ZyWALL 10/10W/50/100

Internet Security Gateway

User's Guide

Versions 3.52 and 3.60

December 2002

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Copyright

Copyright © 2002 by ZyXEL Communications Corporation.

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

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This 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 equipment 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 commercial environment. This equipment 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.

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Certifications

Refer to the product page at www.zyxel.com.

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Industry Canada does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that the compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.

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 value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is 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 of character 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.

Online Registration

Register online registration at www.zyxel.com for free future product updates and information.

Customer Support

When you contact your customer support representative please have the following information ready: Please have the following information ready when you contact customer support.

- Product model and serial number.
- Information in **Menu 24.2.1 – System Information**.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu 300, Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A4 D-52146 Wuerselen, Germany

Table of Contents

List of Figures

List of Tables

Preface

About Your ZyWALL

Congratulations on your purchase of the ZyWALL 10, 10W, 50 or 100 Internet Security Gateway.

About This User's Manual

This manual is designed to guide you through the configuration of your ZyWALL for its various applications. Primarily SMT menus are shown, but web configurator screens are shown for features that do not have SMT menus or the recommendation is to configure via web configurator.

This manual may refer to the ZyWALL 10/10W/50/100 Internet Security Gateway as the ZyWALL.

This manual covers the ZyWALL 10, 10W, 50 and 100 models. Supported features and the details of the features, vary from model to model. Not every feature applies to every model; refer to the *Model Comparison Chart* in chapter 1 to see what features are specific to your ZyWALL model.

Related Documentation

- Support Disk
  Refer to the included CD for support documents.
- Read Me First
  The Read Me First is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.
- Packing List Card
  The Packing List Card lists all items that should have come in the package.
- Certifications
  Refer to the product page at www.zyxel.com for information on product certifications.
- ZyXEL Glossary and Web Site
  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

Syntax Conventions

- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one of the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font.
- The choices of a menu item are in **Bold Arial** font.
- A single keystroke is in Arial font and enclosed in square brackets, for instance, [ENTER] means the Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.

- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity’s sake, we will use “e.g.” as a shorthand for “for instance” and “i.e.” for “that is” or “in other words” throughout this manual.

Part I:

Overview

This part covers Getting to Know Your ZyWALL and Hardware Installation.

Chapter 1 Getting to Know Your ZyWALL

This chapter introduces the main features and applications of the ZyWALL.

1.1 The ZyWALL 10/10W/50/100 Internet Security Gateway

The ZyWALL 10/10W/50/100 are the ideal secure gateways for all data passing between the Internet and the LAN.

By integrating NAT, firewall and VPN capability, ZyXEL's ZyWALL 10/10W/50/100 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 the operating system platform you use.

1.2 Features

The following sections describe the features of the ZyWALL 10/10W/50/100. Features vary by ZyWALL model. Refer to the following table to see the differences between the ZyWALL 10, 50 and 100.

Table 1-1 Model Specific Features

ZYWALL MODEL FEATURES	100	50	10W	10
Firmware Version Number	3.52	3.52	3.60	3.52
Dial Backup (or Auxiliary)	O		*	
PCMCIA Slot	O		O	
PCMCIA Card Release Button			O	
802.11b Wireless LAN Support	O		O	
802.1x Wireless LAN Support	O		O	
Real Time Chip	O	O	O	
Auto-sensing 10/100 Mbps Ethernet LAN			O	
Auto-negotiating 10/100 Mbps Ethernet DMZ	O			
Auto-negotiating 10/100 Mbps Ethernet WAN	O	O	O	
Reset Button	O	O	O	

Table 1-1 Model Specific Features

ZYWALL MODEL FEATURES	100	50	10W	10
Uplink Button	O	O	O	
Power Switch	O			
Traffic Redirect	O	O	O	
Bandwidth Management	O			
IP Policy Routing	O			
Number of Static Routes	50	30	12	12
Number of Firewall Rules	400	100	50	30
Number of IPSec VPN Security Associations	100	50	10	10
UPnP			O	
* The ZyWALL 10W uses the same port for console management and for an auxiliary WAN backup[1].				
Table Key: An "O" in a model's column shows that the model has the specified feature. A number specific to an individual model may alternately be displayed. The information in this table was correct at the time of writing, although it may be subject to change.				

1.2.1 Physical Features

Auto-negotiating 10/100 Mbps Ethernet LAN

The LAN interface automatically detects if it's on a 10 or a 100 Mbps Ethernet.

Auto-sensing 10/100 Mbps Ethernet LAN

The LAN interface automatically adjusts to either a crossover or straight-through Ethernet cable. This feature is not available on all models.

Auto-negotiating 10/100 Mbps Ethernet DMZ

Public servers (Web, FTP, etc.) attached to the DeMilitarized Zone (DMZ) port are visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death) and can also be accessed from the secure LAN. This feature is not available on all models.

[1] The ZyWALL 10W auxiliary WAN backup feature was not available at the time of writing.

10/100 Mbps Ethernet WAN

The 10/100 Mbps Ethernet WAN port attaches to the Internet via broadband modem or router. This feature is not available on all models.

Backup WAN or Auxiliary

The Dial Backup or Auxiliary port can be used in reserve as a traditional dial-up connection when/if ever the broadband connection to the WAN port fails. This feature is not available on all models.

Time and Date

The ZyWALL allows you to get the current time and date from an external server when you turn on your ZyWALL. You can also set the time manually. The Real Time Chip (RTC) keeps track of the time and date (not available in all models).

Reset Button

The ZyWALL reset button is built into the rear panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33. This feature is not available on all models.

PCMCIA Port

The PCMCIA port provides the option of a wireless LAN. This feature is not available on all models.

IEEE 802.11b 11 Mbps Wireless LAN

The optional 11 Mbps wireless LAN card provides mobility and a fast network environment for small and home offices. Users can connect to the local area network without any wiring efforts and enjoy reliable high-speed connectivity. This feature is not available on all models.

1.2.2 Non-Physical Features

Bandwidth Management

Bandwidth management allows you to allocate network resources according to defined policies. This policy-based bandwidth allocation helps your network to better handle real-time applications such as Voice-over-IP (VoIP).

IPSec VPN Capability

Establish a Virtual Private Network (VPN) to connect with business partners and branch offices using data encryption and the Internet to provide secure communications without the expense of leased site-to-site lines. The ZyWALL VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

Firewall

The ZyWALL is 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 ZyWALL firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

RADIUS (RFC2138, 2139)

RADIUS (Remote Authentication Dial In User Service) server enables authentication, authorization and accounting for your wireless network. This feature is not available on all models.

IEEE 802.1x for Network Security

The ZyWALL supports the IEEE 802.1x standard that works with the IEEE 802.11 to enhance user authentication. With the local user profile, the ZyWALL allows you to configure up 32 user profiles without a network authentication server. In addition, centralized user and accounting management is possible on an optional network authentication server. This feature is not available on all models.

Content Filtering

The ZyWALL can block web features such as ActiveX controls, Java applets and cookies, as well as disable web proxies. The ZyWALL can block specific URLs by using the keyword feature. It also allows the administrator to define time periods and days during which content filtering is enabled and to include or exclude a range of users on the LAN from content filtering.

You can configure most features of the ZyWALL via SMT but ZyXEL recommends using the embedded web configurator to configure the firewall and content filtering.

Wireless LAN MAC Address Filtering

MAC Address Filtering together with ESSID (Extended Service Set IDentifier) and WEP (Wired Equivalent Privacy) ensure the most secure wireless solution. This feature is not available on all models.

Brute-Force Password Guessing Protection

The ZyWALL has a special protection mechanism to discourage brute-force password guessing attacks on the ZyWALL's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendices for details about this feature.[2]

Packet Filtering

The packet filtering mechanism blocks unwanted traffic from entering/leaving your network.

[2] Brute Force Password Protection was not available on every model at the time of writing.

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the ZyWALL and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network. This feature is not available on all models.

Call Scheduling

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

PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The ZyWALL supports one PPTP server connection at any given time.

Dynamic DNS Support

With Dynamic DNS (Domain Name System) support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

IP Multicast

Deliver IP packets to a specific group of hosts using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the ZyWALL supports both versions 1 and 2.
IP Alias
IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet LAN interface with the ZyWALL itself as the gateway for each LAN network.

IP Policy Routing

IP Policy Routing provides a mechanism to override the default routing behavior and alter packet forwarding based on the policies defined by the network administrator. This feature is not available on all models.

Central Network Management

Central Network Management (CNM) allows an enterprise or service provider network administrator to manage your ZyWALL. The enterprise or service provider network administrator can configure your ZyWALL, perform firmware upgrades and do troubleshooting for you.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1).

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.

Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway on the LAN when the ZyWALL cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails. This feature is not available on all models.

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. 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.

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 ZyWALL 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 ZyWALL can also act as a surrogate DHCP server (**DHCP Relay**) where it relays IP address assignment from the actual real DHCP server to the clients.

Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyWALL's management settings and configure the firewall. Most functions of the ZyWALL are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection.

RoadRunner Support

In addition to standard cable modem services, the ZyWALL supports Time Warner's RoadRunner Service.

Logging and Tracing

- Built-in message logging and packet tracing.
- Unix syslog facility support.
- Firewall logs.
- Content filtering logs.

Upgrade ZyWALL Firmware via LAN

The firmware of the ZyWALL can be upgraded via the LAN.

Embedded FTP and TFTP Servers

The ZyWALL's embedded FTP and TFTP Servers enable fast firmware upgrades as well as configuration file backups and restoration.

1.2.3 ZyWALL 100 Note

The ZyWALL 100 is designed to act as a secure gateway for all data passing between the Internet and the LAN or the DMZ. It has three Ethernet ports, one RS-232 auxiliary port and one PCMCIA port (for optional wireless applications), which are used to physically separate the network into three areas.

I. LAN Network (a trusted network)

- LAN port: The auto-negotiating 10/100 Mbps Ethernet LAN interface automatically detects if it's on a 10 or a 100 Mbps Ethernet. Attach computers that are to be secured from the outside world to this port. These computers will have access to e-mail, FTP and the World Wide Web but incoming connections (from the Internet) are only allowed if the connection is originally initiated from the LAN computer or a firewall rule has been specifically configured to allow access.

II. DMZ Network

- DMZ port: Attach public servers (Web, FTP, etc.) to the DeMilitarized Zone (DMZ) port. Computers attached to this port are visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death) and can also be accessed from the secure LAN.

III. WAN Network

- WAN port: The 10/100 Mbps Ethernet WAN port attaches to the Internet via broadband modem or router.
- Dial Backup port: This auxiliary port can be used as a backup line when/if the broadband connection to the WAN port fails.

1.3 Applications for the ZyWALL

1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

You can connect a cable modem, DSL or wireless modem to the ZyWALL for broadband Internet access via Ethernet or wireless port on the modem. The ZyWALL guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

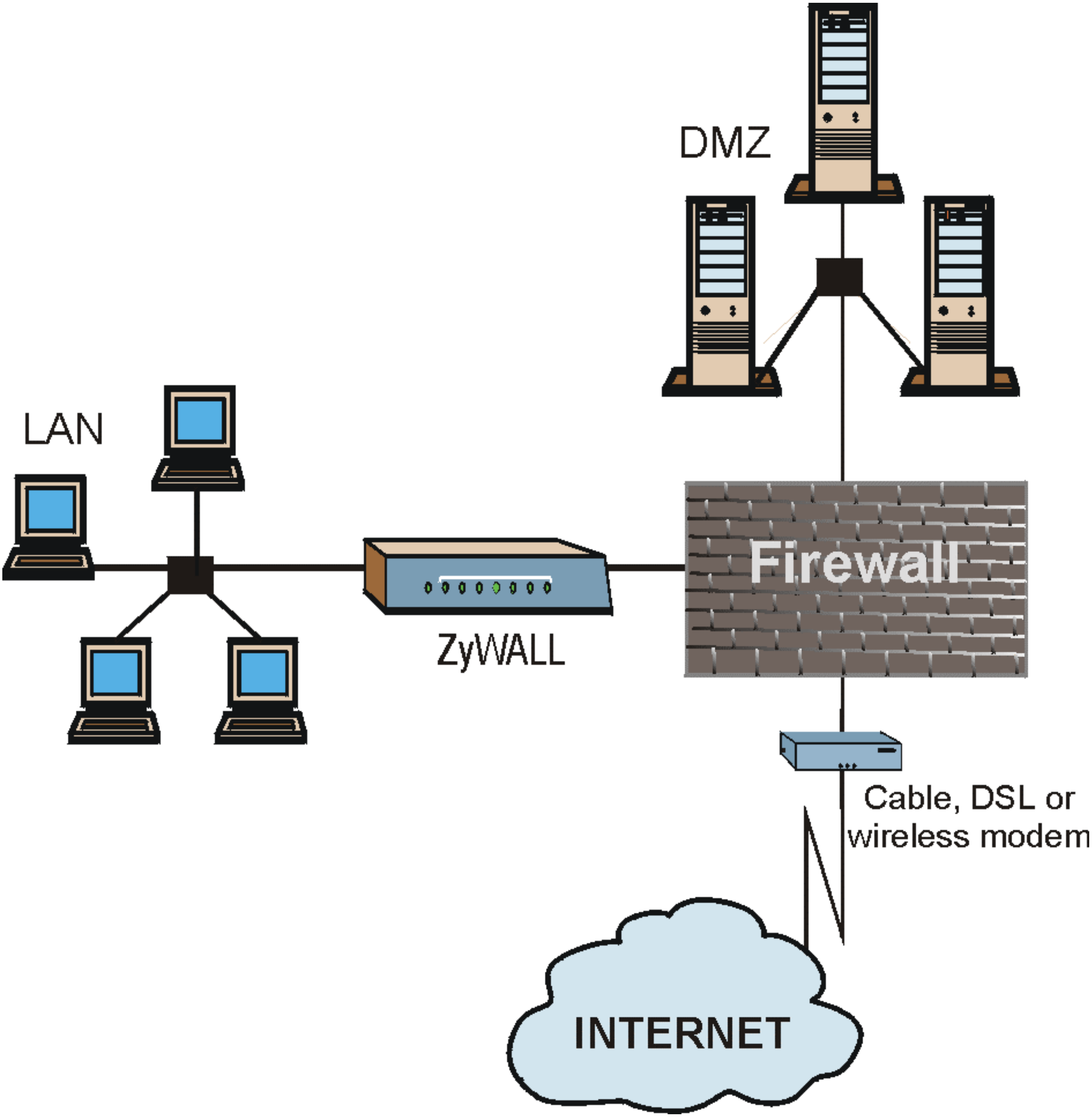


Figure 1-1 Secure Internet Access via Cable, DSL or Wireless Modem

1.3.2 VPN Application

ZyWALL VPN is an ideal cost-effective way to connect branch offices and business partners over the Internet without the need (and expense) for leased lines between sites.

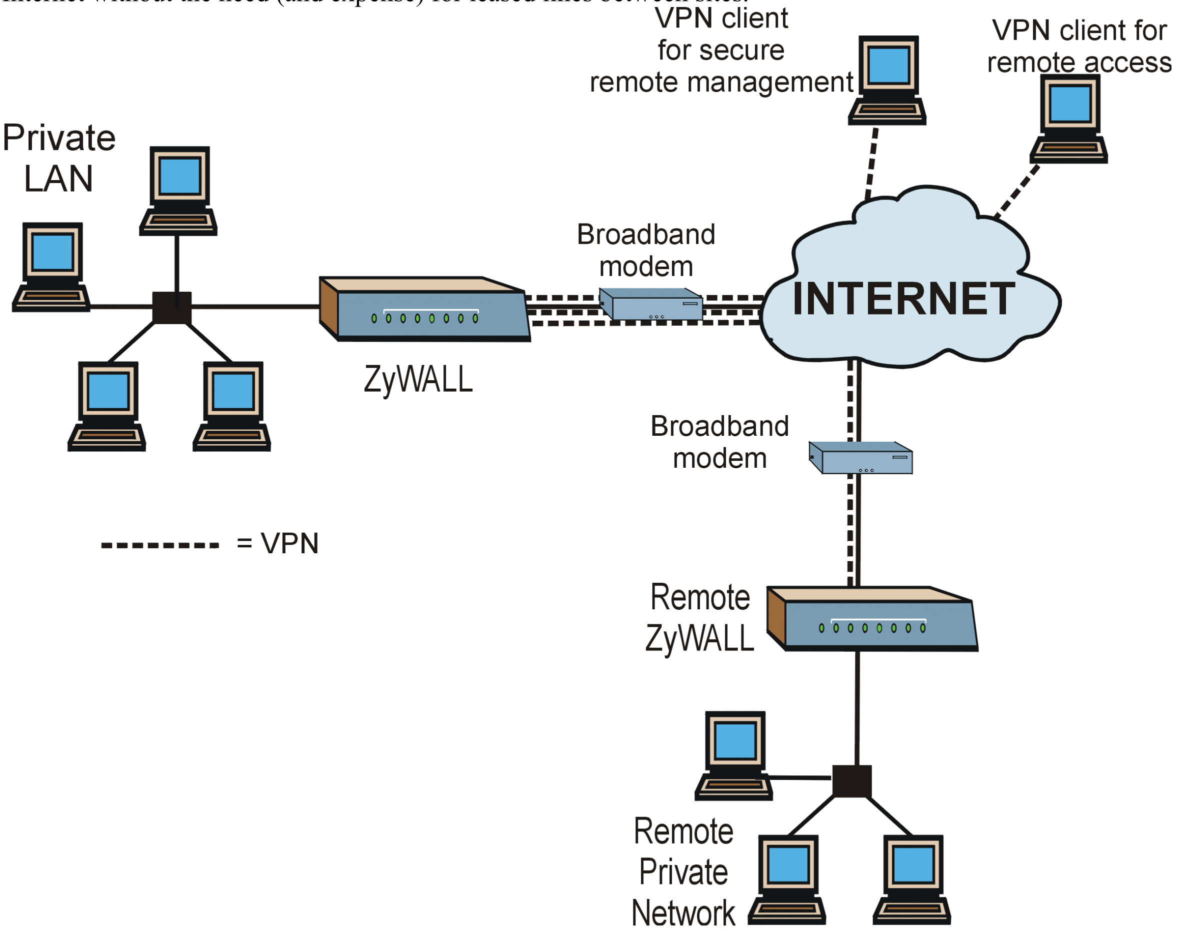


Figure 1-2 VPN Application

Chapter 2 Hardware Installation

This chapter explains the LEDs and ports as well as how to connect the hardware. Refer to Table 1-1 for a list of hardware features that are specific to individual models.

2.1 Front Panel LEDs and Back Panel Ports

2.1.1 Front Panel LEDs

The LEDs on the front panel indicate the operational status of the ZyWALL.

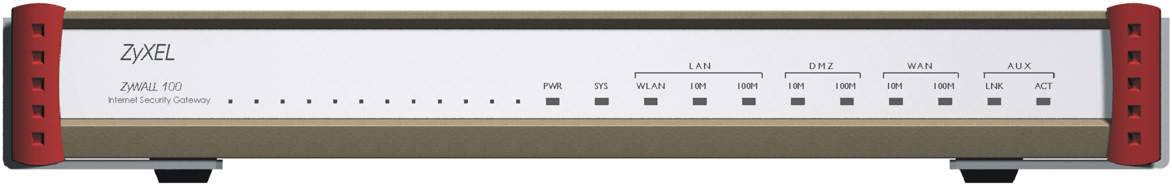


Figure 2-1 ZyWALL 100 Front Panel

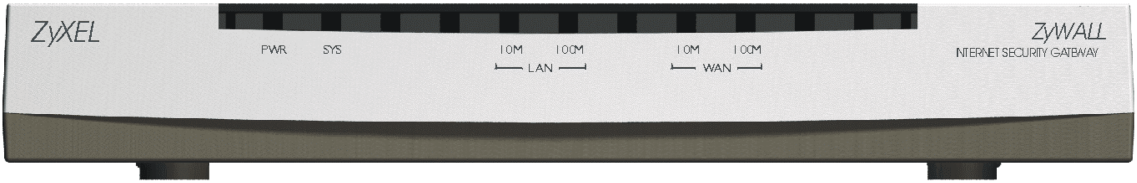


Figure 2-2 ZyWALL 50 Front Panel

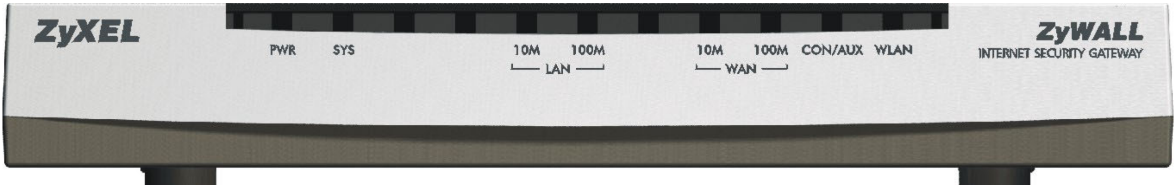


Figure 2-3 ZyWALL 10W Front Panel

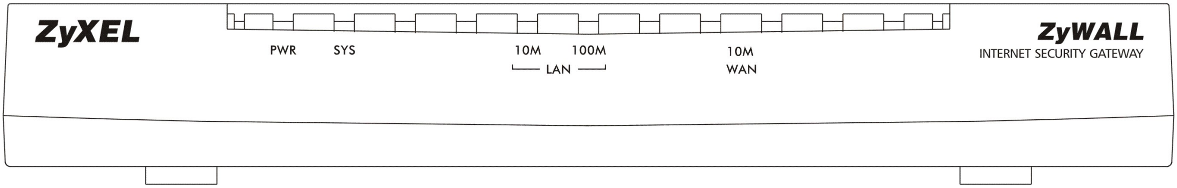


Figure 2-4 ZyWALL 10 Front Panel

The following table describes the LED functions. Not all LEDs are included in every model.

Table 2-1 LED Descriptions

LED	COLOR	STATUS	MEANING
PWR	Green	On	The ZyWALL is turned on.
		Off	The ZyWALL is turned off.
SYS	Green	Off	The ZyWALL is not ready or failed.
		On	The ZyWALL is ready and running.
		Flashing	The ZyWALL is rebooting.
	Red	On	The power to the ZyWALL is too low.
WLAN	Green	Off	The wireless LAN is not ready, or has failed.
		On	The wireless LAN is OK.
		Flashing	The wireless LAN is sending or receiving packets.
LAN 10M	Green	Off	The 10M LAN is not connected.
		On	The ZyWALL is connected to a 10M LAN.
		Flashing	The 10M LAN is sending or receiving packets.
LAN 100M	Orange	Off	The 100M LAN is not connected.
		On	The ZyWALL is connected to a 100Mbps LAN.
		Flashing	The 100M LAN is sending or receiving packets.
DMZ 10M	Green	Off	The 10M DMZ is not connected.
		On	The ZyWALL is connected to a 10M DMZ.
		Flashing	The 10M DMZ is sending/receiving packets.

Table 2-1 LED Descriptions

LED	COLOR	STATUS	MEANING
DMZ 100M	Orange	Off	The 100M DMZ is not connected.
		On	The ZyWALL is connected to a 100Mbps DMZ.
		Flashing	The 100M DMZ is sending or receiving packets.
WAN 10M	Green	Off	The 10M WAN link is not ready, or has failed.
		On	The 10M WAN link is OK.
		Flashing	The 10M WAN link is sending or receiving packets.
WAN 100M	Orange	Off	The 100M WAN link is not ready, or has failed.
		On	The 100M WAN link is OK.
		Flashing	The 100M WAN link is sending or receiving packets.
AUX LNK	Green	Off	The backup port is not connected.
		On	The backup port is connected.
AUX ACT	Green	Off	The auxiliary port is not sending or receiving packets.
		Flashing	The auxiliary port is sending or receiving packets.
CON/AUX	Green	Off	The CON/AUX link is not ready, or has failed.
		On	The CON/AUX switch is set to CON and the CON/AUX port is connected to a management computer.
	Orange	Off	The CON/AUX link is not ready, or has failed.
		On	The CON/AUX switch is set to AUX and the CON/AUX port has an Internet connection through a dial-up modem.
		Flashing	The CON/AUX switch is set to AUX and the CON/AUX port is sending or receiving data through a dial-up modem.

2.2 ZyWALL Rear Panel and Connections

The following figure shows the rear panels of the ZyWALL.

