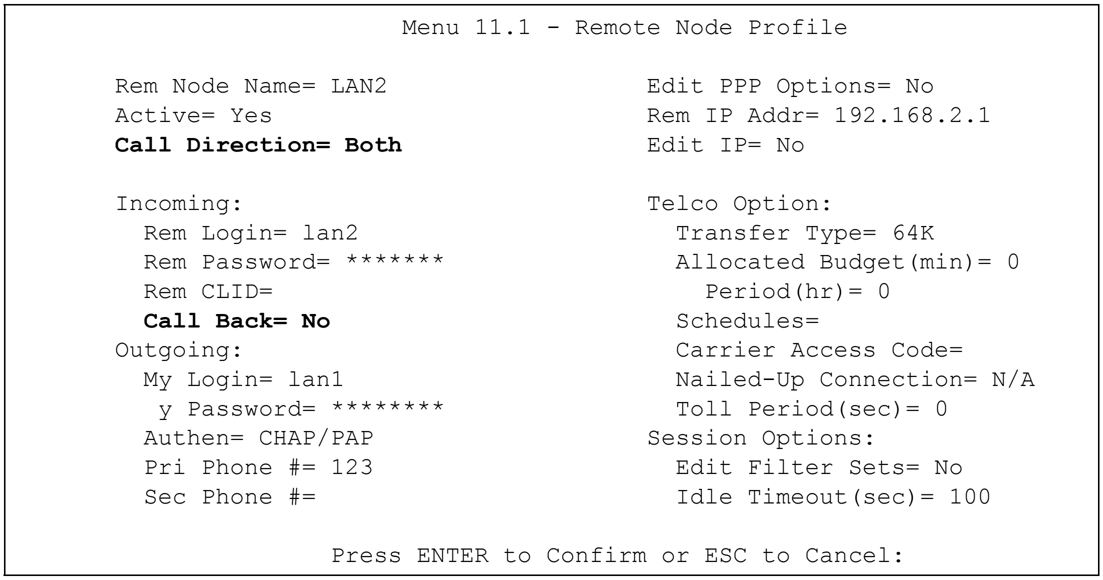


22.7.1 Configuring Callback in LAN-to-LAN Application

In this scenario, LAN 1 first calls LAN 2, then LAN 2 calls back to LAN 1. These are the respective SMT menus.

LAN 1

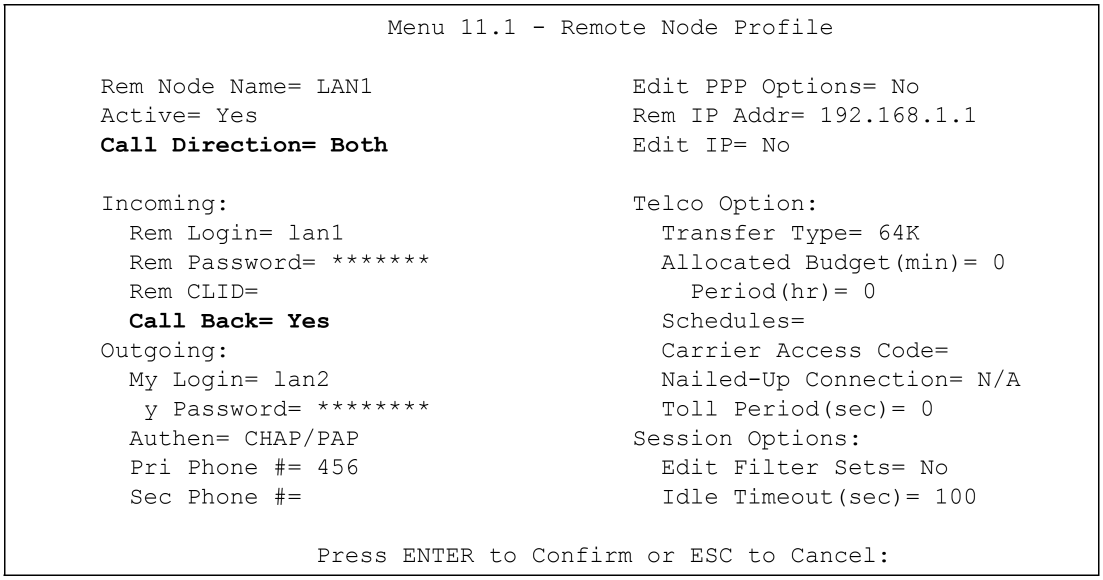
Figure 105 LAN 1 LAN-to-LAN Application



```
                        Menu 11.1 - Remote Node Profile

    Rem Node Name= LAN2                  Edit PPP Options= No
    Active= Yes                          Rem IP Addr= 192.168.2.1
    Call Direction= Both                 Edit IP= No

    Incoming:                            Telco Option:
      Rem Login= lan2                      Transfer Type= 64K
      Rem Password= *******                Allocated Budget(min)= 0
      Rem CLID=                              Period(hr)= 0
      Call Back= No                        Schedules=
    Outgoing:                              Carrier Access Code=
      My Login= lan1                       Nailed-Up Connection= N/A
       y Password= ********                Toll Period(sec)= 0
      Authen= CHAP/PAP                   Session Options:
      Pri Phone #= 123                     Edit Filter Sets= No
      Sec Phone #=                         Idle Timeout(sec)= 100

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

LAN 2

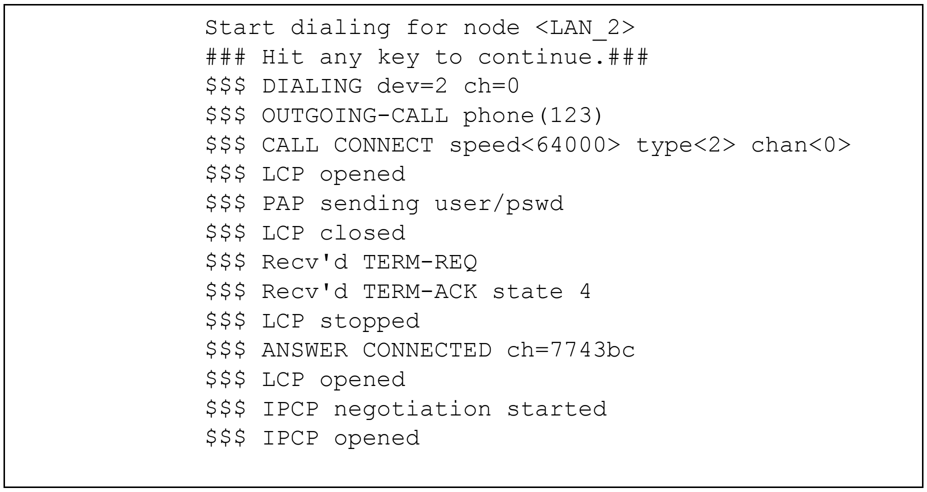
Figure 106 LAN 2 LAN-to-LAN Application



```
                        Menu 11.1 - Remote Node Profile

    Rem Node Name= LAN1                  Edit PPP Options= No
    Active= Yes                          Rem IP Addr= 192.168.1.1
    Call Direction= Both                 Edit IP= No

    Incoming:                            Telco Option:
      Rem Login= lan1                      Transfer Type= 64K
      Rem Password= *******                Allocated Budget(min)= 0
      Rem CLID=                              Period(hr)= 0
      Call Back= Yes                       Schedules=
    Outgoing:                              Carrier Access Code=
      My Login= lan2                       Nailed-Up Connection= N/A
       y Password= ********                Toll Period(sec)= 0
      Authen= CHAP/PAP                   Session Options:
      Pri Phone #= 456                     Edit Filter Sets= No
      Sec Phone #=                         Idle Timeout(sec)= 100

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

Go to menu 24.4.5 of the ZyXEL Device on LAN 1 and enter the numbers that correspond to the menu in LAN 1 above to test callback with your connection.

Figure 107 Testing Callback With Your Connection



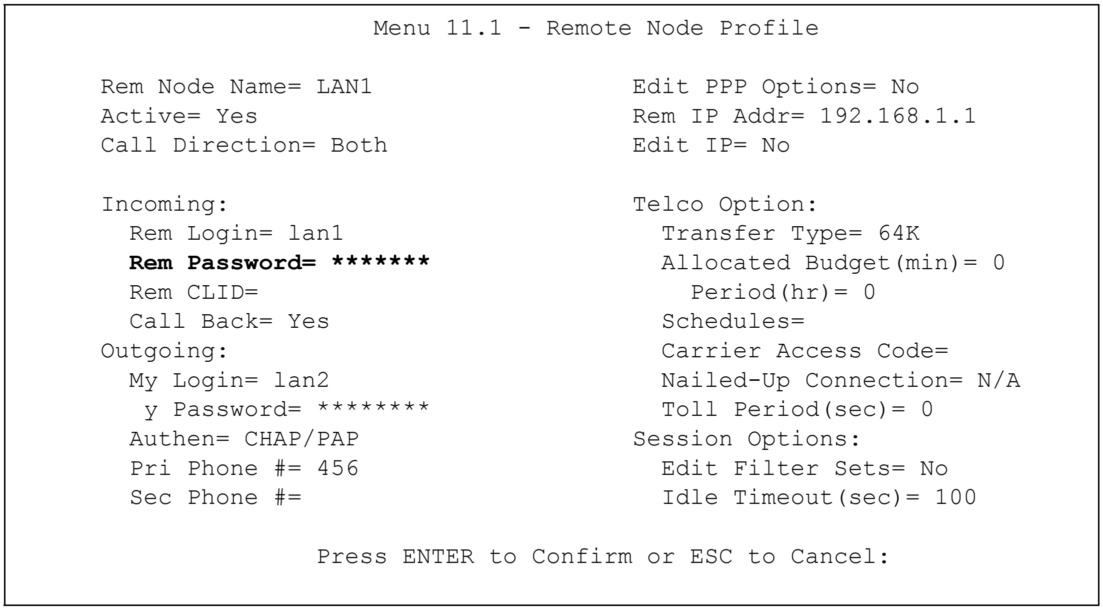
```
Start dialing for node <LAN_2>
### Hit any key to continue.###
$$$ DIALING dev=2 ch=0
$$$ OUTGOING-CALL phone(123)
$$$ CALL CONNECT speed<64000> type<2> chan<0>
$$$ LCP opened
$$$ PAP sending user/pswd
$$$ LCP closed
$$$ Recv'd TERM-REQ
$$$ Recv'd TERM-ACK state 4
$$$ LCP stopped
$$$ ANSWER CONNECTED ch=7743bc
$$$ LCP opened
$$$ IPCP negotiation started
$$$ IPCP opened
```

22.7.2 Configuring With CLID in LAN-to-LAN Application

The only difference between callback with CLID (Calling Line Identification) and callback described above is that you do not pay for the first call, i.e., when the ZyXEL Device on LAN 1 calls the ZyXEL Device on LAN 2. The ZyXEL Device (LAN 2) looks at the ISDN D-channel and verifies that the calling number corresponds with that configured in menu 11. If they do, the ZyXEL Device (LAN 2) hangs up and calls the ZyXEL Device on LAN 1 back.

ZyXEL Device on LAN 2

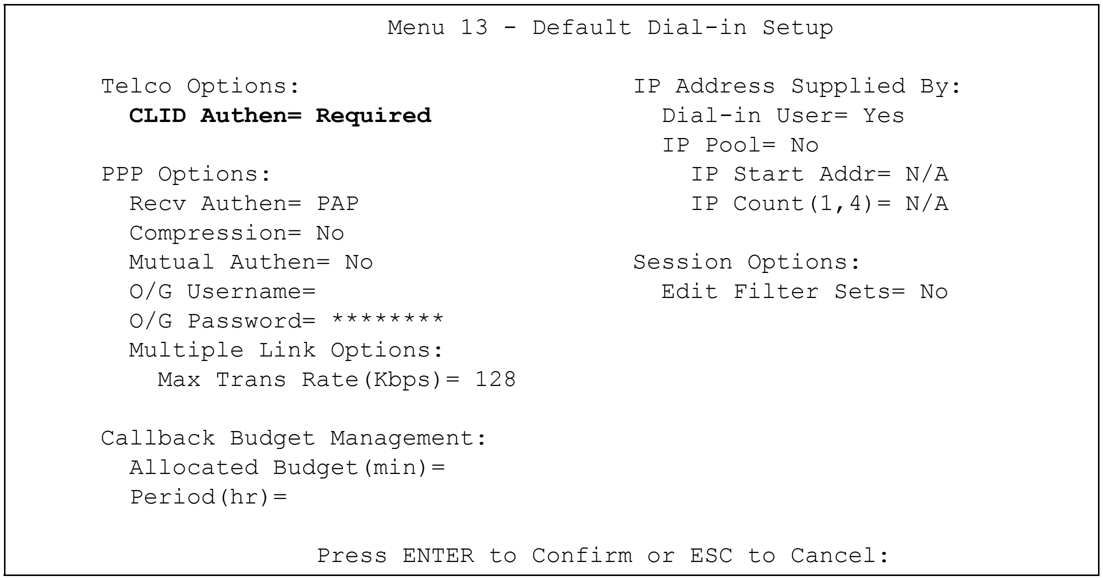
Figure 108 Callback With CLID Configuration



```
                   Menu 11.1 - Remote Node Profile

Rem Node Name= LAN1                  Edit PPP Options= No
Active= Yes                          Rem IP Addr= 192.168.1.1
Call Direction= Both                 Edit IP= No

Incoming:                            Telco Option:
  Rem Login= lan1                      Transfer Type= 64K
  Rem Password= *******                Allocated Budget(min)= 0
  Rem CLID=                              Period(hr)= 0
  Call Back= Yes                       Schedules=
Outgoing:                              Carrier Access Code=
  My Login= lan2                       Nailed-Up Connection= N/A
   y Password= ********                Toll Period(sec)= 0
  Authen= CHAP/PAP                   Session Options:
  Pri Phone #= 456                     Edit Filter Sets= No
  Sec Phone #=                         Idle Timeout(sec)= 100

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

Menu 13

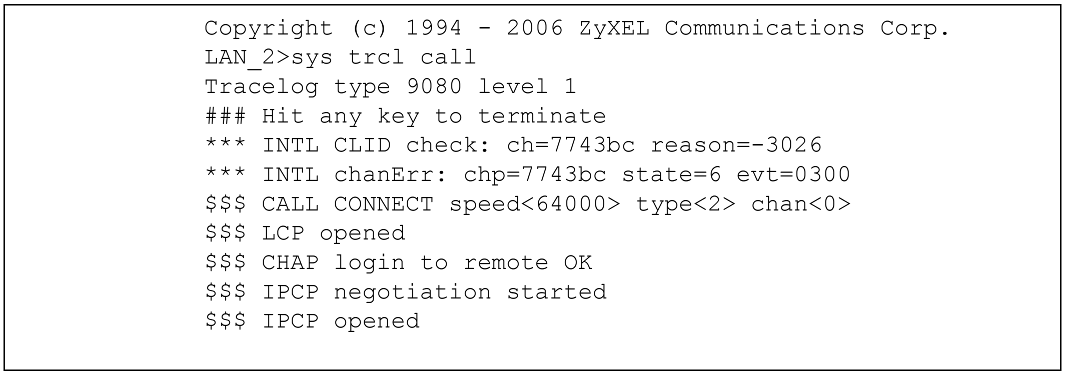
Figure 109 Configuring CLID With Callback



```
                         Menu 13 - Default Dial-in Setup

      Telco Options:                            IP Address Supplied By:
        CLID Authen= Required                     Dial-in User= Yes
                                                  IP Pool= No
      PPP Options:                                  IP Start Addr= N/A
        Recv Authen= PAP                            IP Count(1,4)= N/A
        Compression= No
        Mutual Authen= No                       Session Options:
        O/G Username=                             Edit Filter Sets= No
        O/G Password= ********
        Multiple Link Options:
          Max Trans Rate(Kbps)= 128

      Callback Budget Management:
        Allocated Budget(min)=
        Period(hr)=

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

Go to menu 24.8 (ZyXEL Device on LAN 2) and type "sys trcl call" to test your connection with callback on CLID. The ZyXEL Device displays all communication traces as shown in the next figure. If CLID authentication fails, this means that the calling number does not match the **Rem CLID** number in menu 11.1.

Figure 110 Callback and CLID Connection Test



```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
LAN_2>sys trcl call
Tracelog type 9080 level 1
### Hit any key to terminate
*** INTL CLID check: ch=7743bc reason=-3026
*** INTL chanErr: chp=7743bc state=6 evt=0300
$$$ CALL CONNECT speed<64000> type<2> chan<0>
$$$ LCP opened
$$$ CHAP login to remote OK
$$$ IPCP negotiation started
$$$ IPCP opened
```

CHAPTER 23
Network Address Translation (NAT)

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

23.1 Using NAT

Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device.

23.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See Section 23.3.1 on page 216 for a detailed description of the NAT set for SUA. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

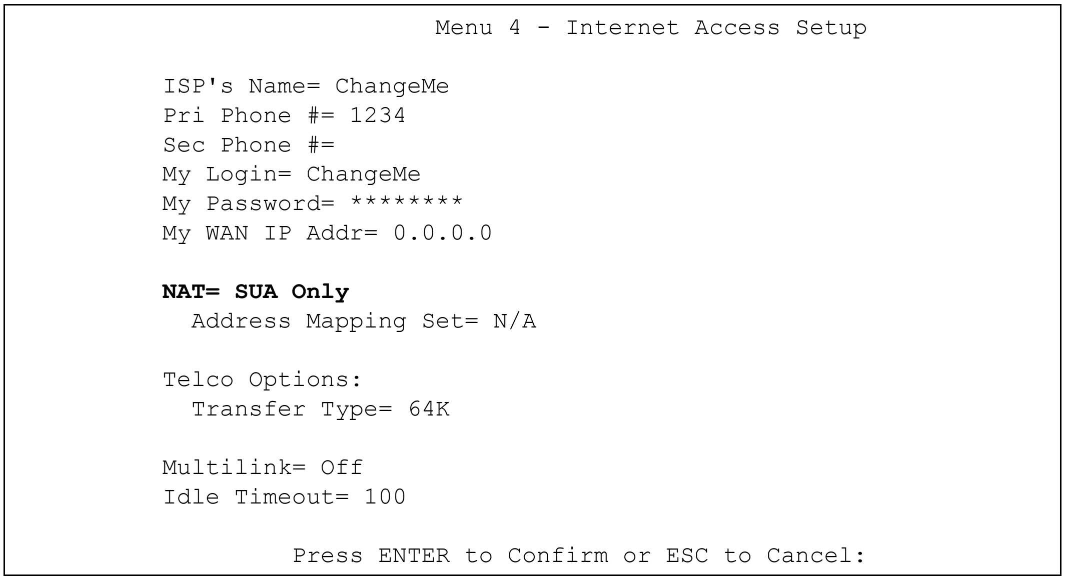
Note: Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.

Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device.

23.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

Figure 111 Menu 4: Applying NAT for Internet Access



```
                         Menu 4 - Internet Access Setup

          ISP's Name= ChangeMe
          Pri Phone #= 1234
          Sec Phone #=
          My Login= ChangeMe
          My Password= ********
          My WAN IP Addr= 0.0.0.0

          NAT= SUA Only
            Address Mapping Set= N/A

          Telco Options:
            Transfer Type= 64K

          Multilink= Off
          Idle Timeout= 100

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

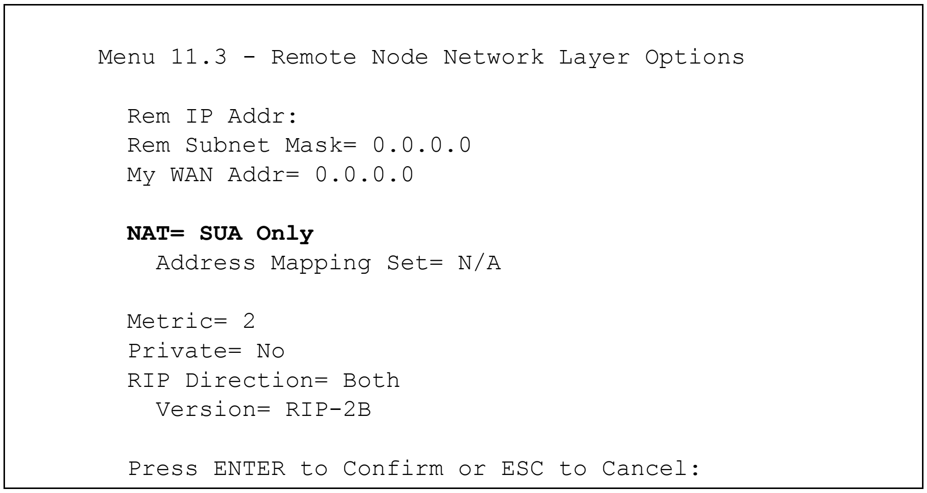
The following figure shows how you apply NAT to the remote node in menu 11.1.

1 Enter 11 from the main menu.

2 When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.

3 Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

Figure 112 Menu 11.3 Applying NAT to the Remote Node



```
      Menu 11.3 - Remote Node Network Layer Options

        Rem IP Addr:
        Rem Subnet Mask= 0.0.0.0
        My WAN Addr= 0.0.0.0

        NAT= SUA Only
          Address Mapping Set= N/A

        Metric= 2
        Private= No
        RIP Direction= Both
          Version= RIP-2B

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

The following table describes the options for Network Address Translation.

Table 73 Applying NAT in Menus 4 & 11.3

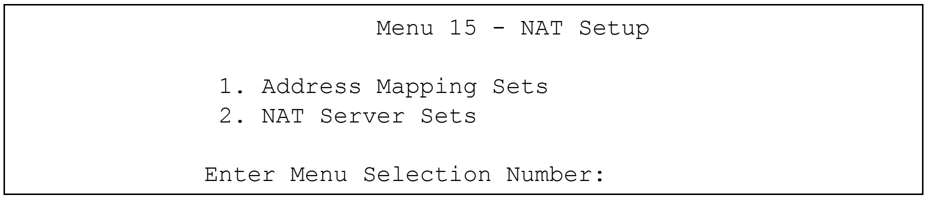
FIELD	DESCRIPTION
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device. The SMT uses the address mapping set that you configure and enter in the **Address Mapping Set** field (menu 15.1 - see section). When you select **Full Feature** you must configure at least one address mapping set.
	Select **None** to disable NAT.
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (menu 15.1 - see section). Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.

23.3 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in the chapter on NAT web configurator screens for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

Figure 113 Menu 15 NAT Setup

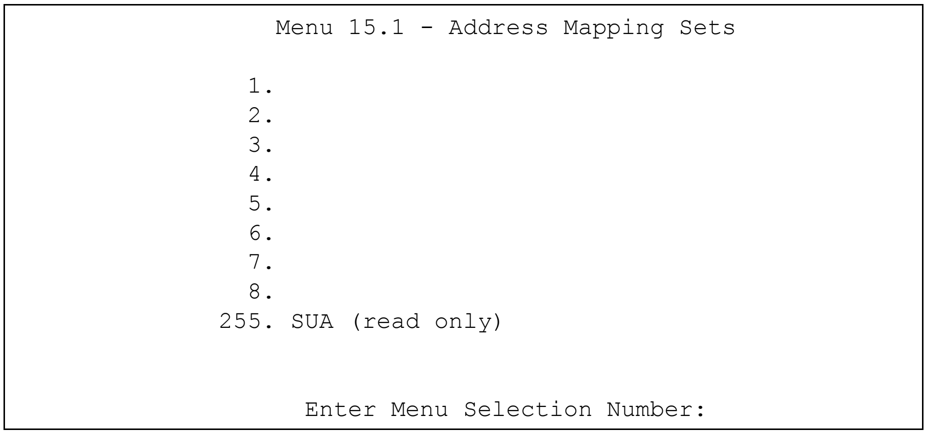


```
                         Menu 15 - NAT Setup

              1. Address Mapping Sets
              2. NAT Server Sets

             Enter Menu Selection Number:
```

23.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 - Address Mapping Sets**.

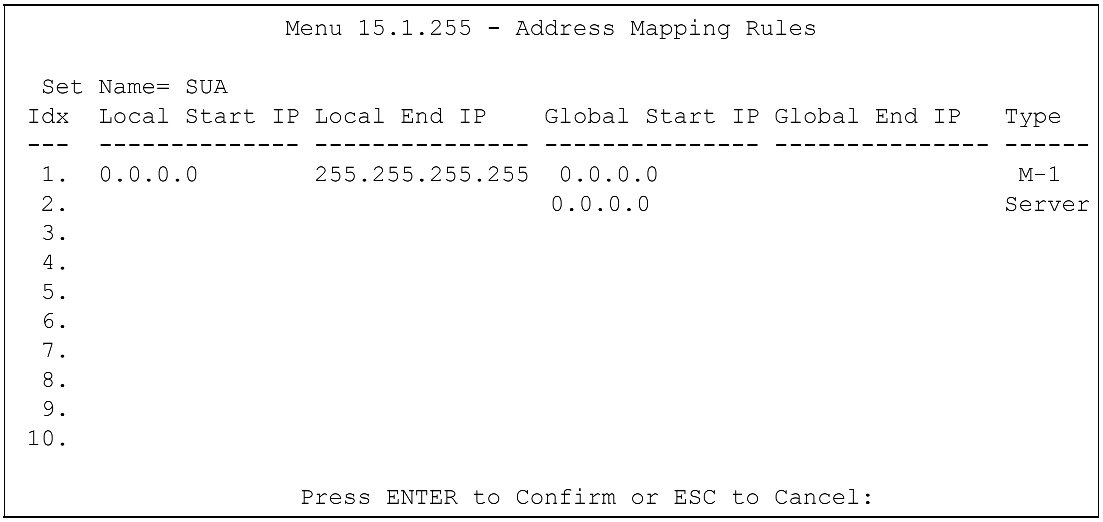
Figure 114 Menu 15.1 Address Mapping Sets



```
                  Menu 15.1 - Address Mapping Sets

                1.
                2.
                3.
                4.
                5.
                6.
                7.
                8.
              255. SUA (read only)


                    Enter Menu Selection Number:
```

Enter 255 to display the next screen, (see Section 23.1.1 on page 214). The fields in this menu cannot be changed.

Figure 115 Menu 15.1.255 SUA Address Mapping Rules



```
                   Menu 15.1.255 - Address Mapping Rules

  Set Name= SUA
 Idx  Local Start IP Local End IP    Global Start IP Global End IP   Type
 ---  -------------- --------------- --------------- --------------- ------
  1.  0.0.0.0        255.255.255.255  0.0.0.0                         M-1
  2.                                 0.0.0.0                         Server
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

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

The following table explains the fields in this menu.

Table 74 Menu 15.1.255 SUA Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	**Local Start IP** is the starting local IP address (ILA).
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.

Table 74 Menu 15.1.255 SUA Address Mapping Rules

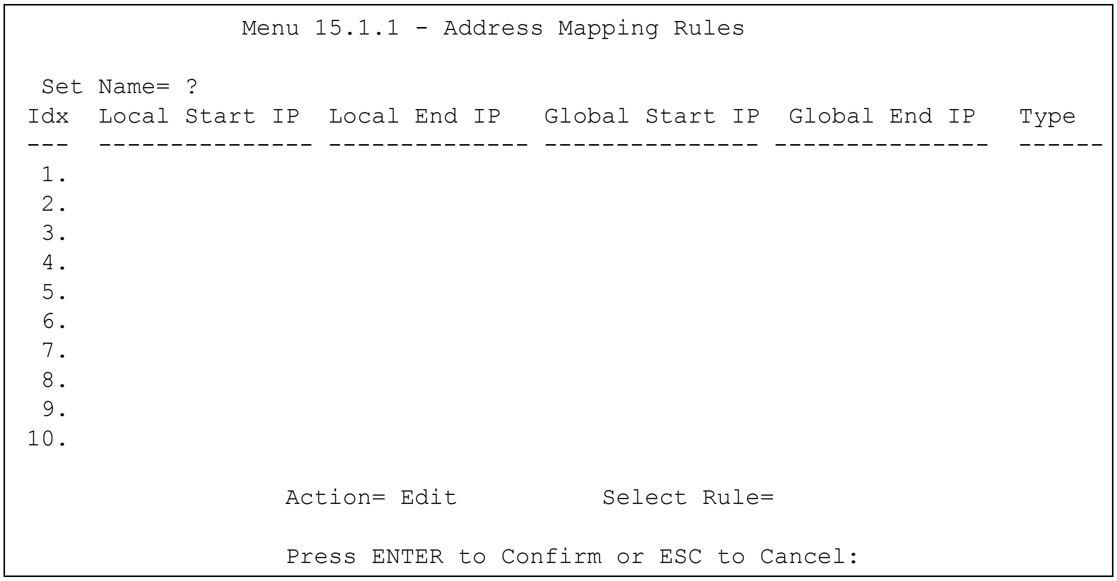
FIELD	DESCRIPTION
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Note: Menu 15.1.255 is read-only.

23.3.1.1 User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

Figure 116 Menu 15.1.1 First Set



```
                Menu 15.1.1 - Address Mapping Rules

 Set Name= ?
Idx  Local Start IP  Local End IP   Global Start IP  Global End IP   Type
---  --------------- -------------- --------------- ---------------  ------
 1.
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                   Action= Edit          Select Rule=

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

Note: If the **Set Name** field is left blank, the entire set will be deleted.

The **Type**, **Local** and **Global Start/End IPs** are configured in menu 15.1.1.1 (described later) and the values are displayed here.

23.3.1.2 Ordering Your 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 as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 75 Menu 15.1.1 First Set

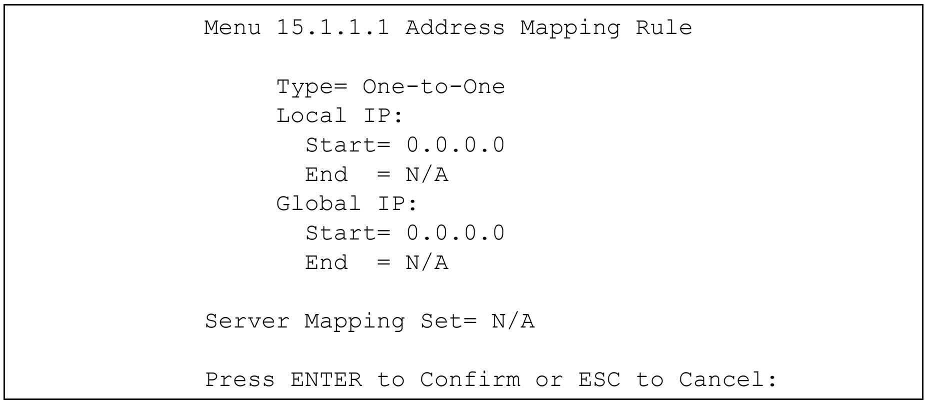
FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see the following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.

Note: You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

Note: An End IP address must be numerically greater than its corresponding IP Start address.

Figure 117 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set



```
              Menu 15.1.1.1 Address Mapping Rule

                   Type= One-to-One
                   Local IP:
                     Start= 0.0.0.0
                     End  = N/A
                   Global IP:
                     Start= 0.0.0.0
                     End  = N/A

              Server Mapping Set= N/A

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

The following table explains the fields in this menu.

Table 76 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section* for an example.
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.
Start	This is the starting local IP address (ILA).
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.
Global IP	
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.
End	This is the ending inside global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.
Server Mapping Set	Only available when **Type** is set to **Server**. Type a number from 1 to 10 to choose a server set from menu 15.2.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

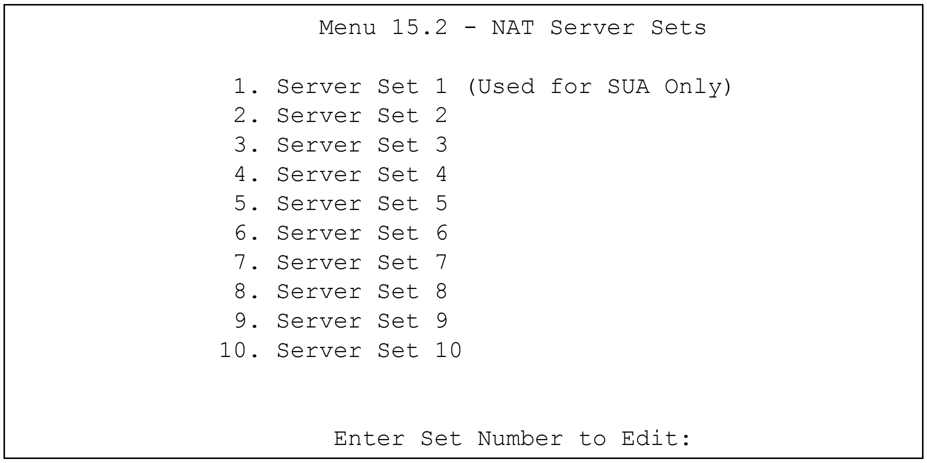
23.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

1 Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.

2 Enter 2 to display **Menu 15.2 - NAT Server Setup** as shown next.

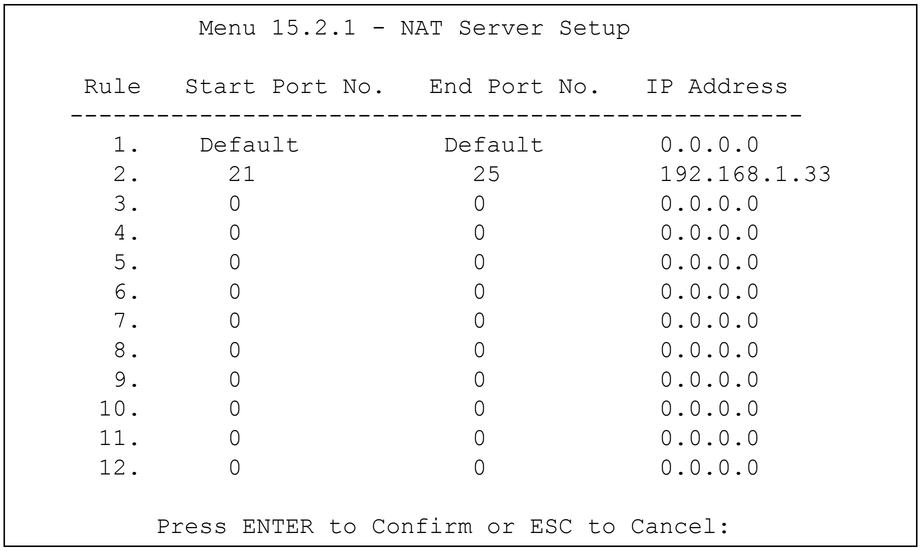
Figure 118 Menu 15.2 NAT Server Sets



```
                     Menu 15.2 - NAT Server Sets

               1. Server Set 1 (Used for SUA Only)
               2. Server Set 2
               3. Server Set 3
               4. Server Set 4
               5. Server Set 5
               6. Server Set 6
               7. Server Set 7
               8. Server Set 8
               9. Server Set 9
              10. Server Set 10



                      Enter Set Number to Edit:
```

3 Enter 1 to go to **Menu 15.2.1 NAT Server Setup** as follows.

Figure 119 Menu 15.2.1 NAT Server Setup



```
              Menu 15.2.1 - NAT Server Setup

      Rule   Start Port No.   End Port No.   IP Address
     ---------------------------------------------------
        1.     Default          Default        0.0.0.0
        2.       21               25           192.168.1.33
        3.       0                0            0.0.0.0
        4.       0                0            0.0.0.0
        5.       0                0            0.0.0.0
        6.       0                0            0.0.0.0
        7.       0                0            0.0.0.0
        8.       0                0            0.0.0.0
        9.       0                0            0.0.0.0
       10.       0                0            0.0.0.0
       11.       0                0            0.0.0.0
       12.       0                0            0.0.0.0

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

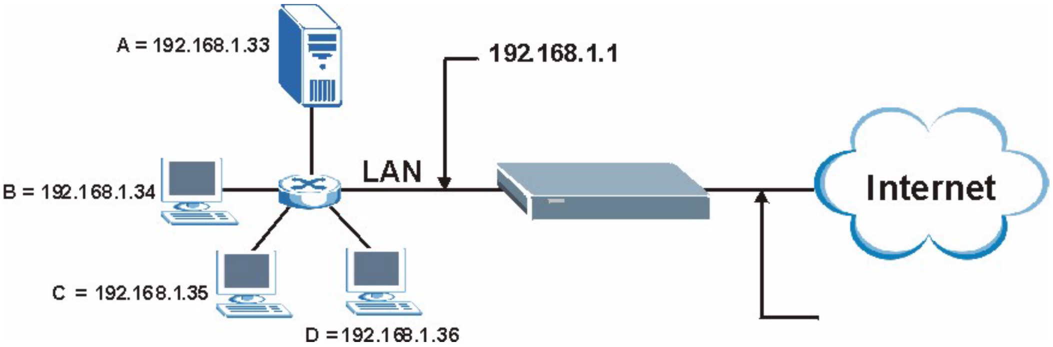
4 Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

5 Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

6 Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. **A** is the FTP/Telnet/SMTP server.