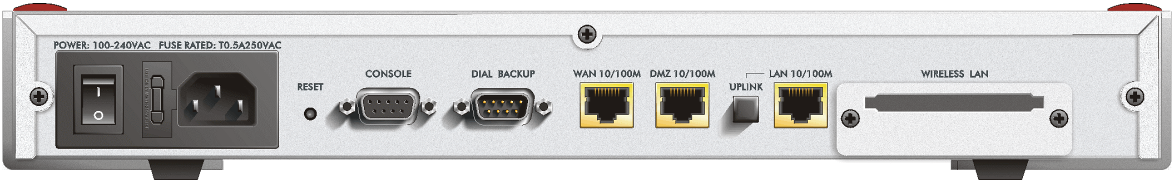


Figure 2-5 ZyWALL 100 Rear Panel

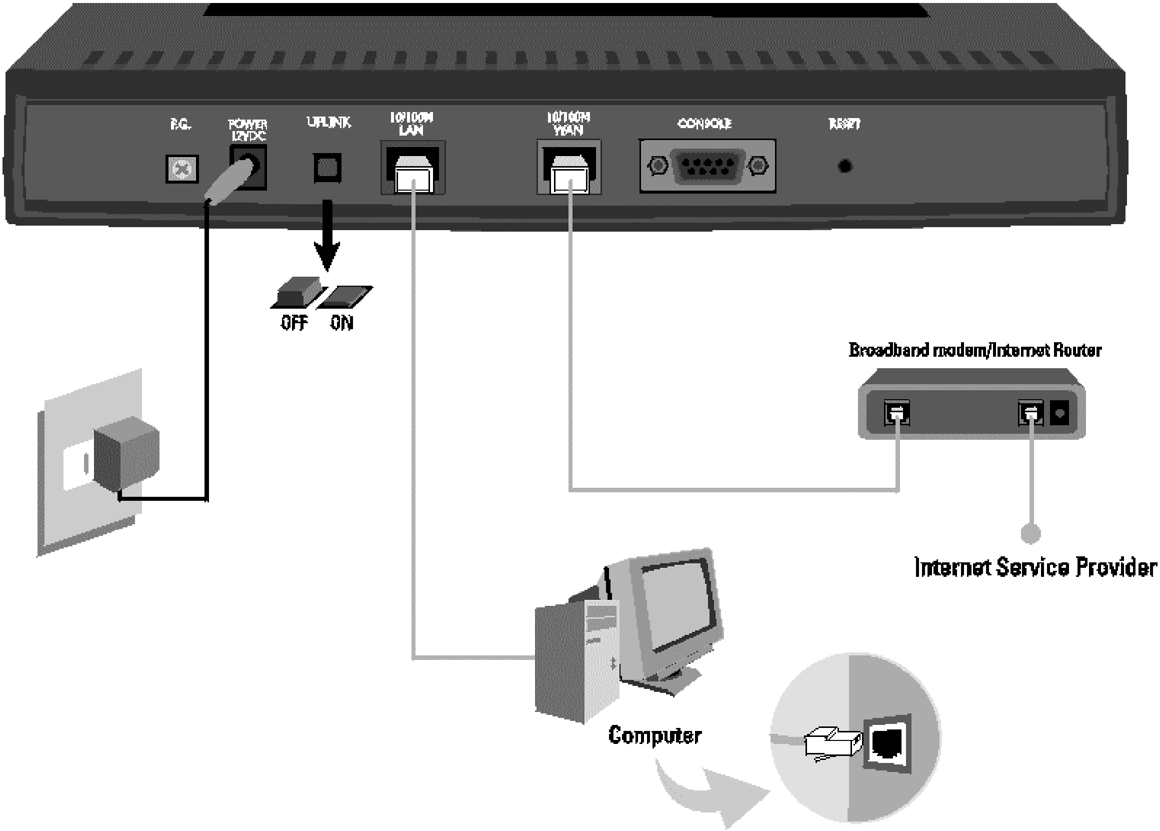


Figure 2-6 ZyWALL 50 Rear Panel

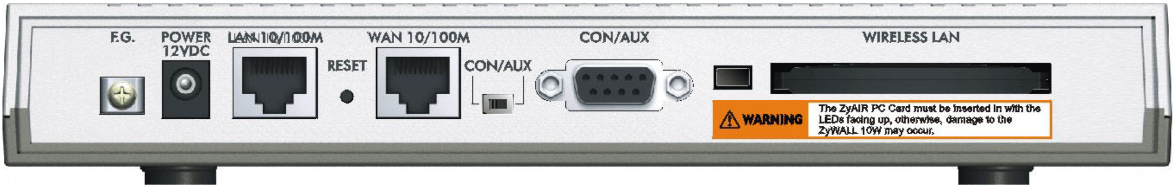

F.G.
POWER 12VDC
LAN 10/100M
RESET
WAN 10/100M
CON/AUX
CON/AUX
WIRELESS LAN
WARNING
The ZyAIR PC Card must be inserted in with the LEDs facing up, otherwise, damage to the ZyWALL 10W may occur.

Figure 2-7 ZyWALL 10W Rear Panel

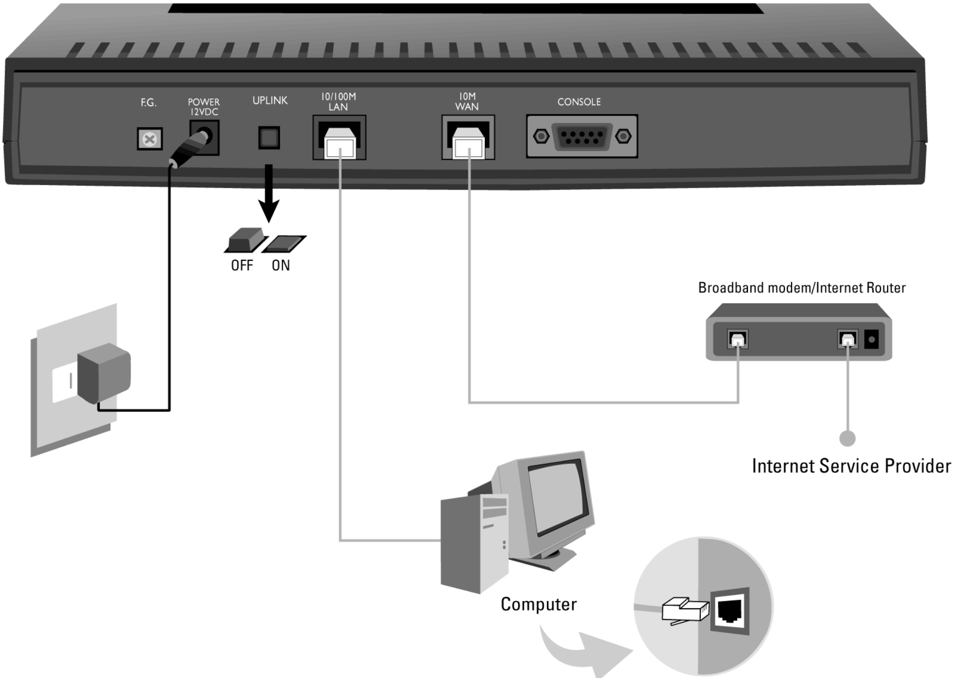


Figure 2-8 ZyWALL 10 Rear Panel

This section outlines how to connect your ZyWALL. If you want to connect a cable modem, you must connect the coaxial cable from your cable service to the threaded coaxial cable connector on the back of the cable modem. Connect a DSL modem to the DSL wall jack. See the Safety *Warnings and Instructions Appendix* for safety instructions when making connections to the ZyWALL. Skip sections that do not apply to your particular ZyWALL model.

2.2.1 Connecting the Console Port

Use terminal emulator software on a computer for configuring your ZyWALL via console port. Connect the 9-pin male end of the console cable to the port labeled **CONSOLE** (or **CON/AUX SOLE** on the ZyWALL 10W and push the **CON/AUX** switch to **CON**) on the ZyWALL and the other end (choice of 9-pin or 25-pin, depending on your computer) to a serial port (COM1, COM2 or other COM port) of your computer. You can use an extension console cable if the enclosed one is too short.

2.2.2 Connecting the Dial Backup Port

- The dial backup port is an RS-232 DB-9M connector. Connect the 9-pin female end of your modem or TA cable to the dial backup port of the ZyWALL and the other end to your modem or TA. This feature is not available on all models.
- With the ZyWALL 10W, the console port is also the auxiliary WAN port. Push the **CON/AUX** switch to **AUX** and use the included CON/AUX converter with the console cable to connect the CON/AUX port to your modem or TA.

2.2.3 Connecting a Broadband Modem to the WAN Port

- Connecting the ZyWALL to a cable modem:
  Connect the port labeled **WAN** on the ZyWALL to the Ethernet port on the cable modem using the Ethernet cable that came with your cable modem. The Ethernet port on a cable modem is sometimes labeled "PC" or "Workstation".
- Connecting the ZyWALL to a DSL modem:
  Connect the port labeled **WAN** on the ZyWALL to the Ethernet port on the DSL modem using the Ethernet cable that came with your DSL modem.
- Connecting the ZyWALL to a wireless modem:
  Connect the port labeled **WAN** on the ZyWALL to the Ethernet port on the wireless modem using the Ethernet cable that came with your wireless modem.

2.2.4 Connecting the DMZ Port

Connect public servers (Web, FTP, etc.) to the DMZ port to make them visible to the outside world. For a single computer, connect the 10/100M DMZ port on the ZyWALL to the network adapter on the computer using a crossover cable.

If you have more than one public server, then you must use an external hub. Connect the 10/100M DMZ port on the ZyWALL to a port on the hub using a straight-through Ethernet cable. This feature is not available on all models.

2.2.5 Connecting the Ethernet LAN

Some ZyWALL models come with an auto-sensing LAN port that automatically adjusts to straight-through or crossover Ethernet cables.

Other ZyWALL models have an uplink button that allows you to switch

When the ZyWALL is on and properly connected to a computer or a hub, the corresponding LAN LED on the front panel turns on.

Table 2-2 LAN Port Connections With an Uplink Button

CABLE FOR CONNECTING TO:	A COMPUTER	A HUB
UPLINK button "on" (pushed in)	Straight-through Ethernet cable	Crossover Ethernet cable
UPLINK button "off" (out)	Crossover Ethernet cable	Straight-through Ethernet cable

2.2.6 Connecting the Wireless LAN

Make sure the ZyWALL is turned off before inserting or removing an 11 Mbps 802.11b-compliant wireless LAN PCMCIA card (to avoid damage). Do not insert or remove the card with the ZyWALL turned on. This feature is not available on all models. Use the PCMCIA card release button (on models that have one) when you remove a PCMCIA card from the slot.

Slide the 64-pin connector end of the PCMCIA wireless LAN card into the slot. See *Figure 2-9* for an example.

Do not force, bend or twist the wireless LAN card.

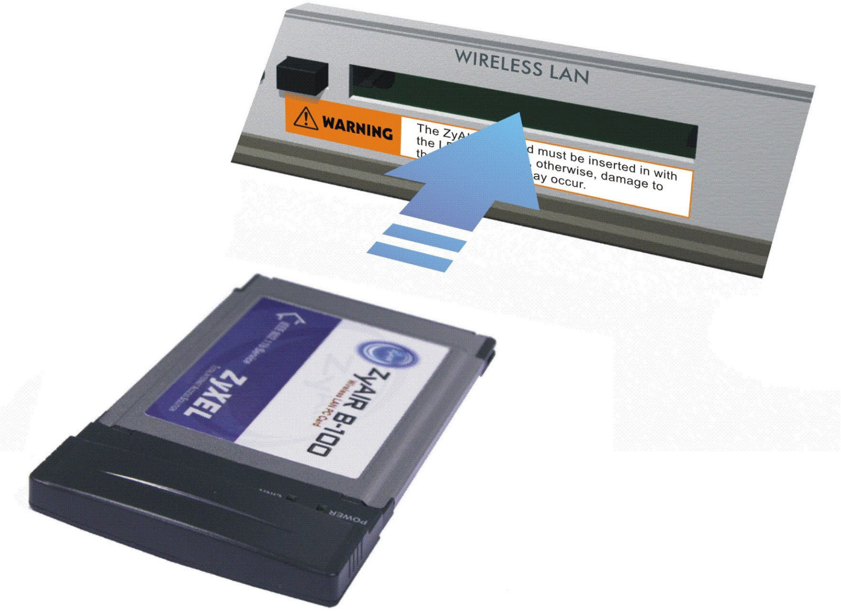


Figure 2-9 Inserting the Wireless LAN Card

2.2.7 Connecting the Power to your ZyWALL

Connect the female end of the included power adaptor or power cord to the port labeled **POWER** on the rear panel of your ZyWALL.

2.3 Additional Installation Requirements

In addition to the contents of your package, there are other hardware and software requirements you need before you can configure and use your ZyWALL. These requirements include:

1. A computer with an installed Ethernet NIC (Network Interface Card).
2. To configure via console port: a computer equipped with communications software configured to the following parameters:
   - VT100 terminal emulation.
   - 9600 Baud.
   - No parity, 8 data bits, 1 stop bit, flow control set to none.
3. A cable/DSL/wireless modem and an ISP account.

After the ZyWALL is properly set up, you can make future changes to the configuration through telnet connections.

To keep the ZyWALL operating at optimal internal temperature, keep the bottom, sides and rear clear of obstructions and away from the exhaust of other equipment.

2.4 Additional Installation Requirements for Using 802.1x

1. A computer with an IEEE 802.11b wireless LAN card.
2. A computer equipped with a web browser (with JavaScript enabled) and/or Telnet.
3. A wireless client computer must be running IEEE 802.1x-compliant software. Currently, this is offered in Windows XP.
4. An optional network RADIUS server for remote user authentication and accounting.

Part II:

Initial Setup and Configuration

This part covers Initial Setup, SMT Menu 1 General Setup, WAN and Dial Backup Setup, LAN Setup, Wireless LAN Setup, DMZ Setup, and Internet Access.

Chapter 3
Initial Setup

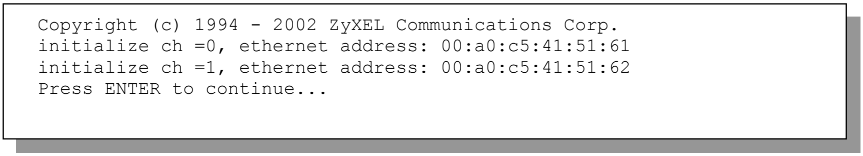
This chapter explains how to perform the initial ZyWALL setup and gives an overview of SMT menus.

3.1 Turning On Your ZyWALL

At this point, you should have connected the console port, the LAN port, the WAN port, the Wireless LAN port and the power port to the appropriate devices or lines. Plug the power cord or power adaptor into an appropriate power source. For models that have a power switch, push the power switch to the on position. The PWR LED turns on. The SYS LED turns on after the system tests are complete. The WAN LED, WLAN LED and one of the LAN LEDs turn on immediately after the SYS LED turns on, if connections have been made to the LAN and WAN ports.

3.1.1 Initial Screen

When you turn on your ZyWALL, it performs several internal tests as well as line initialization.
After the tests, the ZyWALL asks you to press [ENTER] to continue, as shown next.

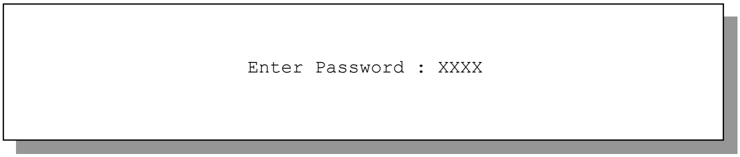


```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:41:51:61
initialize ch =1, ethernet address: 00:a0:c5:41:51:62
Press ENTER to continue...
```

Figure 3-1 Initial Screen

3.1.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below. For your first login, enter the default password "1234". As you type the password, the screen displays an "X" for each character you type.
Please note that if there is no activity for longer than five minutes after you log in, your ZyWALL will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.



```
Enter Password : XXXX
```

Figure 3-2 Password Screen

3.2 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your ZyWALL. Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 3-1 Main Menu Commands

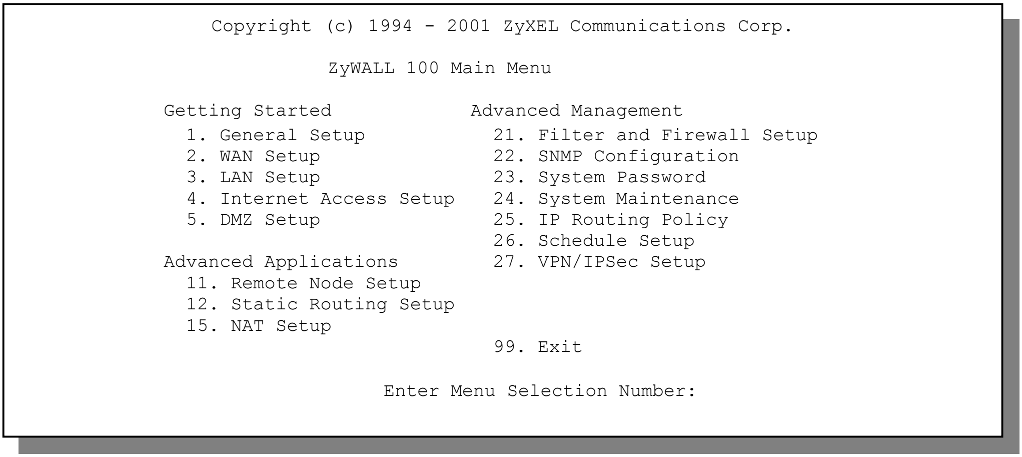
OPERATION	KEYSTROKES	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with “Edit” lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] to change **No** to **Yes**, and then press [ENTER] to go to a “hidden” menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Fill in, or press [SPACE BAR], then press [ENTER] to select from choices.	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	<? >	All fields with the symbol <?> must be filled in order 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.
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.

Table 3-1 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

3.2.1 Main Menu

After you enter the password, the SMT displays the **ZyWALL Main Menu**, as shown next. Not all models have all the features shown.



```
                Copyright (c) 1994 - 2001 ZyXEL Communications Corp.

                          ZyWALL 100 Main Menu

            Getting Started            Advanced Management
              1. General Setup           21. Filter and Firewall Setup
              2. WAN Setup               22. SNMP Configuration
              3. LAN Setup               23. System Password
              4. Internet Access Setup   24. System Maintenance
              5. DMZ Setup               25. IP Routing Policy
                                         26. Schedule Setup
            Advanced Applications        27. VPN/IPSec Setup
              11. Remote Node Setup
              12. Static Routing Setup
              15. NAT Setup
                                         99. Exit

                                 Enter Menu Selection Number:
```

Figure 3-3 Main Menu (ZyWALL 100)

3.2.2 System Management Terminal Interface Summary

Table 3-2 Main Menu Summary

NO.	MENU TITLE	FUNCTION
1	General Setup	Use this menu to set up dynamic DNS and administrative information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN and configure the backup WAN dial-up connection.
3	LAN Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings and configure the wireless LAN port (not available on all models).

Table 3-2 Main Menu Summary

NO.	MENU TITLE	FUNCTION
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
5	DMZ Setup (This feature is not available on all models.)	Use this menu to configure your public servers connected to the DMZ port.
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	Configure IP static routes in this menu.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Password	Change your password in this menu (recommended).
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
25	IP Routing Policy Setup	Use this menu to configure policies for use in IP policy routing.
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 menu to exit (necessary for remote configuration).

3.2.3 SMT Menus at a Glance

The available SMT screens vary by ZyWALL model. The following SMT overview applies to the ZyWALL 100.

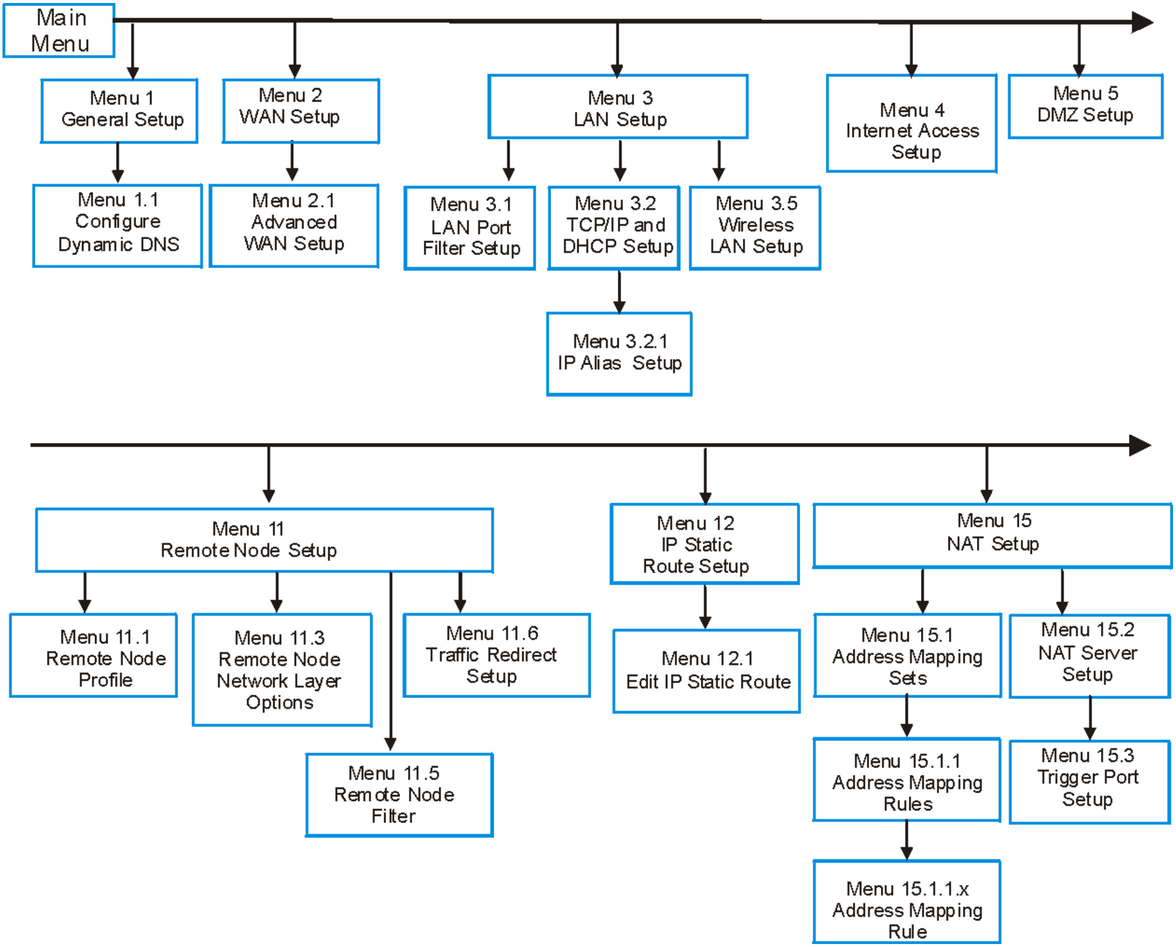

Main Menu
Menu 1 General Setup
Menu 1.1 Configure Dynamic DNS
Menu 2 WAN Setup
Menu 2.1 Advanced WAN Setup
Menu 3 LAN Setup
Menu 3.1 LAN Port Filter Setup
Menu 3.2 TCP/IP and DHCP Setup
Menu 3.2.1 IP Alias Setup
Menu 3.5 Wireless LAN Setup
Menu 4 Internet Access Setup
Menu 5 DMZ Setup
Menu 11 Remote Node Setup
Menu 11.1 Remote Node Profile
Menu 11.3 Remote Node Network Layer Options
Menu 11.5 Remote Node Filter
Menu 11.6 Traffic Redirect Setup
Menu 12 IP Static Route Setup
Menu 12.1 Edit IP Static Route
Menu 15 NAT Setup
Menu 15.1 Address Mapping Sets
Menu 15.1.1 Address Mapping Rules
Menu 15.1.1.x Address Mapping Rule
Menu 15.2 NAT Server Setup
Menu 15.3 Trigger Port Setup

Figure 3-4 Getting Started and Advanced Applications SMT Menus

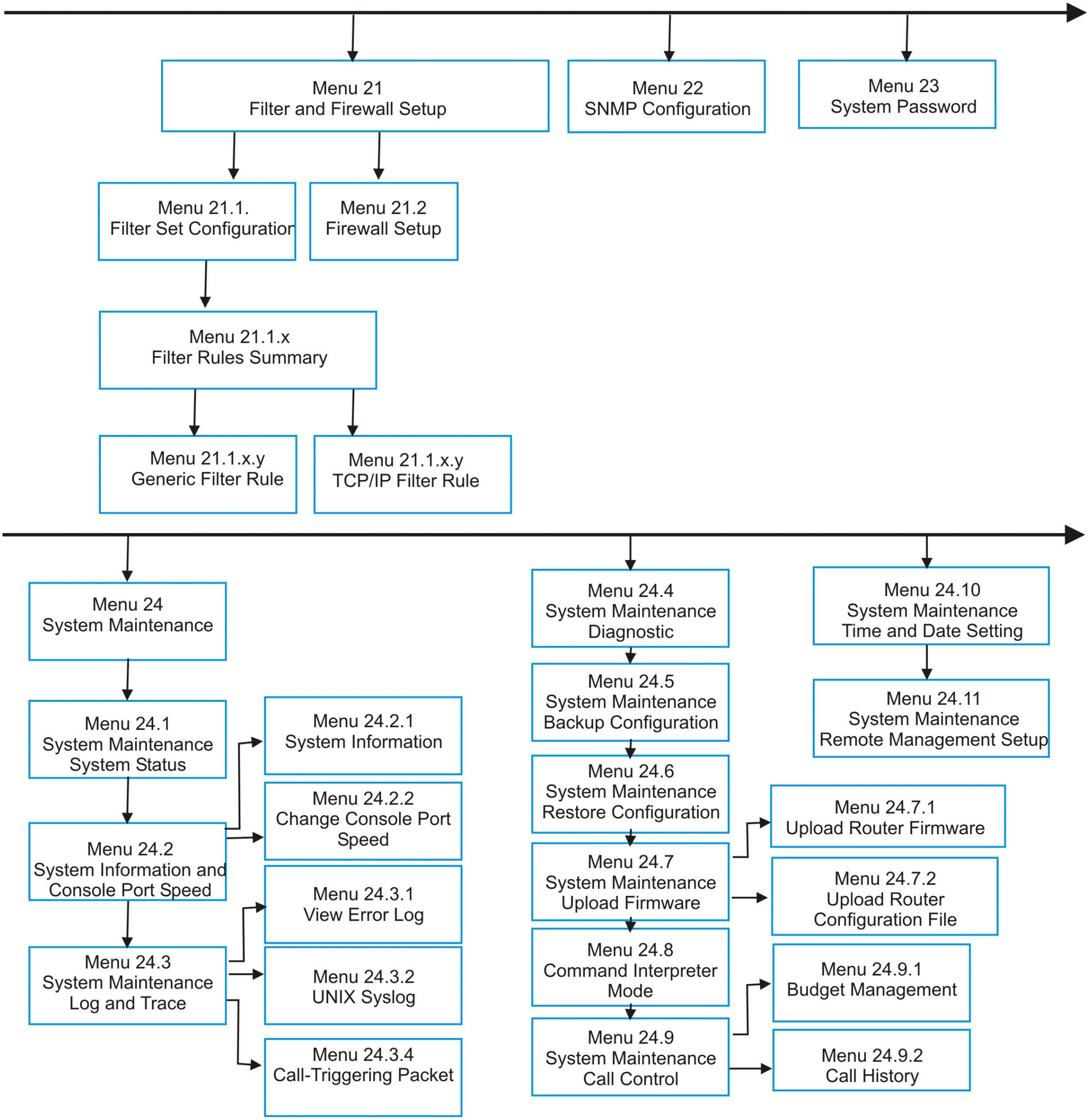


Figure 3-5 Advanced Management SMT Menus

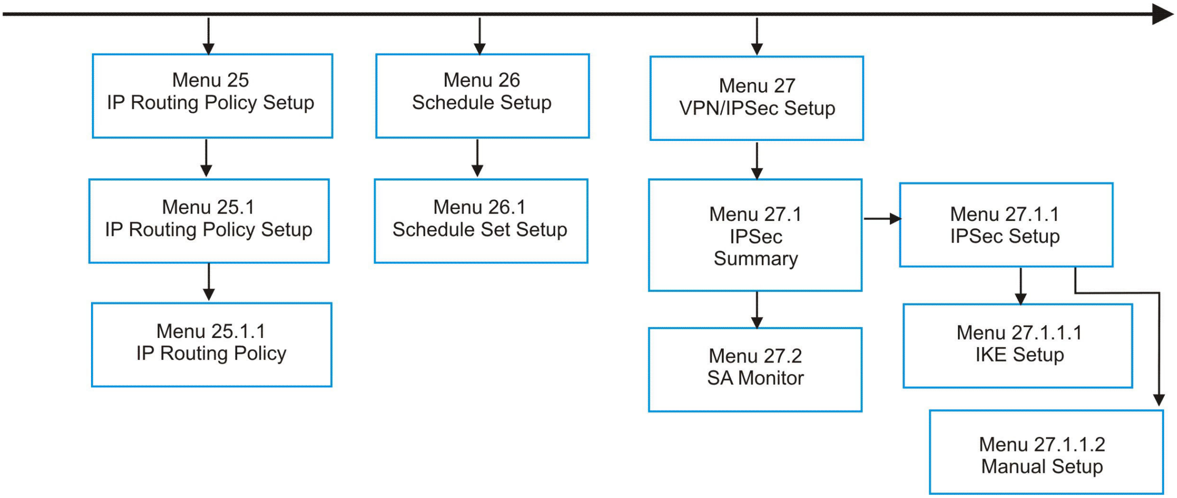
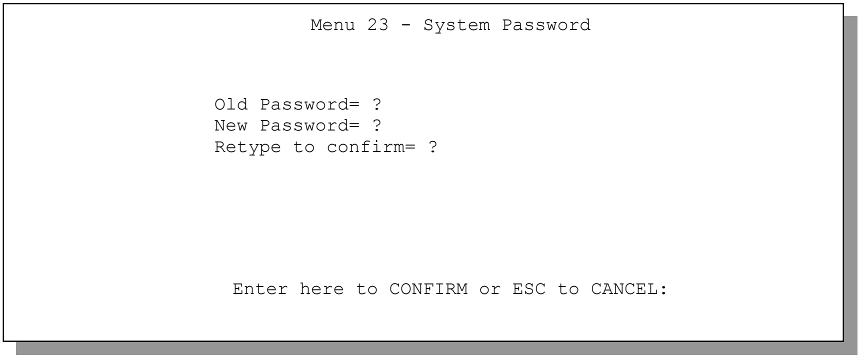


Figure 3-6 Schedule Setup and IPSec VPN Configuration SMT Menus

3.3 Changing the System Password

Change the default system password by following the steps shown next.

Step 1. Enter 23 in the main menu to open **Menu 23 - System Password** as shown next.



```
                            Menu 23 - System Password


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






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

Figure 3-7 Menu 23: System Password

Step 2. Type your existing password and press [ENTER].

Step 3. Type your new system password and press [ENTER].

Step 4. Re-type your new system password for confirmation and press [ENTER].

Note that as you type a password, the screen displays an “X” for each character you type.

3.4 Resetting the ZyWALL

If you forget your password or cannot access the ZyWALL, you will need to reload the factory-default configuration file. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to "1234" and the LAN IP address to 192.168.1.1also.

To obtain the default configuration file, download it from the ZyXEL FTP site, unzip it and save it in a folder. Turn the ZyWALL off and then on to begin a session. When you turn on the ZyWALL again you will see the initial screen. When you see the message "Press any key to enter Debug Mode within 3 seconds" press any key to enter debug mode.

To upload the configuration file, do the following:

1. Type `atlc` after the `Enter Debug Mode` message.
2. Wait for the `Starting XMODEM upload` message before activating XMODEM upload on your terminal.
3. After a successful firmware upload, type `atgo` to restart the ZyWALL.

The ZyWALL is now reinitialized with a default configuration file including the default password of "1234".

3.4.1 Methods of Restoring Factory-Defaults

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

a. Upload the default configuration file via the console port as described above. See later in this User's Guide for more information on how to transfer the configuration file to your ZyWALL using the SMT menus.

b. Use the **RESET** button on the rear panel of the ZyWALL (see the next section). Use this method for cases when the password or IP address of the ZyWALL is not known.

c. Use the web configurator to restore defaults (see the web configurator HTML help).

3.4.2 Procedure To Use The Reset Button

Make sure the **SYS** LED is on (not blinking) before you begin this procedure.

1. Press the **RESET** button for ten seconds, and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the ZyWALL restarts. Otherwise, go to step 2.
2. Turn the ZyWALL off.
3. While pressing the **RESET** button, turn the ZyWALL on.
4. Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the ZyWALL is now restarting.
5. Release the **RESET** button and wait for the ZyWALL to finish restarting.

Chapter 4
SMT Menu 1 - General Setup

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

4.1 System Name

System Name is for identification purposes. ZyXEL recommends you enter your computer's "Computer name".

- In Windows 95/98 click **Start** -> **Settings** -> **Control Panel** and then double-click **Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it in the ZyWALL **System Name** field.
- 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 in the ZyWALL **System Name** field.
- 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 ZyWALL **System Name**.

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

4.2 Dynamic DNS

Dynamic DNS (Domain Name System) 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* or other services). You can also access your FTP server or Web site on your own computer using a DNS-like address (for example, *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 DNS name.

To use this service, you must register with the Dynamic DNS service provider. The Dynamic DNS service provider will give you a password or key. The ZyWALL supports www.dyndns.org. You can apply to this service provider for Dynamic DNS service.

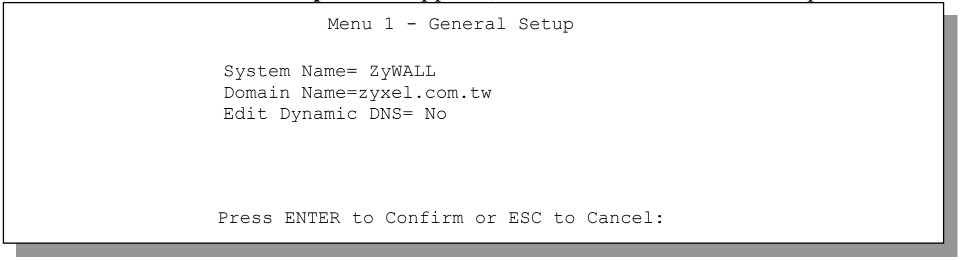
4.2.1 DYNDNS Wildcard

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.

4.3 General Setup

Step 1. Enter 1 in the main menu to open **Menu 1: General Setup**.

Step 2. The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.



```
                           Menu 1 - General Setup

                  System Name= ZyWALL
                  Domain Name=zyxel.com.tw
                  Edit Dynamic DNS= No




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

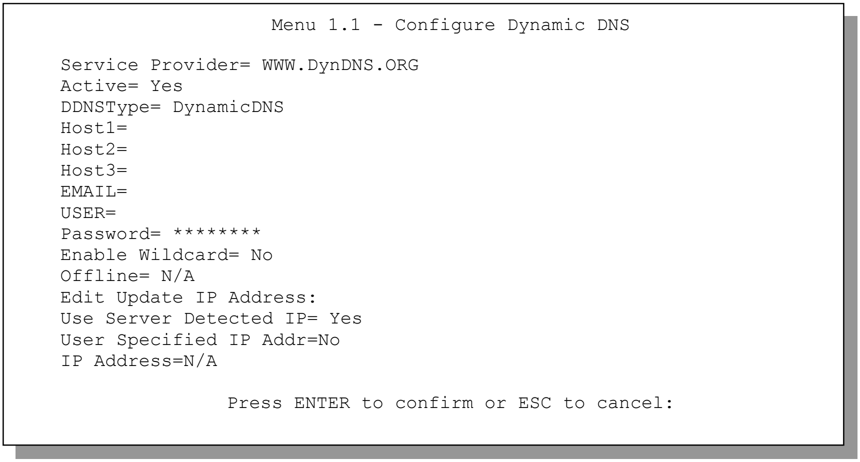
Figure 4-1 Menu 1: General Setup

Table 4-1 General Setup Menu Field

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" (*see section 4.1)* in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	ZyWALL
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 domain name" to see the current domain name used by your router. If you want to clear this field just press [SPACE BAR] and then [ENTER]. The domain name entered by you is given priority over the ISP assigned domain name.	zyxel.com.tw
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.	**No** (default)
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.		

4.3.1 Configuring Dynamic DNS

To configure Dynamic DNS, go to **Menu 1: General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** (shown next). Not all models have every field shown.



```
                     Menu 1.1 - Configure Dynamic DNS

     Service Provider= WWW.DynDNS.ORG
     Active= Yes
     DDNSType= DynamicDNS
     Host1=
     Host2=
     Host3=
     EMAIL=
     USER=
     Password= ********
     Enable Wildcard= No
     Offline= N/A
     Edit Update IP Address:
     Use Server Detected IP= Yes
     User Specified IP Addr=No
     IP Address=N/A

                    Press ENTER to confirm or ESC to cancel:
```

Figure 4-2 Configure Dynamic DNS

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

Table 4-2 Configure Dynamic DNS Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
DDNS Type	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have a dynamic IP address(es). Select **StaticDNS** if you have a static IP address(s). Select **CustomDNS** to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.	**DynamicDNS** (default)
Host1-3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver

Table 4-2 Configure Dynamic DNS Menu Fields

FIELD	DESCRIPTION	EXAMPLE
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your ZyWALL 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.	**No**
Offline	This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).	**Yes**
Edit Update IP Address: You can select **Yes** in either the **Use Server Detected IP** field (recommended) or the **User Specified IP Addr** field, but not both. With the **Use Server Detected IP** and **User Specified IP Addr** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the ZyWALL's WAN IP address. DDNS does not work with a private IP address. When both fields are set to **No**, the ZyWALL must have a public WAN IP address in order for DDNS to work.		
Use Server Detected IP	Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the ZyWALL uses or is behind. You can set this field to **Yes** whether the IP address is public or private, static or dynamic.	**Yes**
User Specified IP Addr	Press [SPACE BAR] to select **Yes** and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below. Only select **Yes** if the ZyWALL uses or is behind a static public IP address.	**No**
IP Address	Enter the static public IP address if you select **Yes** in the **User Specified IP Addr** field.	**N/A**
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.		

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

Chapter 5 WAN and Dial Backup Setup

This chapter describes how to configure the WAN using menu 2 and dial-backup using menus 2.1 and 11.1. Dial-backup applies to the ZyWALL 100 and 10W (see Table 1-1 Model Specific Features).

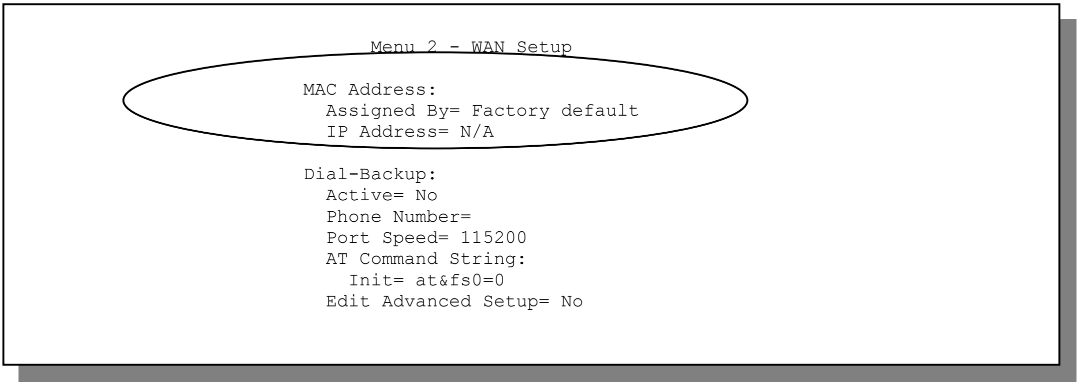
5.1 Cloning The MAC Address

The MAC address field allows users to configure the WAN port's MAC address by using either the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting in menu 2 or upload a different rom file.

ZyXEL recommends that you clone the MAC address of a computer on your LAN even if your ISP does not require MAC address authentication.

5.2 WAN Setup

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



```
                    Menu 2 - WAN Setup

              MAC Address:
                Assigned By= Factory default
                IP Address= N/A

              Dial-Backup:
                Active= No
                Phone Number=
                Port Speed= 115200
                AT Command String:
                  Init= at&fs0=0
                Edit Advanced Setup= No
```

Figure 5-1 MAC Address Cloning in WAN Setup

The following table contains instructions on how to configure your WAN setup.

Table 5-1 MAC Address Cloning in WAN Setup

FIELD	DESCRIPTION	EXAMPLE
MAC Address:		
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP address attached on LAN** to use the MAC Address of that workstation whose IP you give in the following field.	**IP address attached on LAN**
IP Address	This field is applicable only if you choose the **IP address attached on LAN** method in the **Assigned By** field. Enter the IP address of the computer on the LAN whose MAC you are cloning.	192.168.1.35
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.		

5.3 Dial Backup

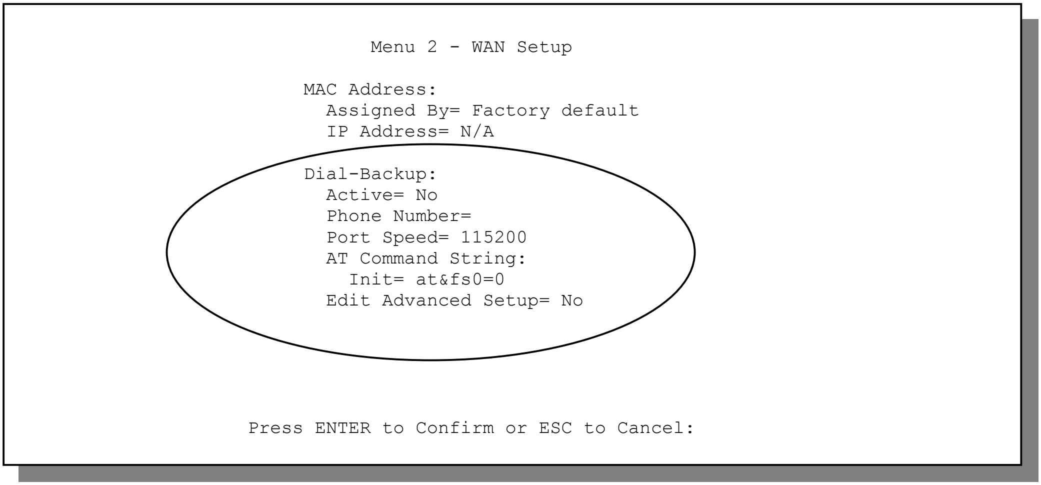
The Dial Backup port or CON/AUX port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. This feature is not available on all models. To set up the auxiliary port (Dial Backup or CON/AUX) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the Hardware Installation chapter), then configure

1. Menu 2 - WAN Setup,
2. Menu 2.1 - Advanced WAN Setup and
3. Menu 11.1 - Remote Node Profile (Backup ISP) as shown next

Refer also to the traffic redirect section in this *User's Guide* for information on an alternate backup WAN connection.

5.4 Configuring Dial Backup in Menu 2

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



```
                    Menu 2 - WAN Setup

              MAC Address:
                Assigned By= Factory default
                IP Address= N/A

              Dial-Backup:
                Active= No
                Phone Number=
                Port Speed= 115200
                AT Command String:
                  Init= at&fs0=0
                Edit Advanced Setup= No




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

Figure 5-2 Menu 2: Dial Backup Setup

Table 5-2 Menu 2: Dial Backup Setup

FIELD	DESCRIPTION	EXAMPLE
Dial-Backup:		
Active	Use this field to turn the dial-backup feature on (**Yes**) or off (**No**).	**No**
Phone Number	Enter the telephone number assigned to your line by your telephone company. This field only accepts digits; do not include dashes and spaces.	1234567
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.	**115200**
AT Command String:		
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.	at&fs0=0
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.1: Advanced Setup**.	**Yes**

Table 5-2 Menu 2: Dial Backup Setup

FIELD	DESCRIPTION	EXAMPLE
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.		

5.5 Advanced WAN Setup

Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.

5.5.1 AT Command Strings

For regular telephone lines, the default "Dial" string tells the modem that the line uses tone dialing. "`ATDT`" is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to "`ATDP`".

For ISDN lines, there are many more protocols and operational modes. Please consult the documentation of your TA. You may need additional commands in both "Dial" and "Init" strings.

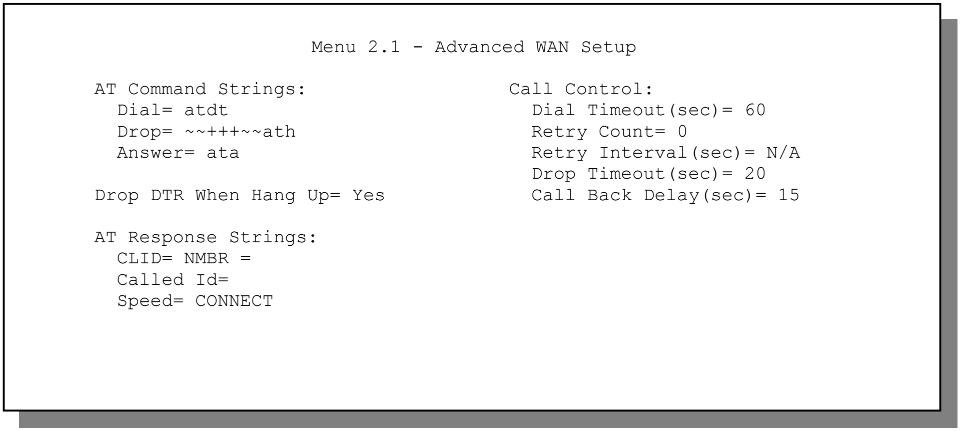
5.5.2 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When "Drop DTR When Hang Up" is set to **Yes**, the ZyWALL uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command "`ATH"`.

5.5.3 Response Strings

The response strings tell the ZyWALL the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2 - WAN Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].



```
                    Menu 2.1 - Advanced WAN Setup

      AT Command Strings:                   Call Control:
        Dial= atdt                            Dial Timeout(sec)= 60
        Drop= ~~+++~~ath                      Retry Count= 0
        Answer= ata                           Retry Interval(sec)= N/A
                                              Drop Timeout(sec)= 20
      Drop DTR When Hang Up= Yes              Call Back Delay(sec)= 15

      AT Response Strings:
        CLID= NMBR =
        Called Id=
        Speed= CONNECT
```

Figure 5-3 Menu 2.1 Advanced WAN Setup

The following table describes fields in this menu.

Table 5-3 Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION	DEFAULT
AT Command Strings:		
Dial	Enter the AT Command string to make a call.	atdt
Drop	Enter the AT Command string to drop a call. "~" represents a one second wait, e.g., "~~~+++~~ath" can be used if your modem has a slow response time.	+++ath
Answer	Enter the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the "AT Command String: Drop" is sent out.	**Yes**
AT Response String:		
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR =

Table 5-3 Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION	DEFAULT
Called Id	Enter the keyword preceding the dialed number.	TO
Speed	Enter the keyword preceding the connection speed.	CONNECT

Table 5-4 Advanced WAN Port Setup: Call Control Parameters

FIELD	DESCRIPTION	DEFAULT
Call Control		
Dial Timeout (sec)	Enter a number of seconds for the ZyWALL to keep trying to set up an outgoing call before timing out (stopping). The ZyWALL times out and stops if it cannot set up an outgoing call within the timeout value.	60 seconds
Retry Count	Enter a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number.	0 to disable the blacklist control
Retry Interval (sec)	Enter a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	
Drop Timeout (sec)	Enter a number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20 seconds
Call Back Delay (sec)	Enter a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the co-responding callback call.	15 seconds

5.6 Backup Remote Node Setup

The rest of this chapter shows you how to configure a remote node for a dial-backup connection.

5.6.1 Metric

The metric sets the priority for the ZyWALL's routes to the Internet. If any two of the default routes have the same metric, the ZyWALL uses the following pre-defined priorities:

1. Normal route: designated by the ISP (see *Remote Node Setup* chapter) or a static route (see the IP Static Route Setup chapter)
2. Traffic-redirect route (see the *Remote Node Setup* chapter)

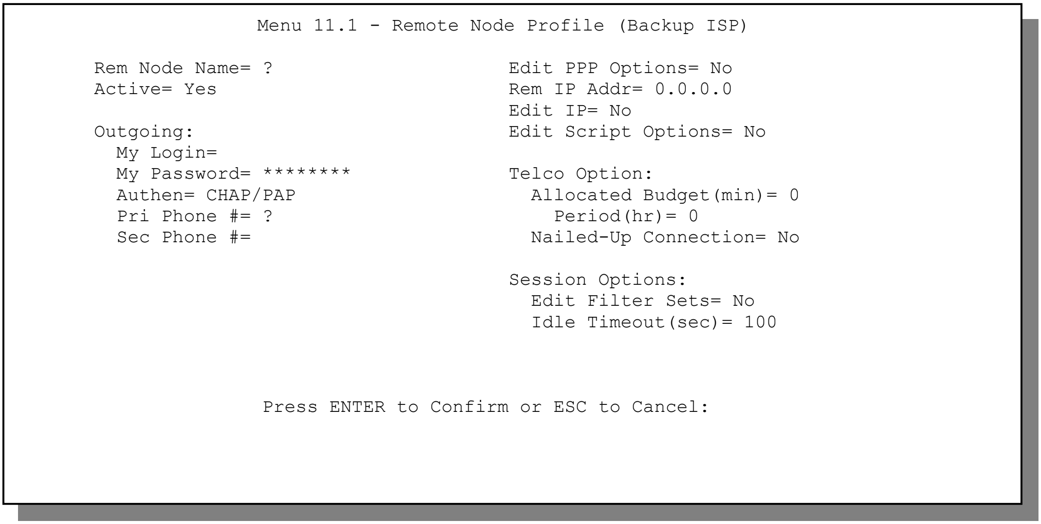
3. Dial-backup route (see the Backup Remote Node Setup chapter)

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the ZyWALL tries the traffic-redirect route next. In the same manner, the ZyWALL uses the dial-backup route if the traffic-redirect route also fails.

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).

5.7 Remote Node Profile (Backup ISP)

Enter **2** in **Menu 11 Remote Node Setup** to open **Menu 11.1 Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection. This feature is not available on all models.



```
                    Menu 11.1 - Remote Node Profile (Backup ISP)

    Rem Node Name= ?                    Edit PPP Options= No
    Active= Yes                         Rem IP Addr= 0.0.0.0
                                        Edit IP= No
    Outgoing:                           Edit Script Options= No
      My Login=
      My Password= ********             Telco Option:
      Authen= CHAP/PAP                    Allocated Budget(min)= 0
      Pri Phone #= ?                        Period(hr)= 0
      Sec Phone #=                        Nailed-Up Connection= No

                                        Session Options:
                                          Edit Filter Sets= No
                                          Idle Timeout(sec)= 100



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

Figure 5-4 Menu 11.1 Remote Node Profile (Backup ISP)

Table 5-5 Fields in Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node.	**Yes**
Outgoing		

Table 5-5 Fields in Menu 11.1 Remote Node Profile (Backup ISP)

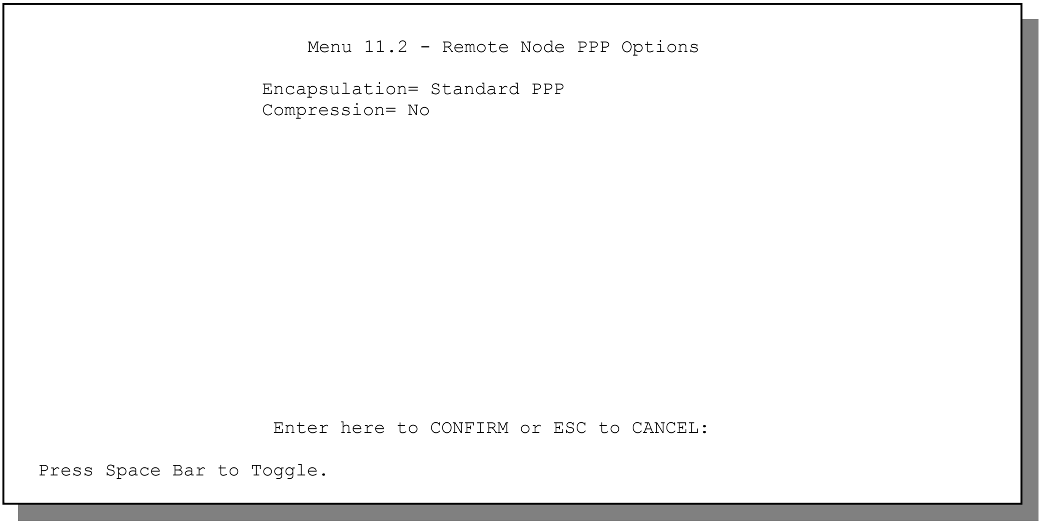
FIELD	DESCRIPTION	EXAMPLE
My Login	Enter the login name assigned by your ISP for this remote node.	jim
My Password	Enter the password assigned by your ISP for this remote node.	*****
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	**CHAP/PAP**
Pri Phone # Sec Phone #	Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.	
Edit PPP Options	Move the cursor to this field and use the space bar to select [Yes] and press [Enter] to edit the PPP options for this remote node. This brings you to Menu 11.2 - Remote Node PPP Options (see *section 5.8*).	**No** (default)
Rem IP Addr	Leave the field set to 0.0.0.0 (default) if the remote gateway has a dynamic IP address. Enter the remote gateway's IP address here if it is static.	0.0.0.0 (default)
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.3 - Remote Node Network Layer Options**. See *section 5.9* for more information.	**No** (default)
Edit Script Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.4 - Remote Node Script**). See *section 5.10* for more information.	**No** (default)
Telco Option		
Allocated Budget	Enter the maximum number of minutes that this remote node may be called within the time period configured in the **Period** field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node.	0 (default)

Table 5-5 Fields in Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Period(hr)	Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).	0 (default)
Nailed-Up Connection	Press [SPACE BAR] to select **Yes** to set this connection to always be on, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection.	**No** (default)
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 *section 5.11* for more details.	**No** (default)
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) that can elapse before the ZyWALL automatically disconnects the PPP connection. This option only applies when the ZyWALL initiates the call.	100 seconds (default)
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.		