Figure 120 Multiple Servers Behind NAT Example



23.5 General NAT Examples

The following are some examples of NAT configuration.

23.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where the ILAs (Inside Local Addresses) of computers **A** through **D** map to one dynamic IGA (Inside Global Address) assigned by your ISP.

Figure 121 NAT Example 1

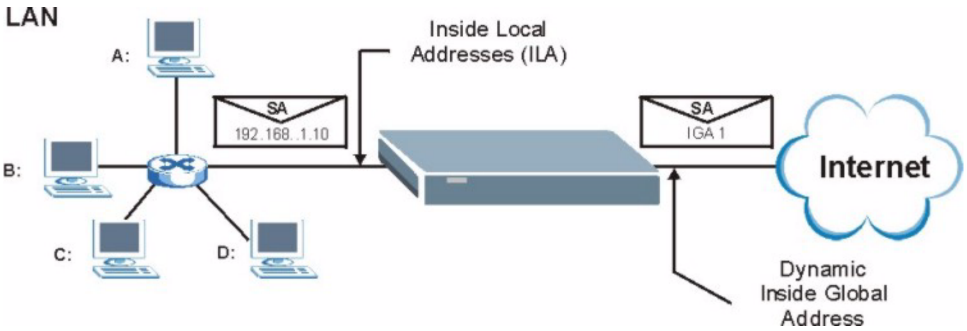
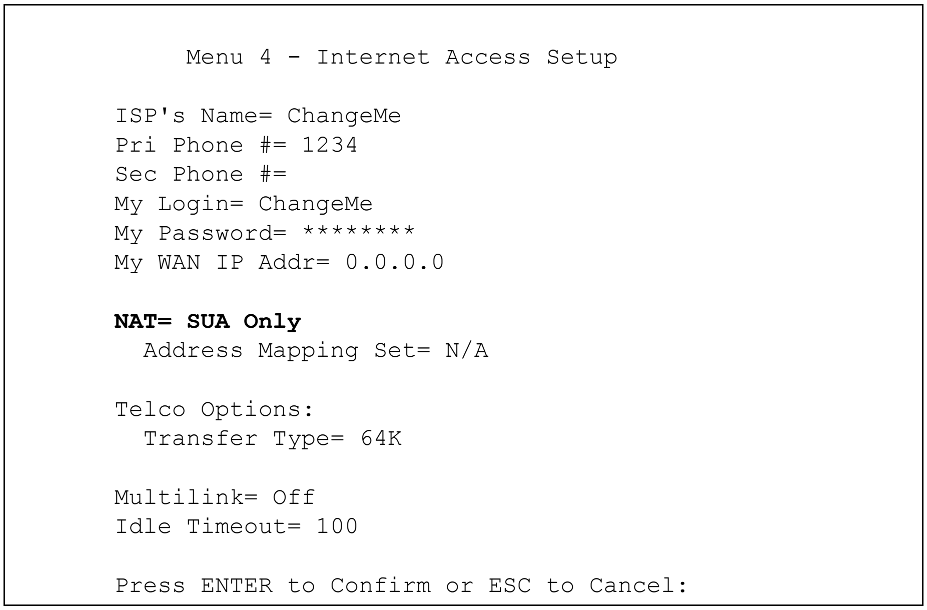


Figure 122 Menu 4 Internet Access & NAT Example



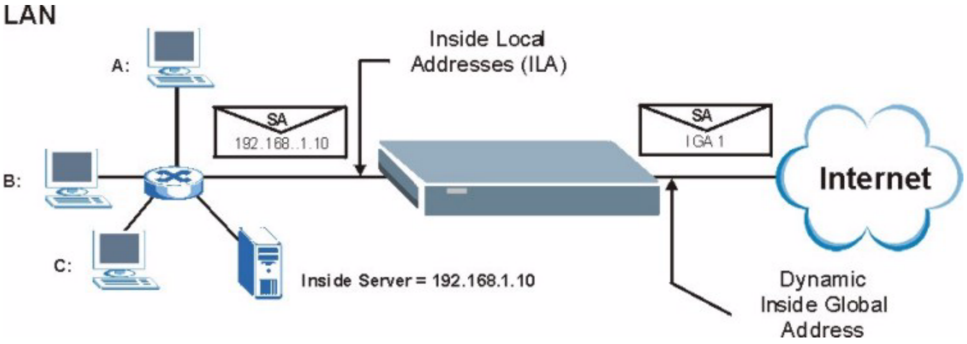
```
          Menu 4 - Internet Access Setup

     ISP's Name= ChangeMe
     Pri Phone #= 1234
     Sec Phone #=
     My Login= ChangeMe
     My Password= ********
     My WAN IP Addr= 0.0.0.0

     NAT= SUA Only
       Address Mapping Set= N/A

     Telco Options:
       Transfer Type= 64K

     Multilink= Off
     Idle Timeout= 100

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

From menu 4, choose the **SUA Only** option from the **NAT** field. This is the Many-to-One mapping discussed in Section 23.5 on page 222. The **SUA Only** read-only option from the **NAT** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

23.5.2 Example 2: Internet Access with an Inside Server

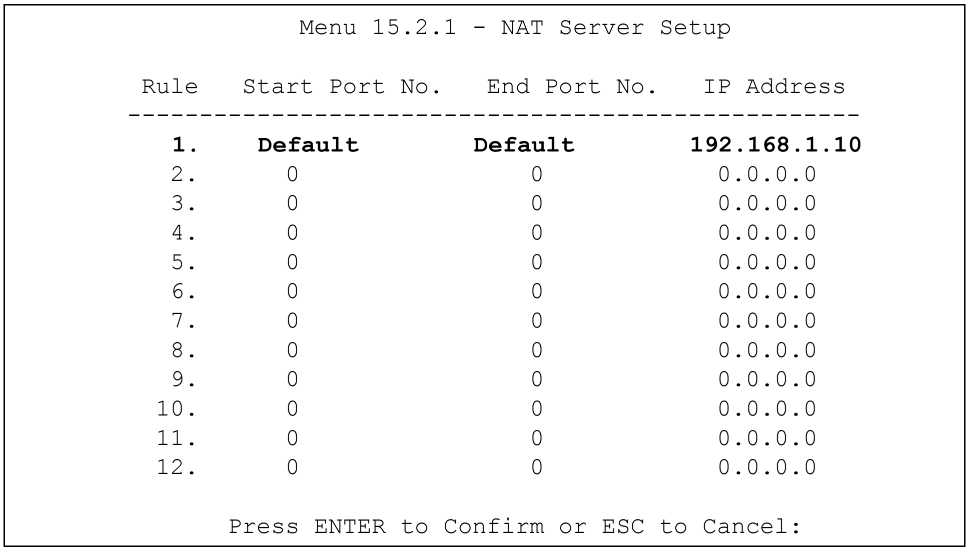
The dynamic Inside Global Address is assigned by the ISP.

Figure 123 NAT Example 2


LAN
A:
B:
C:
Inside Local Addresses (ILA)
SA
192.168..1.10
SA
IGA 1
Internet
Inside Server = 192.168.1.10
Dynamic Inside Global Address

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2.1 to specify the Inside Server behind the NAT as shown in the next figure.

Figure 124 Menu 15.2.1 Specifying an Inside Server



```
                      Menu 15.2.1 - NAT Server Setup

           Rule   Start Port No.   End Port No.   IP Address
          ---------------------------------------------------
             1.     Default          Default        192.168.1.10
             2.       0                0              0.0.0.0
             3.       0                0              0.0.0.0
             4.       0                0              0.0.0.0
             5.       0                0              0.0.0.0
             6.       0                0              0.0.0.0
             7.       0                0              0.0.0.0
             8.       0                0              0.0.0.0
             9.       0                0              0.0.0.0
            10.       0                0              0.0.0.0
            11.       0                0              0.0.0.0
            12.       0                0              0.0.0.0

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

23.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

1 Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

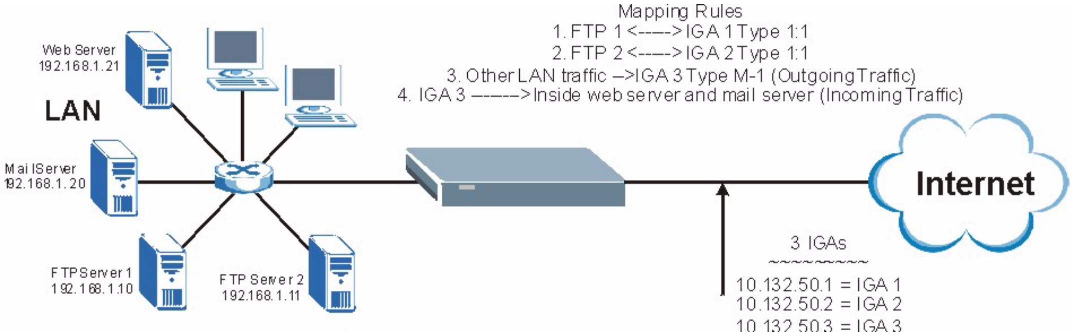
2 Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

3 Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

4 You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

Figure 125 NAT Example 3



1 In this case you need to configure **Address Mapping Set 1** from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **NAT** field (in menu 4 or menu 11.3). See Figure 126 on page 225.

2 Then enter 15 from the main menu.

3 Enter 1 to configure the address mapping Sets.

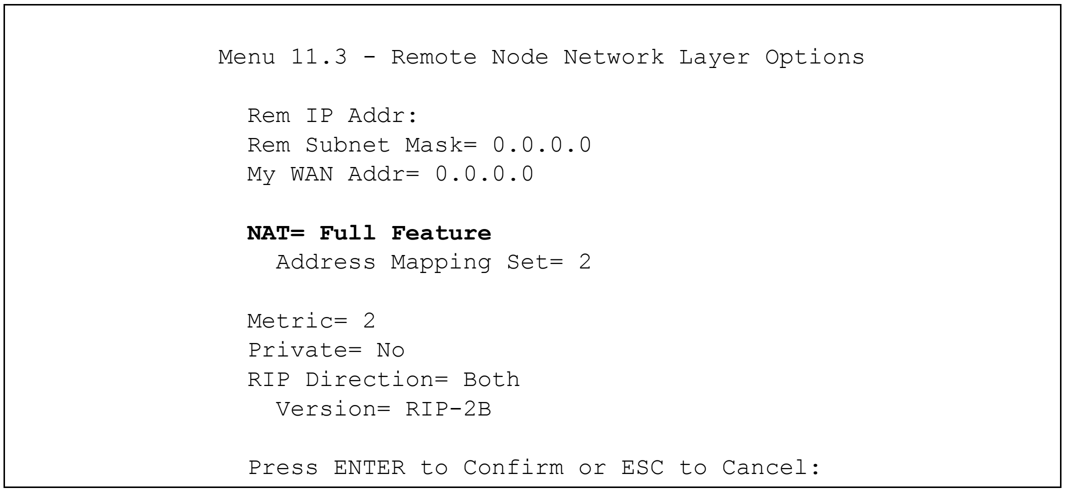
4 Enter 1 to begin configuring this new set. Enter a **Set Name**, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). See Figure 127 on page 225.

6 Repeat the previous step for rules 2 to 4 as outlined above.

7 When finished, menu 15.1.1.1 should look like as shown in Figure 128 on page 226.

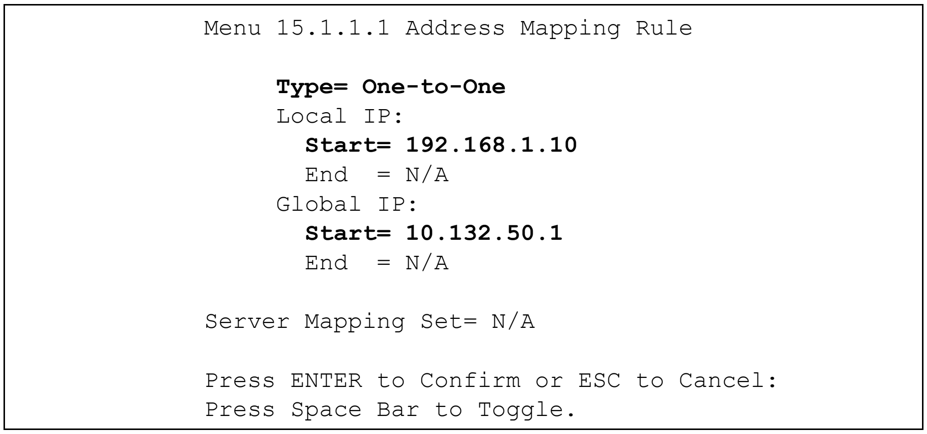
Figure 126 NAT Example 3: Menu 11.3



```
              Menu 11.3 - Remote Node Network Layer Options

                Rem IP Addr:
                Rem Subnet Mask= 0.0.0.0
                My WAN Addr= 0.0.0.0

                NAT= Full Feature
                  Address Mapping Set= 2

                Metric= 2
                Private= No
                RIP Direction= Both
                  Version= RIP-2B

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

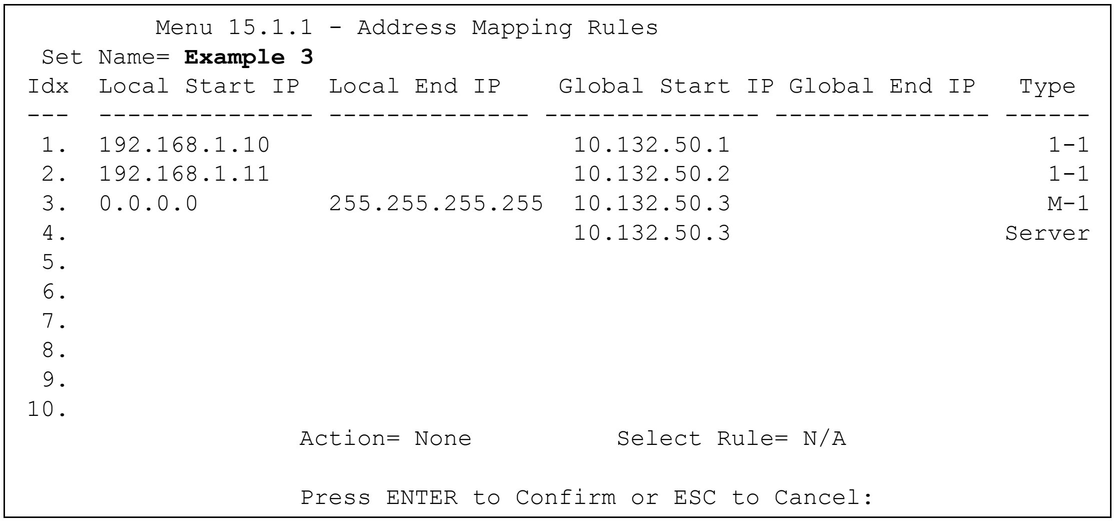
The following figures show how to configure the first rule.

Figure 127 Example 3: Menu 15.1.1.1



```
             Menu 15.1.1.1 Address Mapping Rule

                  Type= One-to-One
                  Local IP:
                    Start= 192.168.1.10
                    End  = N/A
                  Global IP:
                    Start= 10.132.50.1
                    End  = N/A

             Server Mapping Set= N/A

             Press ENTER to Confirm or ESC to Cancel:
             Press Space Bar to Toggle.
```

Figure 128 Example 3: Final Menu 15.1.1



```
         Menu 15.1.1 - Address Mapping Rules
 Set Name= Example 3
Idx  Local Start IP  Local End IP    Global Start IP Global End IP   Type
---  --------------- -------------- --------------- --------------- ------
 1.  192.168.1.10                     10.132.50.1                     1-1
 2.  192.168.1.11                     10.132.50.2                     1-1
 3.  0.0.0.0         255.255.255.255  10.132.50.3                     M-1
 4.                                   10.132.50.3                  Server
 5.
 6.
 7.
 8.
 9.
10.
                   Action= None          Select Rule= N/A

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

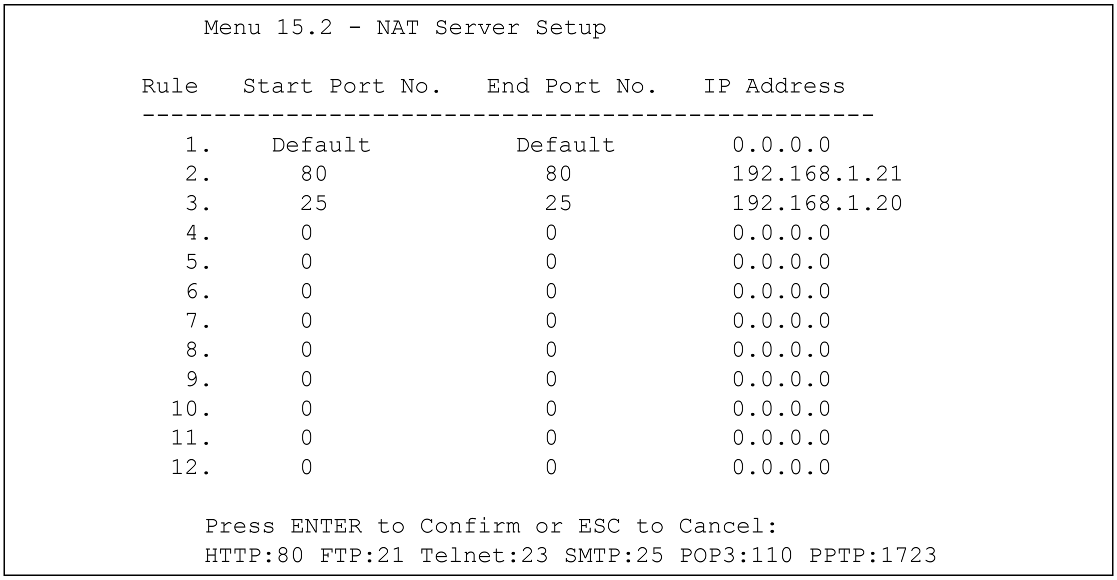
Now configure the IGA3 to map to our web server and mail server on the LAN.

8 Enter 15 from the main menu.

9 Enter 2 in **Menu 15 - NAT Setup**.

10Enter 1 in **Menu 15.2 - NAT Server Setup** to see the following menu. Configure it as shown.

Figure 129 Example 3: Menu 15.2

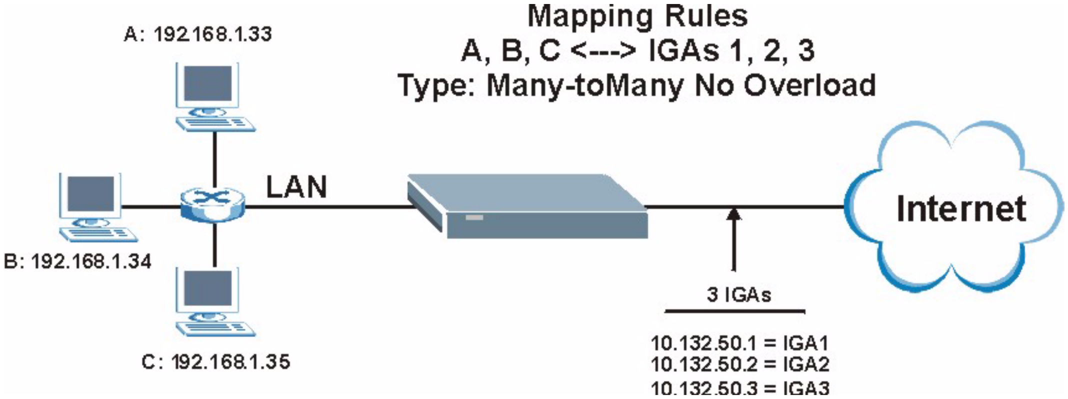


```
    Menu 15.2 - NAT Server Setup

Rule   Start Port No.   End Port No.   IP Address
---------------------------------------------------
   1.    Default          Default        0.0.0.0
   2.      80               80           192.168.1.21
   3.      25               25           192.168.1.20
   4.      0                0            0.0.0.0
   5.      0                0            0.0.0.0
   6.      0                0            0.0.0.0
   7.      0                0            0.0.0.0
   8.      0                0            0.0.0.0
   9.      0                0            0.0.0.0
  10.      0                0            0.0.0.0
  11.      0                0            0.0.0.0
  12.      0                0            0.0.0.0

    Press ENTER to Confirm or ESC to Cancel:
    HTTP:80 FTP:21 Telnet:23 SMTP:25 POP3:110 PPTP:1723
```

23.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

Figure 130 NAT Example 4



Note: Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won’t work through NAT even when using **One-to-One** and **Many-to-Many No Overload** mapping types.

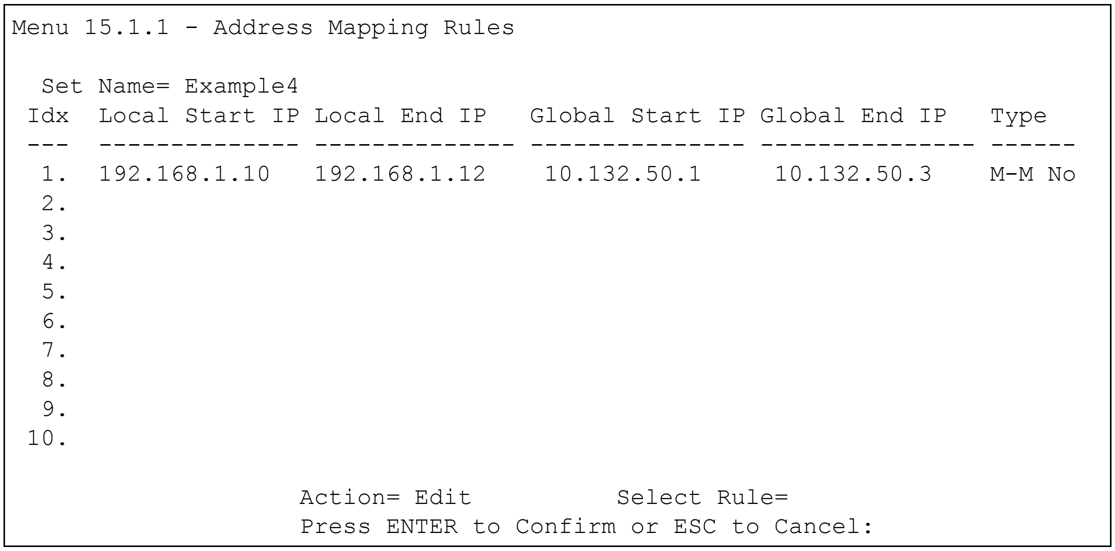
Follow the steps outlined in example 3 to configure these two menus as follows

Figure 131 Example 4: Menu 15.1.1.1 Address Mapping Rule.

```
              Menu 15.1.1.1 Address Mapping Rule

                   Type= Many-to-Many No Overload
                   Local IP:
                     Start= 192.168.1.10
                     End  = 192.168.1.12
                   Global IP:
                     Start= 10.132.50.1
                     End  = 10.132.50.3

              Server Mapping Set= N/A

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

After you’ve configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

Figure 132 Example 4: Menu 15.1.1 Address Mapping Rules



```
Menu 15.1.1 - Address Mapping Rules

  Set Name= Example4
 Idx  Local Start IP Local End IP   Global Start IP Global End IP   Type
 ---  -------------- -------------- --------------- --------------- ------
  1.  192.168.1.10   192.168.1.12    10.132.50.1     10.132.50.3    M-M No
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

                    Action= Edit          Select Rule=
                    Press ENTER to Confirm or ESC to Cancel:
```

CHAPTER 24
Enabling the Firewall

This chapter shows you how to get started with the ZyXEL Device firewall.

24.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management (see the Remote Management chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

24.2 Access Methods

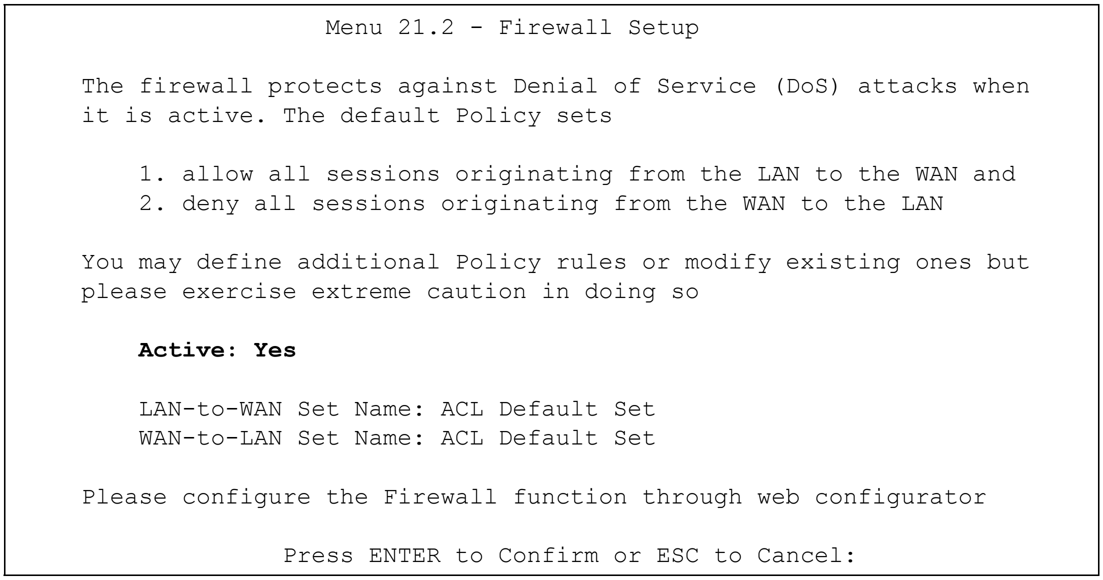
The web configurator is, by far, the most comprehensive firewall configuration tool your ZyXEL Device has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

24.3 Enabling the Firewall

From the main menu enter 21 to go to **Menu 21 - Filter and Firewall Setup** to display the screen shown next**.**

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

Figure 133 Menu 21.2 Firewall Setup



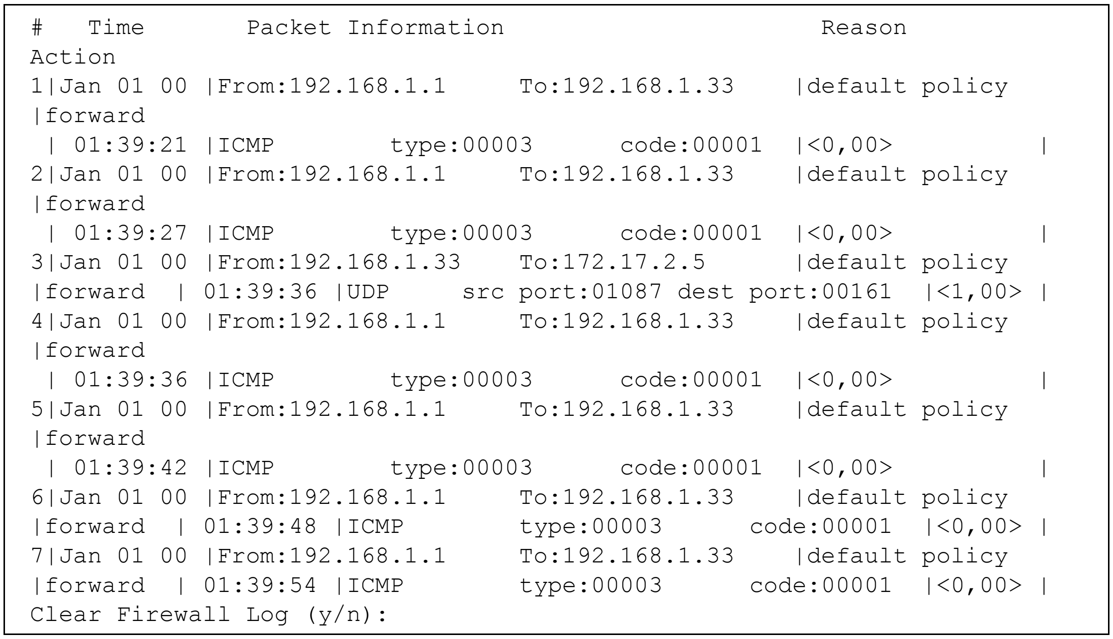
```
                      Menu 21.2 - Firewall Setup

     The firewall protects against Denial of Service (DoS) attacks when
     it is active. The default Policy sets

         1. allow all sessions originating from the LAN to the WAN and
         2. deny all sessions originating from the WAN to the LAN

     You may define additional Policy rules or modify existing ones but
     please exercise extreme caution in doing so

         Active: Yes

         LAN-to-WAN Set Name: ACL Default Set
         WAN-to-LAN Set Name: ACL Default Set

     Please configure the Firewall function through web configurator

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

Note: Use the web configurator or the command interpreter to configure the firewall rules.

24.3.1 Viewing the Firewall Log

In menu 21, enter 3 to view the firewall log. An example of a firewall log is shown next.

Figure 134 Example Firewall Log



```
#   Time       Packet Information                      Reason
Action
1|Jan 01 00 |From:192.168.1.1     To:192.168.1.33    |default policy
|forward
 | 01:39:21 |ICMP        type:00003      code:00001  |<0,00>          |
2|Jan 01 00 |From:192.168.1.1     To:192.168.1.33    |default policy
|forward
 | 01:39:27 |ICMP        type:00003      code:00001  |<0,00>          |
3|Jan 01 00 |From:192.168.1.33    To:172.17.2.5      |default policy
|forward  | 01:39:36 |UDP     src port:01087 dest port:00161  |<1,00> |
4|Jan 01 00 |From:192.168.1.1     To:192.168.1.33    |default policy
|forward
 | 01:39:36 |ICMP        type:00003      code:00001  |<0,00>          |
5|Jan 01 00 |From:192.168.1.1     To:192.168.1.33    |default policy
|forward
 | 01:39:42 |ICMP        type:00003      code:00001  |<0,00>          |
6|Jan 01 00 |From:192.168.1.1     To:192.168.1.33    |default policy
|forward  | 01:39:48 |ICMP        type:00003      code:00001  |<0,00> |
7|Jan 01 00 |From:192.168.1.1     To:192.168.1.33    |default policy
|forward  | 01:39:54 |ICMP        type:00003      code:00001  |<0,00> |
Clear Firewall Log (y/n):
```

Table 77 View Firewall Log

FIELD	DESCRIPTION	EXAMPLES
#	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log wraps around and the old logs are lost.	23
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real time; otherwise the clock will start at 2000/01/01 00:00:00 the last time the ZyXEL Device was reset.	mm:dd:yy: e.g., Jan 1 00 hh:mm:ss: e.g., 00:00:00
Packet Information	This field lists packet information such as protocol and src/dest port numbers (TCP, UDP), or protocol, type and code (ICMP).	From and To IP addresses Protocol and port numbers
Reason	This field states the reason for the log; i.e., was the rule matched, did not match or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol.
	This is a log for a DoS attack.	attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop or syn flood
Action	This field displays whether the packet was blocked or forwarded. None means that no action is dictated by this rule.	block, forward or none
After viewing the firewall log, ENTER "y" to clear the log or "n" to retain it. With either option you will be returned to **Menu 21- Filter and Firewall Setup**.		

24.3.2 Example E-mail Log

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.

```
Subject:
        Firewall Alert From ZyXEL Device
   Date:
        Fri, 07 Apr 2006 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
```

CHAPTER 25
Filter Configuration

This chapter shows you how to create and apply filters.

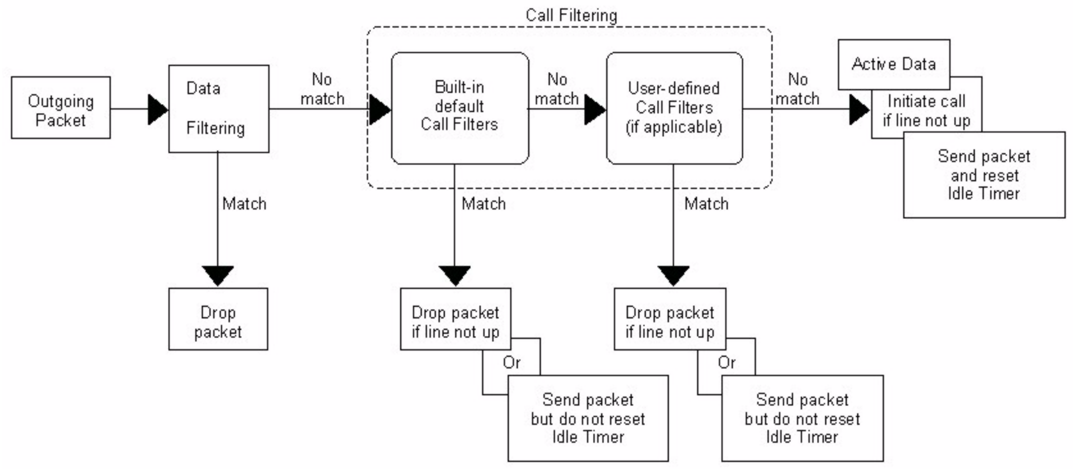
25.1 Introduction to Filters

Your ZyXEL Device uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your ZyXEL Device has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your ZyXEL Device applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

Figure 135 Outgoing Packet Filtering Process


Call Filtering
Outgoing Packet
Data Filtering
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset Idle Timer
Drop packet if line not up
Or
Send packet but do not reset Idle Timer

For incoming packets, your ZyXEL Device applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

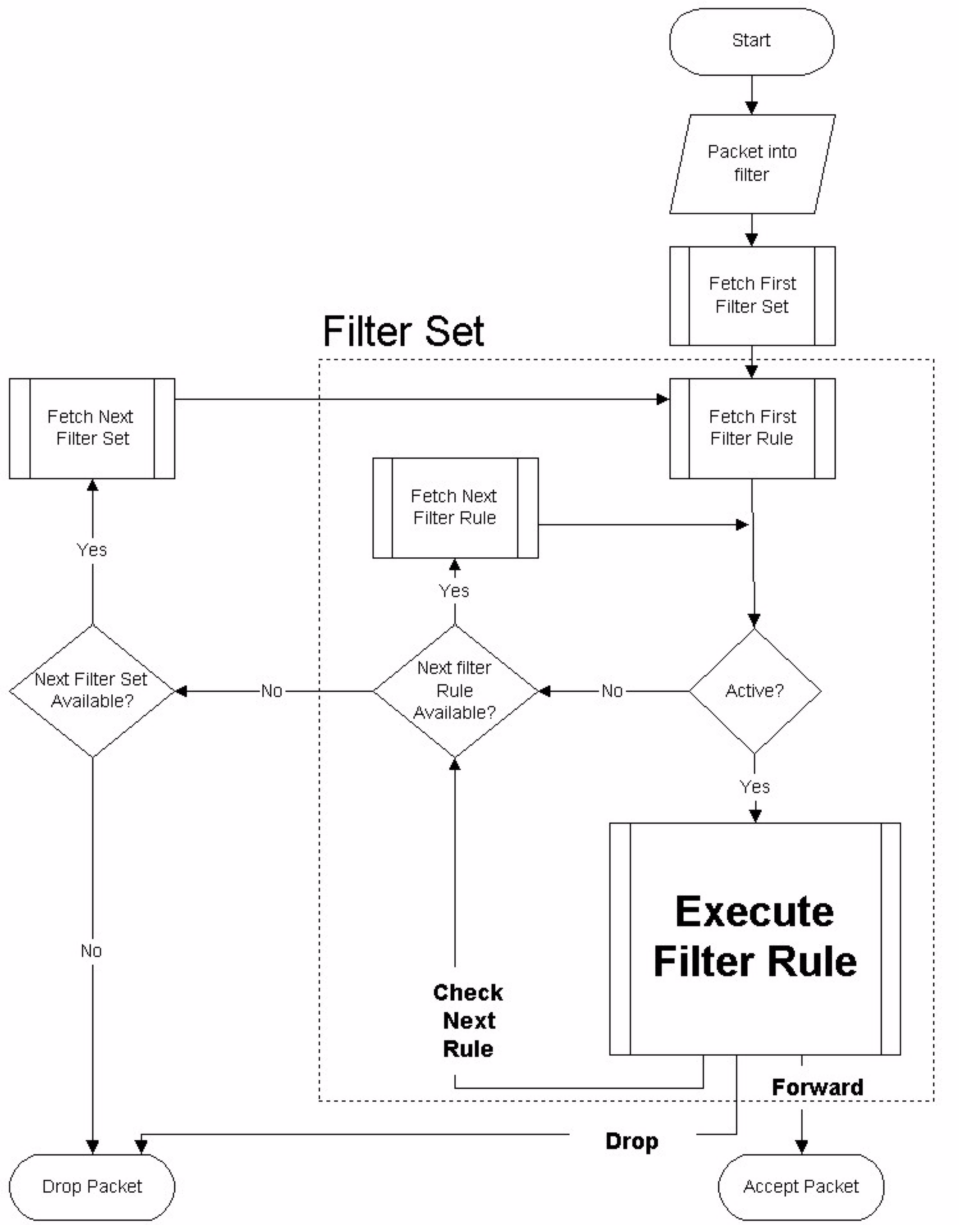
25.1.1 The Filter Structure of the ZyXEL Device

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The ZyXEL Device allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also Figure 144 on page 243 for the logic flow when executing an IP filter.