5.8 Editing PPP Options

The ZyWALL's dial back-up feature uses PPP. 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 the space bar to select **[Yes].** Press [Enter] to open Menu 11.2 as shown next.



```
                    Menu 11.2 - Remote Node PPP Options

                Encapsulation= Standard PPP
                Compression= No














                 Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figure 5-5 Menu 11.2 - Remote Node PPP Options

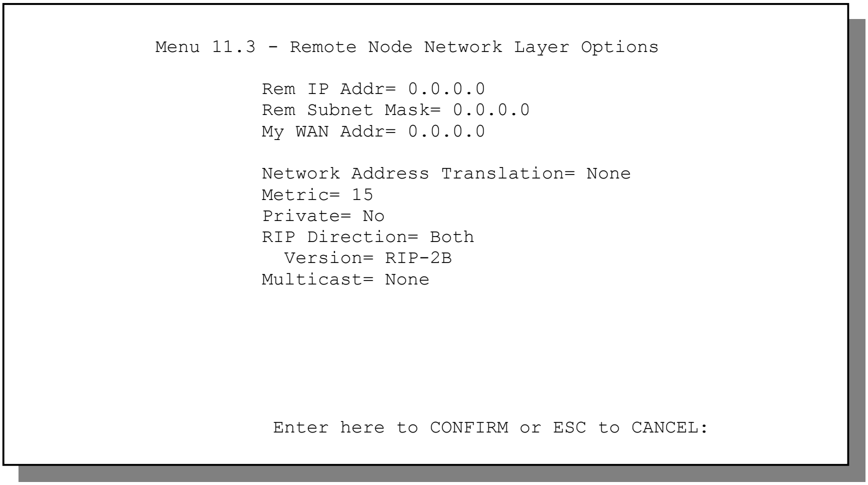
This table describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

Figure 5-6 Remote Node PPP Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **CISCO PPP** if your Dial Backup WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**.	**Standard PPP** (default)
Compression	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable or **No** to disable Stac compression.	**No** (default)

5.9 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**.



```
              Menu 11.3 - Remote Node Network Layer Options

                         Rem IP Addr= 0.0.0.0
                         Rem Subnet Mask= 0.0.0.0
                         My WAN Addr= 0.0.0.0

                         Network Address Translation= None
                         Metric= 15
                         Private= No
                         RIP Direction= Both
                           Version= RIP-2B
                         Multicast= None





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

Figure 5-7 Menu 11.3: Remote Node Network Layer Options

The next table gives you instructions about configuring remote node network layer options.

Table 5-6 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Rem IP Address	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Enter the remote gateway's IP address here if you know it (static).	0.0.0.0 (default)
Rem IP Subnet Mask	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Enter the remote gateway's subnet mask here if you know it (static).	0.0.0.0 (default)
My WAN Addr	Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static). This is the address assigned to your local ZyWALL, not the remote router.	0.0.0.0 (default)

Table 5-6 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Network Address Translation	Press [SPACE BAR] and then [ENTER] to select either **Full Feature, None** or **SUA Only.** See the Network Address Translation (NAT) chapter for a full discussion on this feature.	**None** (default)
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see section *5.6.1*) The smaller the number, the higher priority the route has.	15 (default)
Private	This parameter determines if the ZyWALL 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 broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**No** (default)
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the **RIP direction** from **Both/ None**/**In Only**/**Out Only** and **None**.	**Both** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1**
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See the LAN Setup chapter for more information on this feature.	**None** (default)
Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

5.10 Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The ZyWALL provides a script facility for this purpose. The script has six programmable sets; each set is composed of an 'Expect' string and a 'Send' string. After matching a message from the server to the 'Expect' field, the ZyWALL returns the set's 'Send' string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
Login: myLogin
Password:
```

To handle the first prompt, you specify "`ogin: `" as the 'Expect' string and "`myLogin`" as the 'Send' string in set 1. The reason for leaving out the leading "`L`" is to avoid having to know exactly whether it is upper or lower case. Similarly, you specify "`word:  `" as the 'Expect' string and your password as the 'Send' string for the second prompt in set 2.

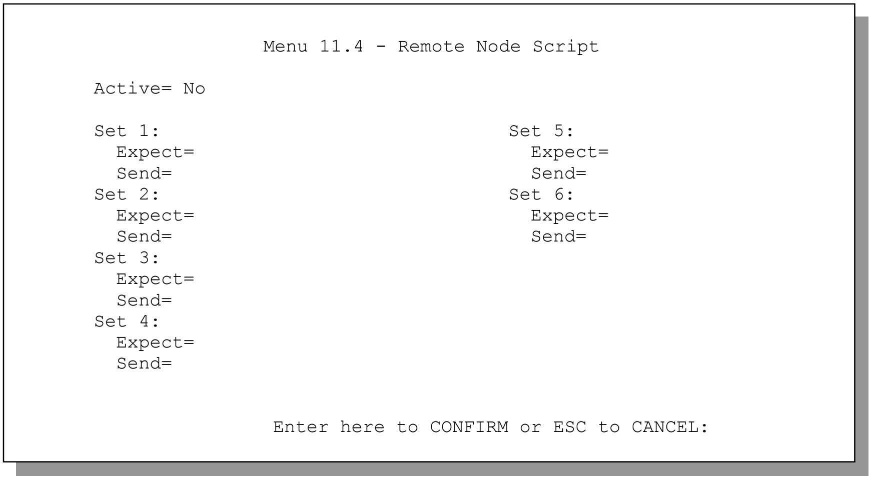
You can use two variables, `$USERNAME` and `$PASSWORD` (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear. They are replaced with the outgoing login name and password in the remote node when the ZyWALL sees them in a 'Send' string. Please note that both variables must been entered exactly as shown. No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

Please note that the ordering of the sets is significant, i.e., starting from set 1, the ZyWALL will wait until the 'Expect' string is matched before it proceeds to set 2, and so on for the rest of the script. When both the 'Expect' and the 'Send' fields of the current set are empty, the ZyWALL will terminate the script processing and start PPP negotiation. This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored. Second, the last set should match the final message sent by the server. For instance, if the server prints:

```
      login successful.
      Starting PPP...
```

after you enter the password, then you should create a third set to match the final "`PPP...`" but without a "Send" string. Otherwise, the ZyWALL will start PPP prematurely right after sending your password to the server.

If there are errors in the script and it gets stuck at a set for longer than the "Dial Timeout" in menu 2 (default 60 seconds), the ZyWALL will timeout and drop the line. To debug a script, go to Menu 24.4 to initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.



```
                       Menu 11.4 - Remote Node Script

        Active= No

        Set 1:                                  Set 5:
          Expect=                                 Expect=
          Send=                                   Send=
        Set 2:                                  Set 6:
          Expect=                                 Expect=
          Send=                                   Send=
        Set 3:
          Expect=
          Send=
        Set 4:
          Expect=
          Send=


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

Figure 5-8 Menu 11.4 – Remote Node Setup Script

The following table describes each field in Menu 11.4 – Remote Node Setup Script.

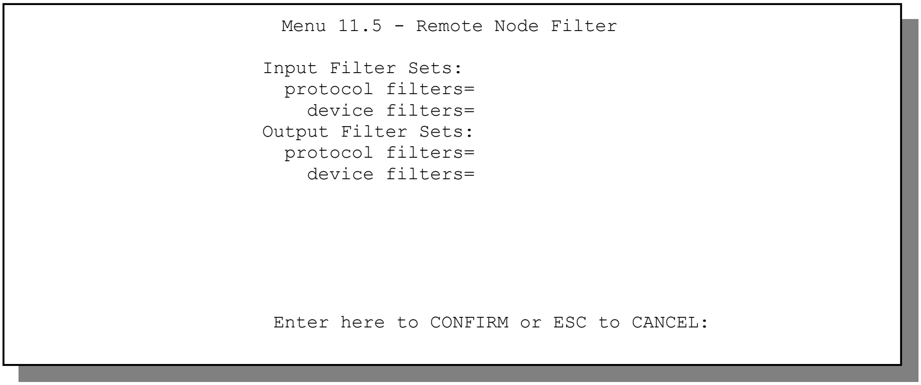
Table 5-7 Remote Node Script Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and then [ENTER] to select either **Yes** to enable the AT strings or **No** to disable them.	**No** (default)
Set 1-6: Expect	Enter an Expect string to match. After matching the Expect string, the ZyWALL returns the string in the **Send** field.	
Set 1-6: Send	Enter a string to send out after the Expect string is matched.	0.0.0.0

5.11 Remote Node Filter

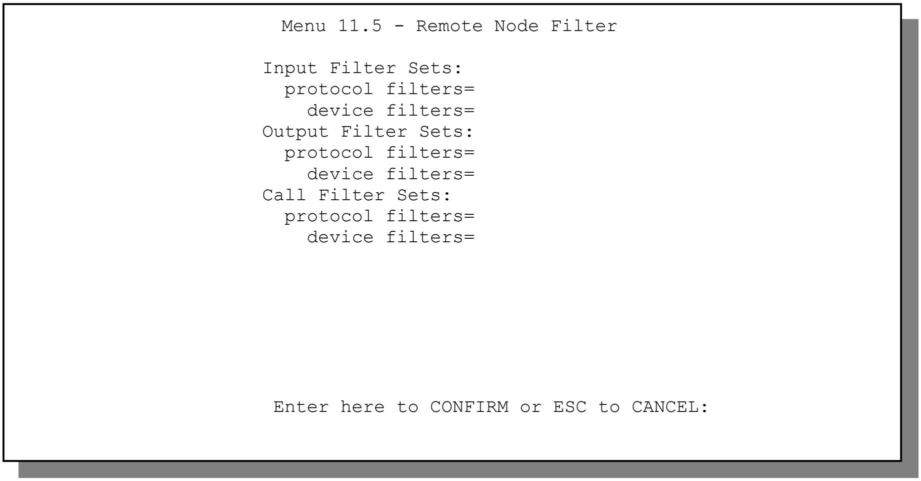
Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to the Filters chapter for more information on defining the filters. With PPPoE and PPTP encapsulations you also have the option of specifying remote node call filter sets.



```
                          Menu 11.5 - Remote Node Filter

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









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

Figure 5-9 Menu 11.5: Remote Node Filter (Ethernet)



```
                          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:
```

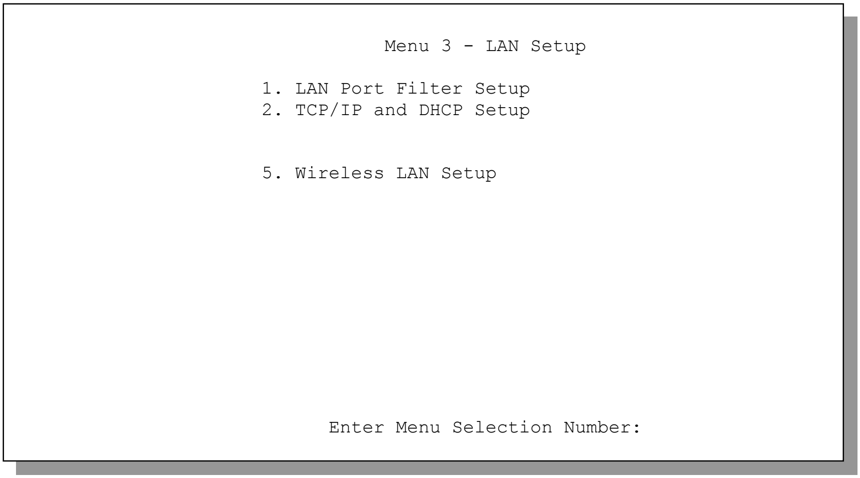
Figure 5-10 Menu 11.5: Remote Node Filter (PPPoE or PPTP)

Chapter 6
LAN Setup

*This chapter describes how to configure the LAN using **Menu 3: LAN Setup**. Wireless LAN is available on the ZyWALL 10W and 100 models.*

6.1 Introduction

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

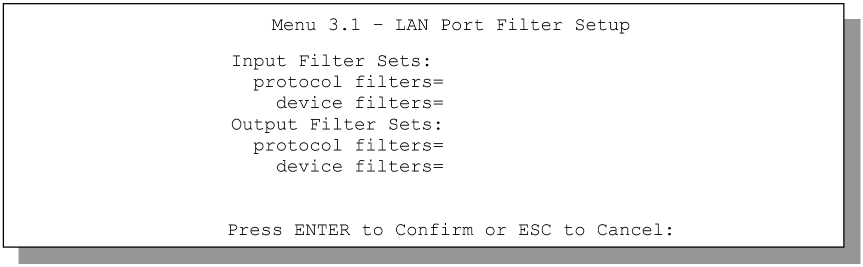


```
                    Menu 3 - LAN Setup

              1. LAN Port Filter Setup
              2. TCP/IP and DHCP Setup


              5. Wireless LAN Setup











                 Enter Menu Selection Number:
```

Figure 6-1 Menu 3: LAN Setup

6.2 LAN Port Filter Setup

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



```
                       Menu 3.1 - LAN Port Filter Setup

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


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

Figure 6-2 Menu 3.1: LAN Port Filter Setup

6.3 TCP/IP and LAN DHCP

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

6.3.1 Factory LAN Defaults

The LAN parameters of the ZyWALL are preset in the factory with the following values:

1. IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits).
2. DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you an explicit DNS server address(es), skip ahead to *section 6.4* to see how to enter the DNS server address(es).

6.3.2 DHCP Configuration

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 ZyWALL as a DHCP server or disable it. When configured as a server, the ZyWALL 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.

IP Pool Setup

The ZyWALL is pre-configured with a pool of 32 IP addresses ranging from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ZyWALL itself) in the lower range for other server machines, e.g., server for mail, FTP, Telnet, web, etc., that you may have.

DNS Server Address

Use DNS to map a domain name to its corresponding IP address and vice versa, for example, the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

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

The first is for an ISP to tell a customer 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 DHCP Setup**.**

The second is to leave this field blank, i.e., 0.0.0.0 — in this case; the ZyWALL acts as a DNS proxy.

Table 6-1 Example Of Network Properties For LAN Servers With Fixed IP Addresses

Choose an IP address	192.168.1.2 - 192.168.1.32; 192.168.1.65 - 192.168.1.254
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1 (ZyWALL LAN IP Address)

6.3.3 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do machines 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 ZyWALL. 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 workstation on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for example192.168.1.1, for your ZyWALL, 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 ZyWALL 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 ZyWALL unless you are instructed to do otherwise.

Private IP Addresses

Every computer on the Internet must have a unique IP 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:

Table 6-2 Private IP Address Ranges

10.0.0.0 — 10.255.255.255
172.16.0.0 — 172.31.255.255
192.168.0.0 — 192.168.255.255

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

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

6.3.4 RIP Setup

RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and the **Version** set to **RIP-1**.

6.3.5 IP Multicast

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

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

The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyWALL queries all directly connected networks to gather group membership. After that, the ZyWALL periodically updates this information. IP Multicasting can be enabled/disabled on the ZyWALL LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

6.3.6 IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Use menu 3.2.1 to configure IP Alias on your ZyWALL.

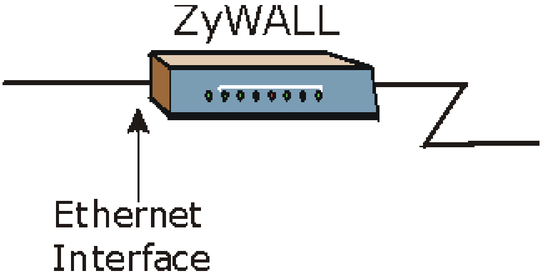


Figure 6-3 Physical Network

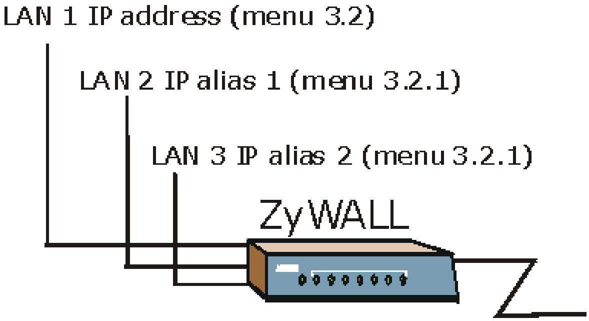
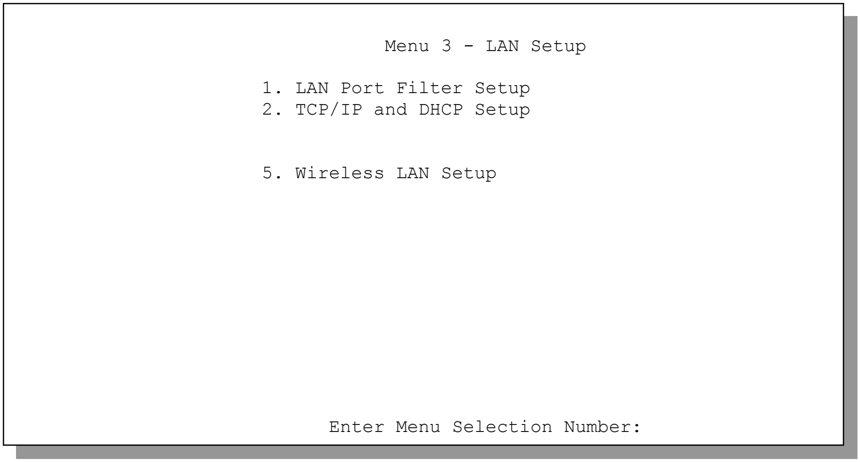

LAN 1 IP address (menu 3.2)
LAN 2 IP alias 1 (menu 3.2.1)
LAN 3 IP alias 2 (menu 3.2.1)
ZyWALL

Figure 6-4 Partitioned Logical Networks

6.4 TCP/IP and DHCP Ethernet Setup Menu

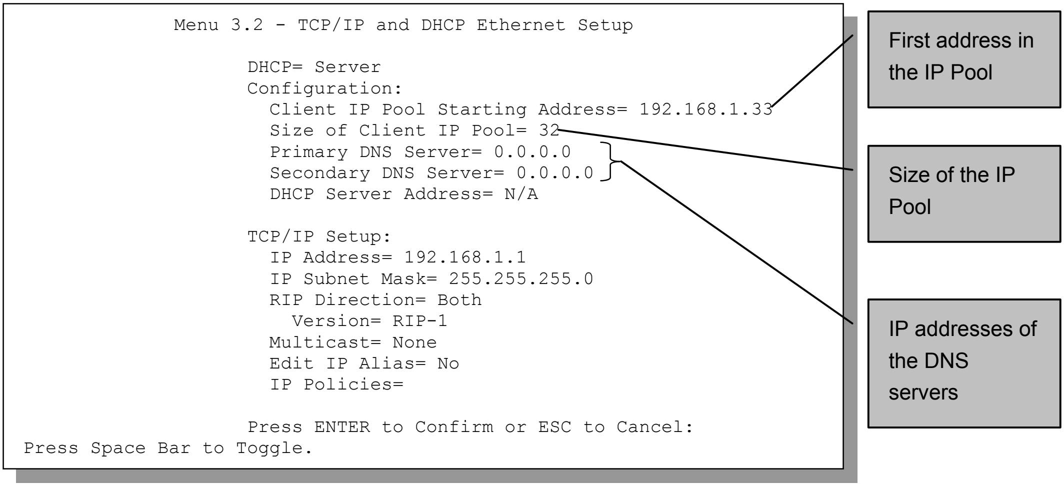
From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.



```
                              Menu 3 - LAN Setup

                   1. LAN Port Filter Setup
                   2. TCP/IP and DHCP Setup


                   5. Wireless LAN Setup














                         Enter Menu Selection Number:
```

Figure 6-5 Menu 3: TCP/IP and DHCP Setup

From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2: TCP/IP and DHCP Ethernet Setup,** as shown next.



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

                     DHCP= Server
                     Configuration:
                       Client IP Pool Starting Address= 192.168.1.33
                       Size of Client IP Pool= 32
                       Primary DNS Server= 0.0.0.0
                       Secondary DNS Server= 0.0.0.0
                       DHCP Server Address= N/A

                     TCP/IP Setup:
                       IP Address= 192.168.1.1
                       IP Subnet Mask= 255.255.255.0
                       RIP Direction= Both
                         Version= RIP-1
                       Multicast= None
                       Edit IP Alias= No
                       IP Policies=

                     Press ENTER to Confirm or ESC to Cancel:
 Press Space Bar to Toggle.
```

First address in the IP Pool

Size of the IP Pool

IP addresses of the DNS servers

Figure 6-6 Menu 3.2: TCP/IP and DHCP Ethernet Setup

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

Table 6-3 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP	This field enables/disables the DHCP server. If set to **Server**, your ZyWALL will act as a DHCP server. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the ZyWALL acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to **Server**, the following items need to be set:	**Server**
Configuration: Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	32
Primary DNS Server Secondary DNS Server	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.	
DHCP Server Address	If **Relay** is selected in the **DHCP** field above, then type the IP address of the actual, remote DHCP server here.	

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

LAN and DMZ IP addresses must be on separate subnets.

Table 6-4 LAN TCP/IP Setup Menu Fields

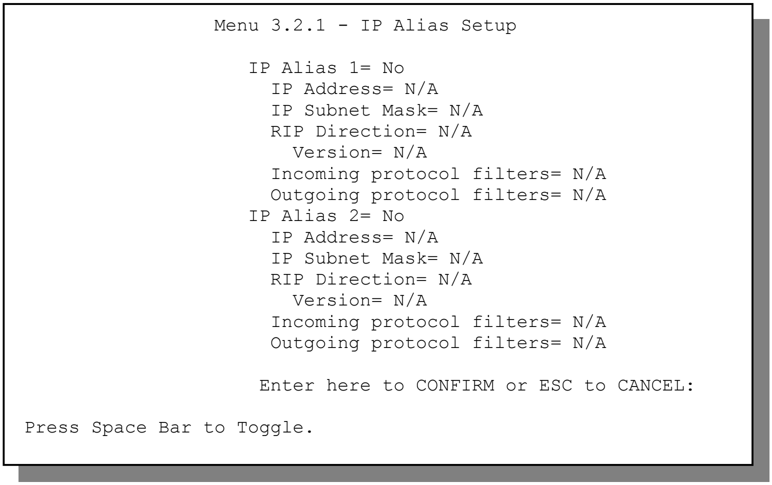
FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup: IP Address	Enter the IP address of your ZyWALL in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.	255.255.255.0

Table 6-4 LAN TCP/IP Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL 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.	**None**
Edit IP Alias	The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1	**Yes**
IP Policies	You can apply up to four IP Policy sets (from twelve) by typing their numbers separated by commas.	2,7,9,11
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.		

6.4.1 IP Alias Setup

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.



```
                 Menu 3.2.1 - IP Alias Setup

                    IP Alias 1= 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
                    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:

Press Space Bar to Toggle.
```

Figure 6-7 Menu 3.2.1: IP Alias Setup

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

Table 6-5 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	DEFAULT
IP Alias	Choose **Yes** to configure the LAN network for the ZyWALL.	**Yes**
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.	192.168.2.1
IP Subnet Mask	Your ZyWALL 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 ZyWALL.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only, Out Only** or **None**.	**None**
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyWALL.	1
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyWALL.	2
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.		

6.5 Wireless LAN

This section introduces the wireless LAN and some basic configuration. Wireless LANs can be as simple as two computers with wireless network interface cards (NICs) communicating in a peer-to-peer network or as complex as a number of computers with wireless NICs communicating through access points which bridge network traffic to the wired LAN. See *Chapter 7* for information on wireless LAN security features.

6.5.1 Channel

IEEE 802.11b wireless devices use ranges of radio frequencies called channels. Choose the radio channel depending on your geographical area. Adjacent Access Points (APs) should use different channels to reduce crosstalk. Crosstalk occurs when radio signals from access points overlap and cause interference that degrades performance.

6.5.2 ESS ID

Extended Service Set (ESS) is defined as one or more APs acting as a bridge between a wired LAN and the associated wireless clients. The ESS ID is a unique ID given to the APs and the wireless clients that participate in the same wireless network. You can think of the ESS ID as being similar to a workgroup name in a Microsoft network.

The ESS ID provides a minimum level of security for your network; see *Chapter 7* for more information.

6.5.3 RTS Threshold

The RTS (Request To Send) Threshold prevents the problem of hidden nodes. The hidden node problem occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates the hidden node problem. Both stations (STA) are within range of the (AP), however, they cannot hear each other. Therefore, they are considered hidden from each other. When a station starts data transmission with the AP, it might not know that the other station is already using the wireless medium. When these two stations send data at the same time, it might collide when arriving simultaneously at the AP. The collision will almost certainly result in a loss of messages for both stations.

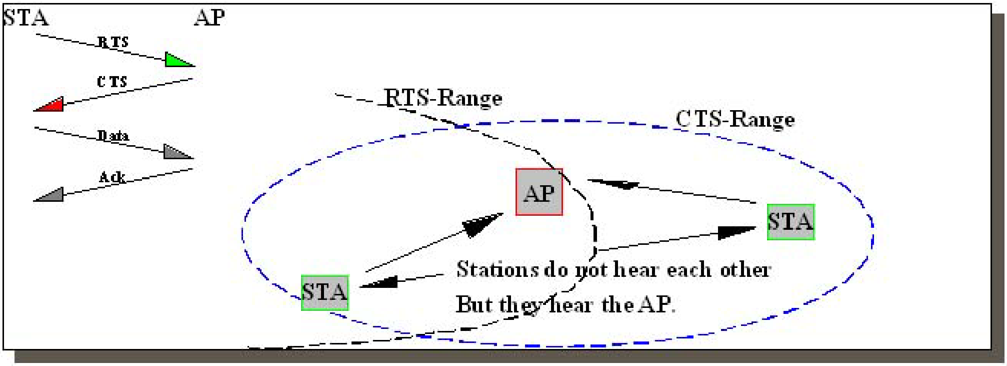


Figure 6-8 RTS Threshold

The RTS Threshold mechanism provides a solution to prevent these data collisions. When you enable RTS Threshold on a possible hidden station, this station and its AP will use a Request to Send/Clear to Send protocol (RTS/CTS). The station send an RTS message to the AP, informing that it is going to transmit the data. Upon receipt, the AP responds with a CTS message to all stations within its range to notify all other stations to defer transmission. It also confirms with the requesting station that the AP has reserved it for the time frame of the requested transmission.

The ZyWALL activates the RTS function if the packet size exceeds the value you set. It is highly recommended that you set the value ranging from 0 to 2432.

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

6.5.4 Fragmentation Threshold

Fragmentation improves efficiency when high traffic flows along in the wireless network.

6.5.5 WEP

As the first line of protection against wireless network intrusion, the ZyWALL provides the standard WEP (Wired Equivalent Privacy) for data encryption. However, there may be a significant degradation of the data throughput on the wireless link when WEP is enabled. See *section 7.2* for more information about configuring WEP data encryption.

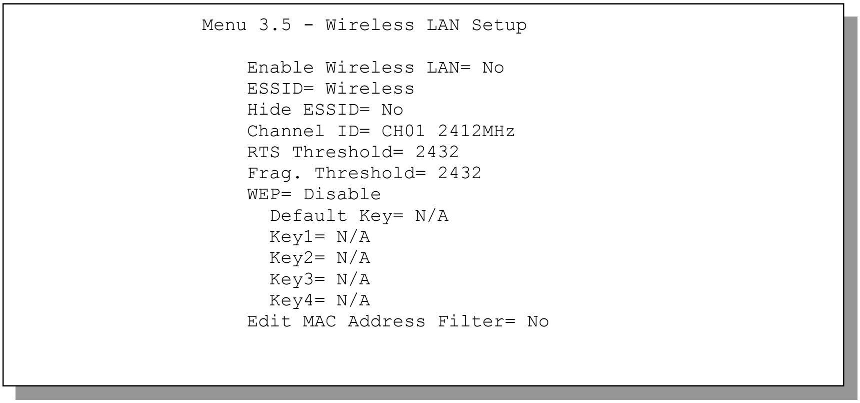
6.6 Wireless LAN Setup

Use menu 3.5 to set up your ZyWALL as the wireless access point.

See *section 7.2* for instructions on WEP and *section 7.5* for instructions on configuring the MAC address filter.

If you are configuring the ZyWALL from a computer connected to the wireless LAN and you change the ZyWALL's ESSID or WEP settings, you will lose your wireless connection when you press [ENTER] to confirm. You must then change the wireless settings of your computer to match the ZyWALL's new settings.

From the main menu, enter 3 to open **Menu 3** – **LAN Setup** to configure the Wireless LAN setup. To edit the wireless LAN configuration, enter 5 to open **Menu 3.5** – **Wireless LAN Setup** as shown next.



```
                  Menu 3.5 - Wireless LAN Setup

                      Enable Wireless LAN= No
                      ESSID= Wireless
                      Hide ESSID= No
                      Channel ID= CH01 2412MHz
                      RTS Threshold= 2432
                      Frag. Threshold= 2432
                      WEP= Disable
                        Default Key= N/A
                        Key1= N/A
                        Key2= N/A
                        Key3= N/A
                        Key4= N/A
                      Edit MAC Address Filter= No
```

Figure 6-9 Menu 3.5 – Wireless LAN Setup

The settings of all client stations on the wireless LAN must match those of the ZyWALL.

Follow the instructions in the next table on how to configure the wireless LAN parameters.

Table 6-6 Wireless LAN Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Enable Wireless LAN	Press [SPACE BAR] to select **Yes** to turn on the wireless LAN. The wireless LAN is off by default. Configure wireless LAN security features such as Mac filters and 802.1X before you turn on the wireless LAN (see *Chapter* 7).	**No** (default)
ESSID	(Extended Service Set IDentification) The ESSID identifies the Service Set the station is to connect to. Wireless clients associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless LAN.	Wireless

Table 6-6 Wireless LAN Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Hide ESSID	Press [SPACE BAR] to select **Yes** to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.	**No** (default)
Channel ID	This allows you to set the operating frequency/channel depending on your particular region. Use the [SPACE BAR] to select a channel. • CH01 2412 MHz / CH02 2417 MHz ~ CH11 2462 MHz (North America/FCC) • CH01 2412 MHz / CH02 2417 MHz ~ CH13 2472 MHz (Europe CE/ ETSI) • CH01 2412 MHz / CH02 2417 MHz ~ Ch14 2484 MHz (Japan) • CH10 2457 MHz / CH11 2462 MHz (Spain) • CH10 2457 MHz / CH11 2462 MHz ~ CH13 2472 MHz (France)	**CH01 2412 MHz**
RTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **0** and **2432**.	2432 (default)
Frag. Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **256** and **2432**.	2432 (default)
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.		

The ZyWALL LAN Ethernet and wireless ports can transparently communicate with each other (transparent bridge).

Chapter 7
Wireless LAN Security Setup

This chapter describes the types of security you can enable on the ZyWALL. Wireless LAN is available on the ZyWALL 10W and 100 models.

7.1 Levels of Security

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

The figure below shows the possible wireless security levels on your ZyWALL. The highest security level is EAP (Extensible Authentication Protocol) authentication. It requires interaction with a RADIUS (Remote Authentication Dial In User Service) server either on the WAN or your LAN to provide authentication service for wireless clients.

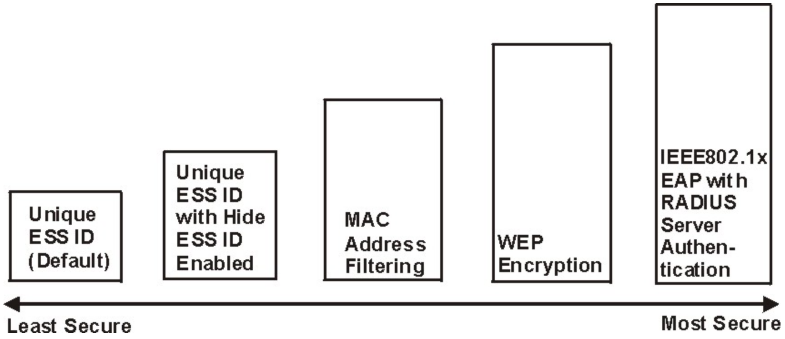

Unique ESS ID (Default)
Unique ESS ID with Hide ESS ID Enabled
MAC Address Filtering
WEP Encryption
IEEE802.1x EAP with RADIUS Server Authen-tication
Least Secure
Most Secure

Figure 7-1 ZyWALL Wireless Security Levels

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

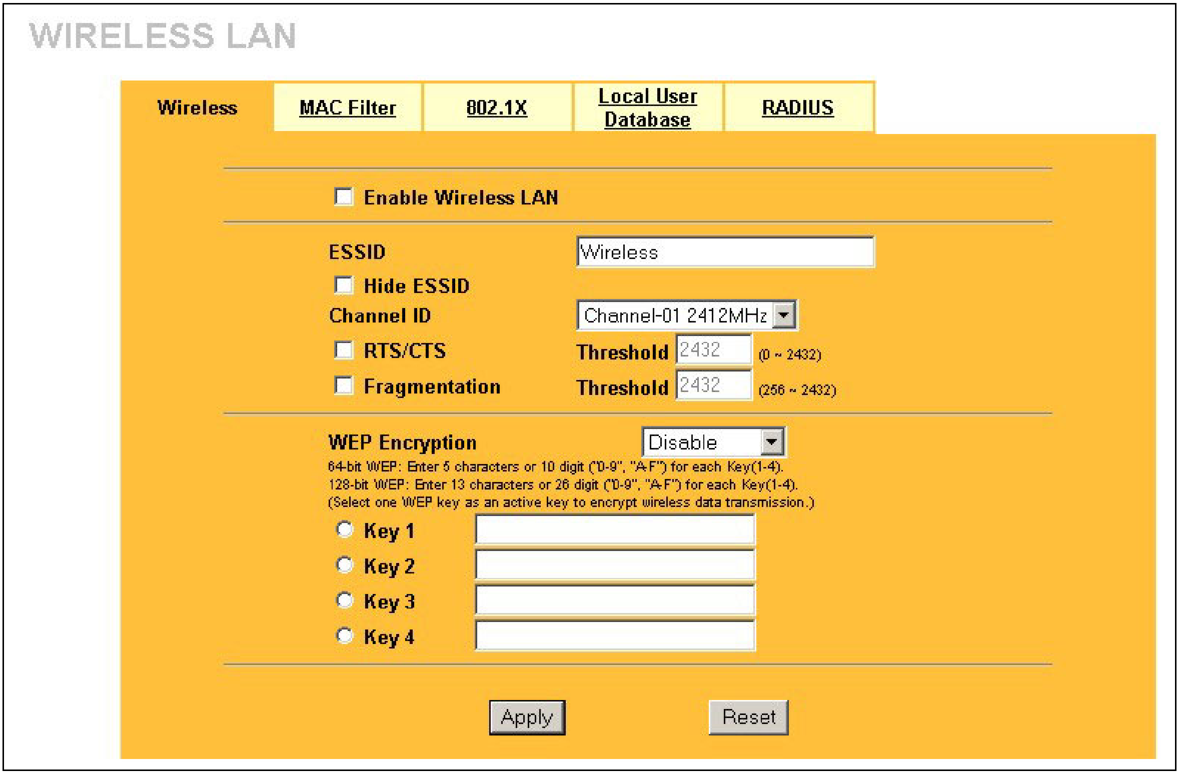
Use the ZyWALL web configurator to configurator to set up your wireless LAN security settings. Refer to the chapter on using the ZyWALL web configurator to see how to access the web configurator.

7.2 Data Encryption with WEP

WEP encryption scrambles the data transmitted between the wireless clients and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless clients and the access points must use the same WEP key for data encryption and decryption. For wireless LAN setup, refer to *section 6.6*.

Your ZyWALL allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; click **Advanced**, **Wireless** and the **Wireless** tab to the display the **Wireless LAN** screen.



WIRELESS LAN

□ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Channel ID: Channel-01 2412MHz

□ RTS/CTS Threshold 2432 (0 ~ 2432)

□ Fragmentation Threshold 2432 (256 ~ 2432)

WEP Encryption: Disable

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

○ Key 1

○ Key 2

○ Key 3

○ Key 4

Figure 7-2 Wireless LAN

The following table describes the WEP related fields in this screen. For wireless LAN field descriptions refer to *section 6.6*.

Table 7-1 Wireless LAN

FIELD	DESCRIPTION	EXAMPLE
Enable Wireless LAN	Before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN.	
WEP	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **Disable** to allow wireless clients to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.	**Disable**
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers.	
Click **Apply** to save your changes back to the ZyWALL. Click **Reset** to begin configuring this screen afresh.		

7.3 Network Authentication

You can set the ZyWALL and your network to authenticate a wireless client before the wireless client can communicate with the ZyWALL and the wired network to which the ZyWALL is connected.

7.3.1 EAP

EAP is an authentication protocol designed originally to run over PPP (Point-to-Point Protocol) frame in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless client and a RADIUS server to perform mutual authentication.

7.3.2 RADIUS

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

- **Authentication**

  Determines the identity of the users.

- **Authorization**

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

- **Accounting**

  Keeps track of the client's network activity.

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

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- **Access-Request**

  Sent by an access point requesting authentication.

- **Access-Reject**

  Sent by a RADIUS server rejecting access.

- **Access-Accept**

  Sent by a RADIUS server allowing access.

- **Access-Challenge**

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- **Accounting-Request**

  Sent by the access point requesting accounting.

- **Accounting-Response**

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

7.3.3 Sequence for EAP Authentication

The following figure shows the authentication steps when you enable EAP and specify a RADIUS server on your access point.

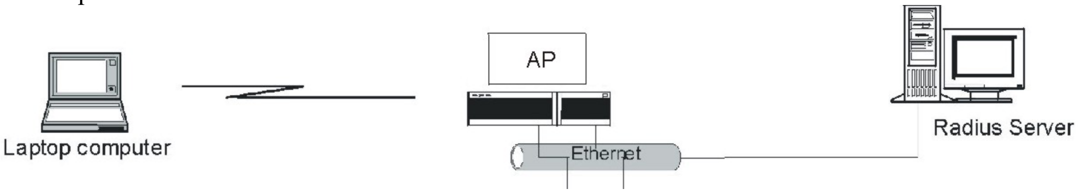


Figure 7-3 Sequence for EAP Authentication

The steps below describe how the IEEE 802.1x EAP authentication works.

Step 1. The wireless client sents a “request” message to the ZyWALL.

Step 2. The ZyWALL sends a “request” message to the wireless client for identity information.

Step 3. The wireless client replies with the password and username information.

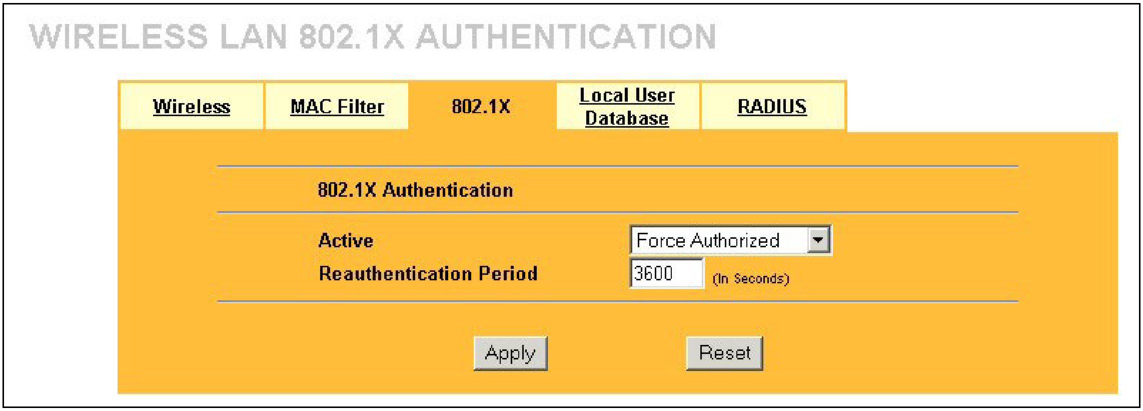
Step 4. The ZyWALL receives the message and repackets this information into an Access-Request package which is then sent to the remote RADIUS server (or the Authentication server).

Step 1. The RADIUS server checks the user information against its user profile database and sends an “accept” or a “deny” packet to the ZyWALL.

Step 2. When the ZyWALL receives the “accept” packet, the client port is placed into an authorized state and traffic is allowed to proceed. Otherwise, no traffic is allowed.

7.3.4 Enable EAP Authentication on Your ZyWALL

Click **Advanced**, **Wireless** and the **802.1X** tab to the display the **Wireless LAN 802.1X Authentication** screen.



WIRELESS LAN 802.1X AUTHENTICATION

802.1X Authentication

Active: Force Authorized

Reauthentication Period: 3600 (In Seconds)

Figure 7-4 Wireless LAN 802.1X Authentication

The following table describes the fields in this screen.

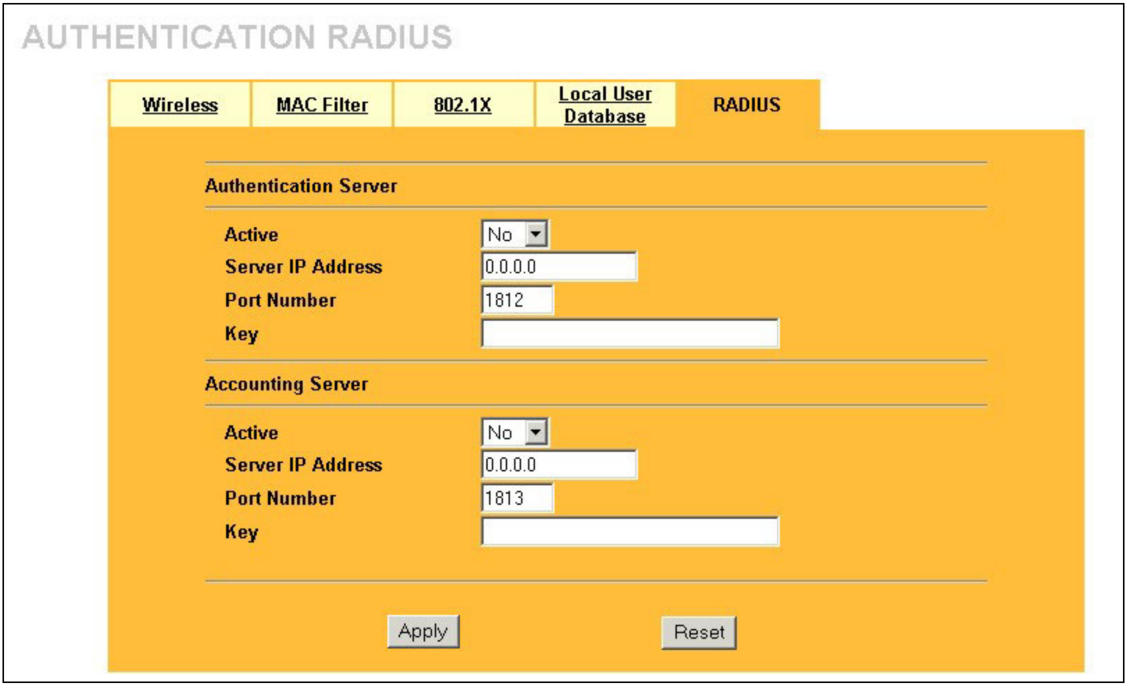
Table 7-2 Wireless LAN 802.1X Authentication

FIELD	DESCRIPTION
Authentication Control	Select **Force Authorized**, **Force UnAuthorized** or **Auto** from the drop-down list box. Select **Auto** to authenticate all wireless clients before they can access the wired network. Select **Force Authorized** to allow all wireless clients to access your wired network without authentication. Select **Force UnAuthorized** to deny all wireless clients access to your wired network.
Reauthentication Period	Specify the time interval between the RADIUS server's authentication checks of wireless users connected to the network. This field is activated only when you select **Auto** authentication control.
Click **Apply** to save these settings back to the ZyWALL. Click **Reset** to start this screen afresh.	

7.3.5 Configuring an External RADIUS Server

Once you enable the EAP authentication, you need to specify the external sever for remote user authentication and accounting.

Click **Advanced**, **Wireless** and the **RADIUS** tab to the display the **Authentication RADIUS** screen.



Authentication Server

Active: No
Server IP Address: 0.0.0.0
Port Number: 1812
Key:

Accounting Server

Active: No
Server IP Address: 0.0.0.0
Port Number: 1813
Key:

Figure 7-5 Authentication RADIUS

The following table describes the fields in this screen.

Table 7-3 Authentication RADIUS

FIELD	DESCRIPTION	EXAMPLE
Authentication Server		
Active	Select **Yes** from the drop-down list box to enable user authentication through an external authentication server. Select **No** to enable user authentication using the local user profile on the ZyWALL.	**No**
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.	10.11.12.13

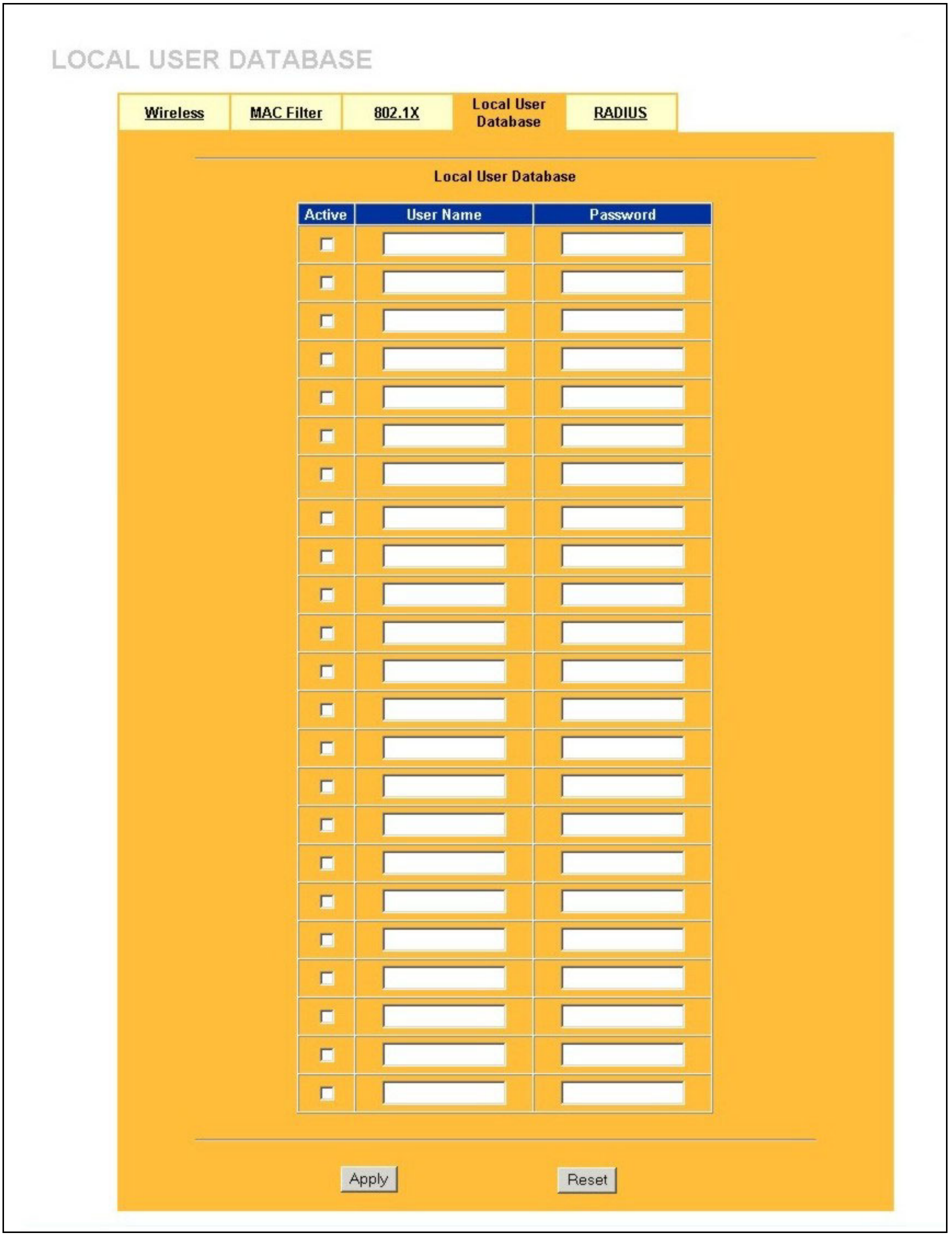
Table 7-3 Authentication RADIUS

FIELD	DESCRIPTION	EXAMPLE
Port Number	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.	**1812**
Key	Enter 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 ZyWALL.	
Accounting Server		
Active	Select **Yes** from the drop-down list box to enable user authentication through an external accounting server.	**No**
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.	10.11.12.13
Port Number	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.	**1813**
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and ZyWALL.	
Click **Apply** to save these settings back to the ZyWALL. Click **Reset** to start this screen afresh.		

7.4 Local User Authentication

By storing user profiles locally, your ZyWALL is able to authenticate wireless users without interacting with a network RADIUS server.

Click **Advanced**, **Wireless** and the **Local User Database** tab to the display the following screen (some of the screen's blank rows are not shown).



Local User Database

Active	User Name	Password
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		
□		

Figure 7-6 Local User Database

The following table describes the fields in this screen.

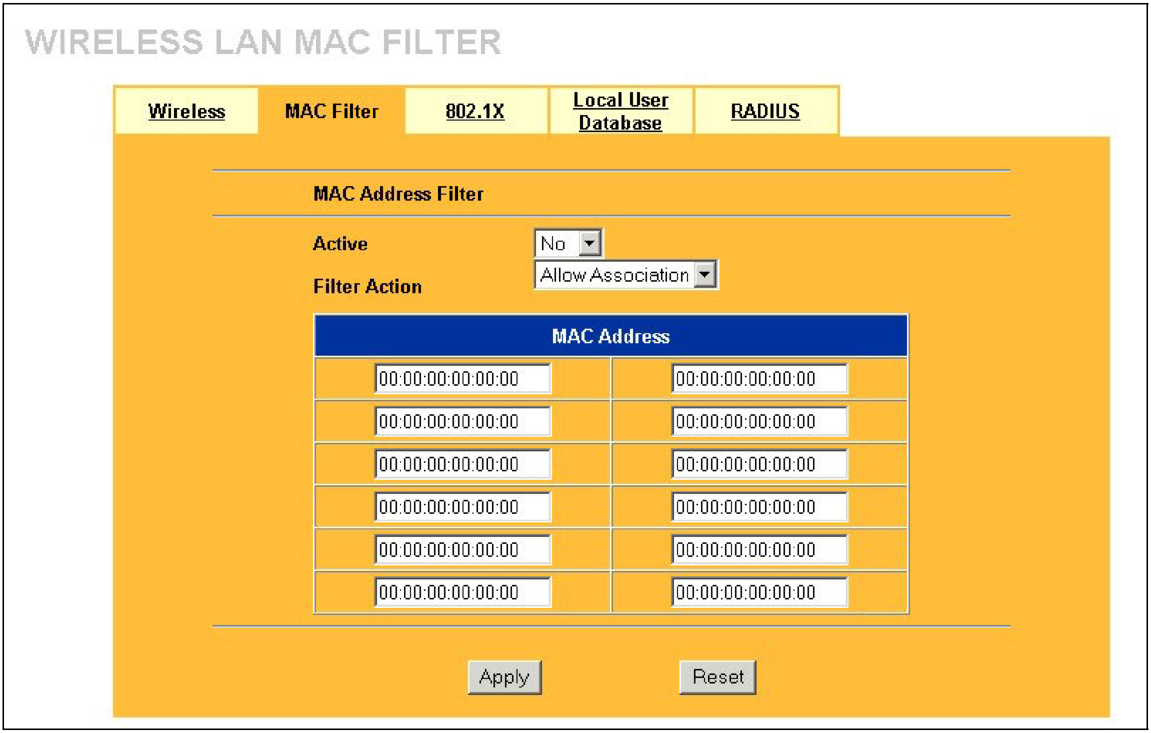
Table 7-4 Local User Database

FIELD	DESCRIPTION
Active	Select this check box to enable the user profile.
User Name	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Click **Apply** to save these settings back to the ZyWALL. Click **Reset** to start this screen afresh.	

7.5 MAC Address Filtering

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

Click **Advanced**, **Wireless** and the **MAC Filter** tab to the display the **Wireless LAN MAC Filter** screen.



WIRELESS LAN MAC FILTER

MAC Address Filter

Active: No

Filter Action: Allow Association

MAC Address	
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00

Figure 7-7 WLAN MAC Address Filter

The following table describes the fields in this menu.

Table 7-5 WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	Use the drop down list box to enable or disable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyWALL in these address fields.

Table 7-5 WLAN MAC Address Filter

FIELD	DESCRIPTION
Click **Apply** to save these settings back to the ZyWALL. Click **Reset** to start this screen afresh.	

Chapter 8 DMZ Setup

This chapter describes how to configure the ZyWALL 100's DMZ using ***Menu 5: DMZ Setup****.*

8.1 Introduction

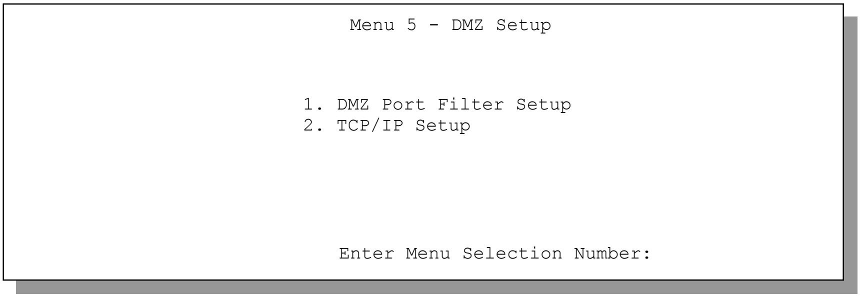
The DeMilitarized Zone (DMZ) auto-negotiating 10/100 Mbps Ethernet port provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

It is highly recommended that you connect all of your public servers to the DMZ port. If you have more than one public server, connect a hub to the DMZ port.

It is also highly recommended that you keep all sensitive information off of the public servers connected to the DMZ port. Store sensitive information on LAN computers.

From the main menu, enter 5 to open **Menu 5 – DMZ Setup**.

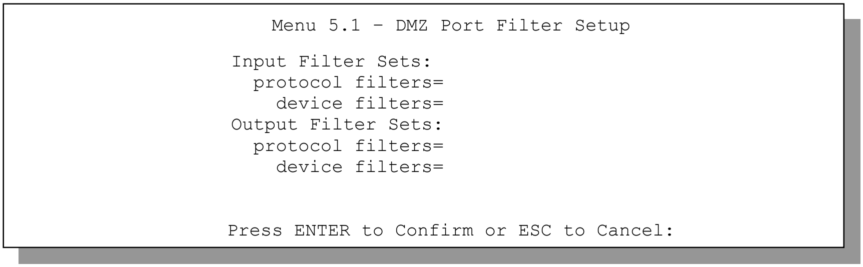


```
                        Menu 5 - DMZ Setup



                    1. DMZ Port Filter Setup
                    2. TCP/IP Setup






                      Enter Menu Selection Number:
```

Figure 8-1 Menu 5: DMZ Setup

8.2 DMZ Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to your public server(s) traffic. This feature is not available on all models.