Figure 136 Filter Rule Process



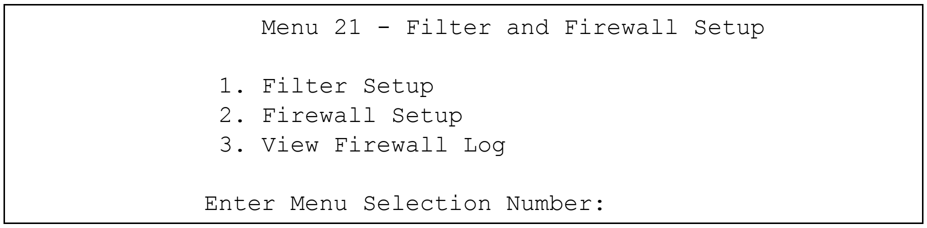
You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

25.2 Configuring a Filter Set

The ZyXEL Device includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

1 Enter 21 in the main menu to open menu 21.

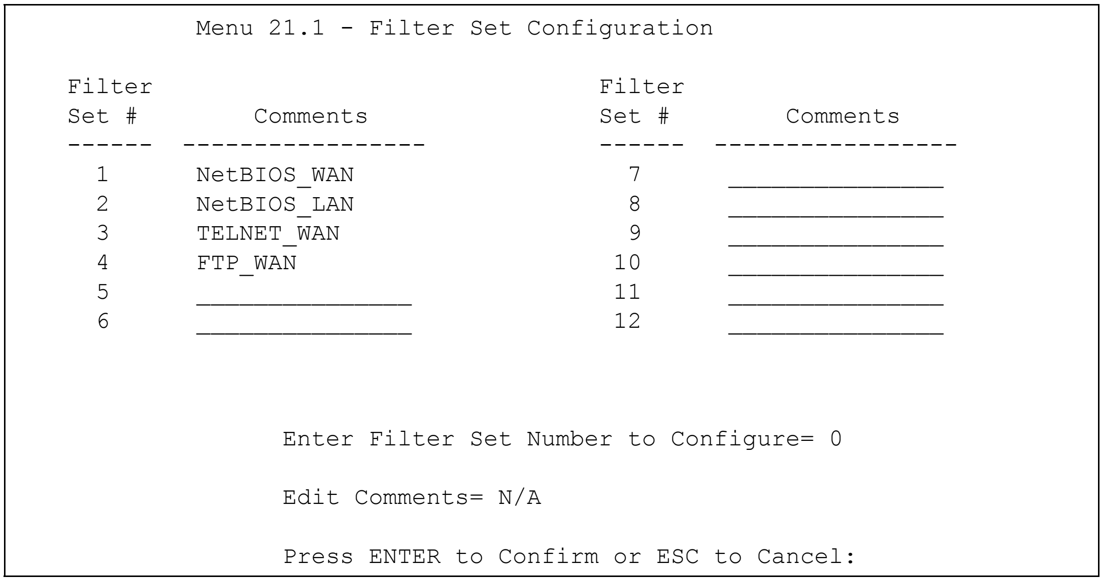
Figure 137 Menu 21: Filter and Firewall Setup



```
                 Menu 21 - Filter and Firewall Setup

              1. Filter Setup
              2. Firewall Setup
              3. View Firewall Log

             Enter Menu Selection Number:
```

2 Enter 1 to bring up the following menu.

Figure 138 Menu 21.1: Filter Set Configuration



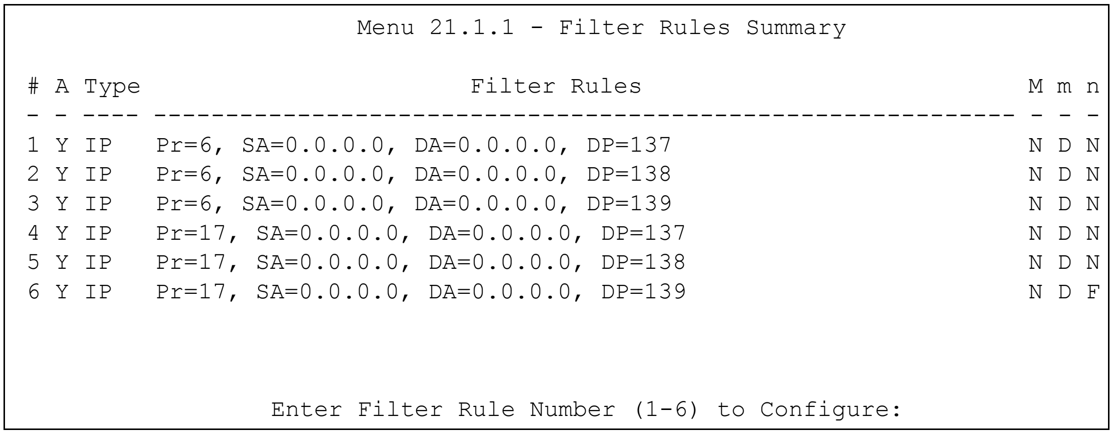
```
             Menu 21.1 - Filter Set Configuration

    Filter                              Filter
    Set #       Comments                Set #       Comments
    ------  -----------------           ------  -----------------
      1      NetBIOS_WAN                  7      _______________
      2      NetBIOS_LAN                  8      _______________
      3      TELNET_WAN                   9      _______________
      4      FTP_WAN                     10      _______________
      5      _______________             11      _______________
      6      _______________             12      _______________



                   Enter Filter Set Number to Configure= 0

                   Edit Comments= N/A

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

3 Select the filter set you wish to configure (1-12) and press [ENTER].

4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

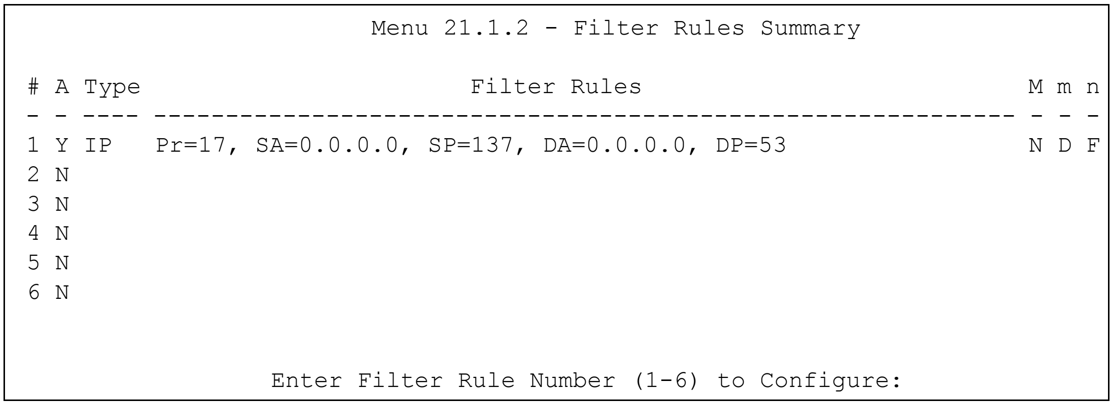
5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**. The following shows filter rules summary screens for filter sets 1 through 4.

Figure 139 NetBIOS_WAN Filter Rules Summary



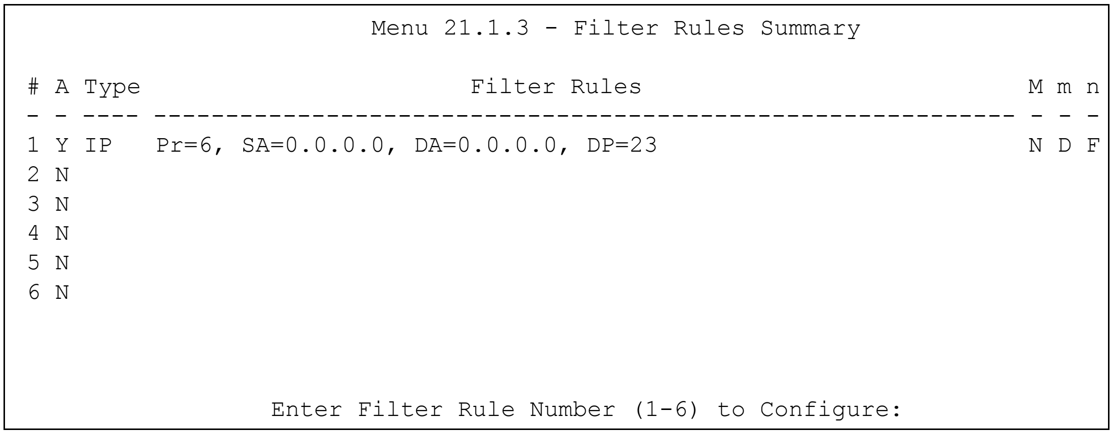
```
                       Menu 21.1.1 - Filter Rules Summary

 # A Type                      Filter Rules                              M m n
 - - ---- ------------------------------------------------------------ - - -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                         N D N
 2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                         N D N
 3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                         N D N
 4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                        N D N
 5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                        N D N
 6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                        N D F



                 Enter Filter Rule Number (1-6) to Configure:
```

Figure 140 NetBIOS _LAN Filter Rules Summary



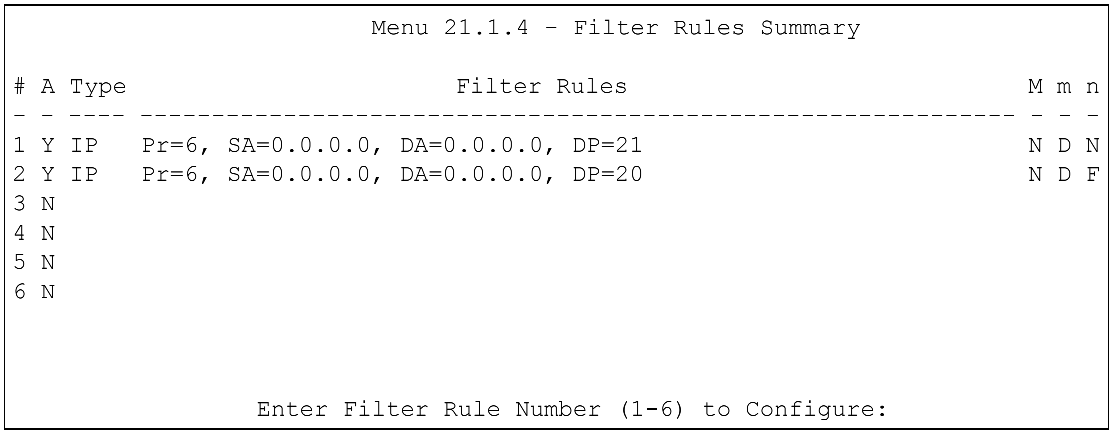
```
                        Menu 21.1.2 - Filter Rules Summary

 # A Type                      Filter Rules                              M m n
 - - ---- ------------------------------------------------------------ - - -
 1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                 N D F
 2 N
 3 N
 4 N
 5 N
 6 N


                 Enter Filter Rule Number (1-6) to Configure:
```

Figure 141 Telnet WAN Filter Rules Summary



```
                        Menu 21.1.3 - Filter Rules Summary

 # A Type                      Filter Rules                              M m n
 - - ---- ------------------------------------------------------------ - - -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                          N D F
 2 N
 3 N
 4 N
 5 N
 6 N



                 Enter Filter Rule Number (1-6) to Configure:
```

Figure 142 FTP_WAN Filter Rules Summary



```
                         Menu 21.1.4 - Filter Rules Summary

# A Type                       Filter Rules                            M m n
- - ---- ------------------------------------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                           N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=20                           N D F
3 N
4 N
5 N
6 N



                 Enter Filter Rule Number (1-6) to Configure:
```

25.2.1 Filter Rules Summary Menus

The following tables contain a brief description of the abbreviations used in the previous menus.

Table 78 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: “Y” means the rule is active. “N” means the rule is inactive.
Type	The type of filter rule: “GEN” for Generic, “IP” for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. “Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. “N” means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N“ means to check the next rule.
n	Action Not Matched “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 79 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

25.2.2 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.x - Filter Rules Summary** and press [ENTER] to open menu 21.1.x.x for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

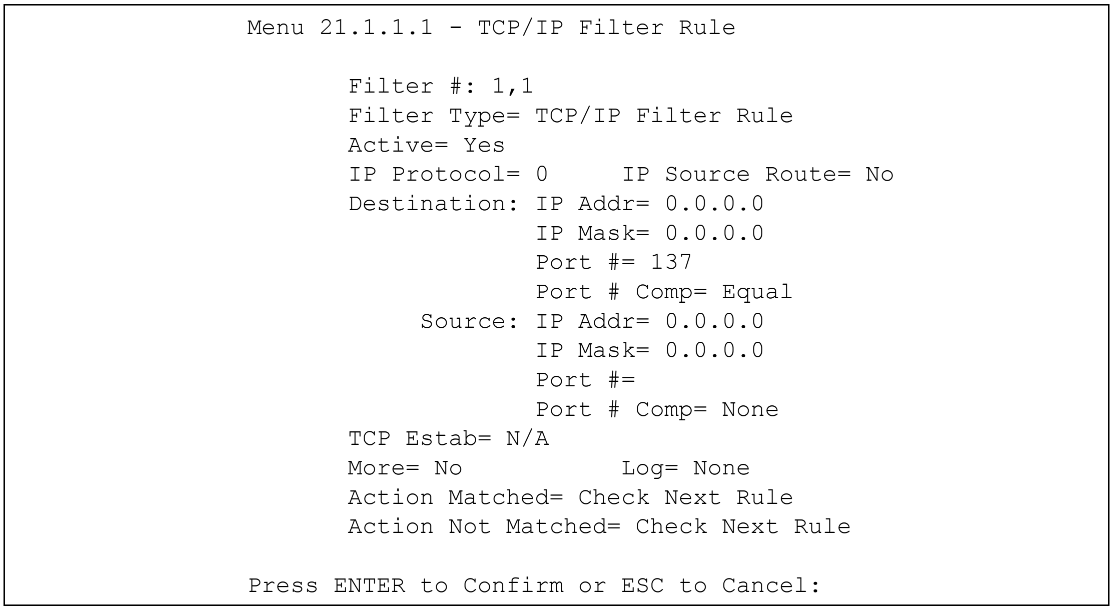
To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the ZyXEL Device will warn you and will not allow you to save.

25.2.3 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.x - TCP/IP Filter Rule**, as shown next

Figure 143 Menu 21.1.1.1 TCP/IP Filter Rule.



```
                 Menu 21.1.1.1 - TCP/IP Filter Rule

                        Filter #: 1,1
                        Filter Type= TCP/IP Filter Rule
                        Active= Yes
                        IP Protocol= 0     IP Source Route= No
                        Destination: IP Addr= 0.0.0.0
                                     IP Mask= 0.0.0.0
                                     Port #= 137
                                     Port # Comp= Equal
                             Source: IP Addr= 0.0.0.0
                                     IP Mask= 0.0.0.0
                                     Port #=
                                     Port # Comp= None
                        TCP Estab= N/A
                        More= No           Log= None
                        Action Matched= Check Next Rule
                        Action Not Matched= Check Next Rule

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

The following table describes how to configure your TCP/IP filter rule.

Table 80 Menu 21.1.x.x TCP/IP Filter Rule

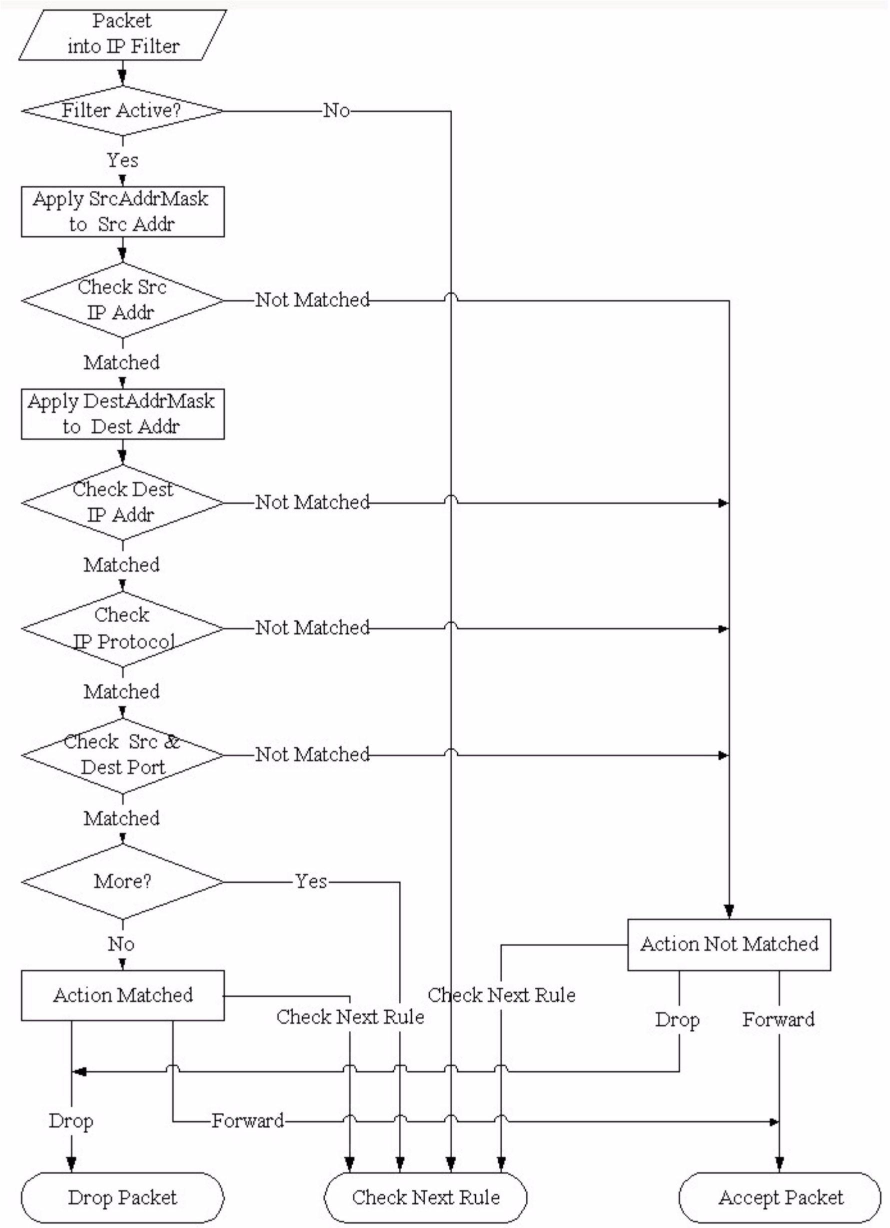
FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	1,1
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different.	TCP/IP Filter Rule Generic Filter Rule
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the filter rule or **No** to deactivate it.	Yes No
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.	0-255
IP Source Route	Press [SPACE BAR] and then [ENTER] to select **Yes** to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.	Yes No
Destination		
IP Address	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Destination: IP Addr**.	0.0.0.0
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535

Table 80 Menu 21.1.x.x TCP/IP Filter Rule

FIELD	DESCRIPTION	OPTIONS
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given **in Destination: Port #**.	None Less Greater Equal Not Equal
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Source: IP Addr**.	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**.	None Less Greater Equal Not Equal
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored.	Yes No
More	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	Yes No
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.	Check Next Rule Forward Drop
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.	Check Next Rule Forward Drop
When you have **Menu 21.1.x.x - TCP/IP Filter Rule** configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.x - Filter Rules Summary**.		

The following figure illustrates the logic flow of an IP filter.

Figure 144 Executing an IP Filter



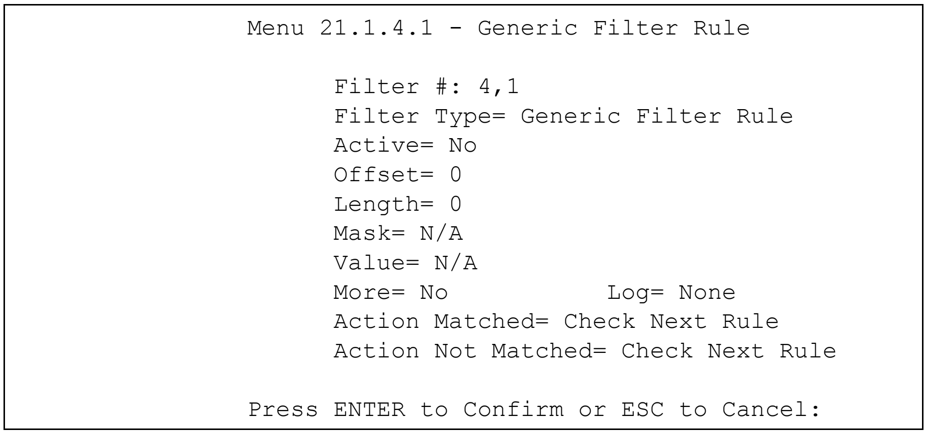
25.2.4 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyXEL Device treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyXEL Device applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, `FFFFFFFF`.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.x.x and press [ENTER] to open Generic Filter Rule, as shown below.

Figure 145 Menu 21.1.4.1 Generic Filter Rule



```
                Menu 21.1.4.1 - Generic Filter Rule

                      Filter #: 4,1
                      Filter Type= Generic Filter Rule
                      Active= No
                      Offset= 0
                      Length= 0
                      Mask= N/A
                      Value= N/A
                      More= No           Log= None
                      Action Matched= Check Next Rule
                      Action Not Matched= Check Next Rule

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

The following table describes the fields in the Generic Filter Rule menu.

Table 81 Menu 21.1.x.x Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	**Generic Filter Rule** **TCP/IP Filter Rule**
Active	Select **Yes** to turn on the filter rule or **No** to turn it off.	Yes / No
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0-255
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0-8
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.	

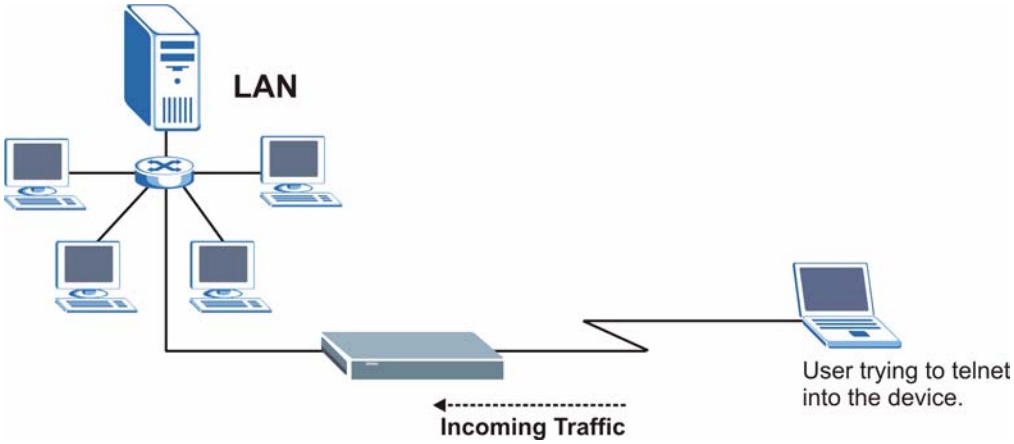
Table 81 Menu 21.1.x.x Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**.	Yes No
Log	Select the logging option from the following: **None** - No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Select the action for a packet matching the rule.	Check Next Rule Forward Drop
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule Forward Drop
Once you have completed filling in **Menu 21.1.x.x - Generic Filter Rule**, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.x - Filter Rules Summary**.		

25.3 Example Filter

Let's look at an example to block outside users from accessing the ZyXEL Device via telnet.

Figure 146 Telnet Filter Example



1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.

2 Enter 1 to open **Menu 21.1 - Filter Set Configuration**.

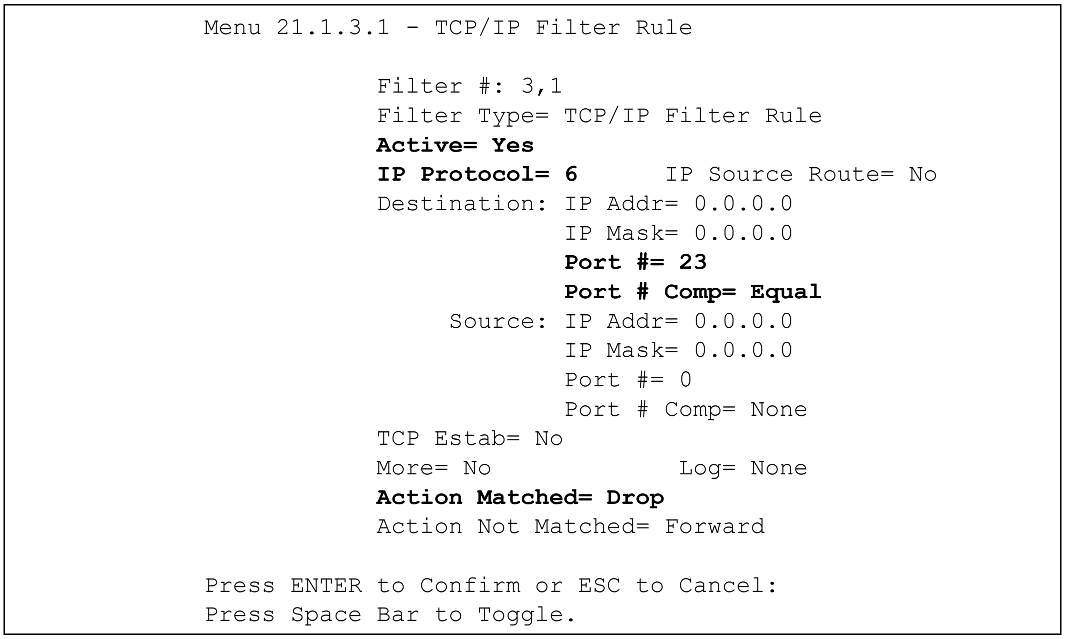
3 Enter the index of the filter set you wish to configure (say 3) and press [ENTER].

4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**

6 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Figure 147 Example Filter: Menu 21.1.3.1

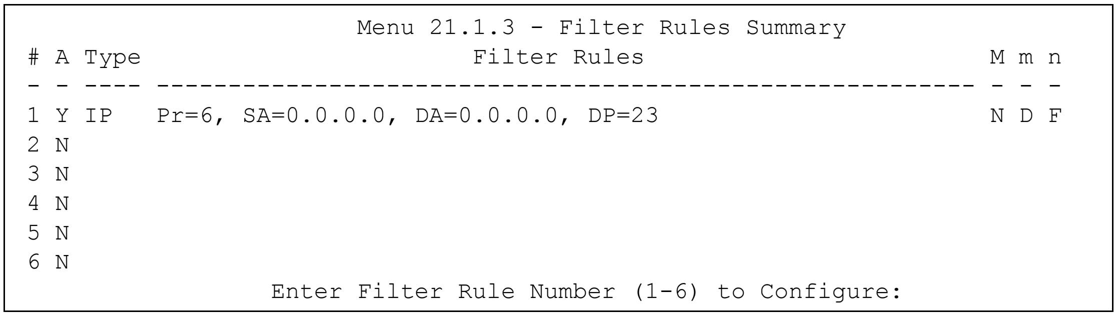


```
              Menu 21.1.3.1 - TCP/IP Filter Rule

                          Filter #: 3,1
                          Filter Type= TCP/IP Filter Rule
                          Active= Yes
                          IP Protocol= 6      IP Source Route= No
                          Destination: IP Addr= 0.0.0.0
                                       IP Mask= 0.0.0.0
                                       Port #= 23
                                       Port # Comp= Equal
                               Source: IP Addr= 0.0.0.0
                                       IP Mask= 0.0.0.0
                                       Port #= 0
                                       Port # Comp= None
                          TCP Estab= No
                          More= No             Log= None
                          Action Matched= Drop
                          Action Not Matched= Forward

              Press ENTER to Confirm or ESC to Cancel:
              Press Space Bar to Toggle.
```

- Select **Yes** from the **Active** field to activate this rule.
- **6** is the TCP **IP Protocol**.
- The **Port #** for the telnet service (TCP protocol) is 23. See RFC 1060 for port numbers of well-known services.
- Select **Equal** from the **Port # Comp** field as you are looking for packets going to port 23 only.
- Select **Drop** in the **Action Matched** field so that the packet will be dropped if its destination is the telnet port.
- Select **Forward** from the **Action Not Matched** field so that the packet will be forwarded if its destination is not the telnet port.
- Press [SPACE BAR] and then [ENTER] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

Figure 148 Example Filter Rules Summary: Menu 21.1.3



```
                        Menu 21.1.3 - Filter Rules Summary
# A Type                        Filter Rules                        M m n
- - ---- -------------------------------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                      N D F
2 N
3 N
4 N
5 N
6 N
                  Enter Filter Rule Number (1-6) to Configure:
```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren’t in this example).

After you’ve created the filter set, you must apply it.

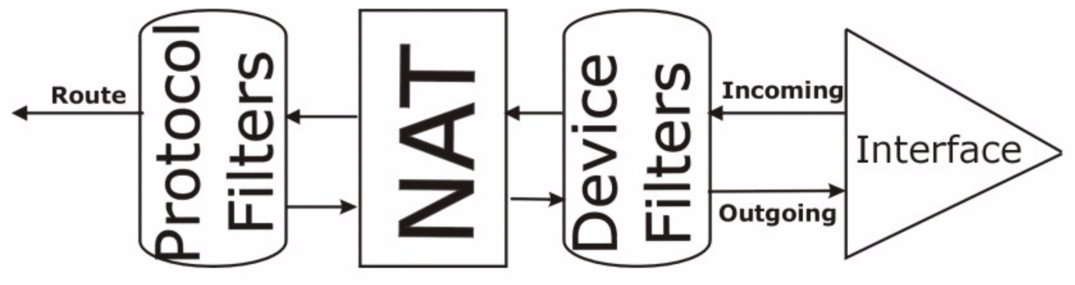
1. Enter 11 from the main menu to go to menu 11.
2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
3. This brings you to menu 11.5. Apply a filter set (our example filter set 3).
4. Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

25.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section.

When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyXEL Device applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyXEL Device is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

Figure 149 Protocol and Device Filter Sets



25.5 Firewall Versus Filters

Firewall configuration is discussed in the firewall chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

25.6 Applying a Filter

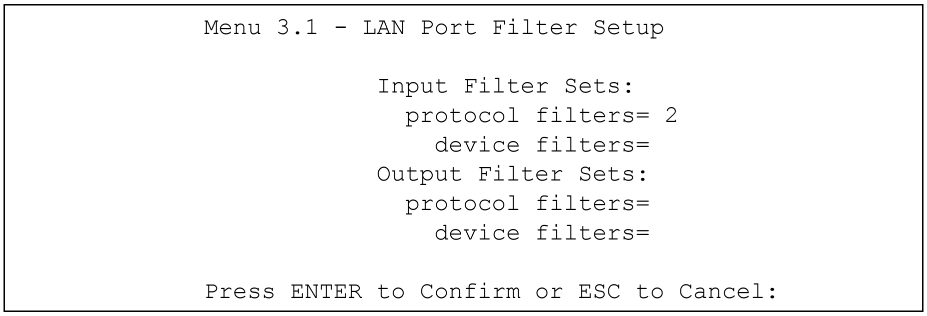
This section shows you where to apply the filter(s) after you design it (them). The ZyXEL Device already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Note: If you do not activate the firewall, it is advisable to apply filters.

25.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server. Input filter sets filter incoming traffic to the ZyXEL Device and output filter sets filter outgoing traffic from the ZyXEL Device.

Figure 150 Filtering LAN Traffic

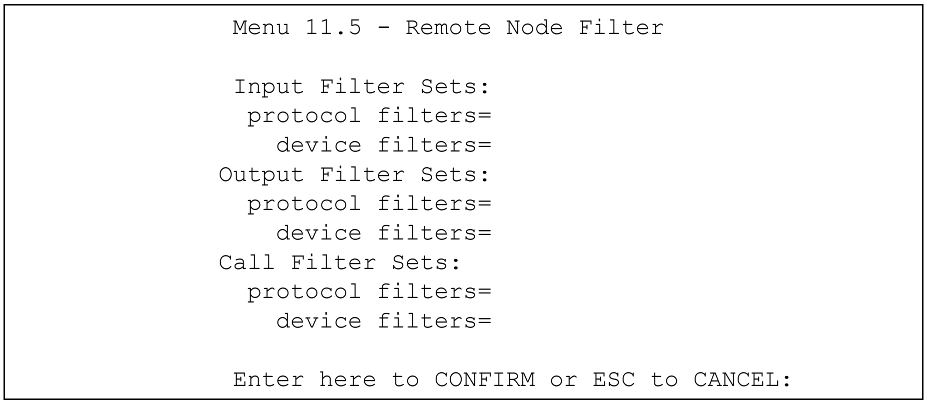


```
Menu 3.1 - LAN Port Filter Setup

            Input Filter Sets:
              protocol filters= 2
                device filters=
            Output Filter Sets:
              protocol filters=
                device filters=

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

25.6.2 Applying Remote Node Filters

Go to menu 11.5 (shown below) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas.