```
                        Menu 5.1 - DMZ Port Filter Setup

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


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

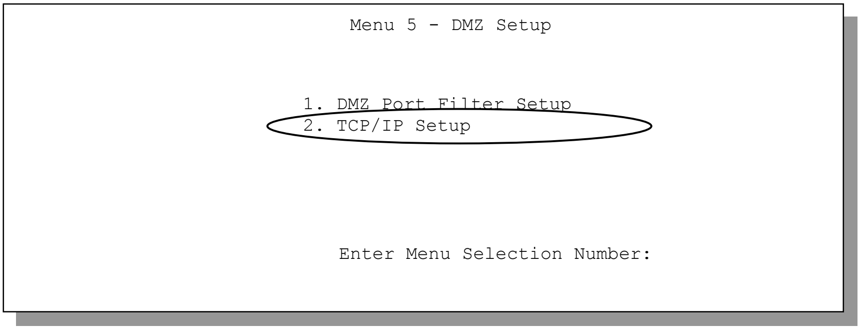
Figure 8-2 Menu 5.1: DMZ Port Filter Setup

8.3 TCP/IP Setup

8.3.1 IP Address

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to the LAN chapter.

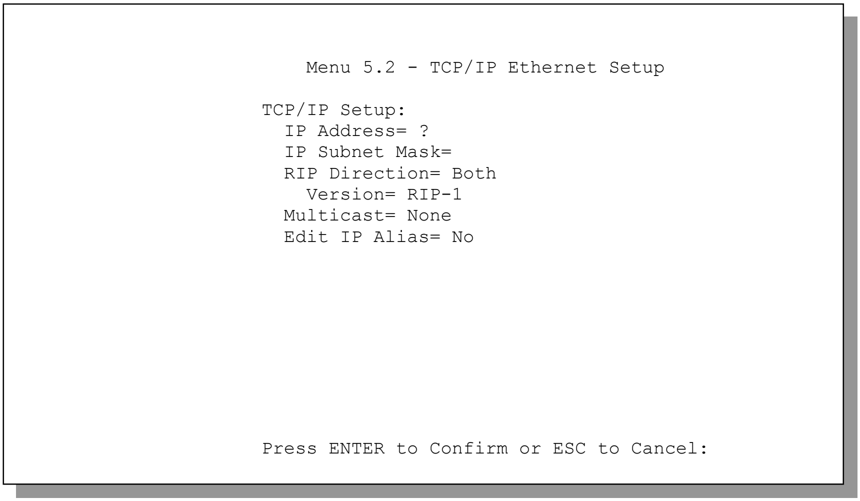
From the main menu, enter 5 to open **Menu 5 - DMZ Setup** to configure TCP/IP (RFC 1155).



```
                              Menu 5 - DMZ Setup


                         1. DMZ Port Filter Setup
                         2. TCP/IP Setup




                            Enter Menu Selection Number:
```

Figure 8-3 Menu 5: TCP/IP Setup

From menu 5, select the submenu option **2. TCP/IP Setup** and press [ENTER]. The screen now displays **Menu 5.2: TCP/IP Setup,** as shown next.



```
                    Menu 5.2 - TCP/IP Ethernet Setup

                TCP/IP Setup:
                  IP Address= ?
                  IP Subnet Mask=
                  RIP Direction= Both
                    Version= RIP-1
                  Multicast= None
                  Edit IP Alias= No










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

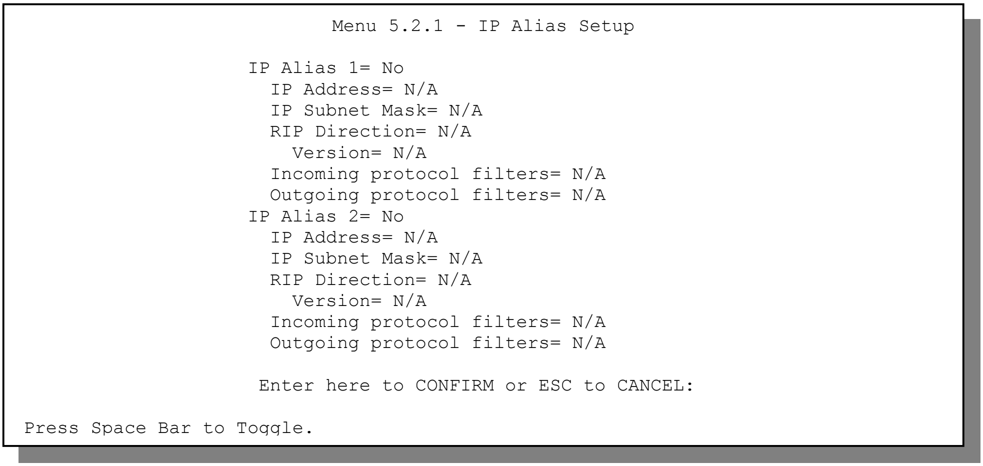
Figure 8-4 Menu 5.2: TCP/IP Setup

The TCP/IP setup fields are the same as the ones in **Menu 3.2 TCP/IP Ethernet Setup**. Each public server will need a unique IP address. Refer to *section 6.4* for information on how to configure these fields.

DMZ and LAN IP addresses must be on separate subnets.
You must also configure NAT for the DMZ port (see the *NAT* chapter) in menus 15.1 and 15.2.

8.3.2 IP Alias Setup

You must use menu 5.2 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. Pressing [ENTER] opens **Menu 5.2.1 - IP Alias Setup**, as shown next.



```
                             Menu 5.2.1 - IP Alias Setup

                      IP Alias 1= 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
                      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:

 Press Space Bar to Toggle.
```

Figure 8-5 Menu 5.2.1: IP Alias Setup

Refer to *Table 6-5* for instructions on configuring IP Alias parameters.

Chapter 9
Internet Access

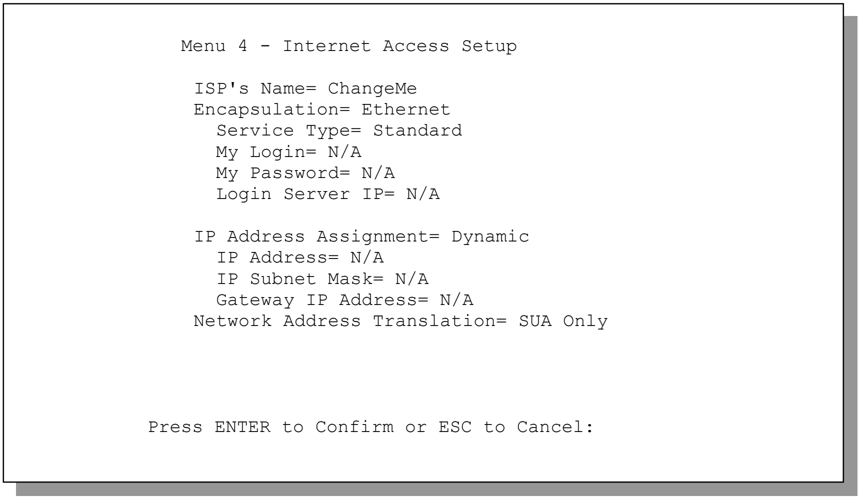
This chapter shows you how to configure your ZyWALL for Internet access.

9.1 Internet Access Setup

You will see three different menu 4 screens depending on whether you chose **Ethernet, PPTP** or **PPPoE Encapsulation**. Contact your ISP to determine what encapsulation type you should use.

9.1.1 Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next screen.



```
                Menu 4 - Internet Access Setup

                 ISP's Name= ChangeMe
                 Encapsulation= Ethernet
                   Service Type= Standard
                   My Login= N/A
                   My Password= N/A
                   Login Server IP= N/A

                 IP Address Assignment= Dynamic
                   IP Address= N/A
                   IP Subnet Mask= N/A
                   Gateway IP Address= N/A
                 Network Address Translation= SUA Only




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

Figure 9-1 Menu 4: Internet Access Setup (Ethernet)

The following table describes this screen.

Table 9-1 Menu 4: Internet Access Setup Menu Fields

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.

Table 9-1 Menu 4: Internet Access Setup Menu Fields

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for the **IP Address** field.
Service Type	Press [SPACE BAR] and then [ENTER] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method) or **RR-Telstra**. Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Note: DSL users must choose the **Standard** option only. The **My Login**, **My Password** and **Login Server** fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Login Server	The ZyWALL will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address Assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature. The choices are **Full Feature**, **None** or **SUA Only**.
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.	

9.1.2 PPTP Encapsulation

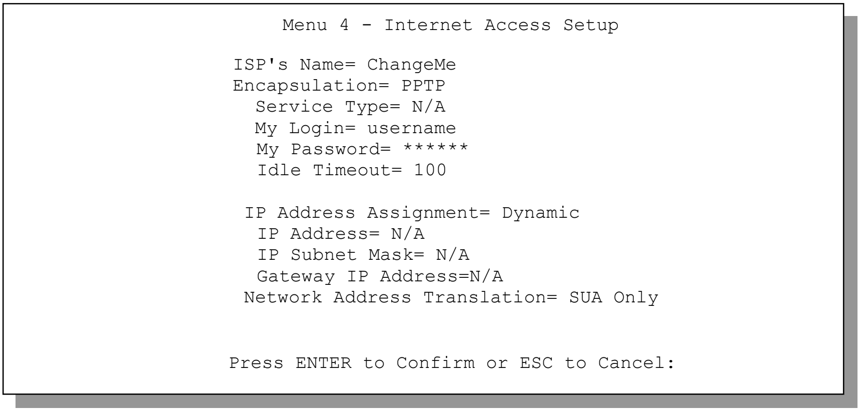
Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

The ZyWALL supports only one PPTP server connection at any given time.

9.1.3 Configuring the PPTP Client

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.



```
                    Menu 4 - Internet Access Setup

               ISP's Name= ChangeMe
               Encapsulation= PPTP
                 Service Type= N/A
                 My Login= username
                 My Password= ******
                 Idle Timeout= 100

                IP Address Assignment= Dynamic
                 IP Address= N/A
                 IP Subnet Mask= N/A
                 Gateway IP Address=N/A
                Network Address Translation= SUA Only


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

Figure 9-2 Internet Access Setup (PPTP)

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

Table 9-2 New Fields in Menu 4 (PPTP) Screen

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPTP**. The encapsulation method influences your choices for the **IP Address** field.	**PPTP**
Idle Timeout	This value specifies the time, in seconds, that elapses before the ZyWALL automatically disconnects from the PPTP server.	100 (default)

9.1.4 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

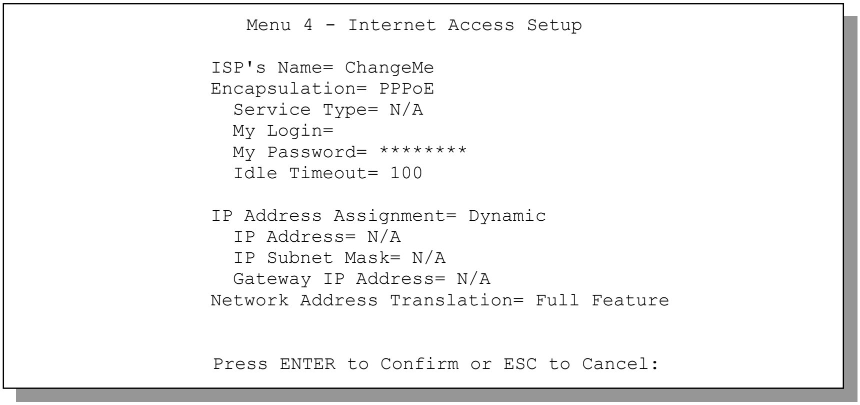
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyWALL (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyWALL does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see the *Appendices*.



```
                     Menu 4 - Internet Access Setup

                  ISP's Name= ChangeMe
                  Encapsulation= PPPoE
                    Service Type= N/A
                    My Login=
                    My Password= ********
                    Idle Timeout= 100

                  IP Address Assignment= Dynamic
                    IP Address= N/A
                    IP Subnet Mask= N/A
                    Gateway IP Address= N/A
                  Network Address Translation= Full Feature


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

Figure 9-3 Internet Access Setup (PPPoE)

Table 9-3 New Fields in Menu 4 (PPPoE) screen

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices in the **IP Address** field.	**PPPoE**
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server.	100 (default)

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

9.2 Basic Setup Complete

Well done! You have successfully connected, installed and set up your ZyWALL to operate on your network as well as access the Internet.

When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

You may deactivate the firewall in menu 21.2 or via the ZyWALL embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the *firewall chapters* for more information on the firewall.

Part III:

Advanced Applications

This part covers Remote Node Setup, IP Static Route Setup and Network Address Translation.

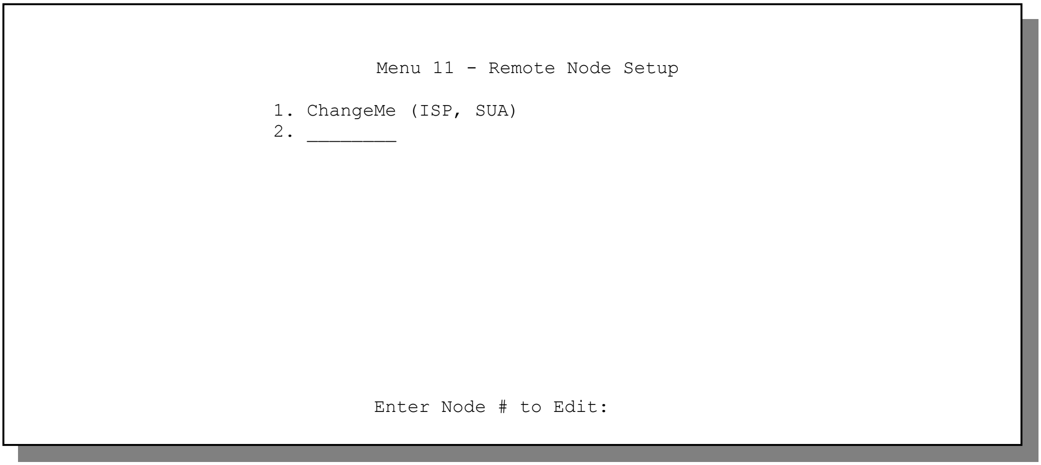
Chapter 10
Remote Node Setup

This chapter shows you how to configure a remote node.

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 a remote node. The following describes how to configure **Menu 11.1 Remote Node Profile, Menu 11.3 - Remote Node Network Layer Options** and **Menu 11.5 - Remote Node Filter**.

10.1 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Setup** (shown below). Then enter **1** to open **Menu 11.1 Remote Node Profile** and configure the setup for your regular ISP. Enter **2** to open **Menu 11.1 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection (see the Backup Remote Node Setup chapter).



```
                    Menu 11 - Remote Node Setup

               1. ChangeMe (ISP, SUA)
               2. ________















                    Enter Node # to Edit:
```

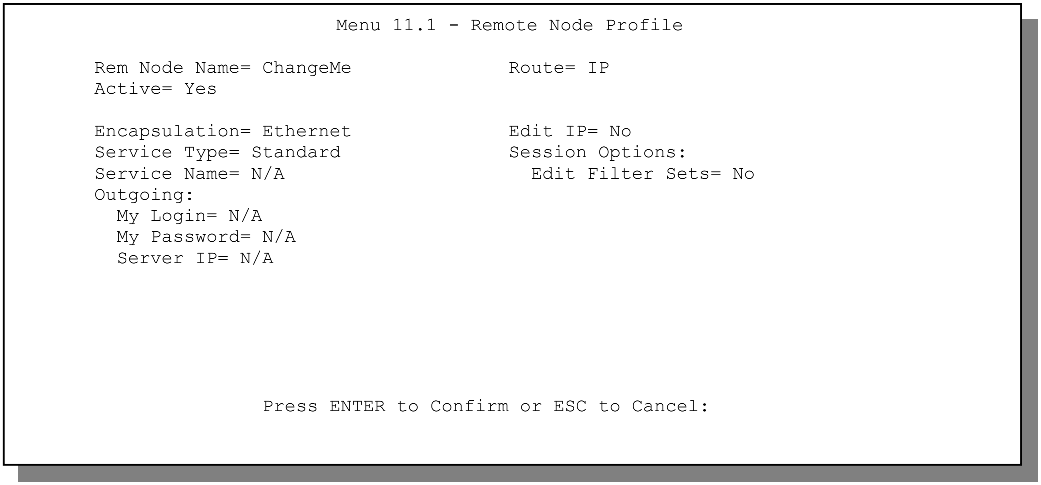
Figure 10-1 Menu 11 Remote Node Setup

10.2 Remote Node Profile

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

10.2.1 Ethernet Encapsulation

There are two variations of menu 11.1 depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation.** You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.



```
                         Menu 11.1 - Remote Node Profile

       Rem Node Name= ChangeMe              Route= IP
       Active= Yes

       Encapsulation= Ethernet              Edit IP= No
       Service Type= Standard               Session Options:
       Service Name= N/A                      Edit Filter Sets= No
       Outgoing:
         My Login= N/A
         My Password= N/A
         Server IP= N/A





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

Figure 10-2 Menu 11.1: Remote Node Profile for Ethernet Encapsulation

Table 10-1 Fields in Menu 11.1

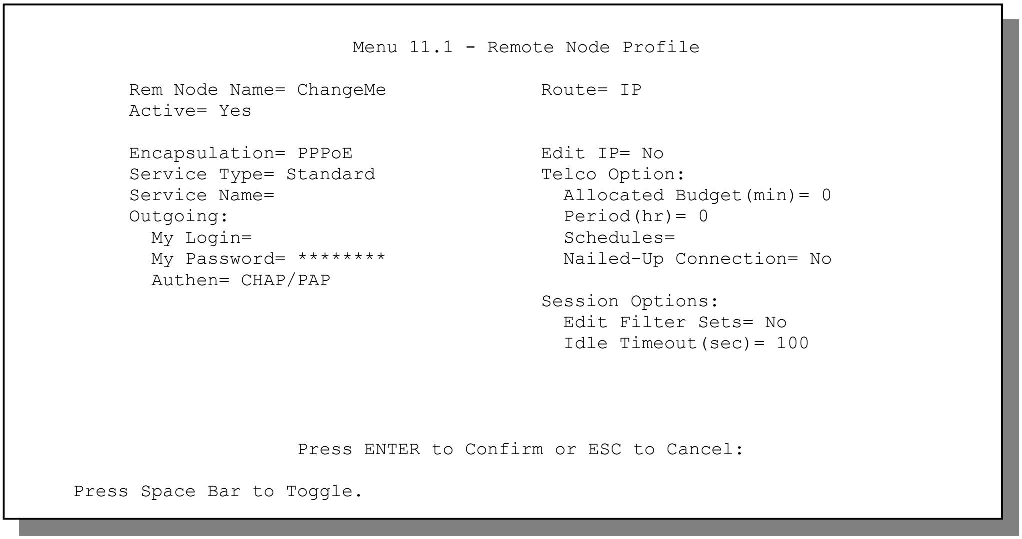
FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node).	**Yes**
Encapsulation	**Ethernet** is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to **PPPoE** or **PPTP** encapsulation.	**Ethernet**

Table 10-1 Fields in Menu 11.1

FIELD	DESCRIPTION	EXAMPLE
Service Type	Press [SPACE BAR] and then [ENTER] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method) or **RR-Manager** (RoadRunner Manager authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.	**Standard**
Service Name	If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation.	poellc
Outgoing My Login	This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the ZyWALL calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server.	jim
My Password	Enter the password assigned by your ISP when the ZyWALL calls this remote node. Valid for **PPPoE** encapsulation only.	*****
Server IP	This field is valid only when **RoadRunner** is selected in the **Service Type** field. The ZyWALL will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.	
Route	This field refers to the protocol that will be routed by your ZyWALL – IP is the only option for the ZyWALL 100.	**IP**
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.3 - Remote Node Network Layer Options**.	**No** (default)
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.	**No** (default)
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.		

10.2.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the ZyWALL with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE,** then you will see the next screen. Please see the *Appendices* for more information on PPPoE.



```
                          Menu 11.1 - Remote Node Profile

      Rem Node Name= ChangeMe              Route= IP
      Active= Yes

      Encapsulation= PPPoE                 Edit IP= No
      Service Type= Standard               Telco Option:
      Service Name=                          Allocated Budget(min)= 0
      Outgoing:                              Period(hr)= 0
        My Login=                            Schedules=
        My Password= ********                Nailed-Up Connection= No
        Authen= CHAP/PAP
                                           Session Options:
                                             Edit Filter Sets= No
                                             Idle Timeout(sec)= 100



                     Press ENTER to Confirm or ESC to Cancel:

 Press Space Bar to Toggle.
```

Figure 10-3 Menu 11.1: Remote Node Profile for PPPoE Encapsulation

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.

Nailed-Up Connection

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

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

The following table describes the fields not already described in *Table 10-1*.

Metric

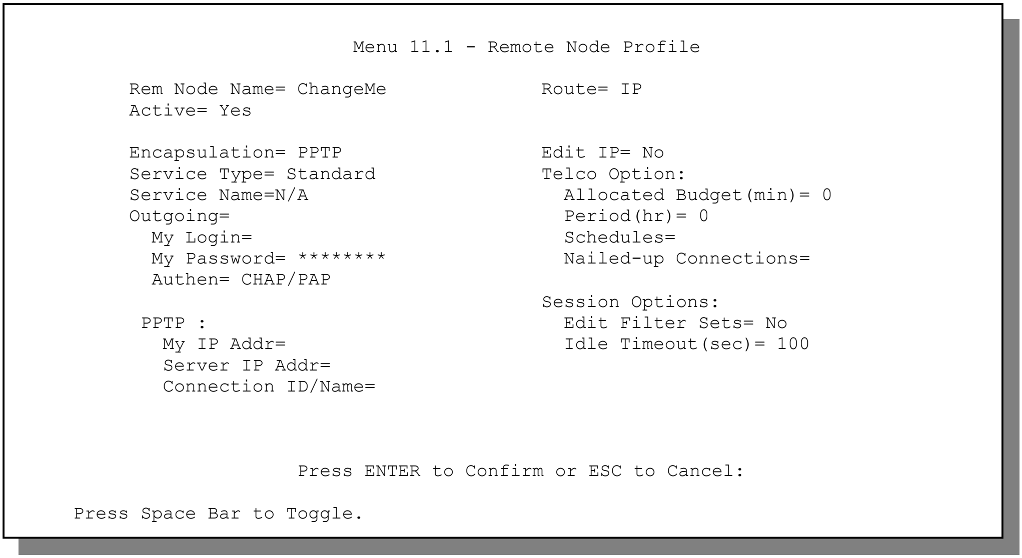
See the *Metric* section in the *WAN and Dial Backup Setup* chapter for details on the **Metric** field.

Table 10-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION	EXAMPLE
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	**CHAP/PAP**
Telco Option Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period(hr)** is 1 (hour).	0 (default)
Schedules	You can apply up to four schedule sets here. For more details please refer to the *Call Schedule Setup* chapter.	
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	**No** (default)
Session Options Idle Timeout	Type the length of idle time (when there is no traffic from the ZyWALL to the remote node) in seconds that can elapse before the ZyWALL automatically disconnects the PPPoE connection. This option only applies when the ZyWALL initiates the call.	100 seconds (default)

10.2.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see the *appendices* for information on PPTP.



```
                       Menu 11.1 - Remote Node Profile

          Rem Node Name= ChangeMe              Route= IP
          Active= Yes

          Encapsulation= PPTP                  Edit IP= No
          Service Type= Standard               Telco Option:
          Service Name=N/A                       Allocated Budget(min)= 0
          Outgoing=                              Period(hr)= 0
            My Login=                            Schedules=
            My Password= ********                Nailed-up Connections=
            Authen= CHAP/PAP
                                               Session Options:
           PPTP :                                Edit Filter Sets= No
             My IP Addr=                         Idle Timeout(sec)= 100
             Server IP Addr=
             Connection ID/Name=



                    Press ENTER to Confirm or ESC to Cancel:

     Press Space Bar to Toggle.
```

Figure 10-4 Menu 11.1: Remote Node Profile for PPTP Encapsulation

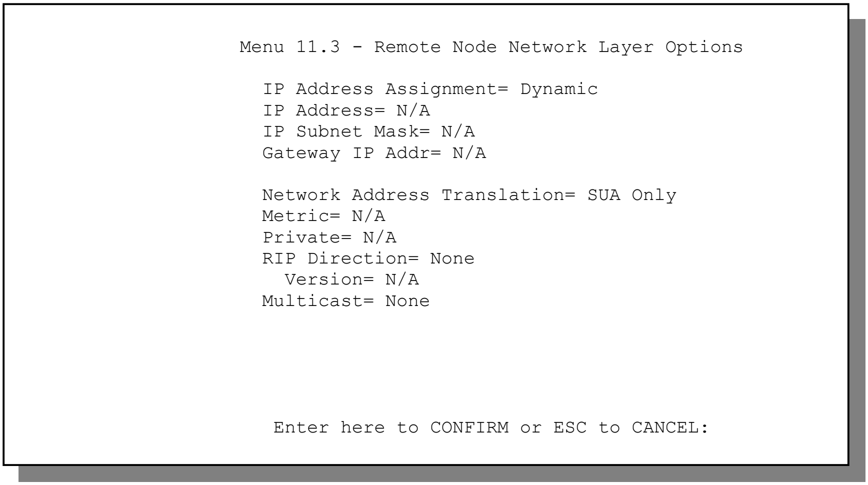
The next table shows how to configure fields in menu 11.1 not previously discussed above.

Table 10-3 Fields in Menu 11.1 (PPTP Encapsulation)

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **PPTP**. You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.	**PPTP**
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
My Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/Name	Enter the connection ID or connection name in the ANT. It must follow the “c:id” and “n:name” format. This field is optional and depends on the requirements of your DSL modem.	N:My ISP
Schedules	You can apply up to four schedule sets here. For more details refer to the *Call Schedule Setup* chapter.	
Nailed-Up Connections	Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to make the connection to this remote node a nailed-up connection.	**No**

10.3 Editing TCP/IP Options (with Ethernet Encapsulation)

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**.