Figure 151 Filtering Remote Node Traffic



```
 Menu 11.5 - Remote Node Filter

 Input Filter Sets:
  protocol filters=
    device filters=
Output Filter Sets:
  protocol filters=
    device filters=
Call Filter Sets:
  protocol filters=
    device filters=

 Enter here to CONFIRM or ESC to CANCEL:
```

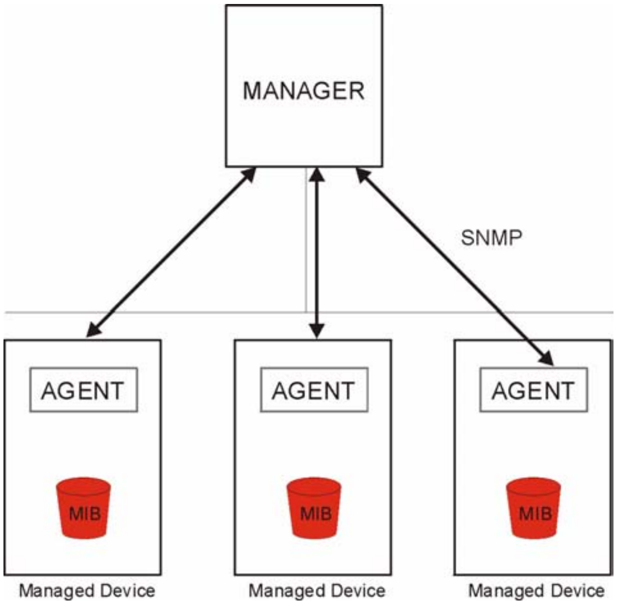
CHAPTER 26
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

26.1 About SNMP

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

Figure 152   SNMP Management Model



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

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

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

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

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

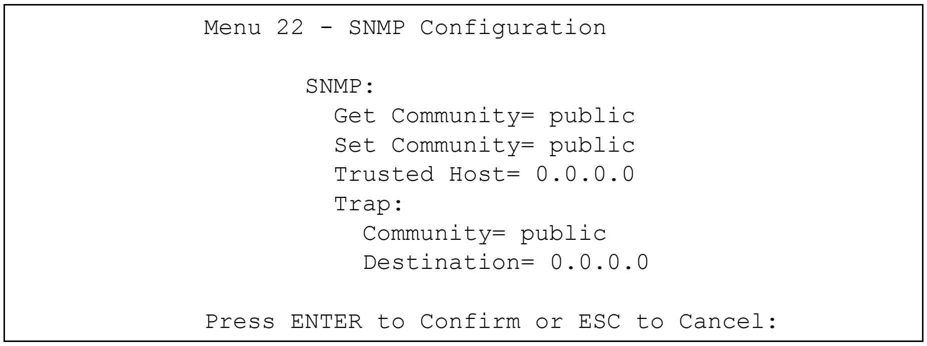
26.2 Supported MIBs

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

26.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 - SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

Figure 153   Menu 22 SNMP Configuration



```
              Menu 22 - SNMP Configuration

                     SNMP:
                       Get Community= public
                       Set Community= public
                       Trusted Host= 0.0.0.0
                       Trap:
                         Community= public
                         Destination= 0.0.0.0

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

The following table describes the SNMP configuration parameters.

Table 82 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the **Set Community**, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your ZyXEL Device will only respond to SNMP messages from this address. A blank (default) field means your ZyXEL Device will respond to all SNMP messages it receives, regardless of source.
Trap:	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

26.4 SNMP Traps

The ZyXEL Device will send traps to the SNMP manager when any one of the following events occurs:

Table 83 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkUp (*defined in RFC-1215*)	A trap is sent with the port number.
4	authenticationFailure *(defined in RFC-1215)*	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (*defined in RFC-1215*)	A trap is sent with the port number when any of the links are down. See the following table.

The port number is its interface index under the interface group.

Table 84 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2

Table 84 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
…	…
13	12
14	xDSL

CHAPTER 27 System Security

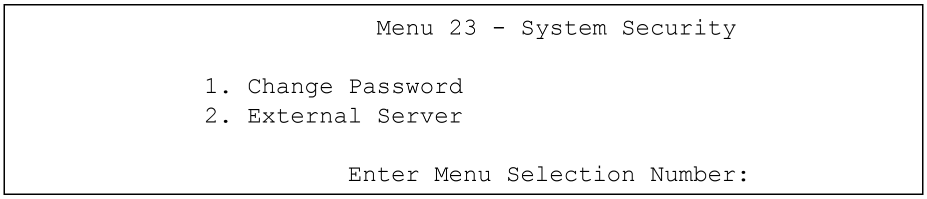
This chapter describes how to configure the system security on the ZyXEL Device.

27.1 System Security

You can configure the system password and an external RADIUS server in this menu.

27.2 System Password

Figure 154 Menu 23 System Security



```
                          Menu 23 - System Security

              1. Change Password
              2. External Server

                        Enter Menu Selection Number:
```

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to the section on changing the system password in the Introducing the SMT chapter and the section on resetting the ZyXEL Device in the chapter about introducing the web configurator .

27.3 RADIUS

RADIUS (Remote Authentication Dial-In User Service) is based on a client-sever model that supports authentication, authorization and accounting. The RADIUS is an external server and handles the following tasks:

- Authentication

  Determines the identity of the users.

- Authorization

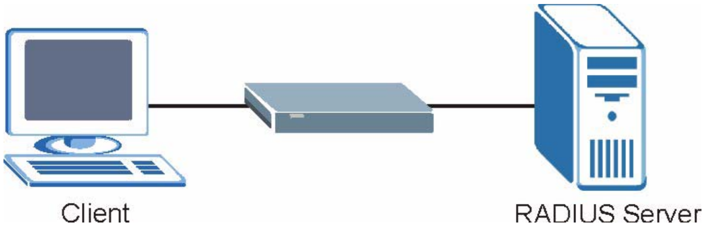
  Determines the network services available to authenticated users once they are connected to the network.

- Accounting

  Keeps track of the client's network activity.

RADIUS authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location

Figure 155 RADIUS Server



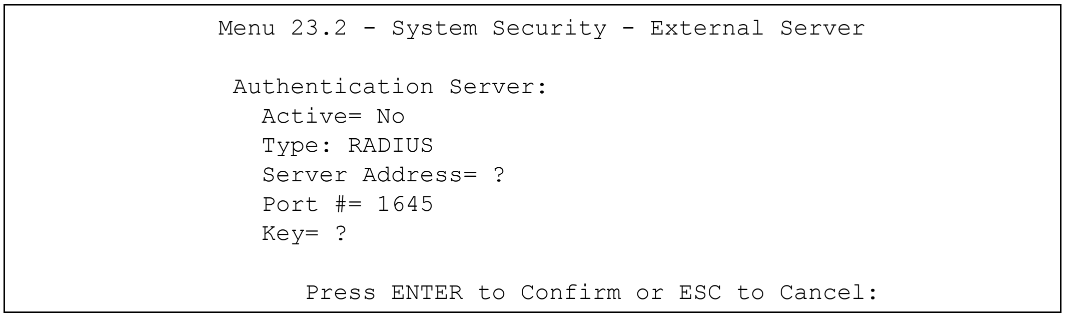
In order to ensure network security, the ZyXEL Device and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

27.4 Configuring External Server

Enter 23 in the main menu to display **Menu 23 - System Security**.

From Menu 23- System Security, enter 2 to display **Menu 23.2 - System Security-External Server** as shown next.

Figure 156 Menu 23.2 System Security : External Server



```
              Menu 23.2 - System Security - External Server

               Authentication Server:
                 Active= No
                 Type: RADIUS
                 Server Address= ?
                 Port #= 1645
                 Key= ?

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

The following table describes the fields in this screen.

Table 85 Menu 23.2 System Security : External Server

FIELD	DESCRIPTION
Authentication Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server.
Type	This field displays the external server type.

Table 85 Menu 23.2 System Security : External Server

FIELD	DESCRIPTION
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port	The default port of the RADIUS server for authentication is 1645. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and ZyXEL Device.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

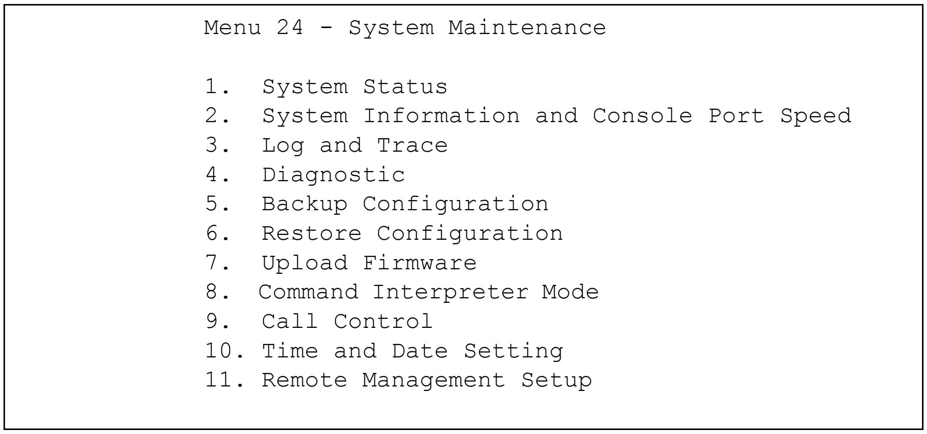
CHAPTER 28 System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

Figure 157 Menu 24 System Maintenance



```
              Menu 24 - System Maintenance

              1.  System Status
              2.  System Information and Console Port Speed
              3.  Log and Trace
              4.  Diagnostic
              5.  Backup Configuration
              6.  Restore Configuration
              7.  Upload Firmware
              8.  Command Interpreter Mode
              9.  Call Control
              10. Time and Date Setting
              11. Remote Management Setup
```

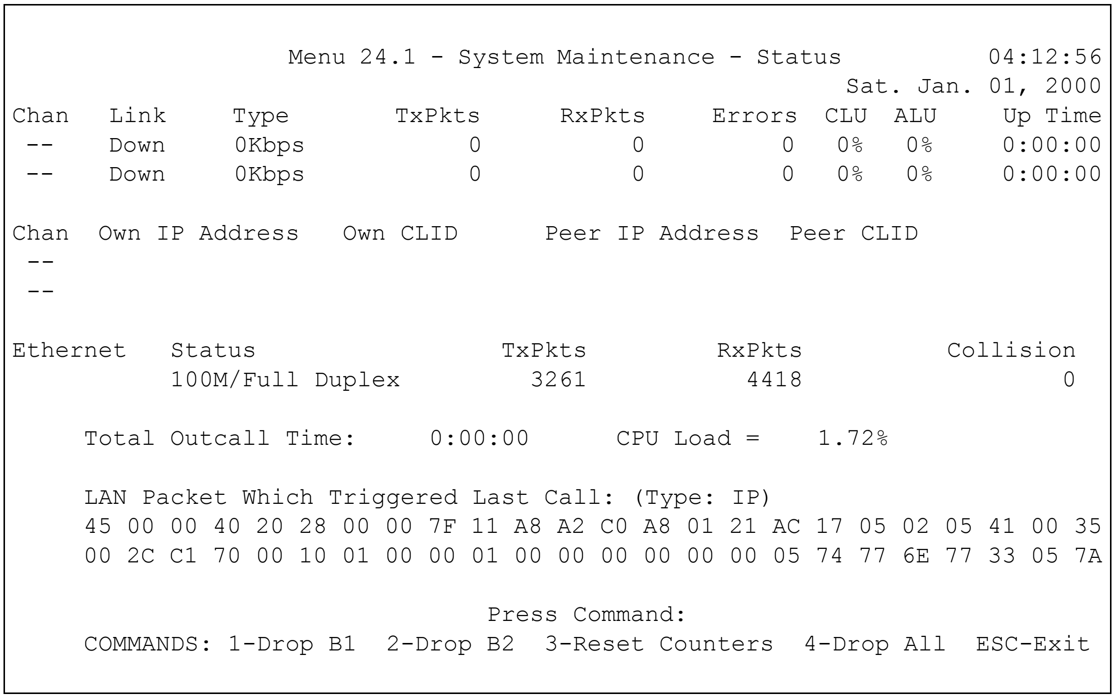
28.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next (see Figure 158 on page 259). System Status is a tool that can be used to monitor your ZyXEL Device.

To get to System Status, type 24 to go to **Menu 24 - System Maintenance.** From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status** which are read-only and meant for diagnostic purposes.

Figure 158 Menu 24.1 System Maintenance : Status



```
                   Menu 24.1 - System Maintenance - Status          04:12:56
                                                          Sat. Jan. 01, 2000
Chan   Link    Type       TxPkts     RxPkts     Errors  CLU  ALU     Up Time
 --    Down    0Kbps           0          0          0   0%   0%     0:00:00
 --    Down    0Kbps           0          0          0   0%   0%     0:00:00

Chan  Own IP Address   Own CLID      Peer IP Address  Peer CLID
 --
 --

Ethernet   Status                 TxPkts         RxPkts          Collision
           100M/Full Duplex         3261           4418                  0

     Total Outcall Time:     0:00:00      CPU Load =    1.72%

     LAN Packet Which Triggered Last Call: (Type: IP)
     45 00 00 40 20 28 00 00 7F 11 A8 A2 C0 A8 01 21 AC 17 05 02 05 41 00 35
     00 2C C1 70 00 10 01 00 00 01 00 00 00 00 00 00 05 74 77 6E 77 33 05 7A

                                 Press Command:
     COMMANDS: 1-Drop B1  2-Drop B2  3-Reset Counters  4-Drop All  ESC-Exit
```

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

Table 86 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Chan	This shows statistics for B1 and B2 channels respectively. This is the information displayed for each channel.
Link	This shows the name of the remote node or the user the channel is currently connected to or the status of the channel (e.g., **Down**, **Idle**, **Calling**, **Answering**, **NetCAPI**, etc.).
Type	This is the current connecting speed.
TxPkts	This is the number of transmitted packets on this channel.
RxPkts	This is the number of received packets on this channel.
Errors	This is the number of error packets on this channel.
CLU	The CLU (Current Line Utilization) is the percentage of current bandwidth used on this channel.
ALU	The ALU (Average Line Utilization) is a 5-second moving average of usage for this channel.
Up Time	Time this channel has been connected to the current remote node.
Chan	This shows statistics for **B1** and **B2** channels respectively. This is the information displayed for each channel.
Own IP Address	This refers to the IP address of the ZyXEL Device.
Own CLID	This shows your Caller ID.

Table 86 System Maintenance: Status Menu Fields

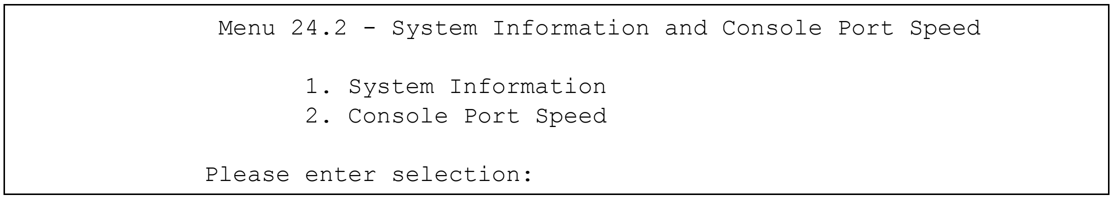
FIELD	DESCRIPTION
Peer IP Address	This refers to the IP address of the peer.
Peer CLID	This shows the Caller ID of the peer.
Ethernet	This shows statistics for the LAN.
Status	This displays the port speed and duplex setting.
TxPkts	This is the number of transmitted packets to the LAN.
RxPkts	This is the number of received packets from the LAN.
Collision	This is the number of collisions.
Total Outcall Time	This shows the total outgoing call time for both B1 and B2 channels since the system has been powered up.
CPU Load	This specifies the percentage of CPU utilization.
LAN Packet Which Triggered Last Call	This shows the first 48 octets of the LAN packet that triggered the last outgoing call.
Commands	
Drop B1	This command drops the B1 channel.
Drop B2	This command drops the B2 channel.
Reset Counters	This command resets all counters.
Drop All	This command drops all channels.

28.2 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

1. Enter 24 to display **Menu 24 - System Maintenance**.
2. Enter 2 to display **Menu 24.2 - System Information and Console Port Speed**.
3. From this menu you have two choices as shown in the next figure:

Figure 159 Menu 24.2 System Information and Console Port Speed

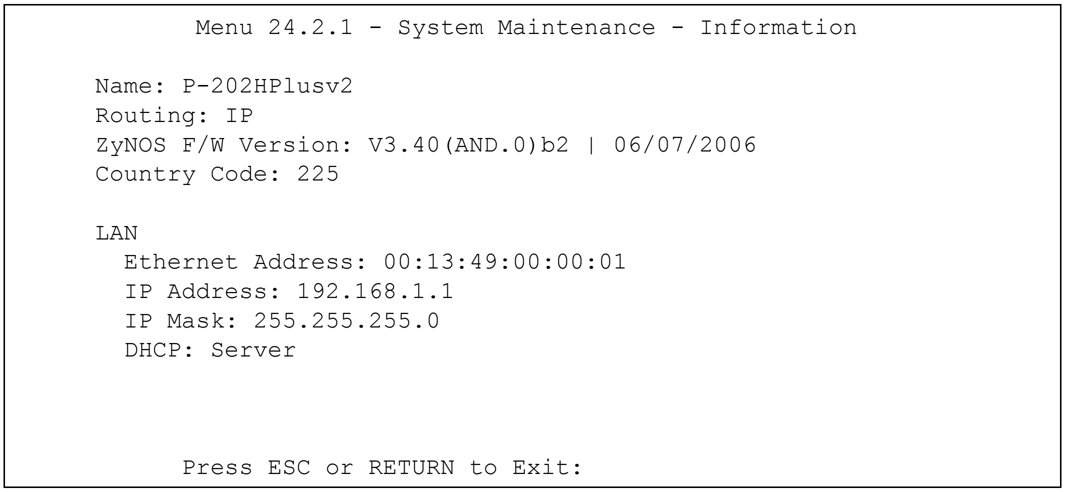


```
               Menu 24.2 - System Information and Console Port Speed

                     1. System Information
                     2. Console Port Speed

              Please enter selection:
```

28.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next

Figure 160 Menu 24.2.1 System Maintenance : Information



```
             Menu 24.2.1 - System Maintenance - Information

      Name: P-202HPlusv2
      Routing: IP
      ZyNOS F/W Version: V3.40(AND.0)b2 | 06/07/2006
      Country Code: 225

      LAN
        Ethernet Address: 00:13:49:00:00:01
        IP Address: 192.168.1.1
        IP Mask: 255.255.255.0
        DHCP: Server



            Press ESC or RETURN to Exit:
```

The following table describes the fields in this menu.

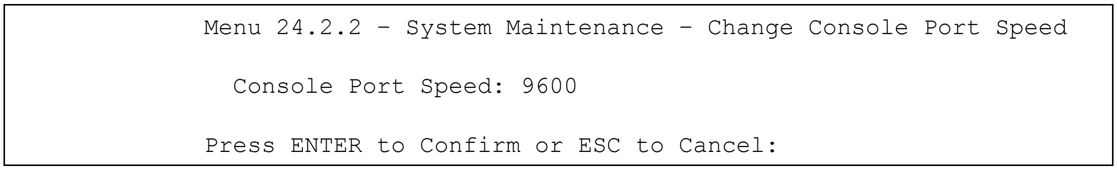
Table 87 Menu 24.2.1 System Maintenance : Information

FIELD	DESCRIPTION
Name	Displays the system name of your ZyXEL Device. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Country Code	Refers to the country code of the firmware.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your ZyXEL Device.
IP Address	This is the IP address of the ZyXEL Device in dotted decimal notation.
IP Mask	This shows the subnet mask of the ZyXEL Device.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the ZyXEL Device.

28.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Change Console Port Speed**. Your ZyXEL Device supports 9600 (default), 19200, 38400, 57600 and 115200 bps. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

Figure 161 Menu 24.2.2 System Maintenance : Change Console Port Speed



```
              Menu 24.2.2 – System Maintenance – Change Console Port Speed

                Console Port Speed: 9600

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

28.3 Log and Trace

Type 3 in menu 24 to open **Menu 24.3-Log and Trace**. This menu allows you to view the error log and the Unix Syslog, configure an accounting server, and see call-triggering packet information.

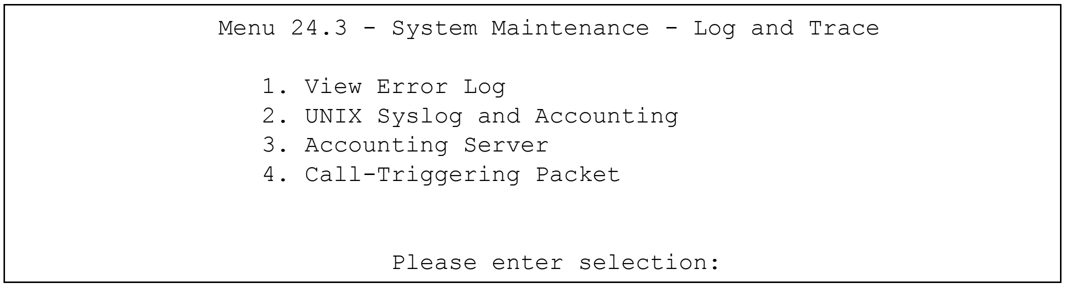
28.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

1 Type 24 in the main menu to display **Menu 24 - System Maintenance**.

2 From menu 24, type 3 to display **Menu 24.3 - System Maintenance - Log and Trace**.

Figure 162 Menu 24.3 System Maintenance Log and Trace

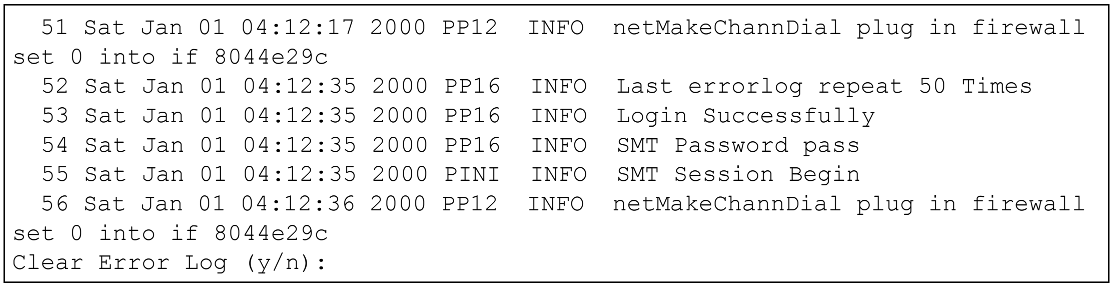


```
               Menu 24.3 - System Maintenance - Log and Trace

                  1. View Error Log
                  2. UNIX Syslog and Accounting
                  3. Accounting Server
                  4. Call-Triggering Packet


                           Please enter selection:
```

3 Enter 1 from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

After the ZyXEL Device finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

Figure 163 Sample Error and Information Messages

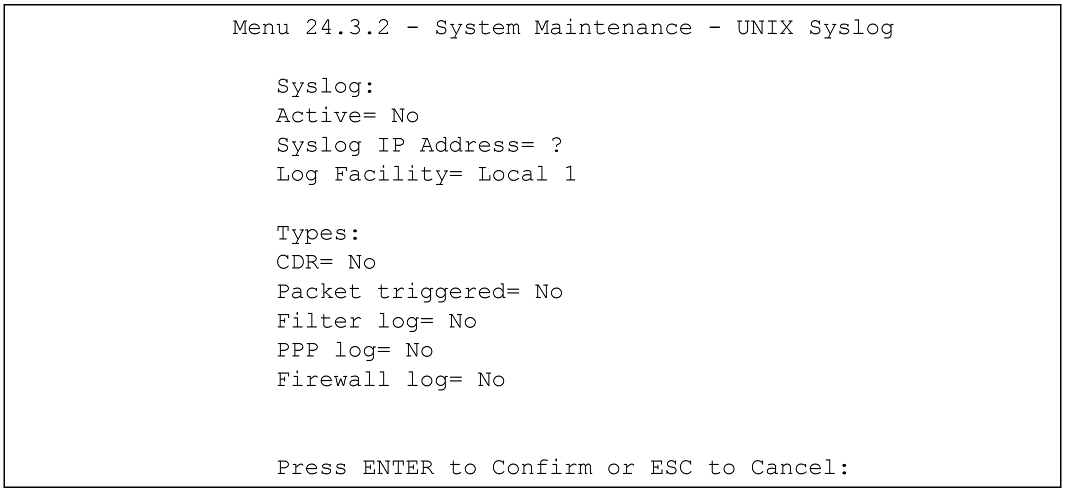


```
  51 Sat Jan 01 04:12:17 2000 PP12  INFO  netMakeChannDial plug in firewall
set 0 into if 8044e29c
  52 Sat Jan 01 04:12:35 2000 PP16  INFO  Last errorlog repeat 50 Times
  53 Sat Jan 01 04:12:35 2000 PP16  INFO  Login Successfully
  54 Sat Jan 01 04:12:35 2000 PP16  INFO  SMT Password pass
  55 Sat Jan 01 04:12:35 2000 PINI  INFO  SMT Session Begin
  56 Sat Jan 01 04:12:36 2000 PP12  INFO  netMakeChannDial plug in firewall
set 0 into if 8044e29c
Clear Error Log (y/n):
```

28.3.2 Unix Syslog

The ZyXEL Device uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - UNIX Syslog**, as shown next.

Figure 164 Menu 24.3.2 - System Maintenance - UNIX Syslog



```
                Menu 24.3.2 - System Maintenance - UNIX Syslog

                   Syslog:
                   Active= No
                   Syslog IP Address= ?
                   Log Facility= Local 1

                   Types:
                   CDR= No
                   Packet triggered= No
                   Filter log= No
                   PPP log= No
                   Firewall log= No


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

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 88 Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to the documentation of your syslog program for more details.
Types:	

Table 88 Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes**.
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes**.
Filter log	No filters are logged when this field is set to **No**. Filters with the individual filter Log Filter field set to **Yes** are logged when this field is set to **Yes**.
PPP log	PPP events are logged when this field is set to **Yes**.
Firewall log	Firewall events are logged when this field is set to **Yes**.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your ZyXEL Device sends five types of syslog messages. Some examples (not all ZyXEL Device specific) of these syslog messages with their message formats are shown next:

28.3.2.1 CDR

```
CDR Message Format
                 SdcmdSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String );
                 String = board xx line xx channel xx, call xx, str
                 board = the hardware board ID
                 line = the WAN ID in a board
                 Channel = channel ID within the WAN
                 call = the call reference number which starts from 1 and increments by
1 for each new call
                 str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
                      L02Tunnel Connected(L2TP)
                      C02 OutCall Connected xxxx (means connected speed) xxxxx (means
Remote Call Number)
                      L02 Call Terminated
                      C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing
Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall
Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call
Terminated
```

28.3.2.2 Packet triggered

```
Packet triggered Message Format
SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
   String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
   Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
   Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c
6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=450000282401400001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

28.3.2.3 Filter log

```
Filter log Message Format
   SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match
(m) drop (D).
   Src: Source Address
   Dst: Destination Address
   prot: Protocol ("TCP","UDP","ICMP")
spo: Source port
dpo: Destination port
Mar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[fffffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[ffffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170  dpo=00021]}S04>R01mF
```

28.3.2.4 PPP log

```
PPP Log Message Format
SdcmdSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing
```

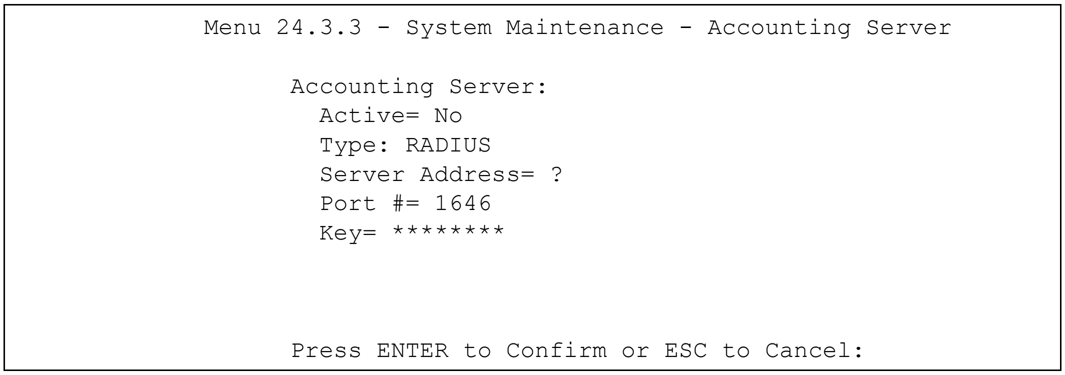
28.3.2.5 POTS log

```
POTS Log Message Format
SdcmdSyslogSend (SYSLOG_POTSLOG, SYSLOG_NOTICE, String);
String = Call Connect / Disconnect: Dir = xx Remote Call= xxxxx Local Call= xxxxx
Dir = Call Direction 1: Incoming call 2: Outgoing call
Remote Call = a string type which represents as the remote call number
```

28.3.3 Accounting Server

Type 3 in menu 24.3 to open **Menu 24.3.3 - Accounting Server**. This menu allows you to activate and configure an accounting server.

Figure 165 Menu 24.3.3 System Maintenance : Accounting Server



```
              Menu 24.3.3 - System Maintenance - Accounting Server

                    Accounting Server:
                      Active= No
                      Type: RADIUS
                      Server Address= ?
                      Port #= 1646
                      Key= ********



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

The following table describes the fields in this screen.

Table 89 Menu 24.3.3 System Maintenance : Accounting Server

FIELD	DESCRIPTION
Accounting Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable client authentication through an external accounting server.
Type	This non-editable field shows the type of accounting server being used.

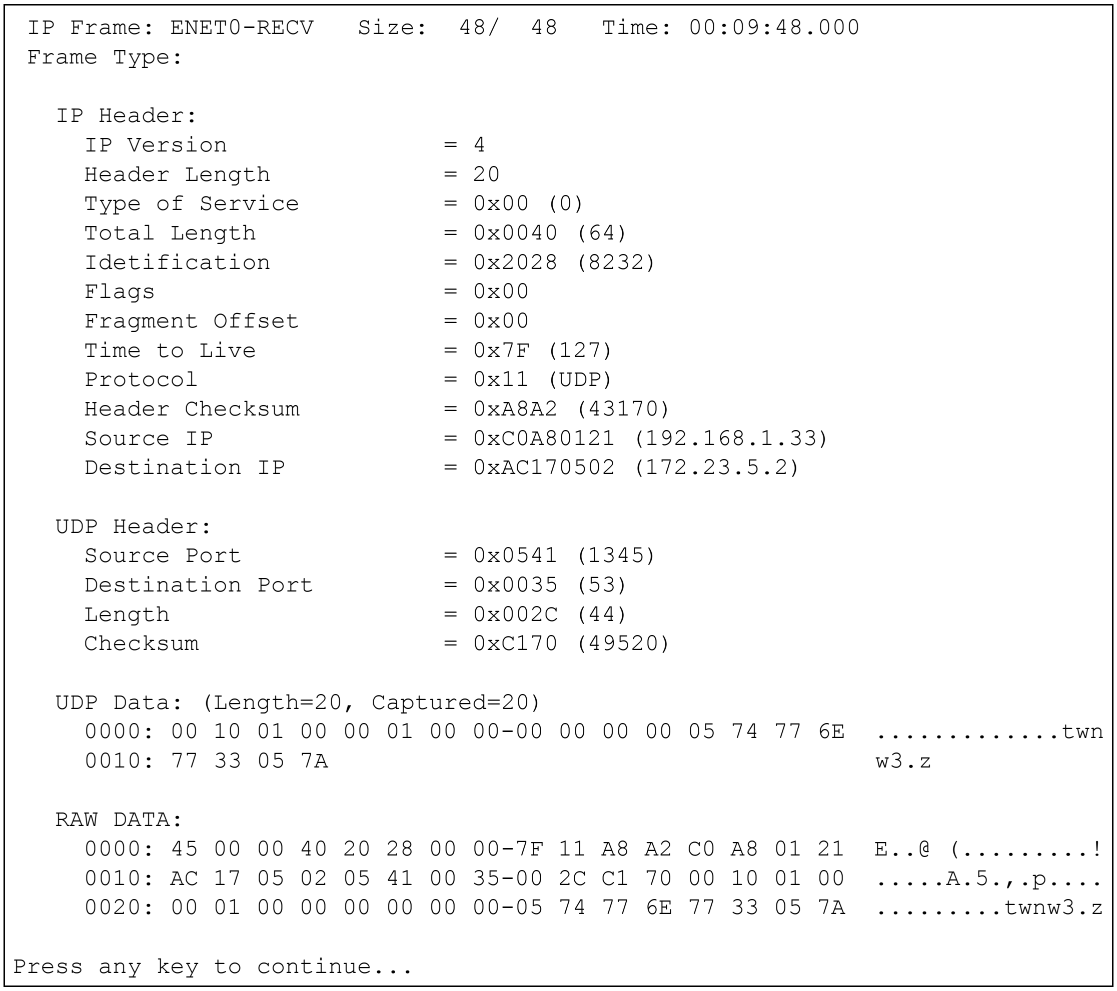
Table 89 Menu 24.3.3 System Maintenance : Accounting Server

FIELD	DESCRIPTION
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port	The default port for the Radius server for accounting is 1646. You do not need to change this value unless your network administrator instructs you to do so.
Key	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

28.3.4 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

Figure 166 Call-Triggering Packet Example



```
 IP Frame: ENET0-RECV   Size:  48/  48   Time: 00:09:48.000
 Frame Type:

   IP Header:
     IP Version               = 4
     Header Length            = 20
     Type of Service          = 0x00 (0)
     Total Length             = 0x0040 (64)
     Idetification            = 0x2028 (8232)
     Flags                    = 0x00
     Fragment Offset          = 0x00
     Time to Live             = 0x7F (127)
     Protocol                 = 0x11 (UDP)
     Header Checksum          = 0xA8A2 (43170)
     Source IP                = 0xC0A80121 (192.168.1.33)
     Destination IP           = 0xAC170502 (172.23.5.2)

   UDP Header:
     Source Port              = 0x0541 (1345)
     Destination Port         = 0x0035 (53)
     Length                   = 0x002C (44)
     Checksum                 = 0xC170 (49520)

   UDP Data: (Length=20, Captured=20)
     0000: 00 10 01 00 00 01 00 00-00 00 00 00 05 74 77 6E  .............twn
     0010: 77 33 05 7A                                      w3.z

   RAW DATA:
     0000: 45 00 00 40 20 28 00 00-7F 11 A8 A2 C0 A8 01 21  E..@ (.........!
     0010: AC 17 05 02 05 41 00 35-00 2C C1 70 00 10 01 00  .....A.5.,.p....
     0020: 00 01 00 00 00 00 00 00-05 74 77 6E 77 33 05 7A  .........twnw3.z

Press any key to continue...
```

28.4 Diagnostic

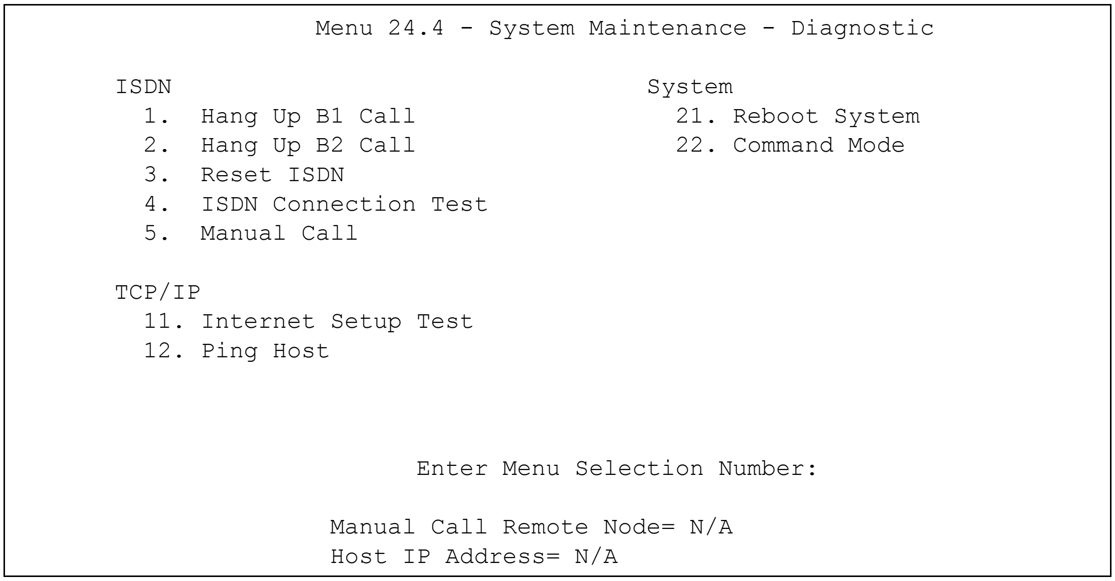
The diagnostic facility allows you to test the different aspects of your ZyXEL Device to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Follow the procedure next to get to Diagnostic:

1 From the main menu, type 24 to open **Menu 24 – System Maintenance**.

2 From this menu, type 4 to open **Menu 24.4 – System Maintenance – Diagnostic**.

Figure 167 Menu 24.4 System Maintenance : Diagnostic



```
                     Menu 24.4 - System Maintenance - Diagnostic

       ISDN                                 System
         1.  Hang Up B1 Call                  21. Reboot System
         2.  Hang Up B2 Call                  22. Command Mode
         3.  Reset ISDN
         4.  ISDN Connection Test
         5.  Manual Call

       TCP/IP
         11. Internet Setup Test
         12. Ping Host



                            Enter Menu Selection Number:

                      Manual Call Remote Node= N/A
                      Host IP Address= N/A
```

The following table describes the diagnostic tests available in menu 24.4 for your ZyXEL Device and associated connections.

Table 90 System Maintenance Menu Diagnostic

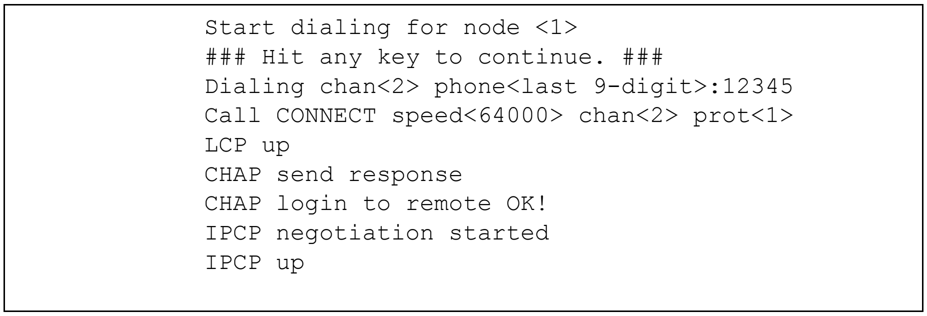
FIELD	DESCRIPTION
Hang Up B1 Call	This tool hangs up the B1 channel. It is only applicable if the B1 channel is currently in use.
Hang Up B2 Call	This tool hangs up the B2 channel. It is only applicable if the B2 channel is currently in use.
Reset ISDN	This command re-initializes the ISDN link to the telephone company.
ISDN Connection Test	You can test to see if your ISDN line is working properly by using this option. This command triggers the ZyXEL Device to perform a loop-back test to check the functionality of the ISDN line. If the test is not successful, note the error message that you receive and consult your network administrator.

Table 90 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Manual Call	This provides a way for you to place a call to a remote node manually. This tests the connectivity to that remote node. When you use this command, the screen displays what is happening during the call setup and protocol negotiation. The following is an example of a successful connection.
Internet Setup Test	This test checks to see if your Internet access configuration has been done correctly. When this option is chosen, the ZyXEL Device places a manual call to the ISP remote node. If everything is working properly, you will receive an appropriate response. Otherwise, note the error message and consult your network administrator.
Ping Host	This diagnostic test pings the host, which determines the functionality of the TCP/IP protocol on both systems and the links in between.
Reboot System	This option reboots the ZyXEL Device.
Command Mode	This option allows you to enter the command mode. It allows you to diagnose and test your ZyXEL Device using a specified set of commands.
Manual Call Remote Node	If you entered **5** above, then enter the remote node number (with reference to the remote node listing on **Menu 11 - Remote Node Setup**) you wish to call.
Host IP Address	If you entered **12** above, then enter the IP address of the machine you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	

The following figure shows an example of a successful connection after selecting option **Manual Call** in **Menu 24.4**.