```
                    Menu 11.3 - Remote Node Network Layer Options

                      IP Address Assignment= Dynamic
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      Gateway IP Addr= N/A

                      Network Address Translation= SUA Only
                      Metric= N/A
                      Private= N/A
                      RIP Direction= None
                        Version= N/A
                      Multicast= None





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

Figure 10-5 Menu 11.3: Remote Node Network Layer Options for Ethernet Encapsulation

The next table gives you instructions about configuring remote node network layer options.

Table 10-4 Remote Node Network Layer Options Menu Fields

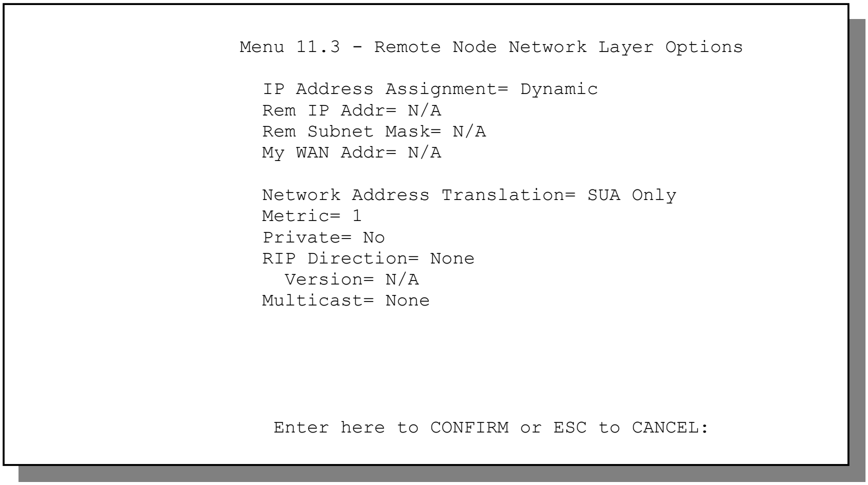
FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.	**Dynamic** (default)
IP Address	If you have a Static IP Assignment, enter the IP address assigned to you by your ISP.	
IP Subnet Mask	If you have a Static IP Assignment, enter the subnet mask assigned to you.	
Gateway IP Addr	If you have a Static IP Assignment, enter the gateway IP address assigned to you.	
Network Address Translation	Press [SPACE BAR] and then [ENTER] to select either **Full Feature**, **None** or **SUA Only**. See the *NAT chapter* for a full discussion on this feature.	**SUA Only** (default)

Table 10-4 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the *Metric* section in the *WAN and Dial Backup Setup* chapter) The smaller the number, the higher priority the route has.	1
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the ZyWALL 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.	**No**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. See the *LAN Setup* chapter for more information on RIP. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting.	**None** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/**RIP-2M** or **None**.	N/A
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2)**. Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See the *LAN Setup* chapter for more information on this feature.	**None** (default)
Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

10.3.1 Editing TCP/IP Options (with PPTP Encapsulation)

Make sure that **Encapsulation** is set to **PPTP** in menu 11.1. Then move the cursor to the **Edit IP** field in menu 11.1, press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**.



```
                    Menu 11.3 - Remote Node Network Layer Options

                      IP Address Assignment= Dynamic
                      Rem IP Addr= N/A
                      Rem Subnet Mask= N/A
                      My WAN Addr= N/A

                      Network Address Translation= SUA Only
                      Metric= 1
                      Private= No
                      RIP Direction= None
                        Version= N/A
                      Multicast= None




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

Figure 10-6 Menu 11.3: Remote Node Network Layer Options for PPTP Encapsulation

The next table gives you instructions about configuring remote node network layer options.

Table 10-5 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.	**Dynamic** (default)
Rem IP Address	If you have a **Static IP Assignment**, enter the IP address assigned to the remote node.	192.168.1.1
Rem IP Subnet Mask	If you have a **Static IP Assignment**, enter the subnet mask assigned to the remote node.	255.255.255.0

Table 10-5 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
My WAN 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 ZyWALL. Note that this is the address assigned to your local ZyWALL, not the remote router.	0.0.0.0
Network Address Translation	Press [SPACE BAR] and then [ENTER] to select either **Full Feature, None** or **SUA Only.** See the NAT chapter for a full discussion on this feature.	**SUA Only**
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the *Metric* section in the *WAN and Dial Backup Setup* chapter). The smaller the number, the higher priority the route has.	**1** (default)
Private	This parameter determines if the ZyWALL 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.	**No** (default)
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the **RIP direction** from **Both/ None**/**In Only**/**Out Only** and **None**.	**None** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1**
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See the LAN Setup chapter for more information on this feature.	**None**
Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

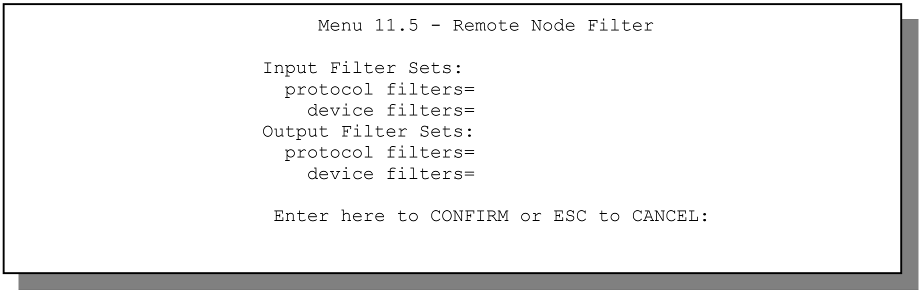
10.3.2 Editing TCP/IP Options (with PPPoE Encapsulation)

Make sure **Encapsulation** is set to **PPPoE** in menu 11.1. Move the cursor to the **Edit IP** field in **Menu 11.1** and press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**. The menu and fields are the same as described for PPTP encapsulation above.

10.4 Remote Node Filter

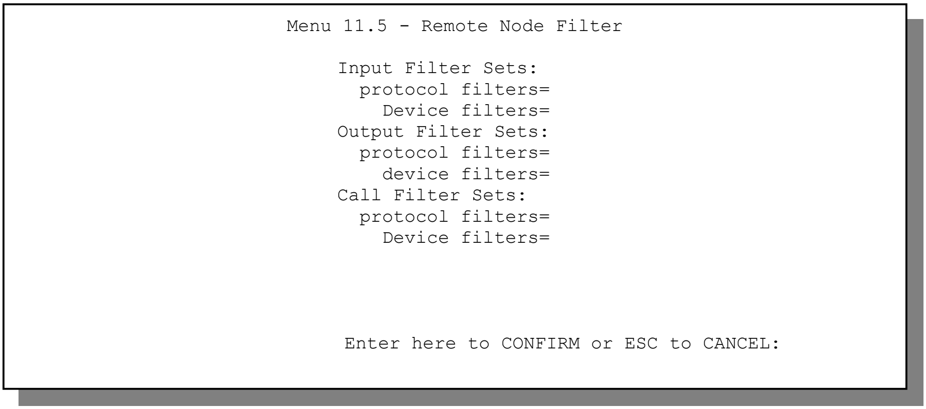
Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL 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.



```
                    Menu 11.5 - Remote Node Filter

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

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

Figure 10-7 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)



```
                    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:
```

Figure 10-8 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)

10.5 Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the ZyWALL cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyWALL still provides firewall protection. This feature is not available on all models.

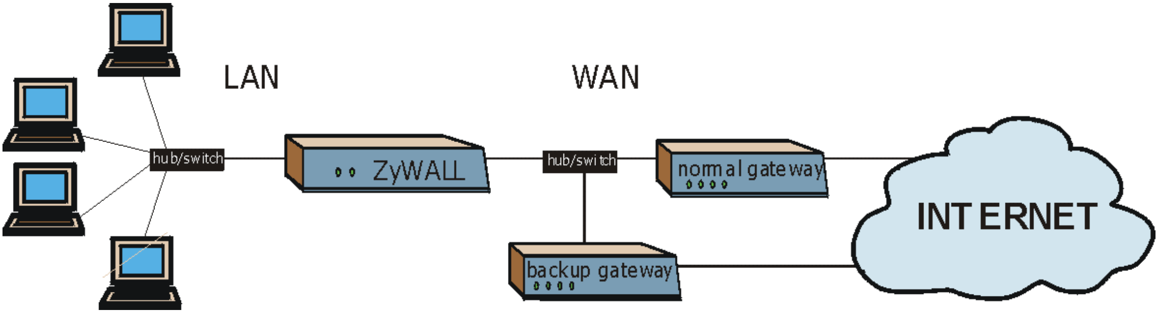


Figure 10-9 Traffic Redirect WAN Setup

The following network topology allows you to avoid triangle route security issues (see appendices) when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the ZyWALL itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/ZyWALL firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

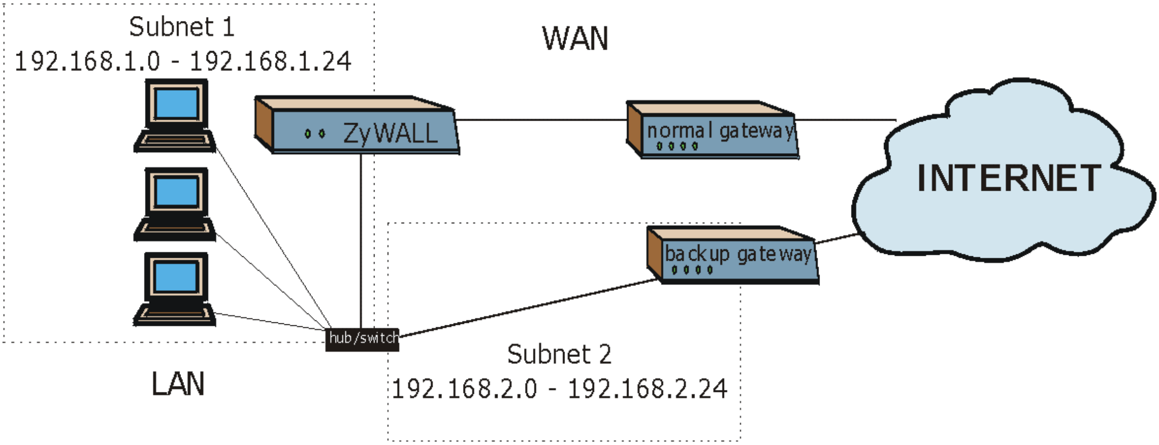
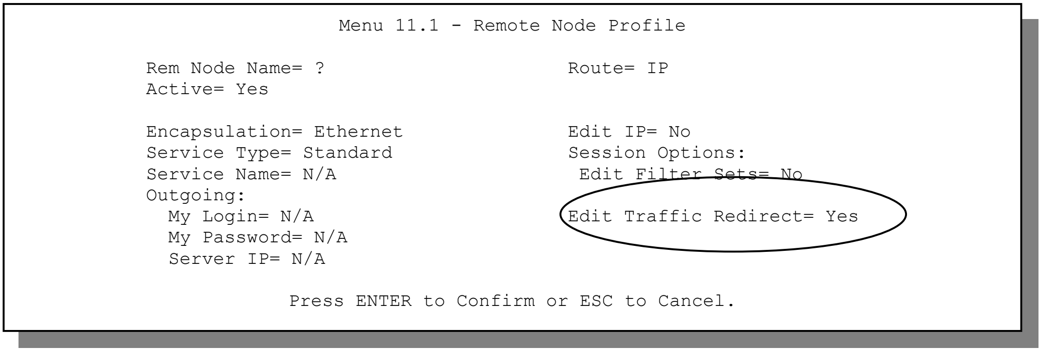


Figure 10-10 Traffic Redirect LAN Setup

To configure the parameters for traffic redirect, enter 11 from the main menu to display **Menu 11.1—Remote Node Profile** as shown next.



```
                             Menu 11.1 - Remote Node Profile

            Rem Node Name= ?                      Route= IP
            Active= Yes

            Encapsulation= Ethernet               Edit IP= No
            Service Type= Standard                Session Options:
            Service Name= N/A                      Edit Filter Sets= No
            Outgoing:
              My Login= N/A                       Edit Traffic Redirect= Yes
              My Password= N/A
              Server IP= N/A

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

Figure 10-11 Menu 11.1: Remote Node Profile

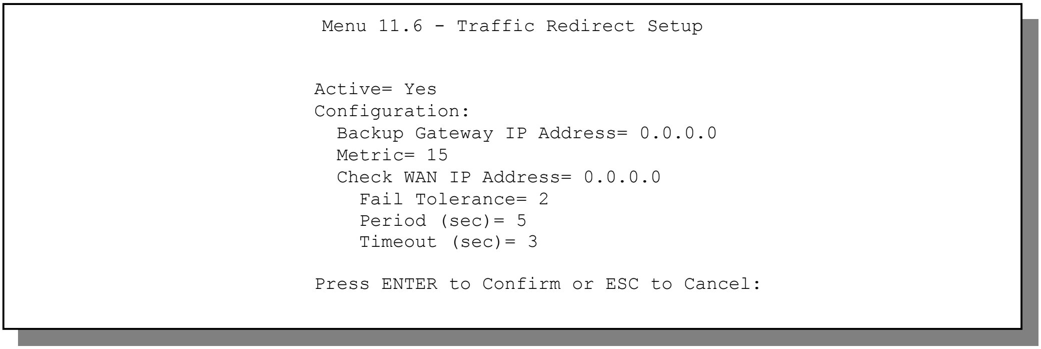
To configure traffic redirect properties, press [SPACE BAR] to select **Yes** in the **Edit Traffic Redirect** field and then press [ENTER].

Table 10-6 Menu 11.1: Remote Node Profile (Traffic Redirect Field)

FIELD	DESCRIPTION	EXAMPLE
Edit Traffic Redirect	Press [SPACE BAR] to select **Yes** or **No**. Select **No** (default) if you do not want to configure this feature. Select **Yes** and press [ENTER] to configure **Menu 11.6 — Traffic Redirect Setup**.	**Yes**
Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

10.5.1 Traffic Redirect Setup

Configure parameters that determine when the ZyWALL will forward WAN traffic to the backup gateway using **Menu 11.6 — Traffic Redirect Setup**.



```
                    Menu 11.6 - Traffic Redirect Setup


                   Active= Yes
                   Configuration:
                     Backup Gateway IP Address= 0.0.0.0
                     Metric= 15
                     Check WAN IP Address= 0.0.0.0
                       Fail Tolerance= 2
                       Period (sec)= 5
                       Timeout (sec)= 3

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

Figure 10-12 Menu 11.6: Traffic Redirect Setup

Table 10-7 Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup. The default is **No**. When the **Active** field is **Yes**, you must configure every field in this screen unless you are using PPPoE or PPTP encapsulation (except **Check WAN IP Address** and **Timeout**). If you don’t configure these fields and are using PPTP or PPPoE encapsulation, then the ZyWALL checks the PPPoE channel or PPTP tunnel to determine if the WAN connection is down.	**Yes**

Table 10-7 Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
Configuration:		
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates.	0.0.0.0
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the *Metric* section in the *WAN and Dial Backup Setup* chapter) The smaller the number, the higher priority the route has.	15 (default)
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your ZyWALL's WAN accessibility. The ZyWALL uses the default gateway IP address if you do not enter an IP address here. If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the ZyWALL to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.	0.0.0.0
Fail Tolerance	Enter the number of times your ZyWALL may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number.	2
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.	5
Timeout (sec)	Enter the number of seconds the ZyWALL waits for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The number in this field should be less than the number in the **Period** field. Three to 50 is usually a good number. The WAN connection is considered "down" after the ZyWALL times out the number of times specified in the **Fail Tolerance** field.	3
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 11
IP Static Route Setup

This chapter shows you how to configure static routes with your ZyWALL*.*

Static routes tell the ZyWALL routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN.

Each remote node specifies only the network to which the gateway is directly connected, and the ZyWALL has no knowledge of the networks beyond. For instance, the ZyWALL knows about network N2 in the following diagram through remote node Router 1. However, the ZyWALL 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 ZyWALL about the networks beyond the remote nodes.

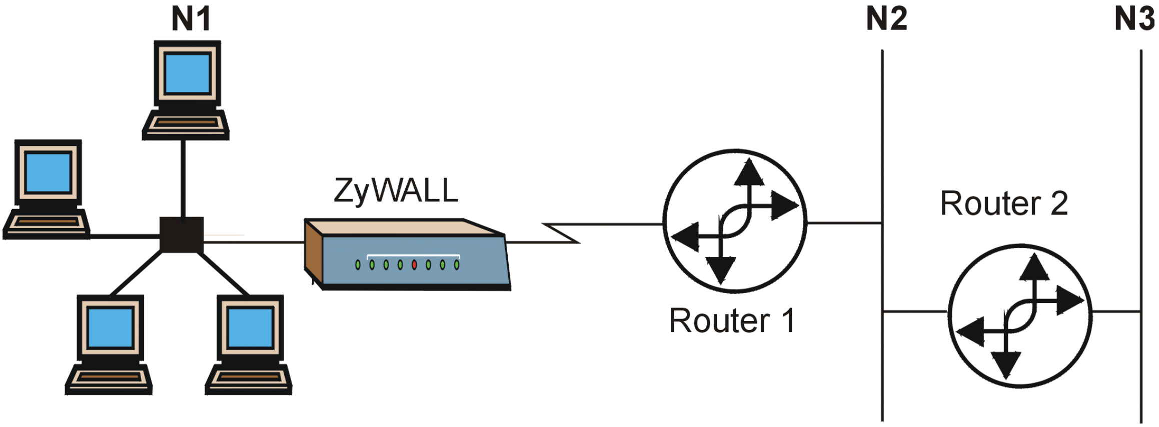
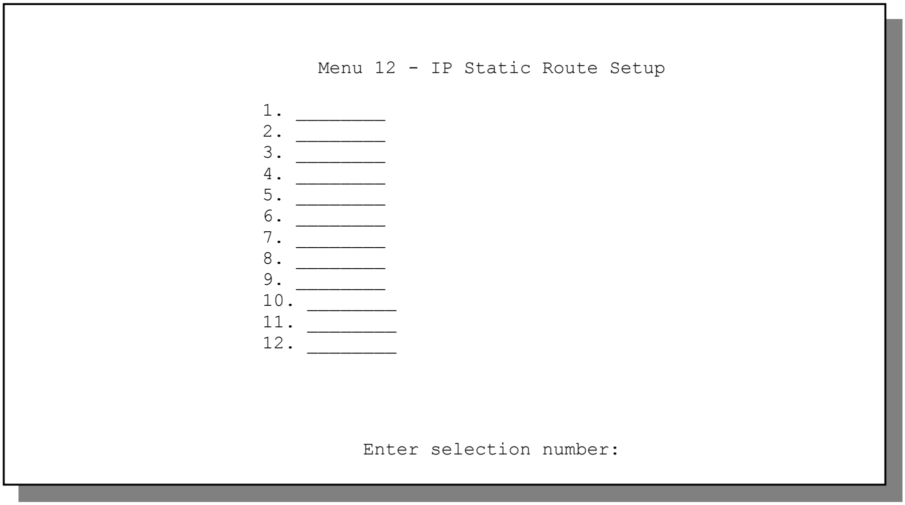


Figure 11-1 Example of Static Routing Topology

11.1 IP Static Route Setup

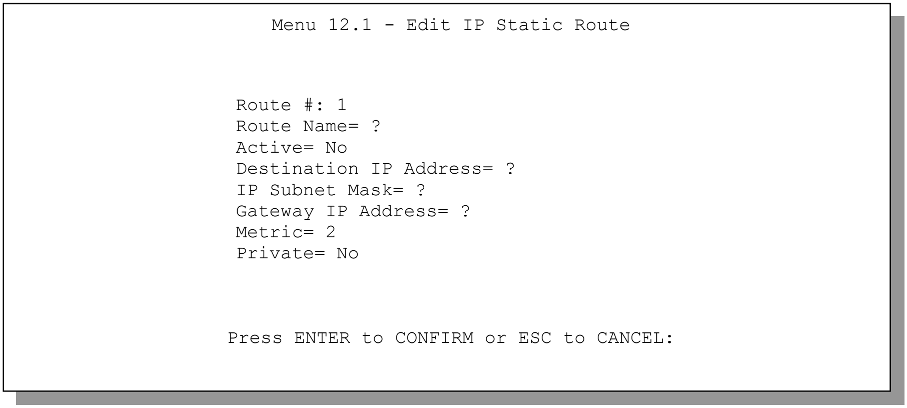
Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12. 1.



```
                    Menu 12 - IP Static Route Setup

               1. ________
               2. ________
               3. ________
               4. ________
               5. ________
               6. ________
               7. ________
               8. ________
               9. ________
               10. ________
               11. ________
               12. ________



                        Enter selection number:
```

Figure 11-2 Menu 12: IP Static Route Setup (ZyWALL 10W)

Now, enter the index number of the static route that you want to configure.



```
                         Menu 12.1 - Edit IP Static Route



                     Route #: 1
                     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:
```

Figure 11-3 Menu 12. 1: Edit IP Static Route

`The following table describes the IP Static Route Menu fields.

Table 11-1 IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes 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	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the *Metric* section in the *WAN and Dial Backup Setup* chapter). The smaller the number, the higher priority the route has.

Table 11-1 IP Static Route Menu Fields

FIELD	DESCRIPTION
Private	This parameter determines if the ZyWALL 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.
Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.	

Chapter 12
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

12.1 Introduction

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 is changed to a different IP address known within another network.

12.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyWALL. 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 12-1 NAT Definitions

TERM	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.**

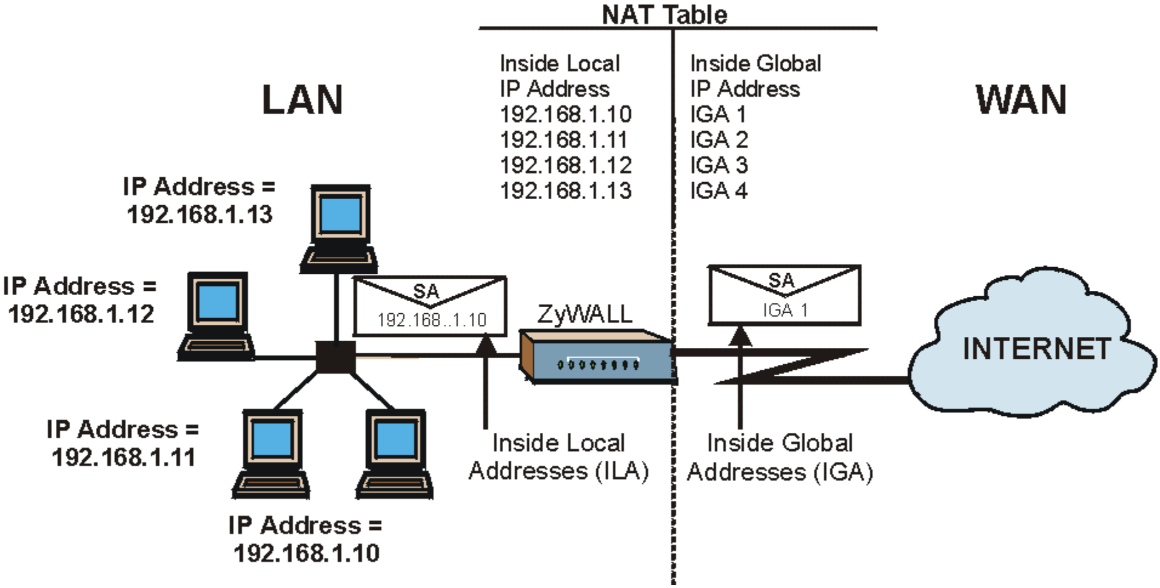
12.1.2 What NAT Does

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. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 12-2*), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyWALL 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)*.

12.1.3 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 ZyWALL keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.