Figure 168 Display for a Successful Manual Call



```
Start dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:12345
Call CONNECT speed<64000> chan<2> prot<1>
LCP up
CHAP send response
CHAP login to remote OK!
IPCP negotiation started
IPCP up
```

CHAPTER 29
Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.

29.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a “rom” filename extension. Once you have customized the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

Note: Only use firmware for your ZyXEL Device’s specific model. Refer to the label on the bottom of your ZyXEL Device.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyXEL Device.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file “config.cfg”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

Table 91 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyXEL Device.	*.bin

29.2 Backup Configuration

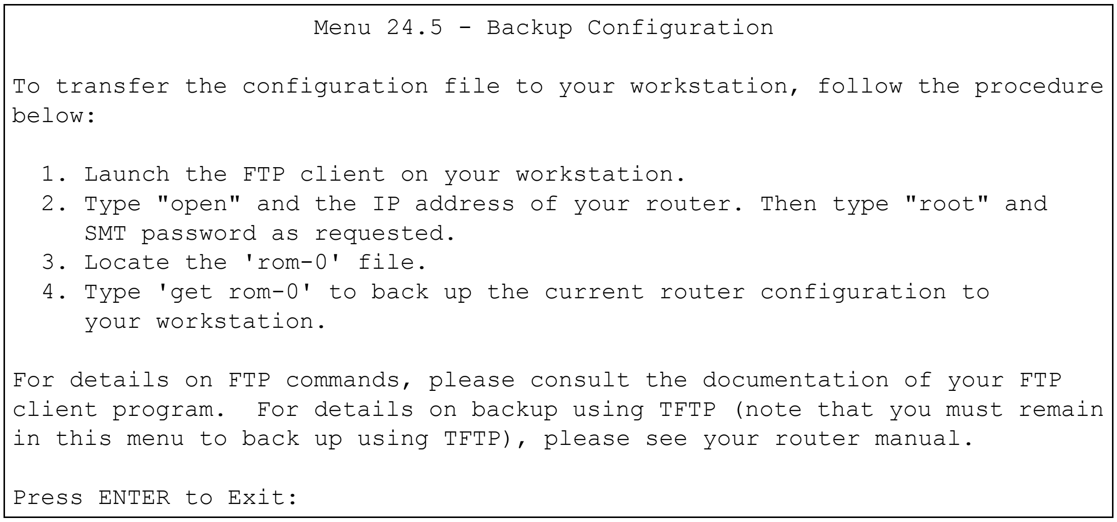
Option 5 from **Menu 24 – System Maintenance** allows you to backup the current ZyXEL Device configuration to your computer. Backup is highly recommended once your ZyXEL Device is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the ZyXEL Device to the computer, while upload means from your computer to the ZyXEL Device.

29.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

Figure 169 Telnet in Menu 24.5



```
                     Menu 24.5 - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure
below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your router. Then type "root" and
     SMT password as requested.
  3. Locate the 'rom-0' file.
  4. Type 'get rom-0' to back up the current router configuration to
     your workstation.

For details on FTP commands, please consult the documentation of your FTP
client program.  For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your router manual.

Press ENTER to Exit:
```

29.2.2 Using the FTP Command from the Command Line

1 Launch the FTP client on your computer.

2 Enter “open”, followed by a space and the IP address of your ZyXEL Device.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is “1234”).

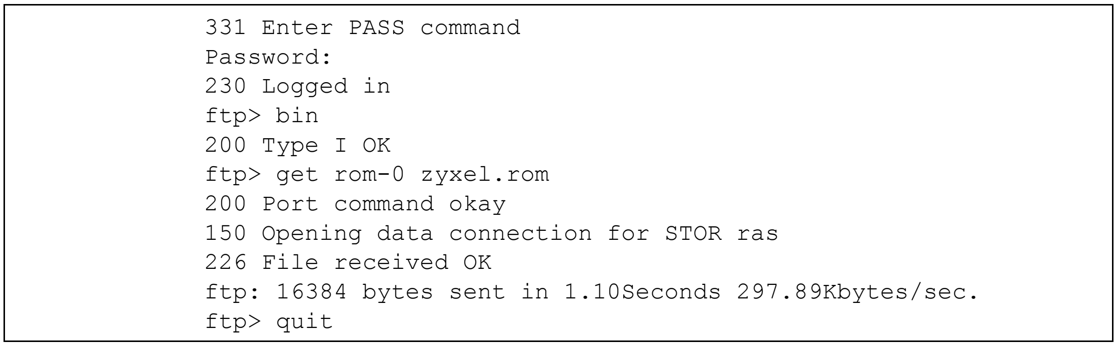
5 Enter “bin” to set transfer mode to binary.

6 Use “get” to transfer files from the ZyXEL Device to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

7 Enter “quit” to exit the ftp prompt.

29.2.3 Example of FTP Commands from the Command Line

Figure 170 FTP Session Example



```
              331 Enter PASS command
              Password:
              230 Logged in
              ftp> bin
              200 Type I OK
              ftp> get rom-0 zyxel.rom
              200 Port command okay
              150 Opening data connection for STOR ras
              226 File received OK
              ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
              ftp> quit
```

29.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 92 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

29.2.5 Remote Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

- You have disabled that service in menu 24.11.
- You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyXEL Device will disconnect the Telnet session immediately.
- You have an SMT console session running.
- 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.
- There is a firewall rule that blocks it.

29.2.6 Backup Configuration Using TFTP

The ZyXEL Device supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

3 Enter command "sys stdio 0" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the ZyXEL Device to the computer and "binary" to set binary transfer mode.

29.2.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyXEL Device IP address, "get" transfers the file source on the ZyXEL Device (rom-0, name of the configuration file on the ZyXEL Device) to the file destination on the computer and renames it config.rom.

29.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 93 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.1 is the ZyXEL Device's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyXEL Device and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyXEL Device. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

29.2.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.5 and enter "y" at the following screen.

Figure 171 System Maintenance: Backup Configuration

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

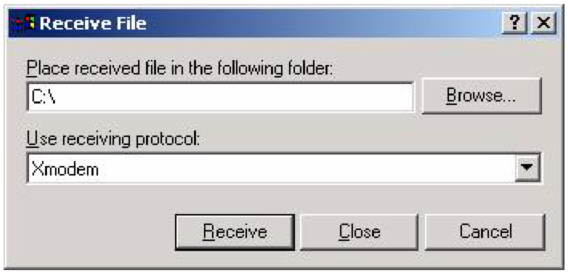
2 The following screen indicates that the Xmodem download has started.

Figure 172 System Maintenance: Starting Xmodem Download Screen

```
You can enter ctrl-x to terminate operation any
time.
Starting XMODEM download...
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

Figure 173 Backup Configuration Example



Place received file in the following folder: C:\

Use receiving protocol: Xmodem

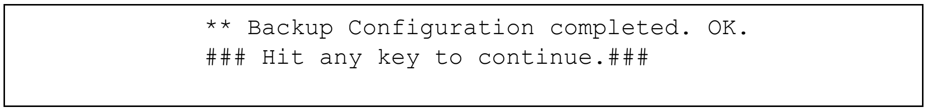
Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

Figure 174 Successful Backup Confirmation Screen



```
              ** Backup Configuration completed. OK.
              ### Hit any key to continue.###
```

29.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

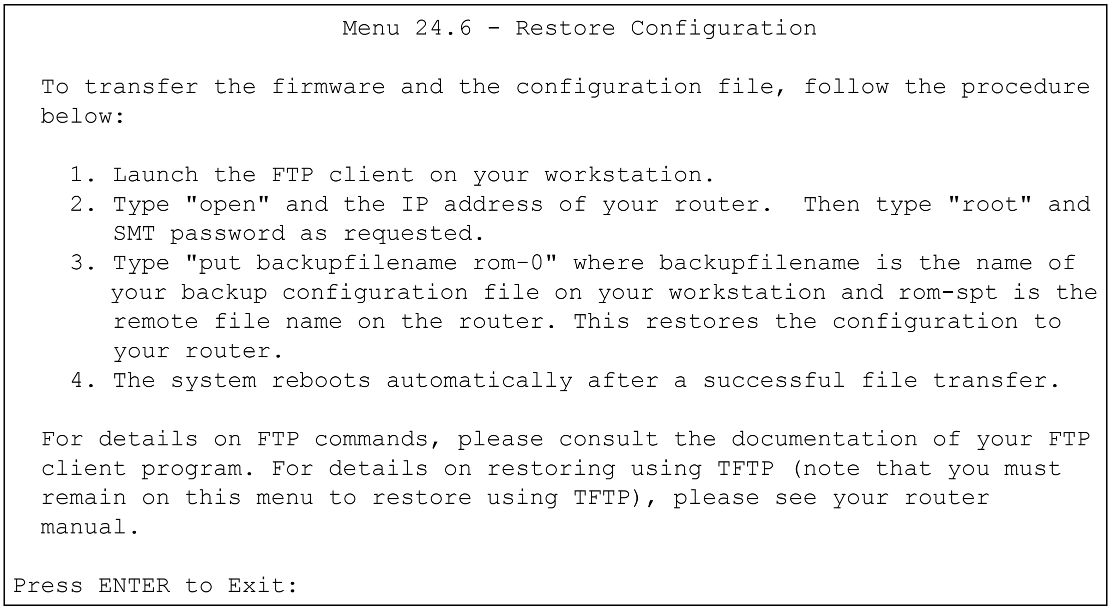
FTP is the preferred method for restoring your current computer configuration to your ZyXEL Device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Note: WARNING! Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyXEL Device.

29.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter

Figure 175 Telnet into Menu 24.6.



```
                       Menu 24.6 - Restore Configuration

  To transfer the firmware and the configuration file, follow the procedure
  below:

    1. Launch the FTP client on your workstation.
    2. Type "open" and the IP address of your router.  Then type "root" and
       SMT password as requested.
    3. Type "put backupfilename rom-0" where backupfilename is the name of
       your backup configuration file on your workstation and rom-spt is the
       remote file name on the router. This restores the configuration to
       your router.
    4. The system reboots automatically after a successful file transfer.

  For details on FTP commands, please consult the documentation of your FTP
  client program. For details on restoring using TFTP (note that you must
  remain on this menu to restore using TFTP), please see your router
  manual.

Press ENTER to Exit:
```

1 Launch the FTP client on your computer.

2 Enter “open”, followed by a space and the IP address of your ZyXEL Device.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is “1234”).

5 Enter “bin” to set transfer mode to binary.

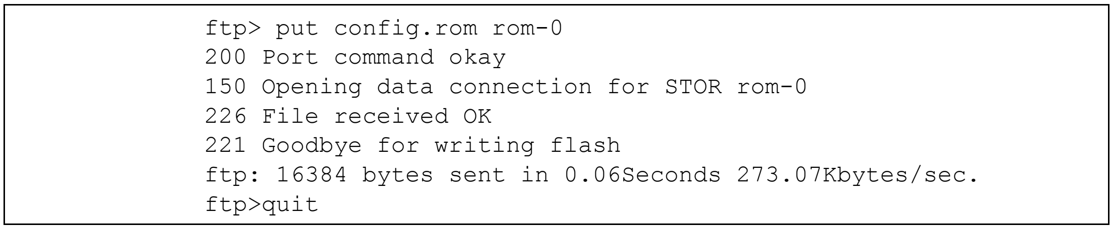
6 Find the “rom” file (on your computer) that you want to restore to your ZyXEL Device.

7 Use “put” to transfer files from the ZyXEL Device to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the ZyXEL Device. See earlier in this chapter for more information on filename conventions.

8 Enter “quit” to exit the ftp prompt. The ZyXEL Device will automatically restart after a successful restore process.

29.3.2 Restore Using FTP Session Example

Figure 176 Restore Using FTP Session Example



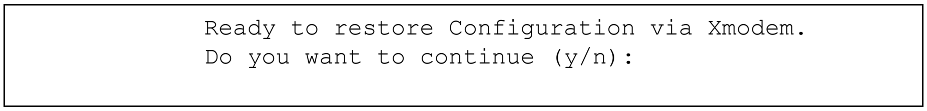
```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

29.3.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.6 and enter “y” at the following screen.

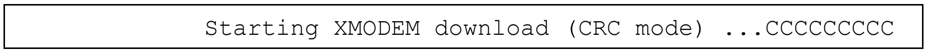
Figure 177 System Maintenance: Restore Configuration



```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

2 The following screen indicates that the Xmodem download has started.

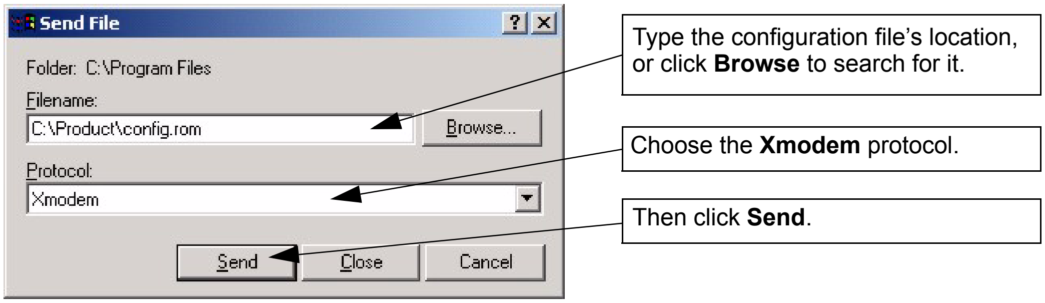
Figure 178 System Maintenance: Starting Xmodem Download Screen



```
Starting XMODEM download (CRC mode) ...CCCCCCCCC
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

Figure 179 Restore Configuration Example



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

4 After a successful restoration you will see the following screen. Press any key to restart the ZyXEL Device and return to the SMT menu.

Figure 180 Successful Restoration Confirmation Screen

```
              Save to ROM
              Hit any key to start system reboot.
```

29.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous section about restoring configuration or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File**.

Note: WARNING! Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyXEL Device.

29.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

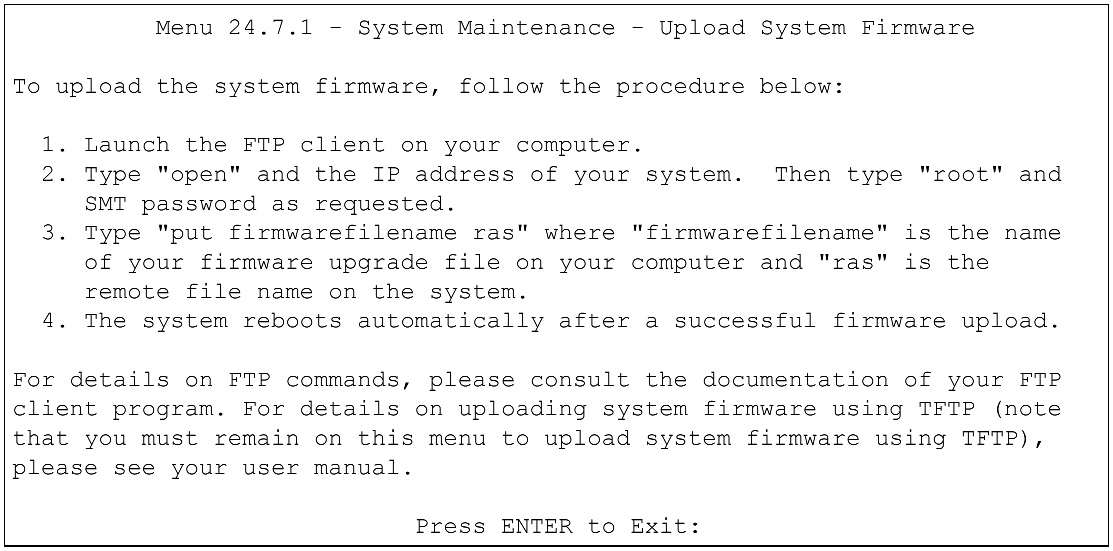
When you telnet into the ZyXEL Device, type 7 in menu 24. You will see **Menu 24.7 - System Maintenance - Upload Firmware** as shown.

Figure 181 System Maintenance Upload Firmware

```
               Menu 24.7 - System Maintenance - Upload Firmware

                   1. Upload Router Firmware
                   2. Upload Router Configuration File


                         Enter Menu Selection Number:
```

Enter 1 in menu 24.7 to display the following screen an upload firmware using FTP.

Figure 182 Menu 24.7.1 Upload System Firmware

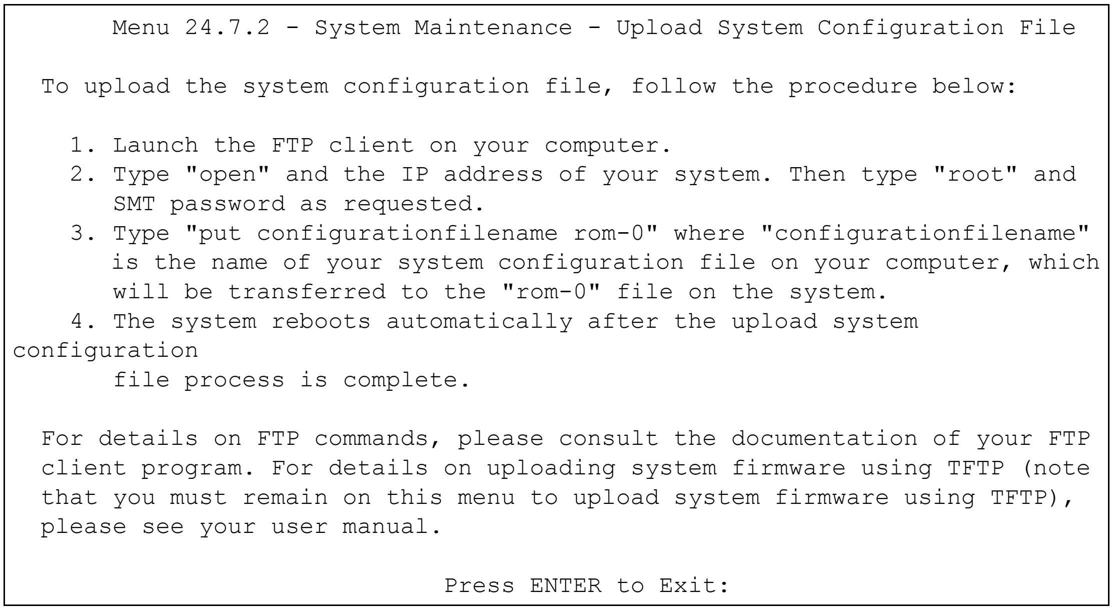


```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

  1. Launch the FTP client on your computer.
  2. Type "open" and the IP address of your system.  Then type "root" and
     SMT password as requested.
  3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your computer and "ras" is the
     remote file name on the system.
  4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your user manual.

                            Press ENTER to Exit:
```

29.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2

Figure 183 Menu 24.7.2 System Maintenance: Upload System Configuration File



```
       Menu 24.7.2 - System Maintenance - Upload System Configuration File

  To upload the system configuration file, follow the procedure below:

    1. Launch the FTP client on your computer.
    2. Type "open" and the IP address of your system. Then type "root" and
       SMT password as requested.
    3. Type "put configurationfilename rom-0" where "configurationfilename"
       is the name of your system configuration file on your computer, which
       will be transferred to the "rom-0" file on the system.
    4. The system reboots automatically after the upload system
configuration
       file process is complete.

  For details on FTP commands, please consult the documentation of your FTP
  client program. For details on uploading system firmware using TFTP (note
  that you must remain on this menu to upload system firmware using TFTP),
  please see your user manual.

                              Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

29.4.3 FTP File Upload Command from the DOS Prompt Example

1 Launch the FTP client on your computer.

2 Enter “open”, followed by a space and the IP address of your ZyXEL Device.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is “1234”).

5 Enter “bin” to set transfer mode to binary.

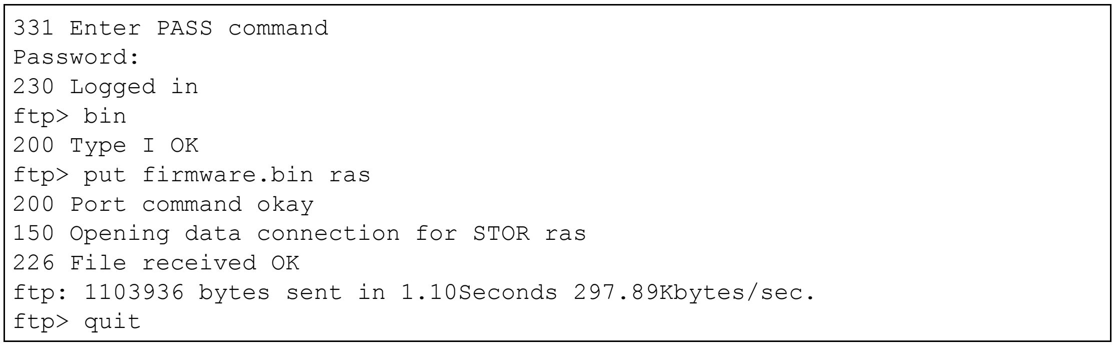
6 Use “put” to transfer files from the computer to the ZyXEL Device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyXEL Device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyXEL Device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

7 Enter “quit” to exit the ftp prompt.

Note: The ZyXEL Device automatically restarts after a successful file upload.

29.4.4 FTP Session Example of Firmware File Upload

Figure 184 FTP Session Example of Firmware File Upload



```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

29.4.5 TFTP File Upload

The ZyXEL Device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

3 Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the ZyXEL Device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyXEL Device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

29.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyXEL Device’s IP address and “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyXEL Device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

29.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyXEL Device. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyXEL Device via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

29.4.8 Uploading Firmware File Via Console Port

1 Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 - System Maintenance - Upload System Firmware**, and then follow the instructions as shown in the following screen.

Figure 185 Menu 24.7.1 As Seen Using the Console Port

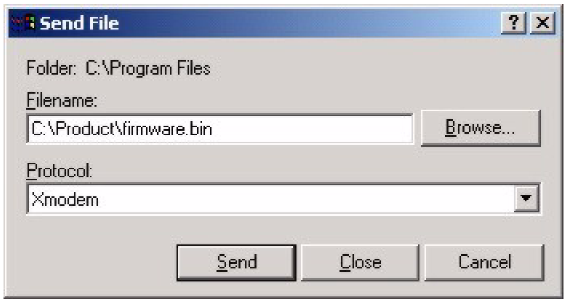
```
            Menu 24.7.1 - System Maintenance - Upload System Firmware

     To upload system firmware:
     1. Enter "y" at the prompt below to go into debug mode.
     2. Enter "atur" after "Enter Debug Mode" message.
     3. Wait for "Starting XMODEM upload" message before activating
     Xmodem upload on your terminal.
     4. After successful firmware upload, enter "atgo" to restart the router.

     Warning: Proceeding with the upload will erase the current system
     firmware.

             Do You Wish To Proceed:(Y/N)
```

2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

29.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 186 Example Xmodem Upload



Folder: C:\Program Files

Filename:
C:\Product\firmware.bin

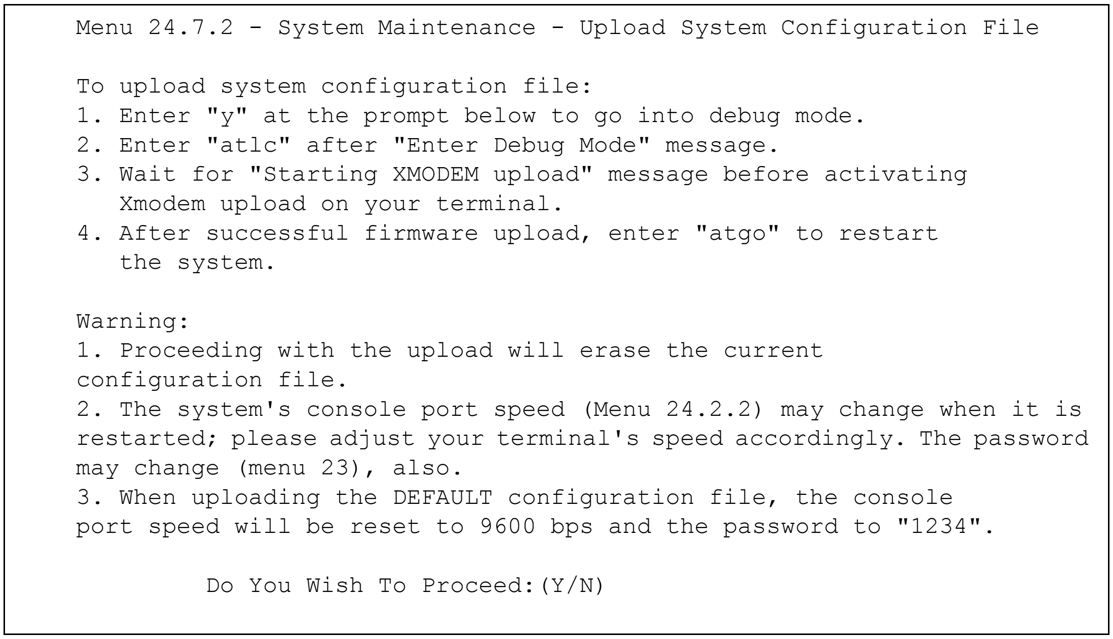
Protocol:
Xmodem

After the configuration upload process has completed, restart the ZyXEL Device by entering "atgo".

29.4.10 Uploading Configuration File Via Console Port

1 Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 - System Maintenance - Upload System Configuration File**. Follow the instructions as shown in the next screen.

Figure 187 Menu 24.7.2 As Seen Using the Console Port



```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart
   the system.

Warning:
1. Proceeding with the upload will erase the current
configuration file.
2. The system's console port speed (Menu 24.2.2) may change when it is
restarted; please adjust your terminal's speed accordingly. The password
may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
port speed will be reset to 9600 bps and the password to "1234".

         Do You Wish To Proceed:(Y/N)
```

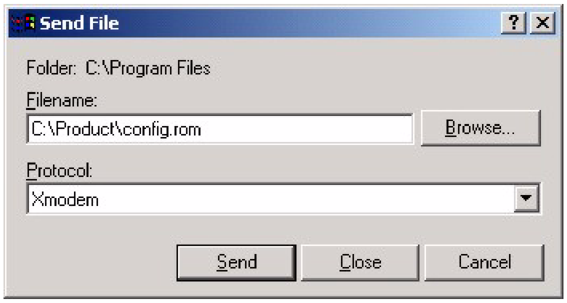
2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter “atgo” to restart the ZyXEL Device.

29.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 188 Example Xmodem Upload



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

After the configuration upload process has completed, restart the ZyXEL Device by entering "atgo".

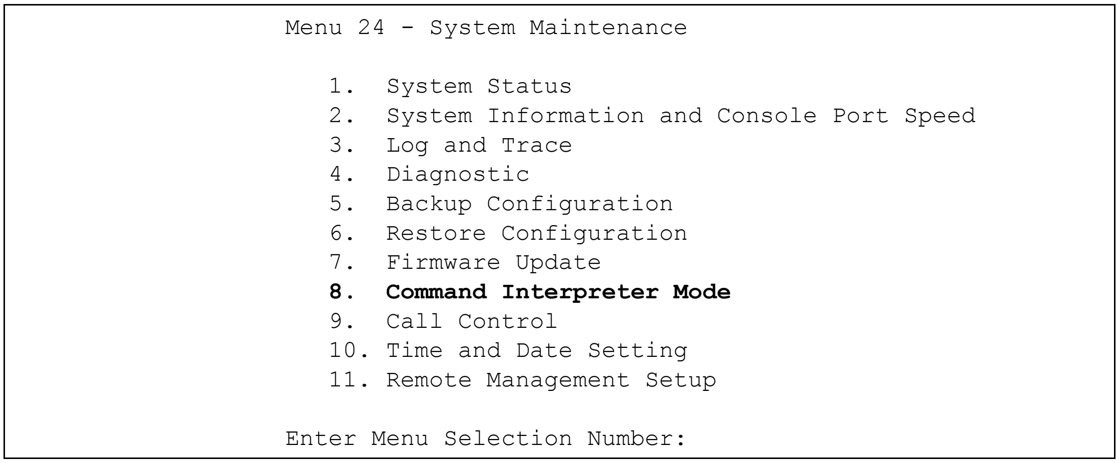
CHAPTER 30 System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

30.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type "exit" to return to the SMT main menu when finished.

Figure 189 Command Mode in Menu 24



```
                    Menu 24 - System Maintenance

                       1.  System Status
                       2.  System Information and Console Port Speed
                       3.  Log and Trace
                       4.  Diagnostic
                       5.  Backup Configuration
                       6.  Restore Configuration
                       7.  Firmware Update
                       8.  Command Interpreter Mode
                       9.  Call Control
                       10. Time and Date Setting
                       11. Remote Management Setup

                    Enter Menu Selection Number:
```

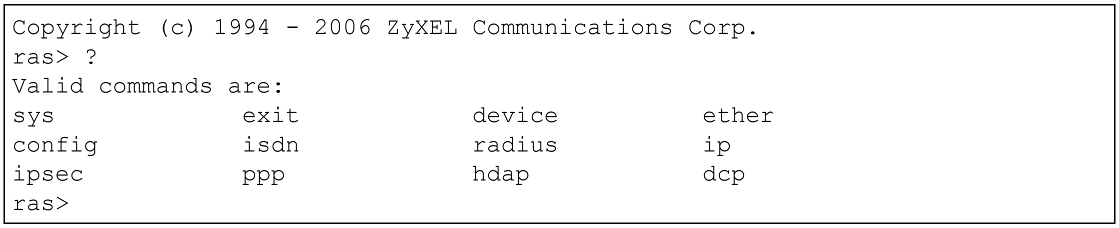
30.1.1 Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means "or".
- For example,
- sys filter netbios config <type> <on|off>
- means that you must specify the type of netbios filter and whether to turn it on or off.

30.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Figure 190 Valid Commands



```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
config          isdn            radius          ip
ipsec           ppp             hdap            dcp
ras>
```

30.2 Call Control Support

The ZyXEL Device provides four call control functions: call control parameters, blacklist, budget management and call history.

Call control parameters allows you to set a dial out time limit, the number of times a number should be called before it is added to the blacklist and the interim between calls.

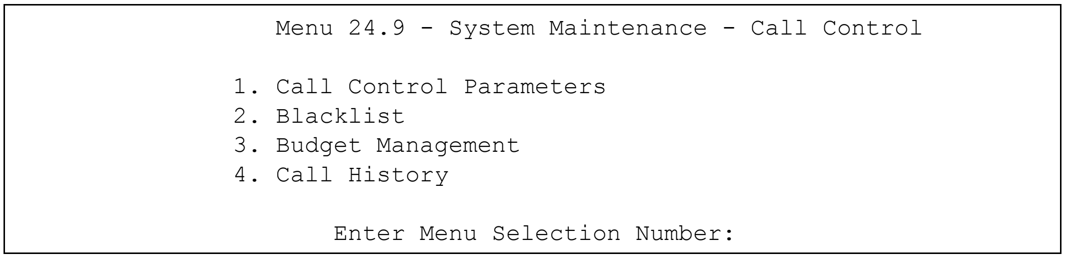
The budget management function allows you to set a limit on the total outgoing call time of the ZyXEL Device over a period of time. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

The blacklist function prevents the ZyXEL Device from re-dialing to an unreachable phone number. It is a list of phone numbers, up to a maximum of 14, to which the ZyXEL Device will not make an outgoing call. If the ZyXEL Device tries to dial to a phone number and fails a certain number of times (configurable in Menu 24.9.1), then the phone number is placed on the blacklist. You will have to enable the number manually before the ZyXEL Device will dial that number again.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

Figure 191 Menu 24.9 System Maintenance : Call Control

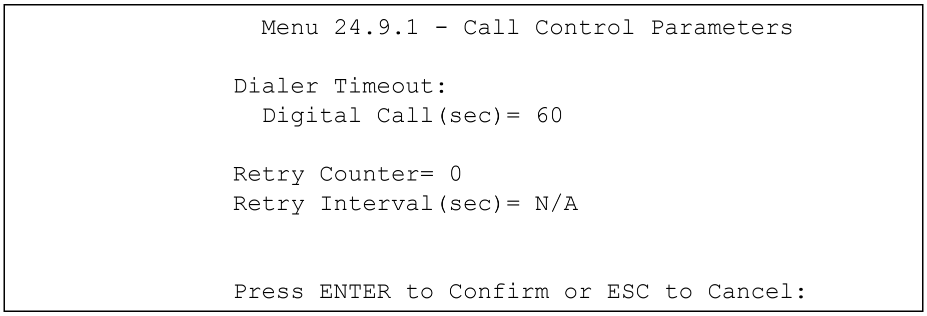


```
                   Menu 24.9 - System Maintenance - Call Control

                1. Call Control Parameters
                2. Blacklist
                3. Budget Management
                4. Call History

                       Enter Menu Selection Number:
```

30.2.1 Call Control Parameters

Menu 24.9.1 shows the call control parameters. Enter 1 from menu 24.9 to bring up the following menu.

Figure 192 Menu 24.9.1 Call Control Parameters



```
                  Menu 24.9.1 - Call Control Parameters

                Dialer Timeout:
                  Digital Call(sec)= 60

                Retry Counter= 0
                Retry Interval(sec)= N/A


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

The following table describes the labels in this menu.

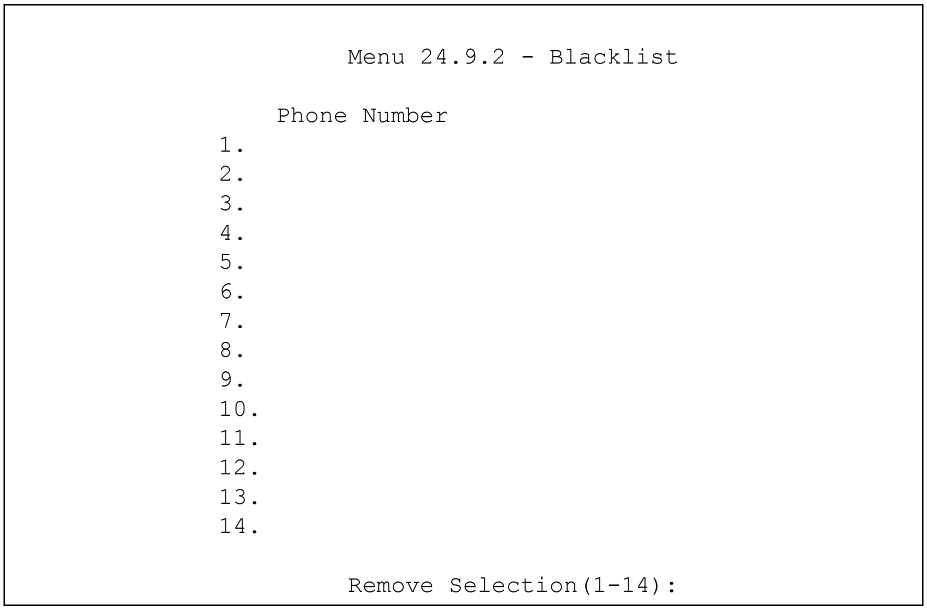
Table 94 Menu 24.9.1 Call Control Parameters

FIELD	DESCRIPTION
Dialer Timeout:	
Digital Call (sec)	The ZyXEL Device will timeout if it cannot set up an outgoing digital call within the timeout value. The default is 30.
Retry Counter	How many times a busy or 'no answer' telephone number is retried before it is put on the blacklist. The default is 0 and the blacklist control is not enabled.
Retry Interval (sec)	Elapsed time after a call fails before another call may be retried. This applies before a telephone number is blacklisted.

30.2.2 Black List

Menu 24.9.2 shows the blacklist. The phone numbers on the blacklist are numbers that the ZyXEL Device had problems connecting to in the past. The only operation allowed is taking a number off the list by entering its index number. Enter 2 from menu 24.9 to bring up the following menu.

Figure 193 Menu 24.9.2 Blacklist

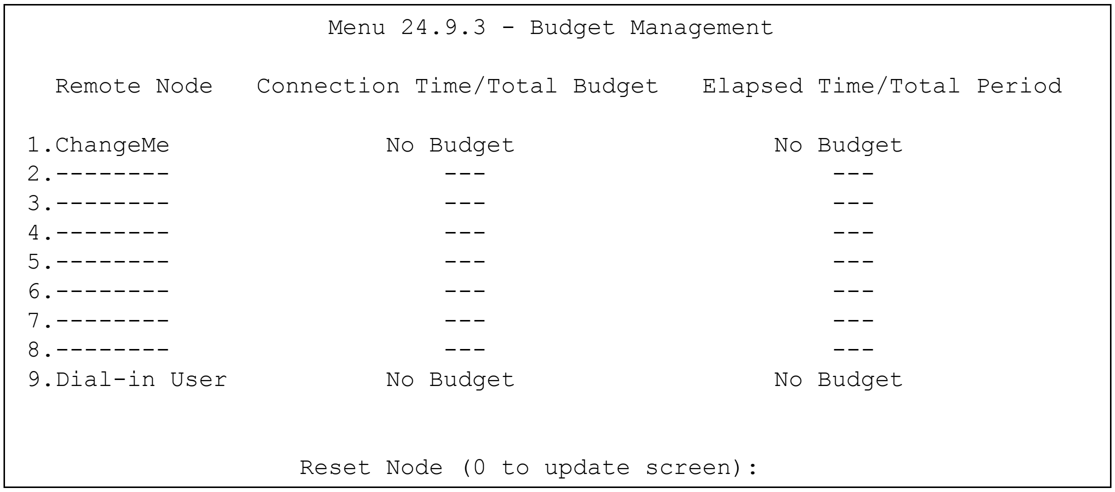


```
                   Menu 24.9.2 - Blacklist

              Phone Number
          1.
          2.
          3.
          4.
          5.
          6.
          7.
          8.
          9.
          10.
          11.
          12.
          13.
          14.

                   Remove Selection(1-14):
```

30.2.3 Budget Management

Menu 24.9.3 shows the budget management statistics for outgoing calls. Enter 3 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Figure 194 Menu 24.9.3 - Budget Management



```
                     Menu 24.9.3 - Budget Management

  Remote Node   Connection Time/Total Budget   Elapsed Time/Total Period

1.ChangeMe               No Budget                      No Budget
2.---------                  ---                            ---
3.---------                  ---                            ---
4.---------                  ---                            ---
5.---------                  ---                            ---
6.---------                  ---                            ---
7.---------                  ---                            ---
8.---------                  ---                            ---
9.Dial-in User           No Budget                      No Budget


                   Reset Node (0 to update screen):
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

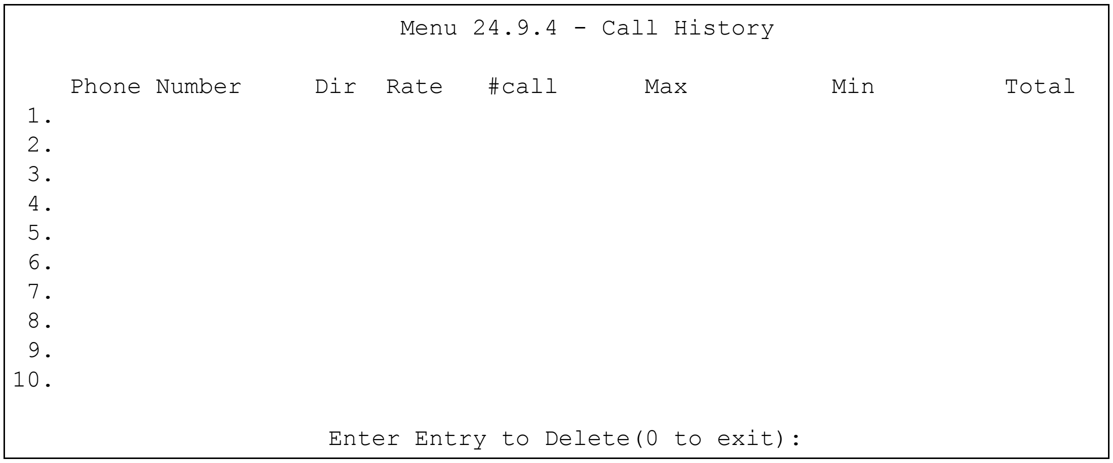
Table 95 Menu 24.9.1 - Budget Management

FIELD	DESCRIPTION
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.
Enter "0" to update the screen or press [ESC] to return to the previous screen.	

30.2.4 Call History

Menu 29.4 displays information about past incoming and outgoing calls. Enter 4 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Figure 195 Menu 24.9.4 - Call History



```
                           Menu 24.9.4 - Call History

    Phone Number     Dir  Rate   #call      Max          Min         Total
 1.
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                      Enter Entry to Delete(0 to exit):
```

The following table describes the fields in this menu.

Table 96 Call History Fields

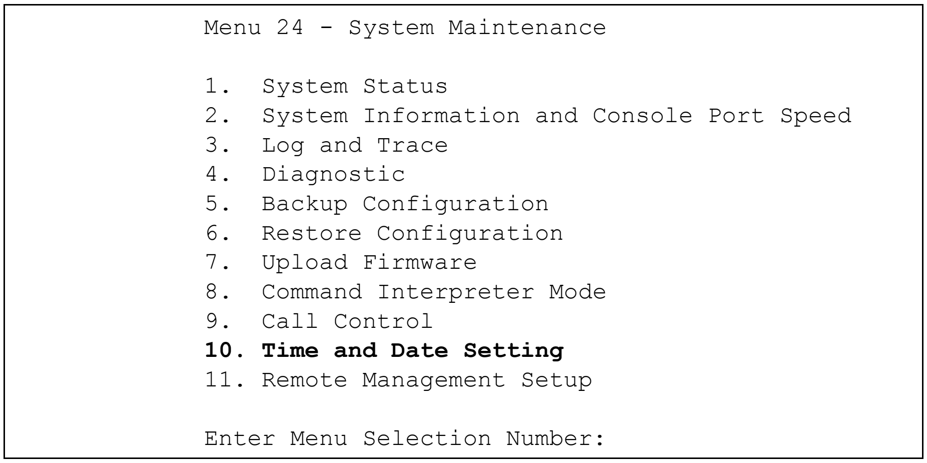
FIELD	DESCRIPTION
Phone Number	This is the telephone number of past incoming and outgoing calls.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or ‘”0” to exit.	

30.3 Time and Date Setting

The Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyXEL Device. Menu 24.10 allows you to update the time and date settings of your ZyXEL Device. The real time is then displayed in the ZyXEL Device error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

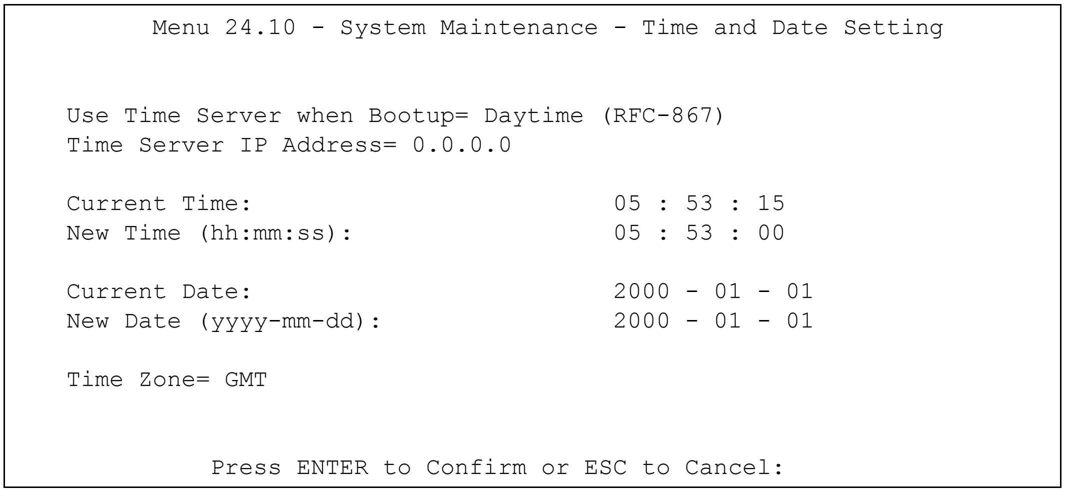
Figure 196 Menu 24: System Maintenance



```
              Menu 24 - System Maintenance

              1.  System Status
              2.  System Information and Console Port Speed
              3.  Log and Trace
              4.  Diagnostic
              5.  Backup Configuration
              6.  Restore Configuration
              7.  Upload Firmware
              8.  Command Interpreter Mode
              9.  Call Control
              10. Time and Date Setting
              11. Remote Management Setup

              Enter Menu Selection Number:
```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your ZyXEL Device as shown in the following screen.

Figure 197 Menu 24.10 System Maintenance: Time and Date Setting



```
         Menu 24.10 - System Maintenance - Time and Date Setting


    Use Time Server when Bootup= Daytime (RFC-867)
    Time Server IP Address= 0.0.0.0

    Current Time:                         05 : 53 : 15
    New Time (hh:mm:ss):                  05 : 53 : 00

    Current Date:                         2000 - 01 - 01
    New Date (yyyy-mm-dd):                2000 - 01 - 01

    Time Zone= GMT


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

The following table describes the fields in this screen.

Table 97 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your timeserver sends when you turn on the ZyXEL Device. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** the default, is similar to **Time (RFC-868)**. **None** enter the time manually.
Time Server IP Address	Enter the IP address or domain name of your timeserver. Check with your ISP/ network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

30.3.1 Resetting the Time

The ZyXEL Device resets the time in three instances:

1 On leaving menu 24.10 after making changes.

2 When the ZyXEL Device starts up, if there is a timeserver configured in menu 24.10.

3 24-hour intervals after starting.

CHAPTER 31 Remote Management

This chapter covers remote management (SMT menu 24.11).

31.1 Remote Management

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

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

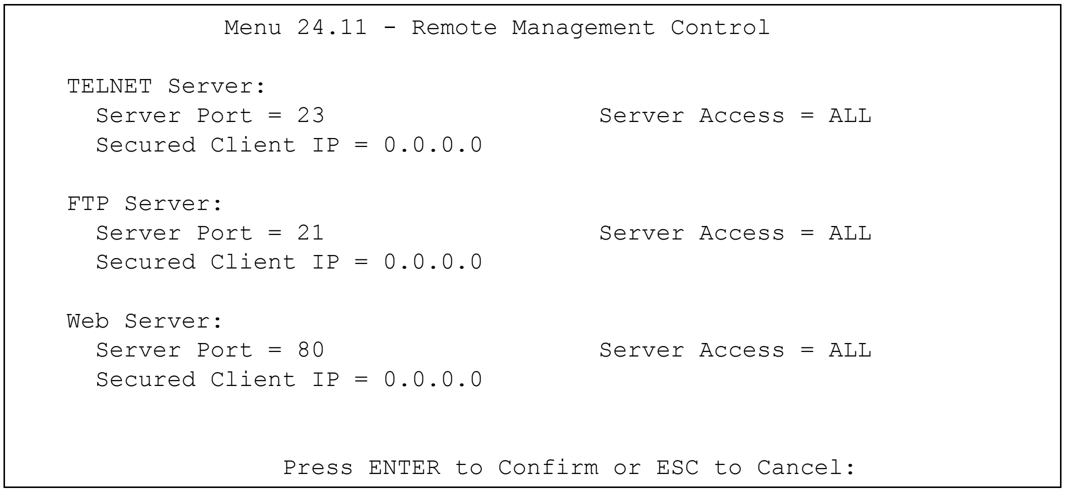
- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- Neither (Disable).

Note: When you choose **WAN only** or **ALL** (LAN & WAN), you still need to configure a firewall rule to allow access.

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

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

Figure 198 Menu 24.11 – Remote Management Control



```
               Menu 24.11 - Remote Management Control

    TELNET Server:
      Server Port = 23                   Server Access = ALL
      Secured Client IP = 0.0.0.0

    FTP Server:
      Server Port = 21                   Server Access = ALL
      Secured Client IP = 0.0.0.0

    Web Server:
      Server Port = 80                   Server Access = ALL
      Secured Client IP = 0.0.0.0


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

The following table describes the fields in this screen.

Table 98 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service or protocol.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the ZyXEL Device.
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.
Secure Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the ZyXEL Device. Enter an IP address to restrict access to a client with a matching IP address.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

31.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
4. There is an SMT console session running.
5. 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.
6. There is a firewall rule that blocks it.

31.2 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.

31.3 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 it is continuously updating the status in menu 24.1 or when sys stdio has been changed on the command line.

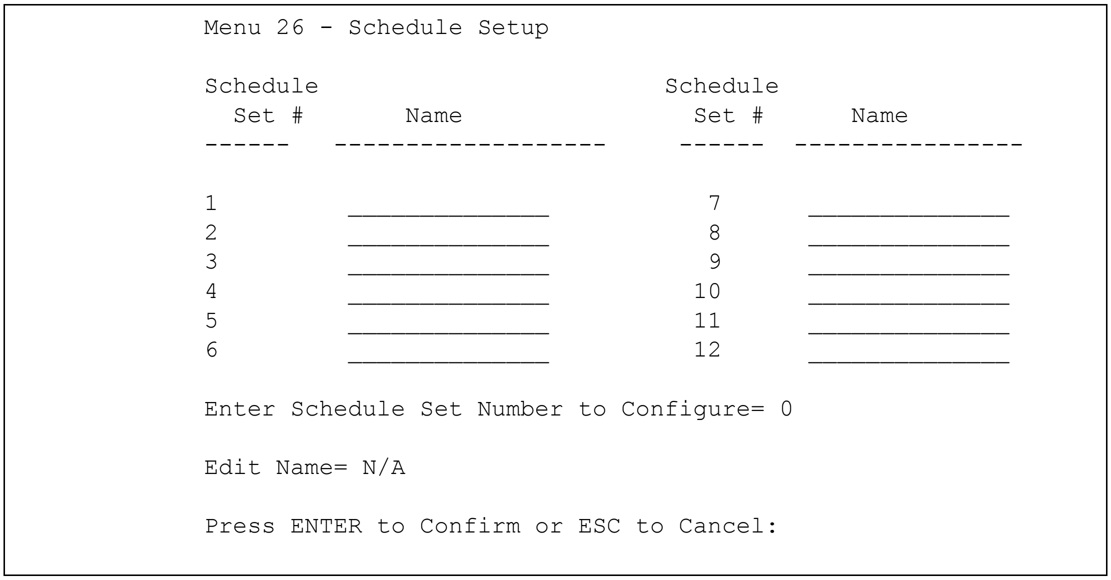
CHAPTER 32 Call Scheduling

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

32.1 Introduction to Call Scheduling

The call scheduling feature allows the ZyXEL Device to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next.

Figure 199 Menu 26 Schedule Setup



```
Menu 26 - Schedule Setup

Schedule                        Schedule
  Set #       Name                Set #      Name
------   -------------------     ------  ----------------

1         ______________          7      ______________
2         ______________          8      ______________
3         ______________          9      ______________
4         ______________         10      ______________
5         ______________         11      ______________
6         ______________         12      ______________

Enter Schedule Set Number to Configure= 0

Edit Name= N/A

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

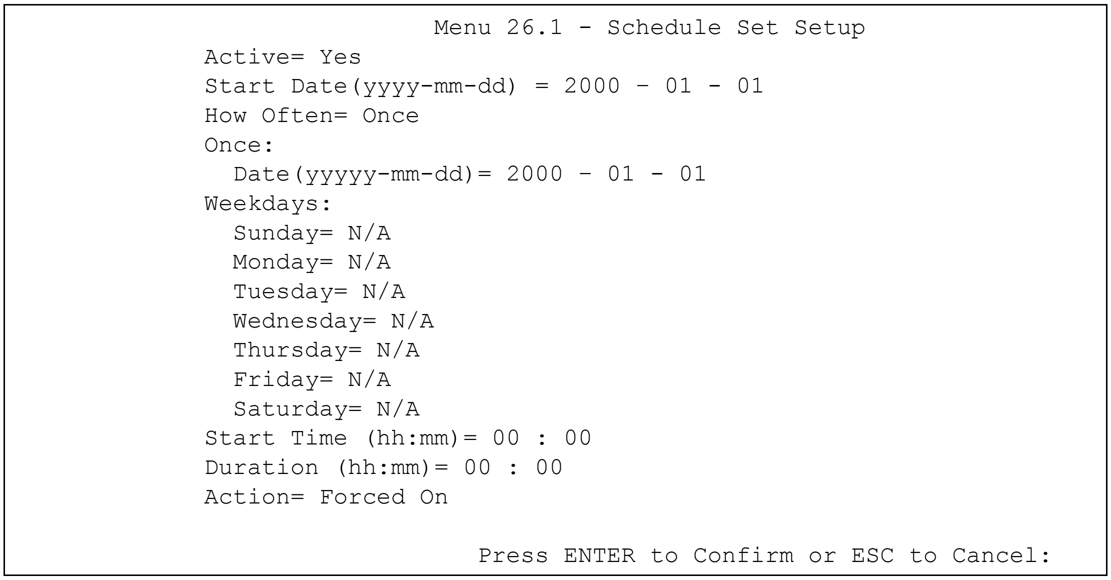
Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2 ,3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the ZyXEL Device, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

Note: To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] (or delete) in the **Edit Name** field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

Figure 200 Menu 26.1 Schedule Set Setup



```
                        Menu 26.1 - Schedule Set Setup
            Active= Yes
            Start Date(yyyy-mm-dd) = 2000 - 01 - 01
            How Often= Once
            Once:
              Date(yyyyy-mm-dd)= 2000 - 01 - 01
            Weekdays:
              Sunday= N/A
              Monday= N/A
              Tuesday= N/A
              Wednesday= N/A
              Thursday= N/A
              Friday= N/A
              Saturday= N/A
            Start Time (hh:mm)= 00 : 00
            Duration (hh:mm)= 00 : 00
            Action= Forced On

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

If a connection has been already established, your ZyXEL Device will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 99 Menu 26.1 Schedule Set Setup

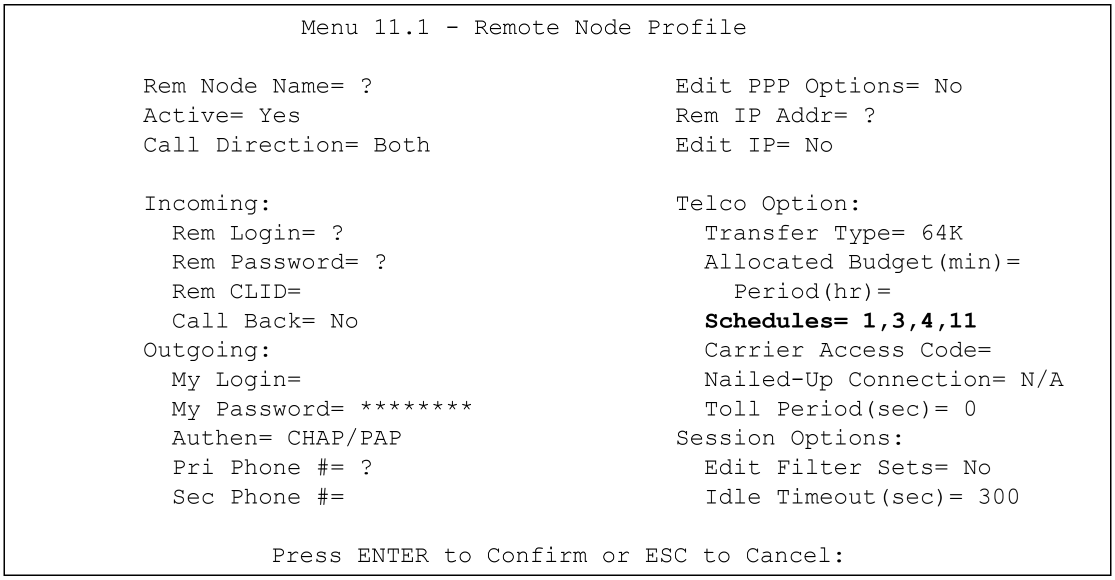
FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.
Weekdays: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.

Table 99 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Figure 201 Applying Schedule Set(s) to a Remote Node



```
                    Menu 11.1 - Remote Node Profile

         Rem Node Name= ?                     Edit PPP Options= No
         Active= Yes                          Rem IP Addr= ?
         Call Direction= Both                 Edit IP= No

         Incoming:                            Telco Option:
           Rem Login= ?                         Transfer Type= 64K
           Rem Password= ?                      Allocated Budget(min)=
           Rem CLID=                              Period(hr)=
           Call Back= No                        Schedules= 1,3,4,11
         Outgoing:                              Carrier Access Code=
           My Login=                            Nailed-Up Connection= N/A
           My Password= ********                Toll Period(sec)= 0
           Authen= CHAP/PAP                   Session Options:
           Pri Phone #= ?                       Edit Filter Sets= No
           Sec Phone #=                         Idle Timeout(sec)= 300

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

CHAPTER 33 VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

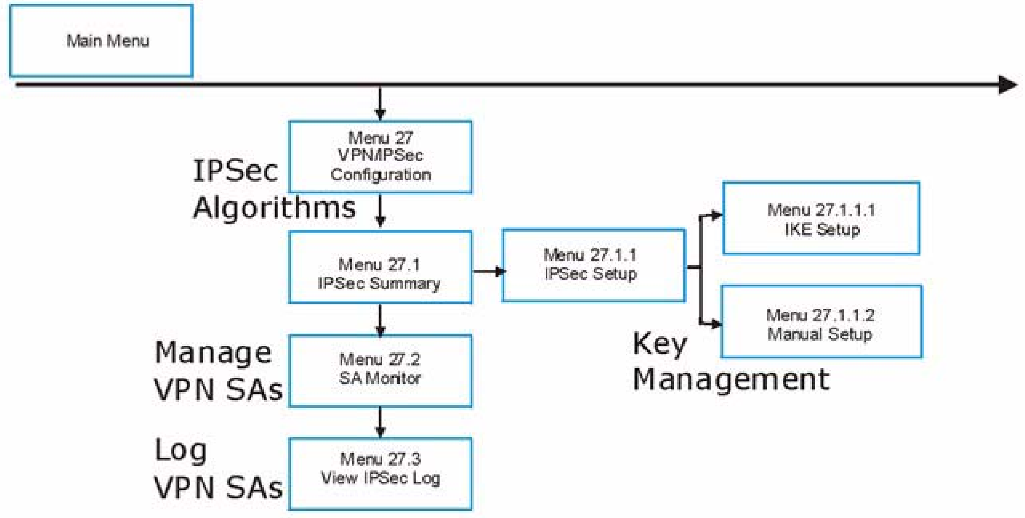
33.1 VPN/IPSec Overview

The VPN/IPSec main SMT menu has these main submenus:

1. Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.
2. **Menu 27.2 - SA Monitor** allows you to manage (refresh or disconnect) your SA connections.
3. View the IPSec connection log in menu 27.3. This menu is also useful for troubleshooting

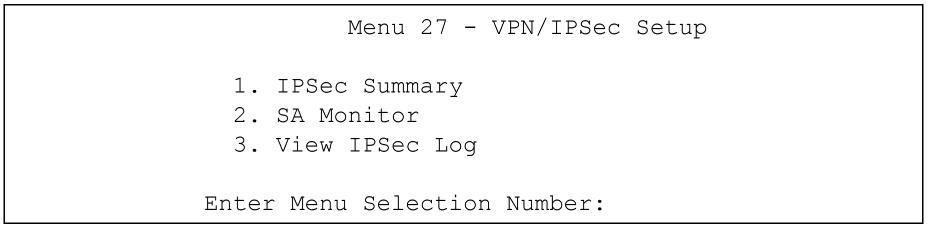
This is an overview of the VPN menu tree.

Figure 202 VPN SMT Menu Tree



From the main menu, enter 27 to display the first VPN menu (shown next).

Figure 203 Menu 27 VPN/IPSec Setup

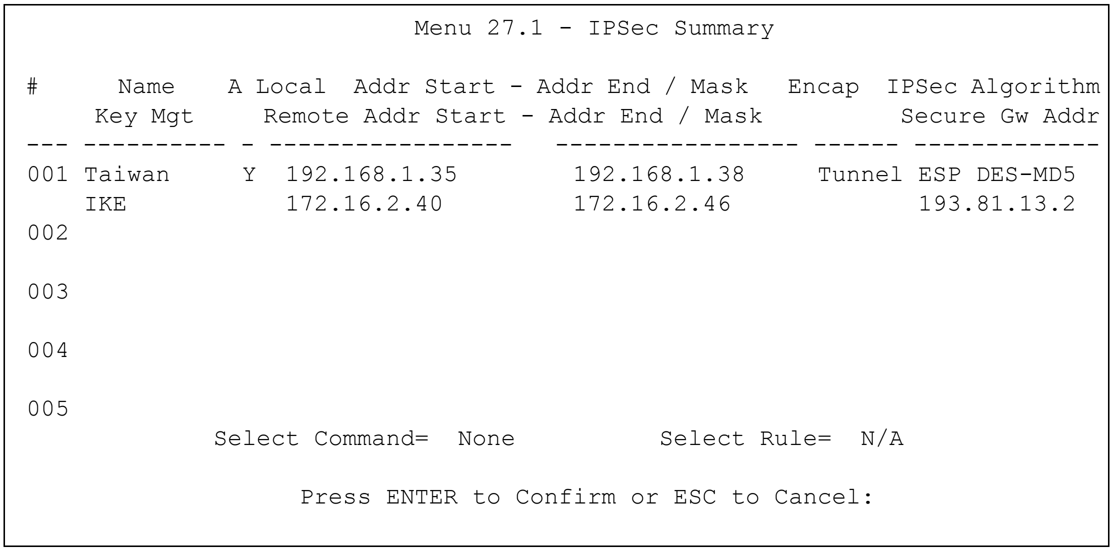


```
                      Menu 27 - VPN/IPSec Setup

              1. IPSec Summary
              2. SA Monitor
              3. View IPSec Log

            Enter Menu Selection Number:
```

33.2 IPSec Summary Screen

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 - IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

Figure 204 Menu 27



```
                           Menu 27.1 - IPSec Summary

#     Name    A Local  Addr Start - Addr End / Mask  Encap  IPSec Algorithm
     Key Mgt    Remote Addr Start - Addr End / Mask          Secure Gw Addr
--- ---------- - -----------------   ----------------- ------ -------------
001 Taiwan     Y  192.168.1.35        192.168.1.38     Tunnel ESP DES-MD5
    IKE           172.16.2.40         172.16.2.46             193.81.13.2
002

003

004

005
             Select Command=  None          Select Rule=  N/A

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

The following table describes the fields in this menu.

Table 100 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION
#	This is the VPN policy index number.
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.
A	**Y** signifies that this VPN rule is active. **N** means inactive.

Table 100 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION
Local Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SINGLE**, this is a (static) IP address on the LAN behind your ZyXEL Device. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **RANGE**, this is the beginning (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a (static) IP address on the LAN behind your ZyXEL Device.
Local Addr End / Mask	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SINGLE**, this is the same (static) IP address as in the Local Addr Start field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **RANGE**, this is the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the LAN behind your ZyXEL Device.
Encap	This field displays **Tunnel** mode or **Transport** mode. See earlier for a discussion of these. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption. **AH** (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits). Both **AH** and **ESP** increase the ZyXEL Device's processing requirements and communications latency (delay). You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.
Key Mgt	This field displays the SA's type of key management, (**IKE** or **Manual**).
Remote Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SINGLE**, this is a static IP address on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **RANGE**, this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.
Remote Addr End / Mask	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SINGLE**, this is the same (static) IP address as in the **Remote Addr Start** field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **RANGE**, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field in SMT 27.1.1 to 0.0.0.0.
Secure GW Addr	This is the WAN IP address or the domain name (up to the first 15 characters are displayed) of the IPSec router with which you are making the VPN connection. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in SMT 27.1.1 to 0.0.0.0.

Table 100 Menu 27.1 IPSec Summary

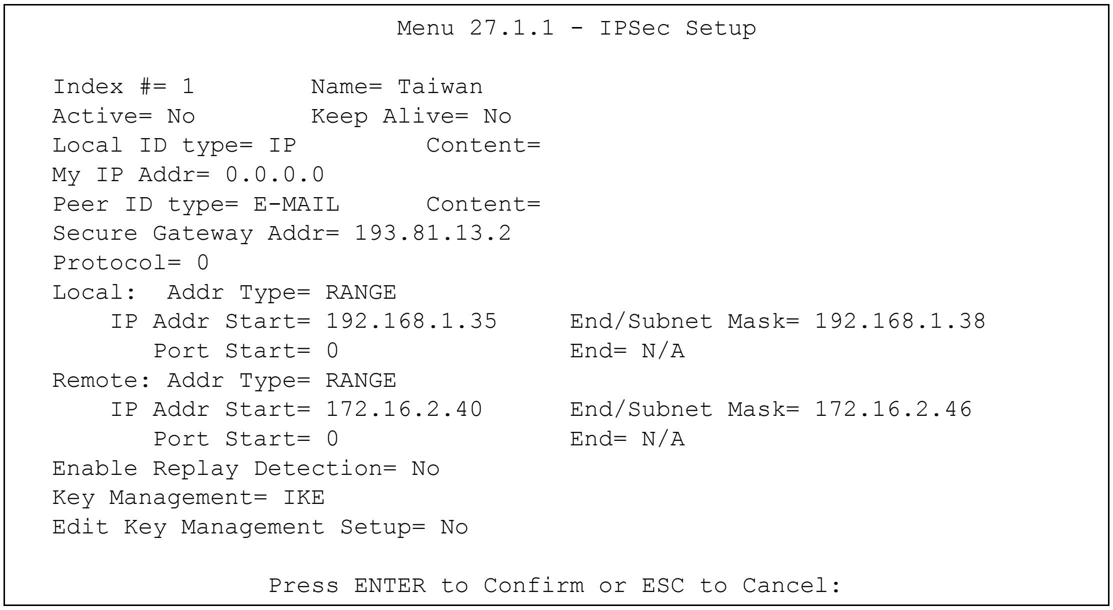
FIELD	DESCRIPTION
Select Command	Press [SPACE BAR] to choose from **None**, **Edit** or **Delete** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit** or **Delete** commands. Select **None** and then press [ENTER] to go to the “Press ENTER to Confirm…” prompt. Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do not move up in the page list.
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

33.3 IPSec Setup

Select **Edit** in the **Select Command** field, type the index number of a rule in the **Select Rule** field and press [ENTER] to edit the VPN using the menu shown next.

Note: You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.

Figure 205 Menu 27.1.1 IPSec Setup



```
                          Menu 27.1.1 - IPSec Setup

  Index #= 1        Name= Taiwan
  Active= No        Keep Alive= No
  Local ID type= IP         Content=
  My IP Addr= 0.0.0.0
  Peer ID type= E-MAIL      Content=
  Secure Gateway Addr= 193.81.13.2
  Protocol= 0
  Local:  Addr Type= RANGE
      IP Addr Start= 192.168.1.35     End/Subnet Mask= 192.168.1.38
         Port Start= 0                End= N/A
  Remote: Addr Type= RANGE
      IP Addr Start= 172.16.2.40      End/Subnet Mask= 172.16.2.46
         Port Start= 0                End= N/A
  Enable Replay Detection= No
  Key Management= IKE
  Edit Key Management Setup= No

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

The following table describes the fields in this menu.

Table 101 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION
Index	This is the VPN rule index number you selected in the previous menu.
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in **Menu 27.1 - IPSec Summary**.
Active	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to have the ZyXEL Device automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
Local ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. Select **IP** to identify this ZyXEL Device by its IP address. Select **DNS** to identify this ZyXEL Device by a domain name. Select **E-mail** to identify this ZyXEL Device by an e-mail address.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer or leave the field blank to have the ZyXEL Device automatically use its own IP address. When you select **DNS** in the **Local ID Type** field, type a domain name (up to 31 characters) by which to identify this ZyXEL Device. When you select **E-mail** in the **Local ID Type** field, type an e-mail address (up to 31 characters) by which to identify this ZyXEL Device. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.
My IP Addr	Enter the IP address of your ZyXEL Device. The ZyXEL Device uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0. The VPN tunnel has to be rebuilt if this IP address changes.
Peer ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	When you select **IP** in the **Peer ID Type** field, type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL Device automatically use the address in the **Secure Gateway Address** field. When you select **DNS** in the **Peer ID Type** field, type a domain name (up to 31 characters) by which to identify the remote IPSec router. When you select **E-mail** in the **Peer ID Type** field, type an e-mail address (up to 31 characters) by which to identify the remote IPSec router. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field below.
Secure Gateway Address	Type the IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**, see later).

Table 101 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Addr Type	This field displays **SINGLE** for a single IP address.
Local IP Addr	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Select **RANGE** for a specific range of IP addresses. Select **SUBNET** to specify IP addresses on a network by their subnet mask.
IP Addr Start	When the **Addr Type** field is configured to **SINGLE**, enter a (static) IP address on the LAN behind your ZyXEL Device. When the **Addr Type** field is configured to **RANGE**, enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyXEL Device. When the **Addr Type** is configured to **SUBNET**, this is a (static) IP address on the LAN behind your ZyXEL Device.
End/Subnet Mask	When the **Addr Type** field is configured to **SINGLE**, this field is N/A. When the **Addr Type** field is configured to **RANGE**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the **Addr Type** field is configured to **SUBNET**, this is a subnet mask on the LAN behind your ZyXEL Device.
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. You cannot create a VPN tunnel if you try to connect using a port number that does not match this port number or range of port numbers. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields are **N/A** when the **Secure Gateway Address** field is configured to 0.0.0.0. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Use **RANGE** for a specific range of IP addresses. Use **SUBNET** to specify IP addresses on a network by their subnet mask.
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the network behind the remote IPSec router. When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field is configured to **SUBNET**, enter a static IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.

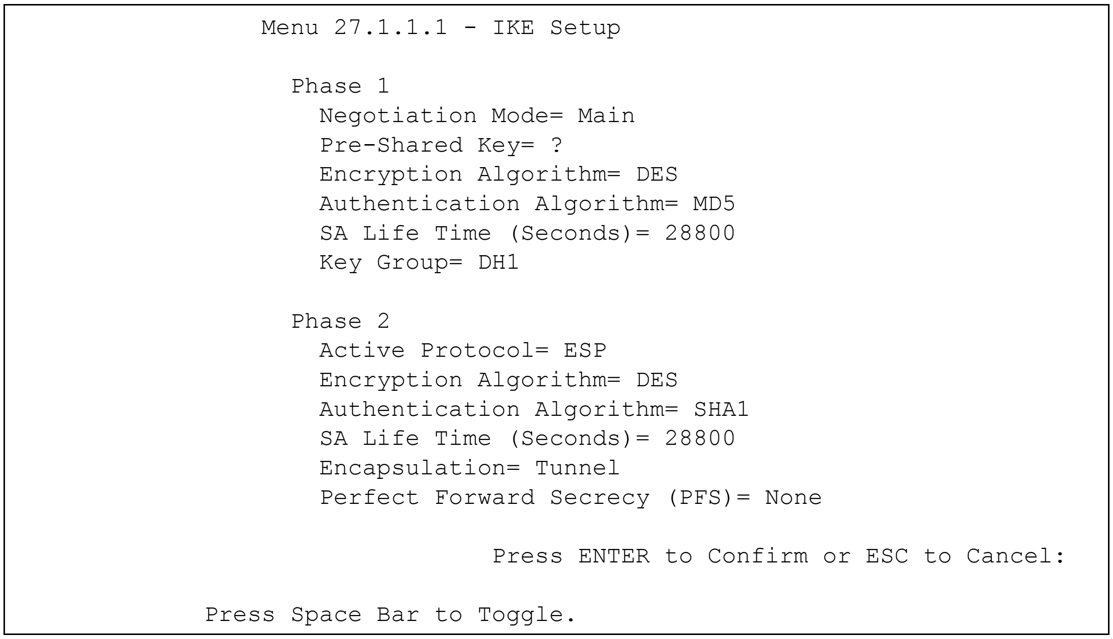
Table 101 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION
End/Subnet Mask	When the **Addr Type** field is configured to **Single**, this field is **N/A**. When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field is configured to **SUBNET**, enter a subnet mask on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Someone behind the remote IPSec router cannot create a VPN tunnel when attempting to connect using a port number that does not match this port number or range of port numbers. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **Yes**. Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to enable replay detection.
Key Management	Press [SPACE BAR] to choose either **IKE** or **Manual** and then press [ENTER]. **Manual** is useful for troubleshooting if you have problems using **IKE** key management.
Edit Key Management Setup	Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the **Key Management** field to **IKE**, this will take you to **Menu 27.1.1.1 – IKE Setup**. If you set the **Key Management** field to **Manual**, this will take you to **Menu 27.1.1.2 – Manual Setup**.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

33.4 IKE Setup

To edit this menu, the **Key Management** field in **Menu 27.1.1 – IPSec Setup** must be set to **IKE**. Move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 – IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 – IKE Setup**.

Figure 206 Menu 27.1.1.1 IKE Setup



```
                  Menu 27.1.1.1 - IKE Setup

                    Phase 1
                      Negotiation Mode= Main
                      Pre-Shared Key= ?
                      Encryption Algorithm= DES
                      Authentication Algorithm= MD5
                      SA Life Time (Seconds)= 28800
                      Key Group= DH1

                    Phase 2
                      Active Protocol= ESP
                      Encryption Algorithm= DES
                      Authentication Algorithm= SHA1
                      SA Life Time (Seconds)= 28800
                      Encapsulation= Tunnel
                      Perfect Forward Secrecy (PFS)= None

                                  Press ENTER to Confirm or ESC to Cancel:

              Press Space Bar to Toggle.
```

The following table describes the fields in this menu.

Table 102 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION
Phase 1	
Negotiation Mode	Press [SPACE BAR] to choose from **Main** or **Aggressive** and then press [ENTER]. See earlier for a discussion of these modes. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Pre-Shared Key	ZyXEL Device gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. ZyXEL Device **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**), is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in slightly increased latency and decreased throughput. Press [SPACE BAR] to choose from **3DES** or **DES** and then press [ENTER].
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slightly slower. Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].

Table 102 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IKE Security automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short **SA Life Time** increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Press [SPACE BAR] to choose from **ESP** or **AH** and then press [ENTER]. See earlier for a discussion of these protocols.
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Select **NULL** to set up a tunnel without encryption.
Authentication Algorithm	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].
SA Life Time (Seconds)	Define the length of time before an IPSec Security automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).
Encapsulation	Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

33.5 Manual Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPSec Setup**. Manual key management is useful if you have problems with **IKE** key management.

33.5.1 Active Protocol

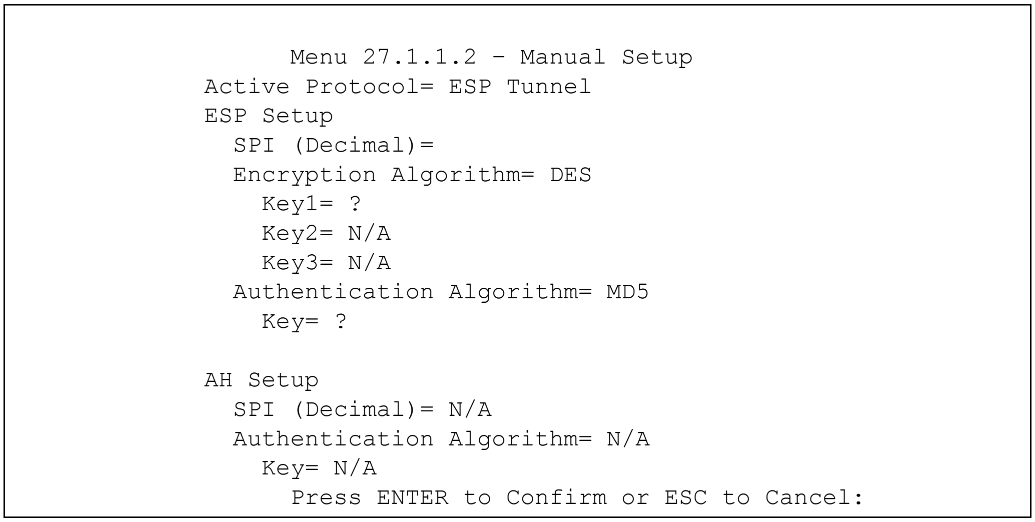
This field is a combination of mode and security protocols used for the VPN. See the Web Configurator part on VPN for more information on these parameters.

Table 103 Active Protocol: Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

To edit this menu, move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 – IPSec Setup** press [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 27.1.1.2 – Manual Setup**.

Figure 207 Menu 27.1.1.2 Manual Setup



```
                    Menu 27.1.1.2 - Manual Setup
              Active Protocol= ESP Tunnel
              ESP Setup
                SPI (Decimal)=
                Encryption Algorithm= DES
                  Key1= ?
                  Key2= N/A
                  Key3= N/A
                Authentication Algorithm= MD5
                  Key= ?

              AH Setup
                SPI (Decimal)= N/A
                Authentication Algorithm= N/A
                  Key= N/A
                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 104 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION
Active Protocol	Press [SPACE BAR] to choose from **ESP Tunnel**, **ESP Transport**, **AH Tunnel** or **AH Transport** and then press [ENTER]. Choosing an **ESP** combination causes the **AH Setup** fields to be non-applicable (**N/A**)
ESP Setup	The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**.
SPI (Decimal)	The **SPI** must be unique and from one to four integers ("0" to "9").
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Fill in the **Key1** field below when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter any encryption keys.
Key1	Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated. Fill in the **Key1** field when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**.
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.

Table 104 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION
AH Setup	The **AH Setup** fields are **N/A** if you chose an **ESP Active Protocol**.
SPI (Decimal)	The **SPI** must be from one to four unique decimal characters ("0" to "9") long.
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 34
SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

34.1 SA Monitor Overview

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

Note: When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the Web configurator part on keep alive to have the ZyXEL Device renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

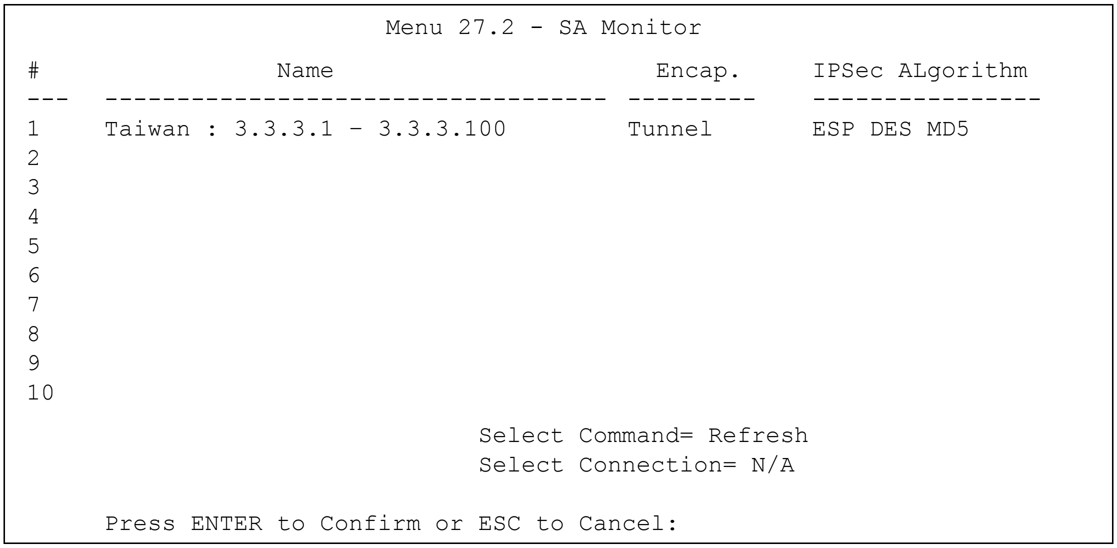
34.2 Using SA Monitor

1 Use the **Refresh** function to display active VPN connections.

2 Use the **Disconnect** function to cut off active connections.

3 Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

Figure 208 Menu 27.2 SA Monitor



```
                           Menu 27.2 - SA Monitor

 #               Name                       Encap.        IPSec ALgorithm
---   -----------------------------------  ---------     ----------------
1     Taiwan : 3.3.3.1 - 3.3.3.100          Tunnel        ESP DES MD5
2
3
4
5
6
7
8
9
10
                                  Select Command= Refresh
                                  Select Connection= N/A

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

The following table describes the fields in this menu.

Table 105 Menu 27.2 SA Monitor

FIELD	DESCRIPTION
#	This is the security index number.
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a public static IP address. When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this same VPN rule. In this case, the name is followed by the remote IP address as configured in **Menu 27.1.1. – IPSec Setup**. Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule.
Encap.	This field displays **Tunnel** mode or **Transport** mode. See previous for discussion.
IPSec ALgorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption. An incoming SA may have an **AH** in addition to **ESP**. The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits). Both **AH** and **ESP** increase ZyXEL Device processing requirements and communications latency (delay).
Select Command	Press [SPACE BAR] to choose from **Refresh**, **Disconnect** or **None** and then press [ENTER]. You must select a connection in the next field when you choose the **Disconnect** command. **Refresh** displays current active VPN connections. **None** allows you to jump to the "Press ENTER to Confirm…" prompt.
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

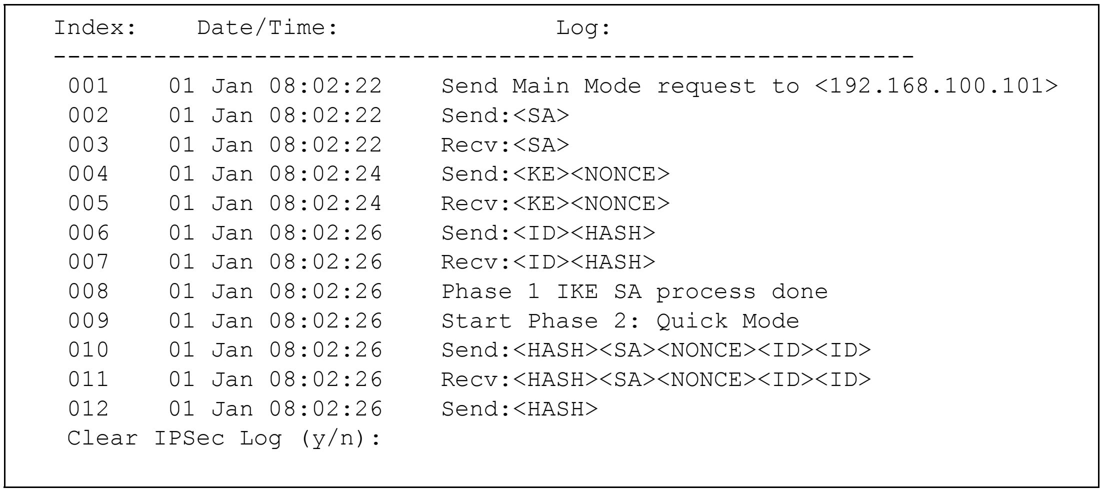
Chapter 35
IPSec Log

This chapter interprets common IPSec log messages.

35.1 IPSec Logs

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log as shown next. The following figure shows a typical log from the initiator of a VPN connection.

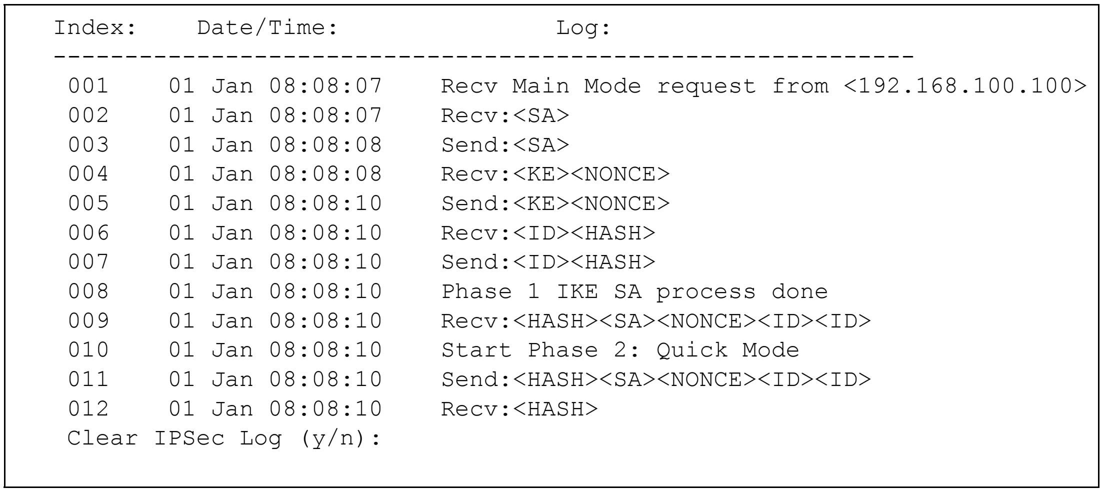
Figure 209 Example VPN Initiator IPSec Log



```
Index:    Date/Time:               Log:
------------------------------------------------------------
 001    01 Jan 08:02:22    Send Main Mode request to <192.168.100.101>
 002    01 Jan 08:02:22    Send:<SA>
 003    01 Jan 08:02:22    Recv:<SA>
 004    01 Jan 08:02:24    Send:<KE><NONCE>
 005    01 Jan 08:02:24    Recv:<KE><NONCE>
 006    01 Jan 08:02:26    Send:<ID><HASH>
 007    01 Jan 08:02:26    Recv:<ID><HASH>
 008    01 Jan 08:02:26    Phase 1 IKE SA process done
 009    01 Jan 08:02:26    Start Phase 2: Quick Mode
 010    01 Jan 08:02:26    Send:<HASH><SA><NONCE><ID><ID>
 011    01 Jan 08:02:26    Recv:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:02:26    Send:<HASH>
 Clear IPSec Log (y/n):
```

The following figure shows a typical log from the VPN connection peer.

Figure 210 Example VPN Responder IPSec Log



```
 Index:    Date/Time:              Log:
 ------------------------------------------------------------
  001    01 Jan 08:08:07    Recv Main Mode request from <192.168.100.100>
  002    01 Jan 08:08:07    Recv:<SA>
  003    01 Jan 08:08:08    Send:<SA>
  004    01 Jan 08:08:08    Recv:<KE><NONCE>
  005    01 Jan 08:08:10    Send:<KE><NONCE>
  006    01 Jan 08:08:10    Recv:<ID><HASH>
  007    01 Jan 08:08:10    Send:<ID><HASH>
  008    01 Jan 08:08:10    Phase 1 IKE SA process done
  009    01 Jan 08:08:10    Recv:<HASH><SA><NONCE><ID><ID>
  010    01 Jan 08:08:10    Start Phase 2: Quick Mode
  011    01 Jan 08:08:10    Send:<HASH><SA><NONCE><ID><ID>
  012    01 Jan 08:08:10    Recv:<HASH>
  Clear IPSec Log (y/n):
```

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.

Note: Double exclamation marks (!!) denote an error or warning message.

The following table shows sample log messages during IKE key exchange.

Table 106 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
Cannot find outbound SA for rule <#d>	The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.
Send Main Mode request to <IP> Send Aggressive Mode request to <IP>	The ZyXEL Device has started negotiation with the peer.
Recv Main Mode request from <IP> Recv Aggressive Mode request from <IP>	The ZyXEL Device has received an IKE negotiation request from the peer.
Send:<Symbol><Symbol> Recv:<Symbol><Symbol>	IKE uses the ISAKMP protocol (refer to RFC2408 - ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log - see Table 108 on page 317.
Phase 1 IKE SA process done	Phase 1 negotiation is finished.
Start Phase 2: Quick Mode	Phase 2 negotiation is beginning using Quick Mode.
!! IKE Negotiation is in process	The ZyXEL Device has begun negotiation with the peer for the connection already, but the IKE key exchange has not finished yet.
!! Duplicate requests with the same cookie	The ZyXEL Device has received multiple requests from the same peer but it is still processing the first IKE packet from that peer.

Table 106 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
!! No proposal chosen	The parameters configured for Phase 1 or Phase 2 negotiations don't match. Please check all protocols and settings for these phases. For example, one party may be using 3DES encryption, but the other party is using DES encryption, so the connection will fail.
!! Verifying Local ID failed !! Verifying Remote ID failed	During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, then the connection fails.
!! Local / remote IPs of incoming request conflict with rule <#d>	If the security gateway is "0.0.0.0", the ZyXEL Device will use the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule then the connection is not allowed.
!! Invalid IP <IP start>/<IP end>	The peer's "Local IP Addr" range is invalid.
!! Remote IP <IP start> / <IP end> conflicts	If the security gateway is "0.0.0.0", the ZyXEL Device will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the ZyXEL Device will not accept VPN connection requests from this peer.
!! Active connection allowed exceeded	The ZyXEL Device limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
!! IKE Packet Retransmit	The ZyXEL Device did not receive a response from the peer and so retransmits the last packet sent.
!! Failed to send IKE Packet	The ZyXEL Device cannot send IKE packets due to a network error.
!! Too many errors! Deleting SA	The ZyXEL Device deletes an SA when too many errors occur.

The following table shows sample log messages during packet transmission.

Table 107 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
!! WAN IP changed to <IP>	If the ZyXEL Device's WAN IP changes, all configured "My IP Addr" are changed to b "0.0.0.0".. If this field is configured as 0.0.0.0, then the ZyXEL Device will use the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find Phase 2 SA	The ZyXEL Device cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
!! Discard REPLAY packet	If the ZyXEL Device receives a packet with the wrong sequence number it will discard it.
!! Inbound packet authentication failed	The authentication configuration settings are incorrect. Please check them.
!! Inbound packet decryption failed	The decryption configuration settings are incorrect. Please check them.
Rule <#d> idle time out, disconnect	If an SA has no packets transmitted for a period of time (configurable via CI command), the ZyXEL Device drops the connection.

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

Table 108 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
LOG DISPLAY	PAYLOAD TYPE
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

CHAPTER 36 Troubleshooting

This chapter covers potential problems and the corresponding remedies.

36.1 Problems Starting Up the ZyXEL Device

Table 109 Troubleshooting Starting Up Your ZyXEL Device

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the ZyXEL Device.	Make sure that the ZyXEL Device’s power adaptor is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure that the ZyXEL Device and the power source are both turned on. Turn the ZyXEL Device off and on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.
Cannot access the ZyXEL Device via the console port.	1. Check to see if the ZyXEL Device is connected to your computer's console port. 2. Check to see if the communications program is configured correctly. The communications software should be configured as follows: • VT100 terminal emulation • 9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed. • No parity, 8 data bits, 1 stop bit, data flow set to none.

36.2 Problems with the LAN

Table 110 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	Check your Ethernet cable connections (refer to the Quick Start Guide for details). Check for faulty Ethernet cables.
	Make sure your computer’s Ethernet Card is working properly.
Cannot ping any computer on the LAN.	Check the Ethernet LEDs on the front panel. One of these LEDs should be on. If they are all off, check the cables between your ZyXEL Device and hub or the computer.
	Verify that the IP address and the subnet mask of the ZyXEL Device and the computers are on the same subnet.

36.3 Problems with the ISDN Line

Table 111 Troubleshooting the ISDN Line

PROBLEM	CORRECTIVE ACTION
The ISDN initialization failed. This problem occurs when you attempt to save the parameters entered in the **Wizard Setup** or **WAN** screen or SMT Menu 2, but receive the message, 'Save successful, but Failed to initialize ISDN; Press [Esc] to exit'.	Check the error log (in **Menu 24.3.1**), you should see a log entry for the ISDN initialization failure in the format, '**ISDN init failed. code<n> . . .**'. Note the code number, n. If the code is **1**, the ISDN link is not up. This problem could be either the ISDN line is not properly connected to the ZyXEL Device or the ISDN line is not activated. Verify that the ISDN line is connected to the ZyXEL Device and to the wall telephone jack. If the code is **3**, this indicates a general failure. Verify the provisioning information for your switch by contacting your telephone company. Check your SPID numbers if the ISDN LED is blinking slowly as this indicates that SPID negotiation has failed (North America only).
The ISDN loopback test failed.	If the ISDN initialization is successful, then the loopback test should also work. Verify the telephone numbers that have been entered in the **Wizard Setup** or **WAN** screen or SMT **Menu 2**. The loopback test dials the number entered in the second Phone **#** field (except for switch types with only one phone number). If you need to dial a prefix (e.g., '9') to get an outside line, then you have to enter the telephone number as '95551212' or '914085551212'. If it is an internal line, you may only need to enter the last four or five digits (according to your internal dialing plan), e.g., 51212.

36.4 Problems with Remote User Dial-in

Table 112 Troubleshooting Remote User Dial-in

PROBLEM	CORRECTIVE ACTION
A remote user cannot dial-in.	First verify that you have configured the authentication parameters in Menu 13. These would be **CLID Authen** and **Recv Authen**. In Menu 14.1, verify the user name and password for the remote dial-in user. If the remote dial-in user is negotiating IP, verify that the IP address is supplied correctly in Menu 13. Check that either the remote dial-in user is supplying a valid IP address, or that the ZyXEL Device is assigning a valid address from the IP pool. If the remote dial-in user is negotiating IPX, verify that the IPX network number is valid from the IPX pool (if it is being used).

36.5 Problems Accessing the ZyXEL Device

Table 113 Troubleshooting Accessing the ZyXEL Device

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	The default user password is "user" and admin password is "1234". The **Password** field is case-sensitive. Make sure that you enter the correct password using the proper case. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.
I cannot access the web configurator.	Make sure that there is not a Telnet session running. Use the ZyXEL Device's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection. Use the ZyXEL Device's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details. Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access. If you changed the ZyXEL Device's LAN IP address, then enter the new one as the URL. Make sure that pop-up windows, JavaScripts and Java permissions are allowed. See the appendix for how to enable them.

APPENDIX A

Product Specifications

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

Specification Tables

Table 114 Device

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.38
Dimensions (W x D x H)	230 x 161 x 35 mm
Power Specification	12VAC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
Operation Temperature	0º C ~ 40º C
Storage Temperature	-20º ~ 60º C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH
Distance between the centers of the holes on the device's back.	108 mm
Screw size for wall-mounting	M3*10

Table 115 Firmware

ISDN Switch Type	Europe: DSS1 (NET3) with the following deltas: German, French, Swiss, Italy, U.K., N. Europe
ISDN Standards	IETF RFC 1661 Point-to-Point Protocol (PPP) IETF RFC 1990 Multilink PPP IEEE 802.3 10Base-T physical layer specification
Other Protocol Support	Transparent bridging for unsupported network layer protocols. DHCP Server/Client/Relay RIP I/RIP II ICMP ATM QoS IP Multicasting IGMP v1 and v2 IGMP Proxy

Table 115 Firmware (continued)

Management	Embedded Web Configurator Menu-driven SMT (System Management Terminal) management Remote Management via Telnet or Web FTP/TFTP for firmware downloading, configuration backup and restoration. Built-in Diagnostic Tools for FLASH memory, ISDN circuitry, RAM and LAN port
Firewall	Stateful Packet Inspection. Prevent Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc. Real time E-mail alerts. Reports and logs.
VPN (ICSA Certified)	Manual key, IKE PKI (X.509) Encryption (DES and 3DES) Authentication (SHA-1 and MD5) DH1/2, RSA signature
Supplemental Phone Service	Call Waiting Call Hold Call Retrieve Three Party Conference Call Forwarding Multiple Subscriber Number (MSN) / Subaddress Terminal Portability:

Appendix B
Wall-mounting Instructions

Do the following to hang your ZyXEL Device on a wall.

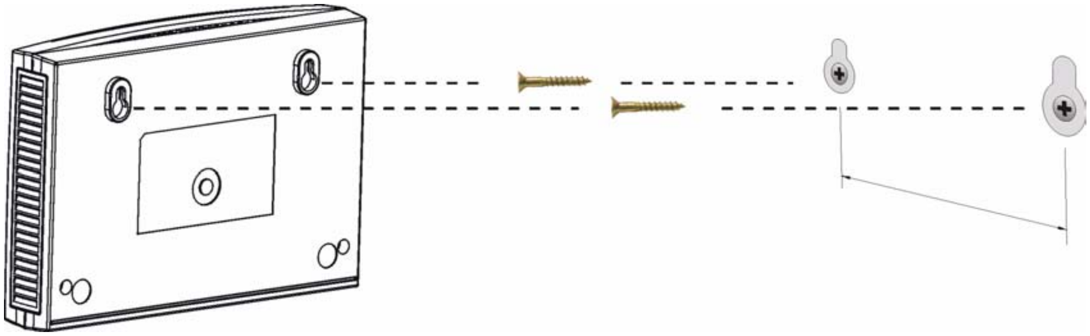
Note: See the product specifications appendix for the size of screws to use and how far apart to place them.

1. Locate a high position on wall that is free of obstructions. Use a sturdy wall.
2. Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

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

3. Do not screw 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 211 Wall-mounting Example



Appendix C
Log Descriptions

This appendix provides descriptions of example log messages.

Table 116 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`WAN interface gets IP:%s`	A WAN interface got a new IP address from the DHCP, or ISDN server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns%s`	The DHCP server assigned an IP address to a client.
`Successful WEB login`	Someone has logged on to the router's web configurator interface.
`WEB login failed`	Someone has failed to log on to the router's web configurator interface.
`Successful TELNET login`	Someone has logged on to the router via telnet.
`TELNET login failed`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the router via ftp.
`FTP login failed`	Someone has failed to log on to the router via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Starting Connectivity Monitor`	Starting Connectivity Monitor.
`Too large ICMP packet has been dropped`	The router dropped an ICMP packet that was too large.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The router is saving configuration changes.

Table 117 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
`setNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.

Table 117 System Error Logs (continued)

LOG MESSAGE	DESCRIPTION
`readNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`WAN connection is down.`	A WAN connection is down. You cannot access the network through this interface.

Table 118 Access Control Logs

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

Table 119 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
`Under SYN flood attack, sent TCP RST`	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
`Exceed TCP MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
`Peer TCP state out of order, sent TCP RST`	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.

Table 119 TCP Reset Logs (continued)

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

Table 120 Packet Filter Logs

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

Table 121 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting. For type and code details, see Table 129 on page 336.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn’t match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. For type and code details, see Table 129 on page 336.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn’t have a corresponding NAT table entry.

Table 121 ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 122 CDR Logs

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

Table 123 Attack Logs

LOG MESSAGE	DESCRIPTION
`attack [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
`attack ICMP (type:%d, code:%d)`	The firewall detected an ICMP attack. For type and code details, see Table 129 on page 336.
`land [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
`land ICMP (type:%d, code:%d)`	The firewall detected an ICMP land attack. For type and code details, see Table 129 on page 336.
`ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall detected an IP spoofing attack on the WAN port.
`ip spoofing - WAN ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack on the WAN port. For type and code details, see Table 129 on page 336.
`icmp echo: ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack. For type and code details, see Table 129 on page 336.
`syn flood TCP`	The firewall detected a TCP syn flood attack.
`ports scan TCP`	The firewall detected a TCP port scan attack.
`teardrop TCP`	The firewall detected a TCP teardrop attack.
`teardrop UDP`	The firewall detected an UDP teardrop attack.

Table 123 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack. For type and code details, see Table 129 on page 336.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall classified a packet with no source routing entry as an IP spoofing attack.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack. For type and code details, see Table 129 on page 336.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack. For type and code details, see Table 129 on page 336.

Table 124 IPSec Logs

LOG MESSAGE	DESCRIPTION
`Discard REPLAY packet`	The router received and discarded a packet with an incorrect sequence number.
`Inbound packet authentication failed`	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
`Receive IPSec packet, but no corresponding tunnel exists`	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
`Rule <%d> idle time out, disconnect`	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes.
`WAN IP changed to <IP>`	The router dropped all connections with the “MyIP” configured as “0.0.0.0” when the WAN IP address changed.

Table 125 IKE Logs

LOG MESSAGE	DESCRIPTION
`Active connection allowed exceeded`	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
`Start Phase 2: Quick Mode`	Phase 2 Quick Mode has started.
`Verifying Remote ID failed:`	The connection failed during IKE phase 2 because the router and the peer’s Local/Remote Addresses don’t match.

Table 125 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Verifying Local ID failed:`	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
`IKE Packet Retransmit`	The router retransmitted the last packet sent because there was no response from the peer.
`Failed to send IKE Packet`	An Ethernet error stopped the router from sending IKE packets.
`Too many errors! Deleting SA`	An SA was deleted because there were too many errors.
`Phase 1 IKE SA process done`	The phase 1 IKE SA process has been completed.
`Duplicate requests with the same cookie`	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
`IKE Negotiation is in process`	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
`No proposal chosen`	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
`Local / remote IPs of incoming request conflict with rule <%d>`	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
`Cannot resolve Secure Gateway Addr for rule <%d>`	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
`Peer ID: <peer id> <My remote type> -<My local type>`	The displayed ID information did not match between the two ends of the connection.
`vs. My Remote <My remote> - <My remote>`	The displayed ID information did not match between the two ends of the connection.
`vs. My Local <My local>-<My local>`	The displayed ID information did not match between the two ends of the connection.
`Send <packet>`	A packet was sent.
`Recv <packet>`	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
`Recv <Main or Aggressive> Mode request from <IP>`	The router received an IKE negotiation request from the peer address specified.
`Send <Main or Aggressive> Mode request to <IP>`	The router started negotiation with the peer.
`Invalid IP <Peer local> / <Peer local>`	The peer's "Local IP Address" is invalid.
`Remote IP <Remote IP> / <Remote IP> conflicts`	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
`Phase 1 ID type mismatch`	This router's "Peer ID Type" is different from the peer IPSec router's "Local ID Type".
`Phase 1 ID content mismatch`	This router's "Peer ID Content" is different from the peer IPSec router's "Local ID Content".

Table 125 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`No known phase 1 ID type found`	The router could not find a known phase 1 ID in the connection attempt.
`ID type mismatch. Local / Peer: <Local ID type/Peer ID type>`	The phase 1 ID types do not match.
`ID content mismatch`	The phase 1 ID contents do not match.
`Configured Peer ID Content: <Configured Peer ID Content>`	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
`Incoming ID Content: <Incoming Peer ID Content>`	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
`Unsupported local ID Type: <%d>`	The phase 1 ID type is not supported by the router.
`Build Phase 1 ID`	The router has started to build the phase 1 ID.
`Adjust TCP MSS to%d`	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
`Rule <%d> input idle time out, disconnect`	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
`XAUTH succeed! Username: <Username>`	The router used extended authentication to authenticate the listed username.
`XAUTH fail! Username: <Username>`	The router was not able to use extended authentication to authenticate the listed username.
`Rule[%d] Phase 1 negotiation mode mismatch`	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
`Rule [%d] Phase 1 encryption algorithm mismatch`	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
`Rule [%d] Phase 1 authentication algorithm mismatch`	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.
`Rule [%d] Phase 1 authentication method mismatch`	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
`Rule [%d] Phase 1 key group mismatch`	The listed rule's IKE phase 1 key group did not match between the router and the peer.
`Rule [%d] Phase 2 protocol mismatch`	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
`Rule [%d] Phase 2 encryption algorithm mismatch`	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.
`Rule [%d] Phase 2 authentication algorithm mismatch`	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
`Rule [%d] Phase 2 encapsulation mismatch`	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
`Rule [%d]> Phase 2 pfs mismatch`	The listed rule's IKE phase 2 perfect forward secret (pfs) setting did not match between the router and the peer.

Table 125 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rule [%d] Phase 1 ID mismatch`	The listed rule’s IKE phase 1 ID did not match between the router and the peer.
`Rule [%d] Phase 1 hash mismatch`	The listed rule’s IKE phase 1 hash did not match between the router and the peer.
`Rule [%d] Phase 1 preshared key mismatch`	The listed rule’s IKE phase 1 pre-shared key did not match between the router and the peer.
`Rule [%d] Tunnel built successfully`	The listed rule’s IPSec tunnel has been built successfully.
`Rule [%d] Peer's public key not found`	The listed rule’s IKE phase 1 peer’s public key was not found.
`Rule [%d] Verify peer's signature failed`	The listed rule’s IKE phase 1verification of the peer’s signature failed.
`Rule [%d] Sending IKE request`	IKE sent an IKE request for the listed rule.
`Rule [%d] Receiving IKE request`	IKE received an IKE request for the listed rule.
`Swap rule to rule [%d]`	The router changed to using the listed rule.
`Rule [%d] Phase 1 key length mismatch`	The listed rule’s IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
`Rule [%d] phase 1 mismatch`	The listed rule’s IKE phase 1 did not match between the router and the peer.
`Rule [%d] phase 2 mismatch`	The listed rule’s IKE phase 2 did not match between the router and the peer.
`Rule [%d] Phase 2 key length mismatch`	The listed rule’s IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.

Table 126 PKI Logs

LOG MESSAGE	DESCRIPTION
`Enrollment successful`	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
`Enrollment failed`	The SCEP online certificate enrollment failed. The Destination field records the certification authority server’s IP address and port.
`Failed to resolve <SCEP CA server url>`	The SCEP online certificate enrollment failed because the certification authority server’s address cannot be resolved.
`Enrollment successful`	The CMP online certificate enrollment was successful. The Destination field records the certification authority server’s IP address and port.
`Enrollment failed`	The CMP online certificate enrollment failed. The Destination field records the certification authority server’s IP address and port.
`Failed to resolve <CMP CA server url>`	The CMP online certificate enrollment failed because the certification authority server’s IP address cannot be resolved.

Table 126 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rcvd ca cert: <subject name>`	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd user cert: <subject name>`	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd CRL <size>: <issuer name>`	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd ARL <size>: <issuer name>`	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ca cert`	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received user cert`	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 127 on page 334 for the corresponding descriptions of the codes.

Table 127 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.

Table 127 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 128 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L)	LAN to LAN/ ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W)	WAN to WAN/ ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.

Table 129 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

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

Table 130 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

APPENDIX D
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.

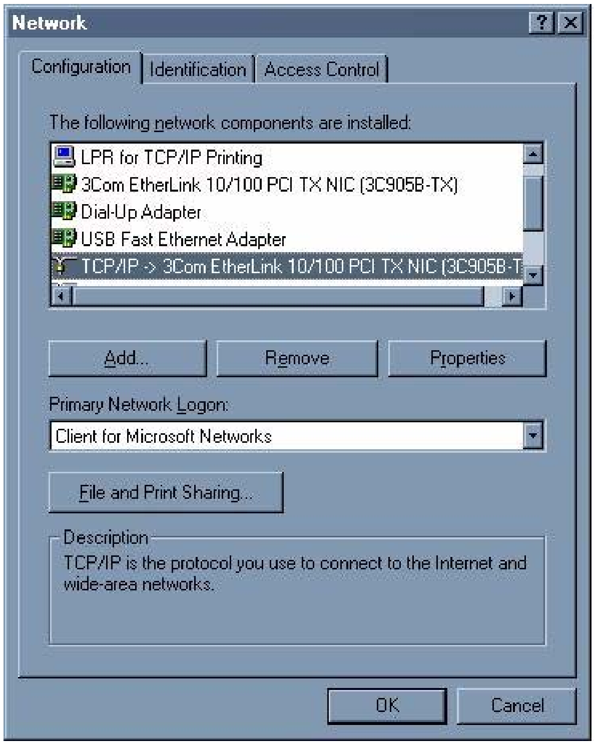
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 212 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

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

Primary Network Logon:
Client for Microsoft Networks

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

Installing Components

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

If you need the adapter:

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

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

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

If you need TCP/IP:

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

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

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

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

If you need Client for Microsoft Networks:

1 Click **Add**.

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

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

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

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

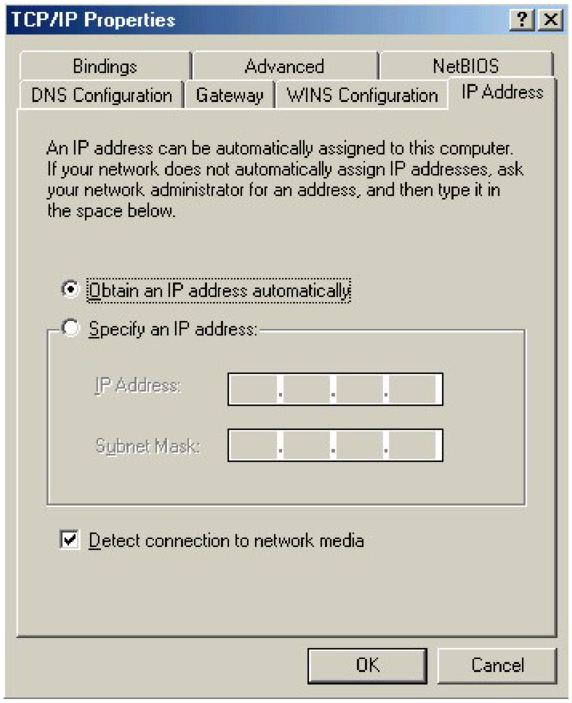
Configuring

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

2 Click the **IP Address** tab.

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

Figure 213 Windows 95/98/Me: TCP/IP Properties: IP Address



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

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

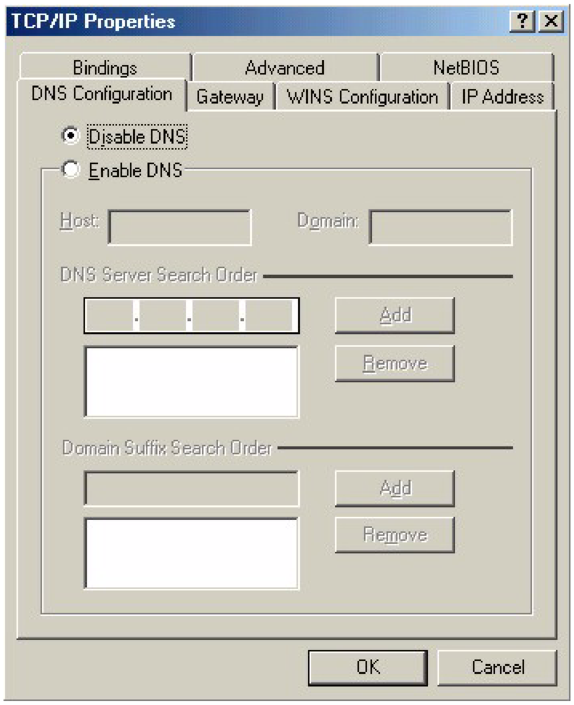
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

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

Figure 214 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

4 Click the **Gateway** tab.

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

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

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

7 Turn on your 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.

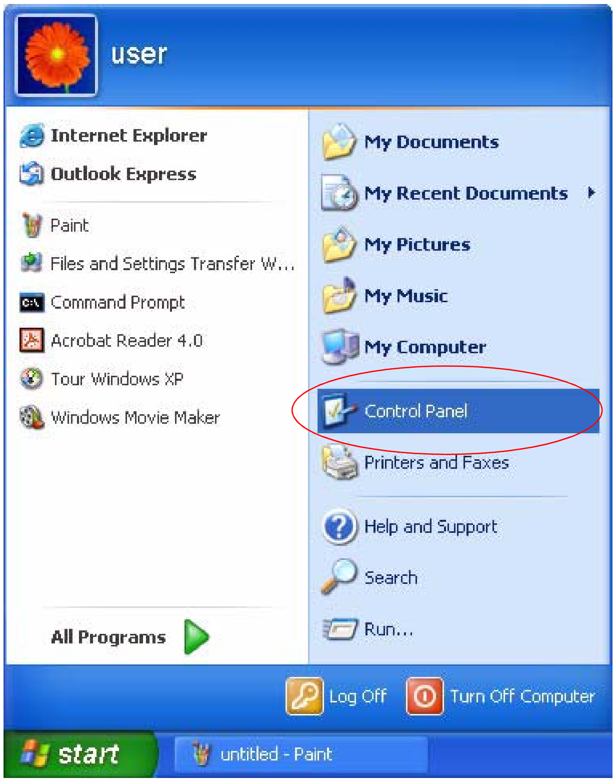
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

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

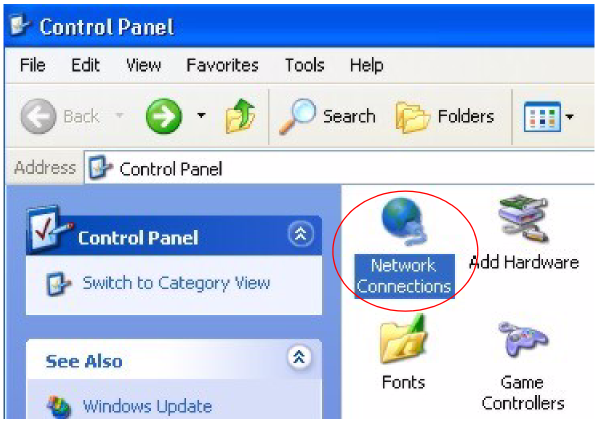
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 215 Windows XP: Start Menu



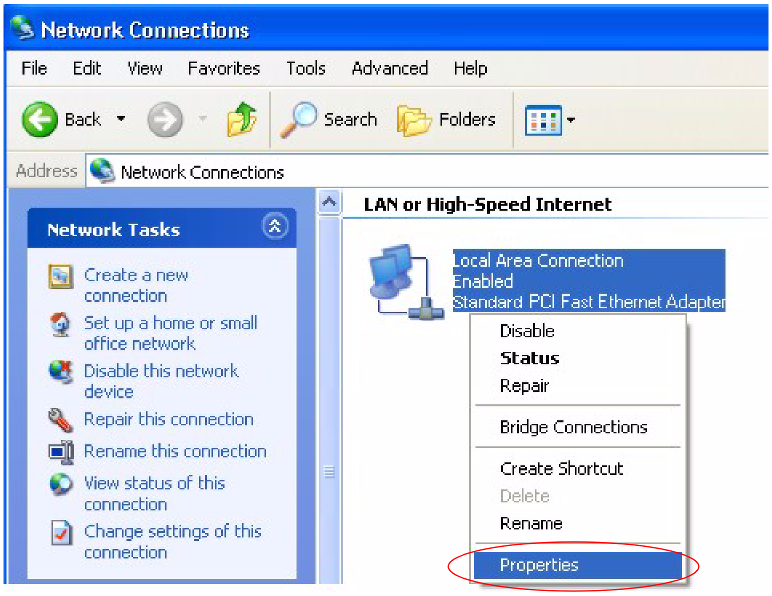
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 216 Windows XP: Control Panel



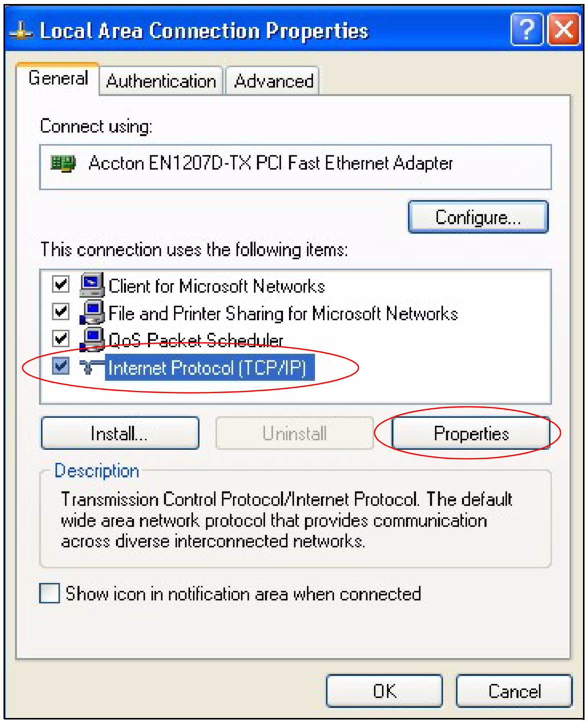
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 217 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 218 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

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

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

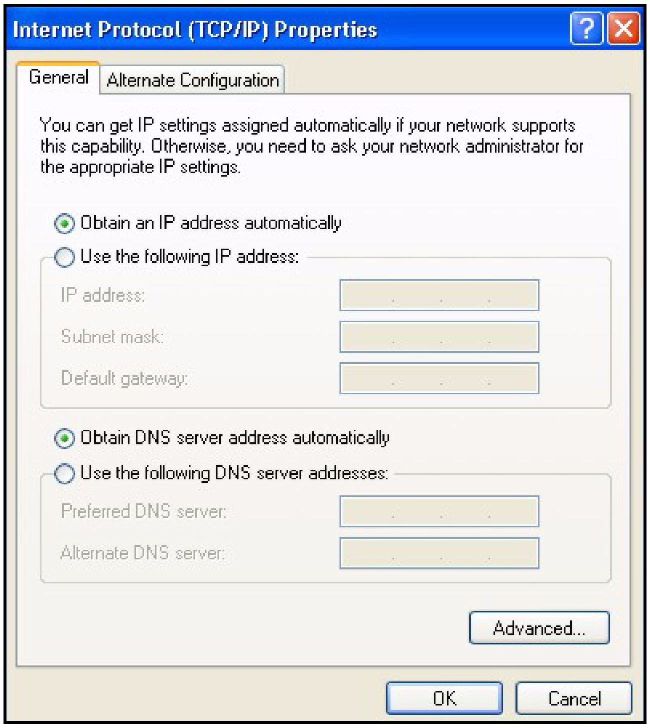
☐ Show icon in notification area when connected

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

- If you have a dynamic IP address click **Obtain an IP address automatically**.

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

Figure 219 Windows XP: Internet Protocol (TCP/IP) Properties



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

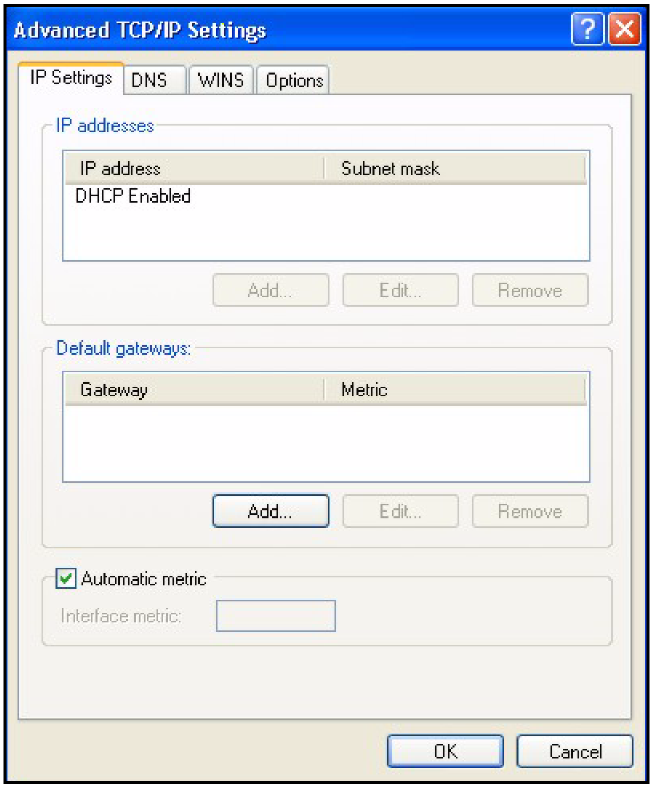
Alternate DNS server: . . .

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

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

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

Figure 220 Windows XP: Advanced TCP/IP Properties

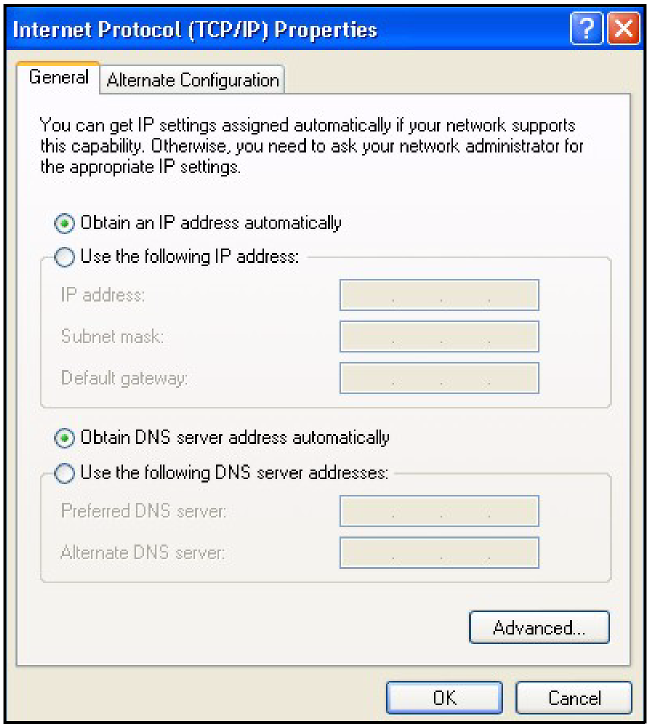


7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

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



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

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

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

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

Verifying Settings

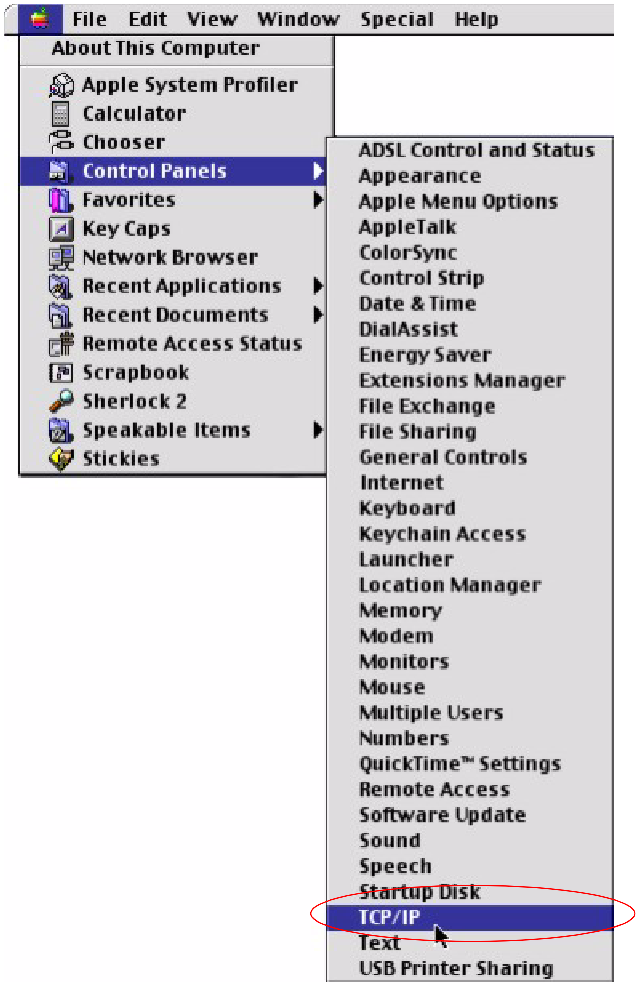
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

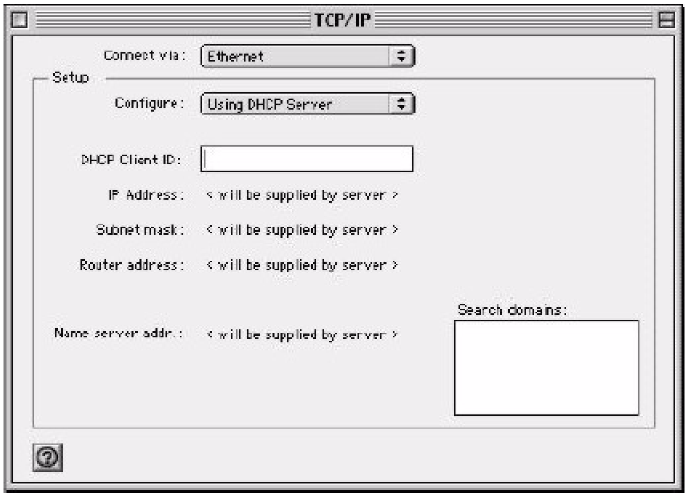
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 222 Macintosh OS 8/9: Apple Menu



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

Figure 223 Macintosh OS 8/9: TCP/IP



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

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

Search domains:

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

4 For statically assigned settings, do the following:

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

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

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

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

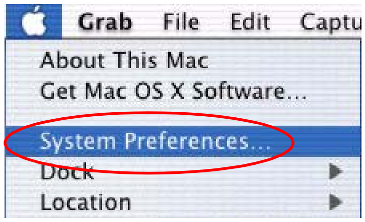
Verifying Settings

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

Macintosh OS X

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

Figure 224 Macintosh OS X: Apple Menu

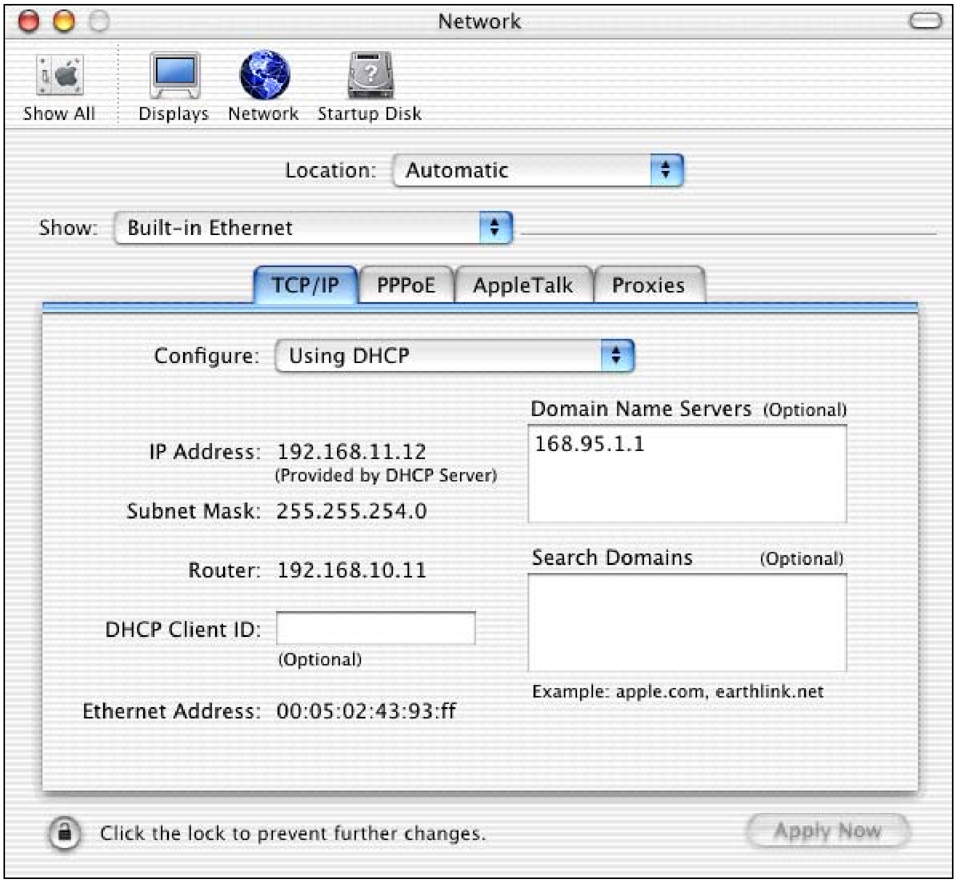


2 Click **Network** in the icon bar.

- 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 225 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

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

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

4 For statically assigned settings, do the following:

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

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

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

Verifying Settings

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

Linux

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

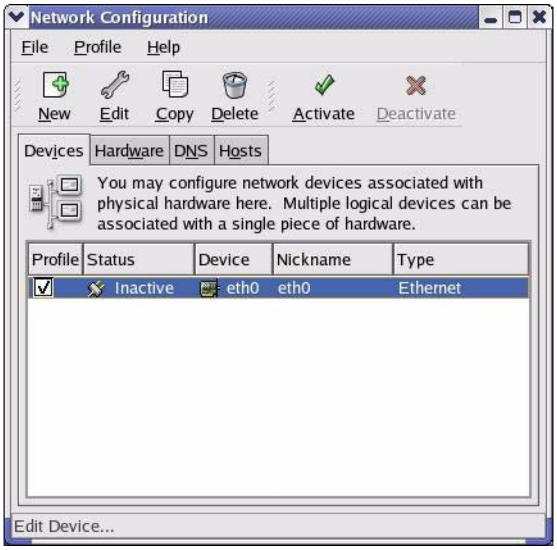
Note: Make sure you are logged in as the root administrator.

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 226 Red Hat 9.0: KDE: Network Configuration: Devices

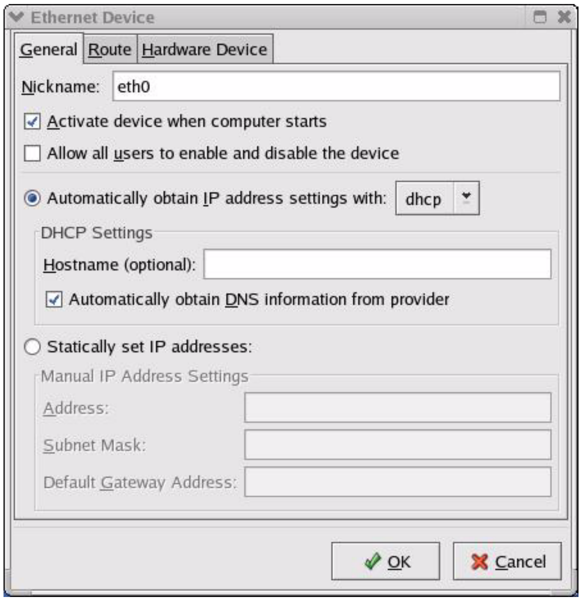


You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

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

Figure 227 Red Hat 9.0: KDE: Ethernet Device: General



Nickname: eth0

☑ Activate device when computer starts

☐ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

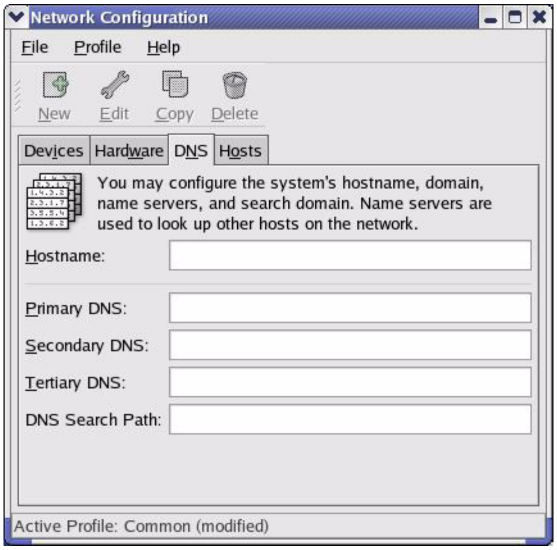
Default Gateway Address:

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

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

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

Figure 228 Red Hat 9.0: KDE: Network Configuration: DNS



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

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

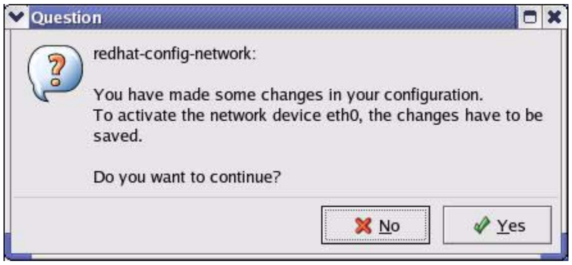
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

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

Figure 229 Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

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

Do you want to continue?

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

Using Configuration Files

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

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

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 230 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 231 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 232 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 233 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]
```

36.5.1 Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 234 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]#
```

Appendix E
IP Addresses and Subnetting

This appendix introduces IP addresses, IP address classes and subnet masks. You use subnet masks to subdivide a network into smaller logical networks.

Introduction to IP Addresses

An IP address has two parts: the network number and the host ID. Routers use the network number to send packets to the correct network, while the host ID identifies a single device on the network.

An IP address is made up of four octets, written in dotted decimal notation, for example, 192.168.1.1. (An octet is an 8-digit binary number. Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.)

There are several classes of IP addresses. The first network number (192 in the above example) defines the class of IP address. These are defined as follows:

- Class A: 0 to 127
- Class B: 128 to 191
- Class C: 192 to 223
- Class D: 224 to 239
- Class E: 240 to 255

IP Address Classes and Hosts

The class of an IP address determines the number of hosts you can have on your network.

- In a class A address the first octet is the network number, and the remaining three octets are the host ID.
- In a class B address the first two octets make up the network number, and the two remaining octets make up the host ID.
- In a class C address the first three octets make up the network number, and the last octet is the host ID.

The following table shows the network number and host ID arrangement for classes A, B and C.

Table 131 Classes of IP Addresses

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	**Network number**	Host ID	Host ID	Host ID
Class B	**Network number**	**Network number**	Host ID	Host ID
Class C	**Network number**	**Network number**	**Network number**	Host ID

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 for example). Therefore, to determine the total number of hosts allowed in a network, deduct two as shown next:

- A class C address (1 host octet: 8 host bits) can have 2^8 – 2, or 254 hosts.
- A class B address (2 host octets: 16 host bits) can have 2^{16} – 2, or 65534 hosts.

A class A address (3 host octets: 24 host bits) can have 2^{24} – 2 hosts, or approximately 16 million hosts.

IP Address Classes and Network ID

The value of the first octet of an IP address determines the class of an address.

- Class A addresses have a **0** in the leftmost bit.
- Class B addresses have a **1** in the leftmost bit and a **0** in the next leftmost bit.
- Class C addresses start with **1 1 0** in the first three leftmost bits.
- Class D addresses begin with **1 1 1 0**. Class D addresses are used for multicasting, which is used to send information to groups of computers.
- There is also a class E. It is reserved for future use.

The following table shows the allowed ranges for the first octet of each class. This range determines the number of subnets you can have in a network.

Table 132 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239
Class E (reserved)	**1111**0000 to **1111**1111	240 to 255

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation).

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The “natural” masks for class A, B and C IP addresses are as follows.

Table 133 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits.

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

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

Table 134 Alternative Subnet Mask Notation

SUBNET MASK	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224

Table 134 Alternative Subnet Mask Notation (continued)

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 135 Two Subnets Example

IP/SUBNET MASK	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C").

To make two networks, divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to make network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Table 136 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000

Table 136 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 137 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is 2^7 – 2 or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all zeroes is the subnet itself, all ones is the broadcast address on the subnet).

Table 138 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 138 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 139 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 140 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 141 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows class C IP address last octet values for each subnet.

Table 142 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

The following table is a summary for class "C" subnet planning.

Table 143 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Table 131 on page 355) available for subnetting.

The following table is a summary for class "B" subnet planning.

Table 144 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

APPENDIX F

Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

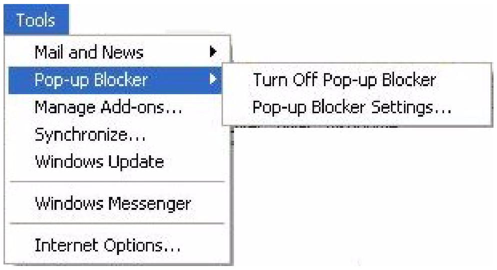
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 235 Pop-up Blocker

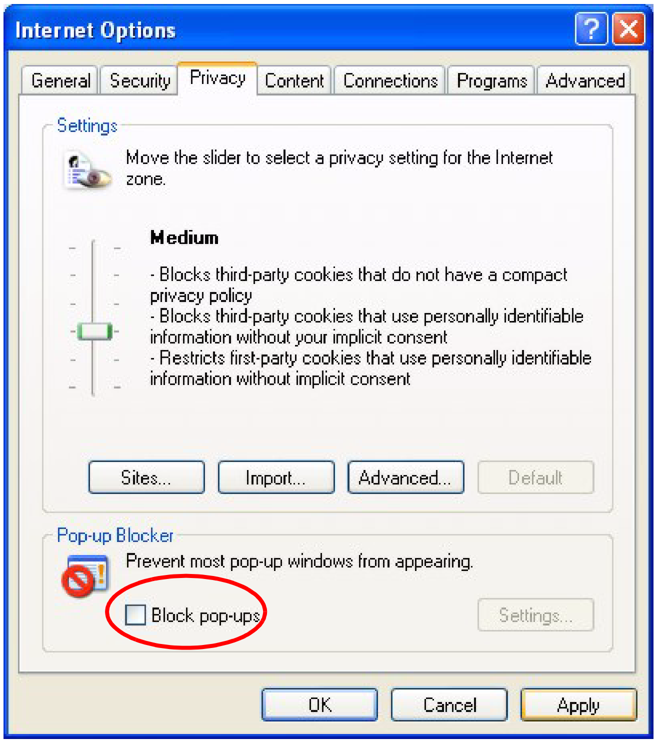


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 236 Internet Options



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

Medium

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

Prevent most pop-up windows from appearing.

□ Block pop-ups

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

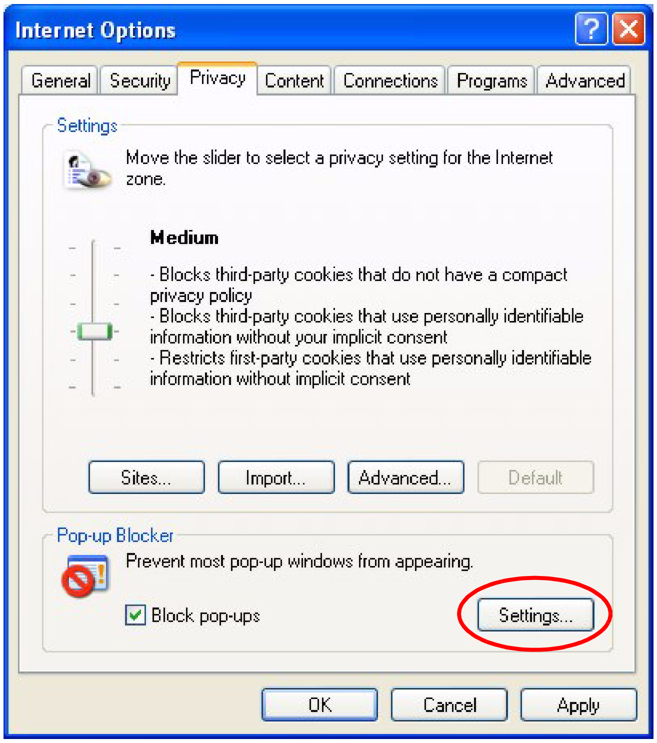
Enable pop-up Blockers with Exceptions

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

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

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

Figure 237 Internet Options



Internet Options

Settings

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

Medium

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

Pop-up Blocker

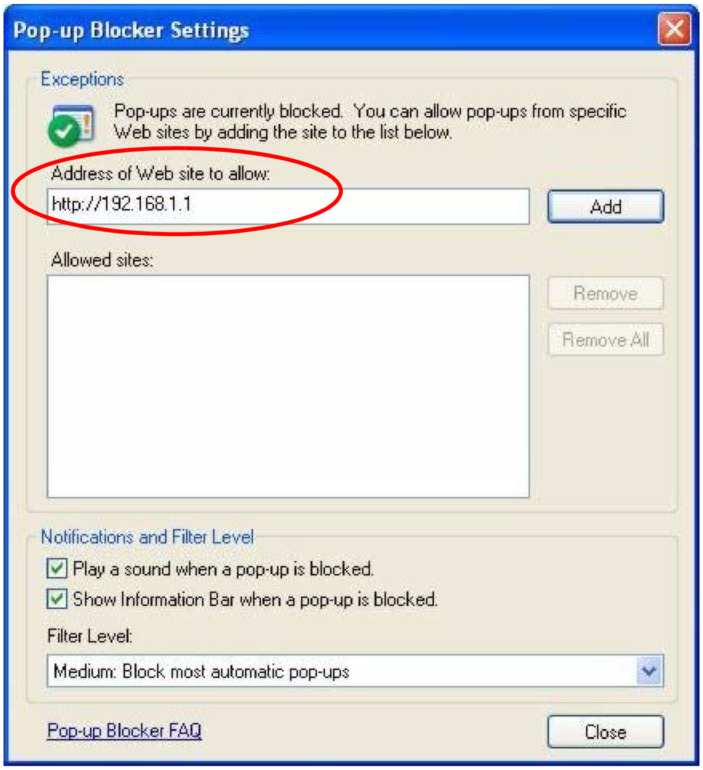
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

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

Figure 238 Pop-up Blocker Settings



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

Address of Web site to allow: http://192.168.1.1

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

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

Filter Level: Medium: Block most automatic pop-ups

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

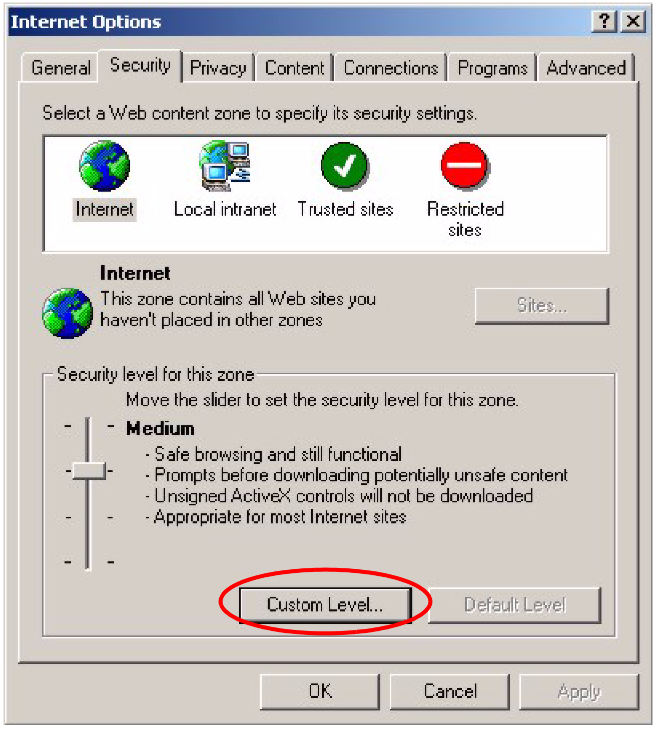
6 Click **Apply** to save this setting.

JavaScripts

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

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

Figure 239 Internet Options



Select a Web content zone to specify its security settings.

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

Security level for this zone

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

Medium

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

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

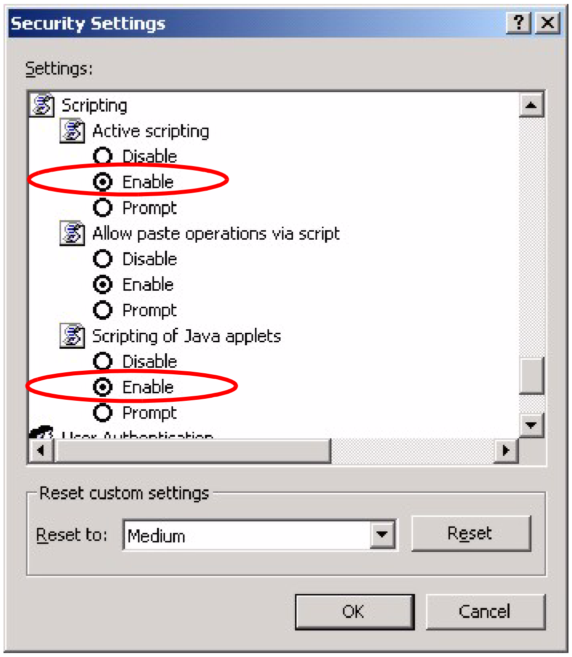
3 Scroll down to **Scripting**.

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

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

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

Figure 240 Security Settings - Java Scripting



Security Settings

Settings:

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

Reset custom settings

Reset to: Medium

Java Permissions

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

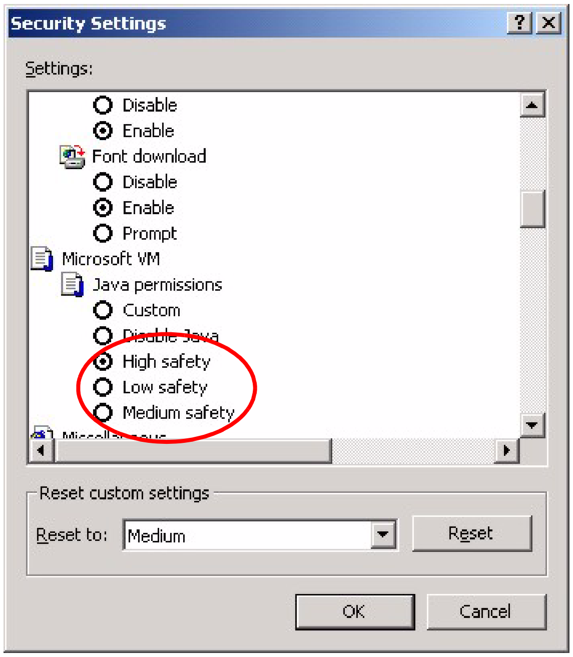
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

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

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

Figure 241 Security Settings - Java



Settings:

○ Disable
● Enable

Font download
○ Disable
● Enable
○ Prompt

Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety

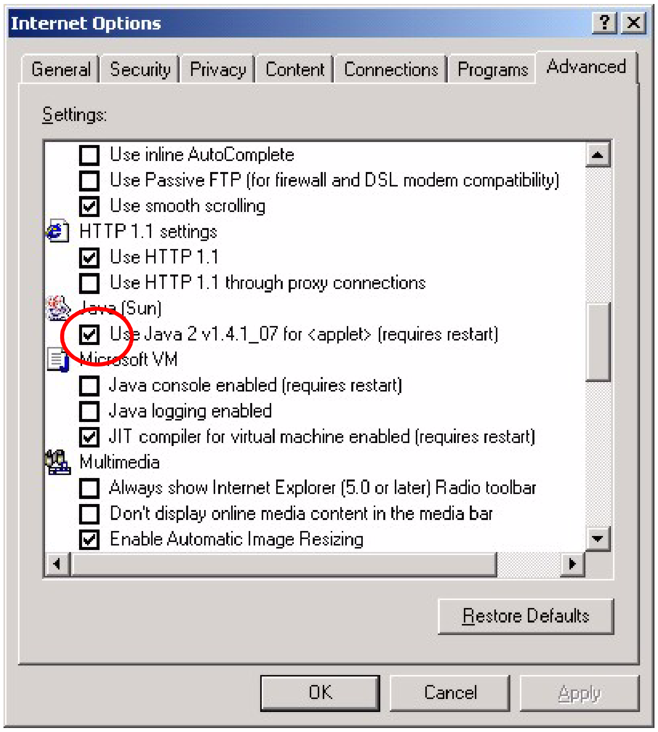
Miscellaneous

Reset to: Medium

JAVA (Sun)

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2. make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3. Click **OK** to close the window.

Figure 242 Java (Sun)



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

HTTP 1.1 settings

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

Java (Sun)

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

Microsoft VM

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

Multimedia

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

Index