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

LAN
WAN
IP Address = 192.168.1.13
IP Address = 192.168.1.12
IP Address = 192.168.1.11
IP Address = 192.168.1.10
SA
192.168..1.10
ZyWALL
SA
IGA 1
INTERNET
Inside Local Addresses (ILA)
Inside Global Addresses (IGA)

Figure 12-1 How NAT Works

12.1.4 NAT Application

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

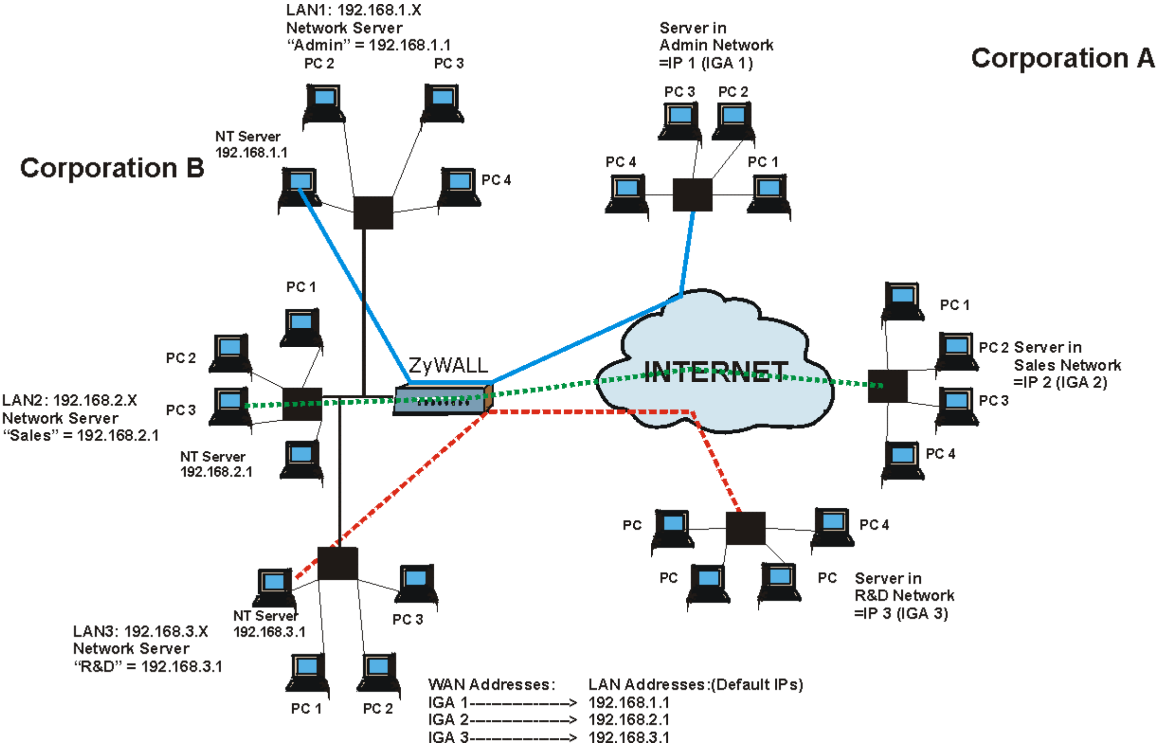


Figure 12-2 NAT Application With IP Alias

12.1.5 NAT Mapping Types

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

1. **One to One**: In One-to-One mode, the ZyWALL maps one local IP address to one global IP address.

2. **Many to One**: In Many-to-One mode, the ZyWALL 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 (the SUA Only option).
3. **Many to Many Overload**: In Many-to-Many Overload mode, the ZyWALL maps the multiple local IP addresses to shared global IP addresses.
4. **Many One to One**: In Many-One-to-One mode, the ZyWALL maps each local IP address to a unique global IP address.
5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

Port numbers do not **change for** One-to-One **and** Many-One-to-One **NAT mapping types.**

The following table summarizes these types.

Table 12-2 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

Table 12-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION

Many-One-to-One	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA3
	…
		M-1-1

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

12.2 Using NAT

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

12.2.1 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 12.3.1* for a detailed description of the NAT set for SUA. The ZyWALL 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 12-2*.

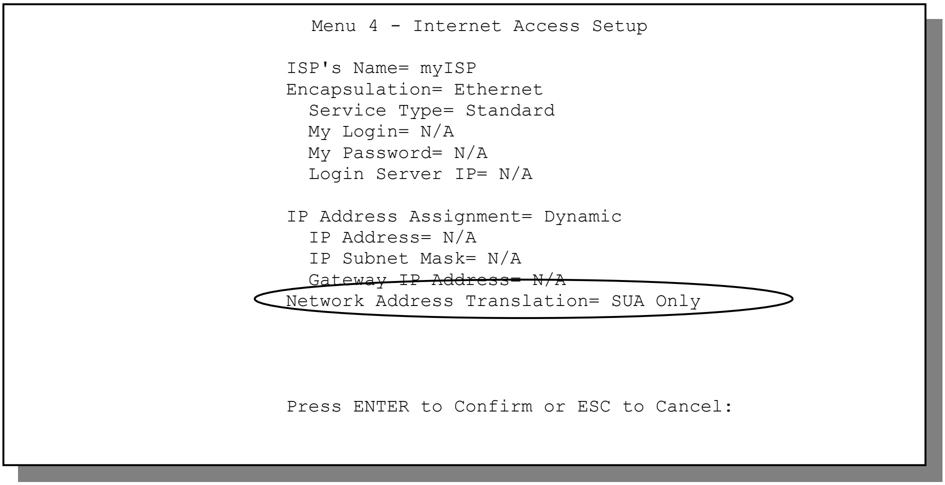
1. **Choose** SUA Only **if you have just one public WAN IP address for your ZyWALL.**

2. **Choose** Full Feature **if you have multiple public WAN IP addresses for your ZyWALL.**

12.2.2 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**

.



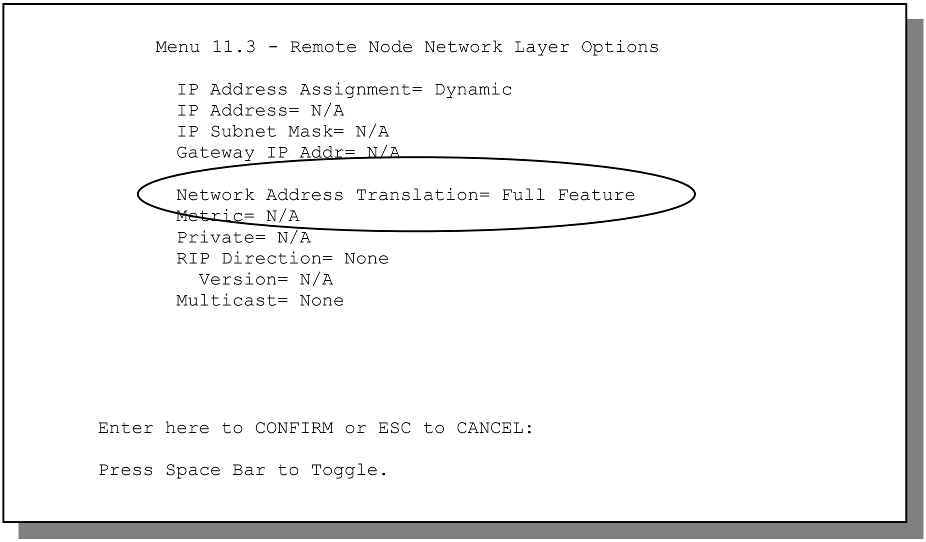
```
                    Menu 4 - Internet Access Setup

                  ISP's Name= myISP
                  Encapsulation= Ethernet
                    Service Type= Standard
                    My Login= N/A
                    My Password= N/A
                    Login Server IP= N/A

                  IP Address Assignment= Dynamic
                    IP Address= N/A
                    IP Subnet Mask= N/A
                    Gateway IP Address= N/A
                  Network Address Translation= SUA Only



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

Figure 12-3 Menu 4: Applying NAT for Internet Access

The following figure shows how you apply NAT to the remote node in menu 11.1.

Step 1. Enter 11 from the main menu.

Step 2. 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.**



```
          Menu 11.3 - Remote Node Network Layer Options

            IP Address Assignment= Dynamic
            IP Address= N/A
            IP Subnet Mask= N/A
            Gateway IP Addr= N/A

            Network Address Translation= Full Feature
            Metric= N/A
            Private= N/A
            RIP Direction= None
              Version= N/A
            Multicast= None




     Enter here to CONFIRM or ESC to CANCEL:

     Press Space Bar to Toggle.
```

Figure 12-4 Menu 11.3: Applying NAT to the Remote Node

The following table describes the options for Network Address Translation.

Table 12-3 Applying NAT in Menus 4 & 11.3

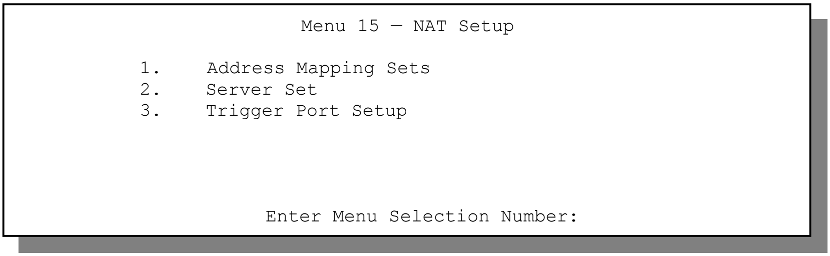
FIELD	DESCRIPTION	OPTIONS
Network Address Translation	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see *section 12.3.1* for further discussion). You can configure any of the mapping types described in *Table 12-2*. Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL.	**Full Feature**
	NAT is disabled when you select this option.	**None**
	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see *section 12.3.1*). Choose **SUA Only** if you have just one public WAN IP address for your ZyWALL.	**SUA Only**

12.3 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 and the DMZ. You can see two NAT address mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or

11.3, the SMT will use **Set 1**, which supports all mapping types as outlined in *Table 12-2.* When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN and DMZ servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see *section 12.4* for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.



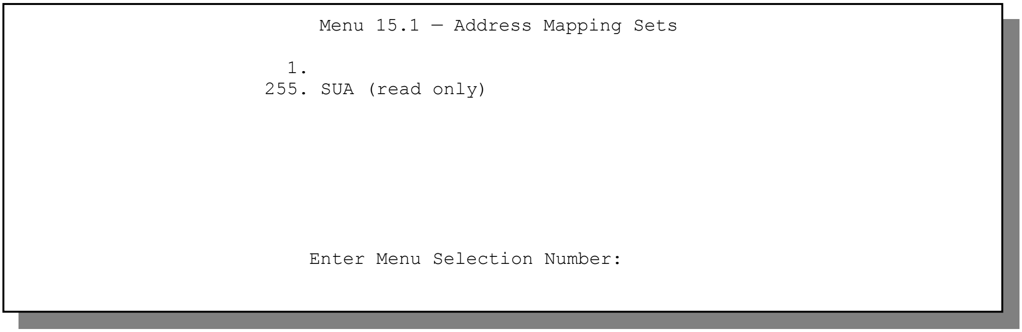
```
                    Menu 15 — NAT Setup

              1.    Address Mapping Sets
              2.    Server Set
              3.    Trigger Port Setup




                 Enter Menu Selection Number:
```

Figure 12-5 Menu 15: NAT Setup

Configure DMZ and LAN IP addresses in NAT menus 15.1 and 15.2. DMZ IP addresses must be on subnets separate from LAN IP addresses.

12.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

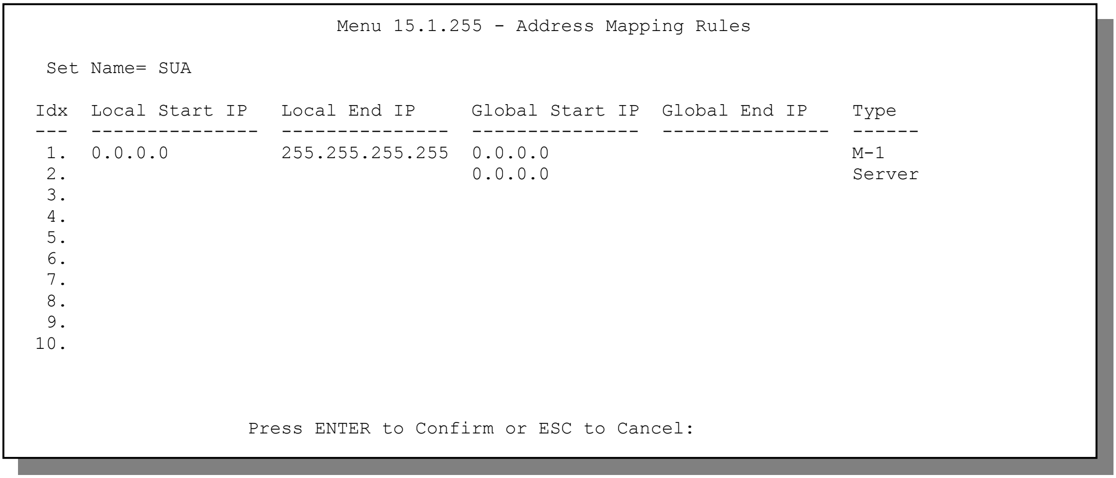


```
                    Menu 15.1 — Address Mapping Sets

                      1.
                    255. SUA (read only)







                    Enter Menu Selection Number:
```

Figure 12-6 Menu 15.1: Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 12.2.1)*. The fields in this menu cannot be changed.



```
                              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:
```

Figure 12-7 Menu 15.1.255: SUA Address Mapping Rules

The following table explains the fields in this screen.

Menu 15.1.255 is read-only.

Table 12-4 SUA Address Mapping Rules

FIELD	DESCRIPTION	I XAMPLE
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.	SUA
Idx	This is the index or rule number.	1
Local Start IP	**Local Start IP** is the starting local IP address (ILA) (see *Figure 12-1)*.	0.0.0.0
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.	255.255.255.255
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**.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	
Type	These are the mapping types discussed above (see *Table 12-2*). **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server

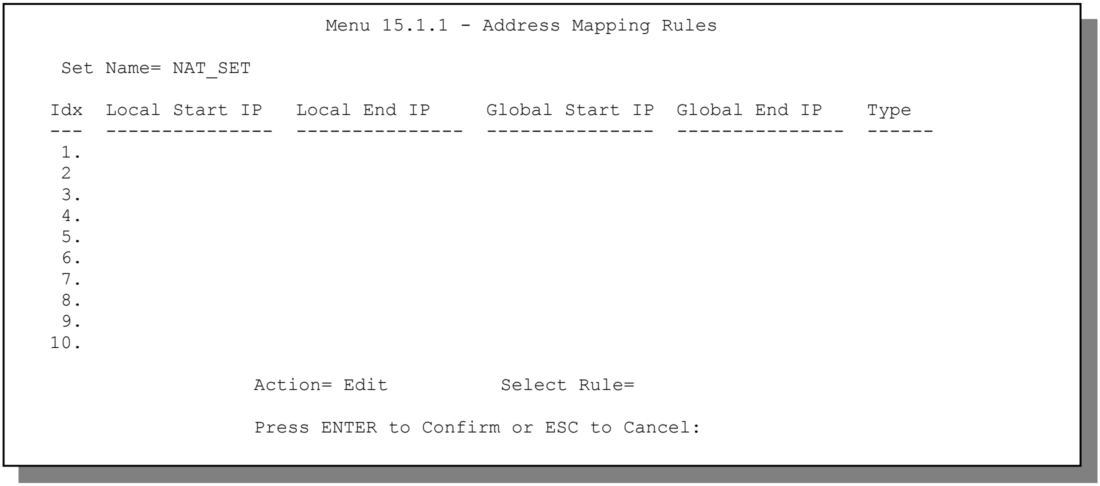
Table 12-4 SUA Address Mapping Rules

FIELD	DESCRIPTION	I XAMPLE
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.		

User-Defined Address Mapping Sets

Now look at option 1 in menu 15.1. Enter 1 to bring up this menu. 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.

The entire set will be deleted if you leave the Set Name **field blank and press [ENTER] are the bottom of the screen.**



```
                         Menu 15.1.1 - Address Mapping Rules

    Set Name= NAT_SET

   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:
```

Figure 12-8 Menu 15.1.1: First Set

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

Ordering Your Rules

Ordering your rules is important because the ZyWALL applies the rules in the order that you specify. When a rule matches the current packet, the ZyWALL 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.

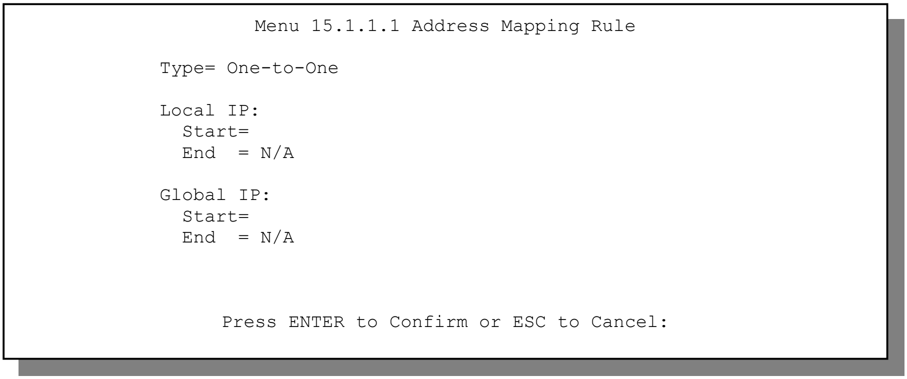
Table 12-5 Fields in Menu 15.1.1

FIELD	DESCRIPTION	EXAMPLE
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.	NAT_SET
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see 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.	**Edit**
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.	1

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**.

An IP End address must be numerically greater than its corresponding IP Start address.



```
                      Menu 15.1.1.1 Address Mapping Rule

              Type= One-to-One

              Local IP:
                Start=
                End  = N/A

              Global IP:
                Start=
                End  = N/A



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

Figure 12-9 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

Table 12-6 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in Table 12-2. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 12.5.3* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	Enter the starting local IP address (ILA).	0.0.0.0
End	Enter 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.	N/A
Global IP		
Start	Enter the starting 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**.	0.0.0.0
End	Enter the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.	N/A
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.		

12.4 NAT Server Sets – Port Forwarding

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world. The ZyWALL 100 provides the additional safety of a DMZ port for connecting your publicly accessible servers. This makes the LAN more secure by physically separating it from your public servers.

Use **Menu 15 - NAT Setup** to forward incoming service requests to the server(s) on your local network. 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. Entry 12 (port 1026) is non-editable (see *Figure 12-10*).

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

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.

The most often used port numbers are shown in the following table. Please refer to *RFC 1700* for further information about port numbers. Please also refer to the included disk for more examples and details on NAT.

Table 12-7 Services & Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25

Table 12-7 Services & Port Numbers

SERVICES	PORT NUMBER
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

12.4.1 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

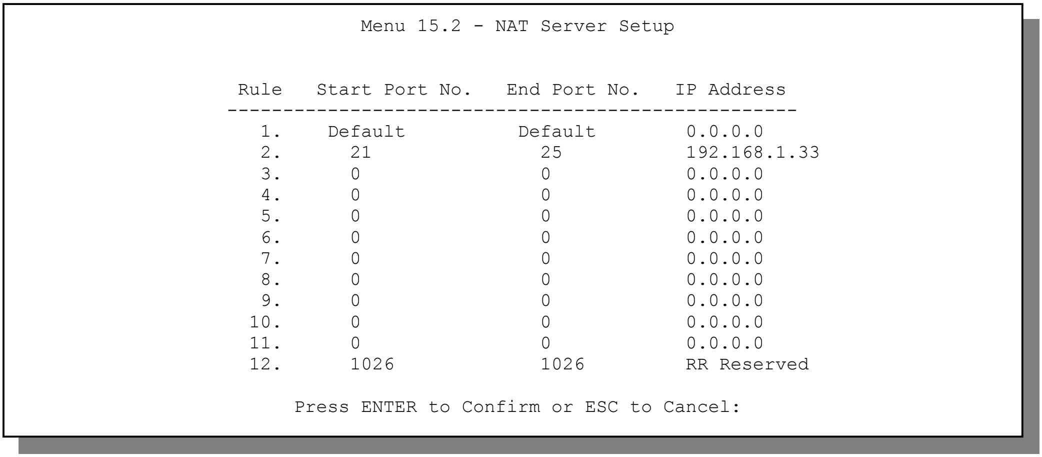
Step 1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

Step 2. Enter 2 to go to **Menu 15.2 - NAT Server Setup**.

Step 3. 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.

Step 4. 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.

Step 5. 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.



```
                          Menu 15.2 - 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.       1026             1026         RR Reserved

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

Figure 12-10 Menu 15.2: NAT Server Setup

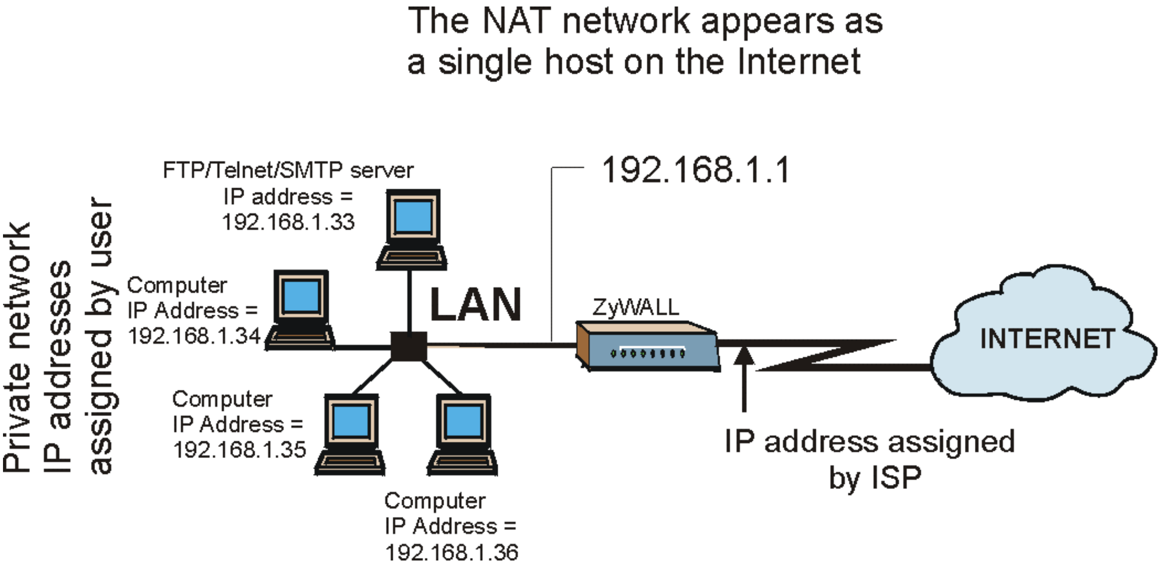


Figure 12-11 Multiple Servers Behind NAT Example

12.5 General NAT Examples

12.5.1 Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

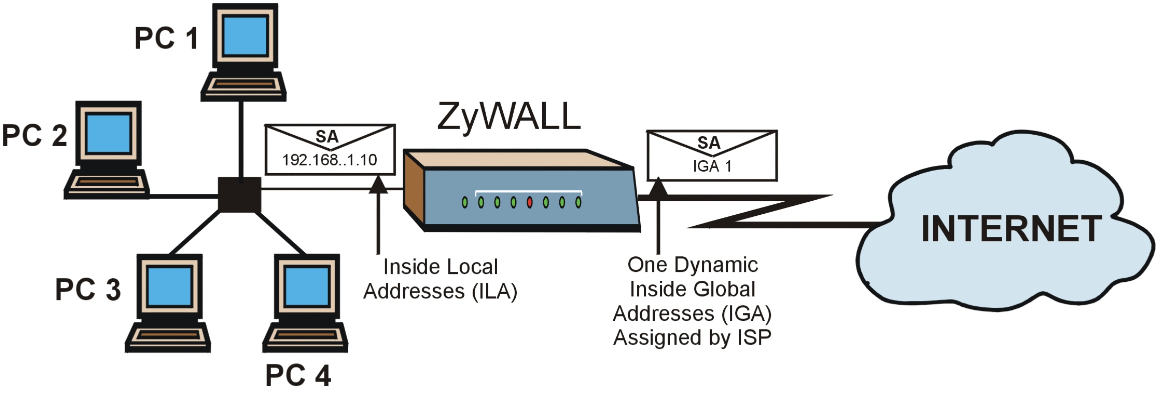
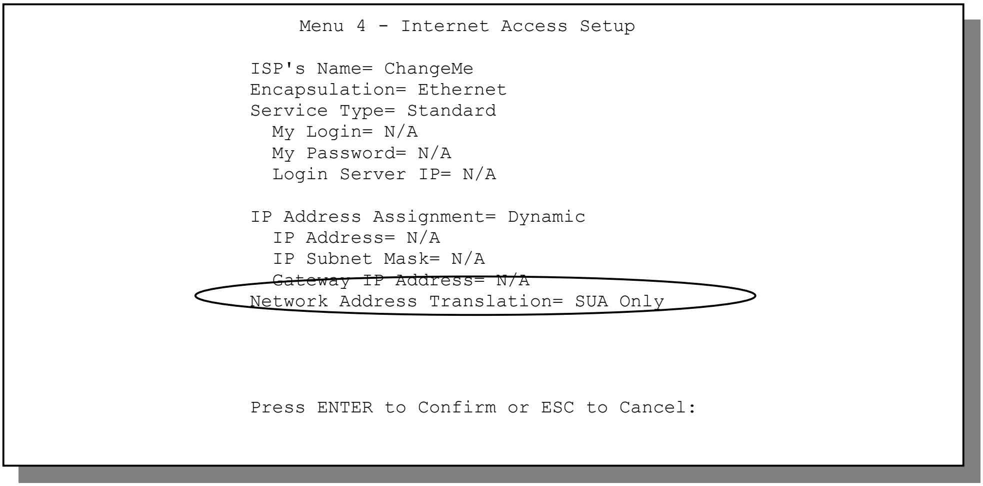


Figure 12-12 NAT Example 1



```
                Menu 4 - Internet Access Setup

            ISP's Name= ChangeMe
            Encapsulation= Ethernet
            Service Type= Standard
              My Login= N/A
              My Password= N/A
              Login Server IP= N/A

            IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Address= N/A
            Network Address Translation= SUA Only




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

Figure 12-13 Menu 4: Internet Access & NAT Example

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 12.5.* The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

12.5.2 Example 2: Internet Access with an Inside Server

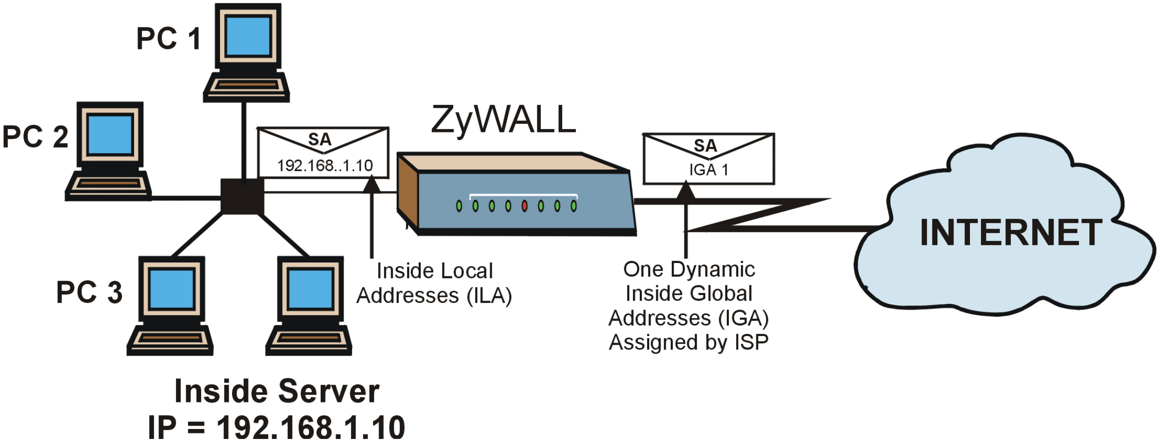
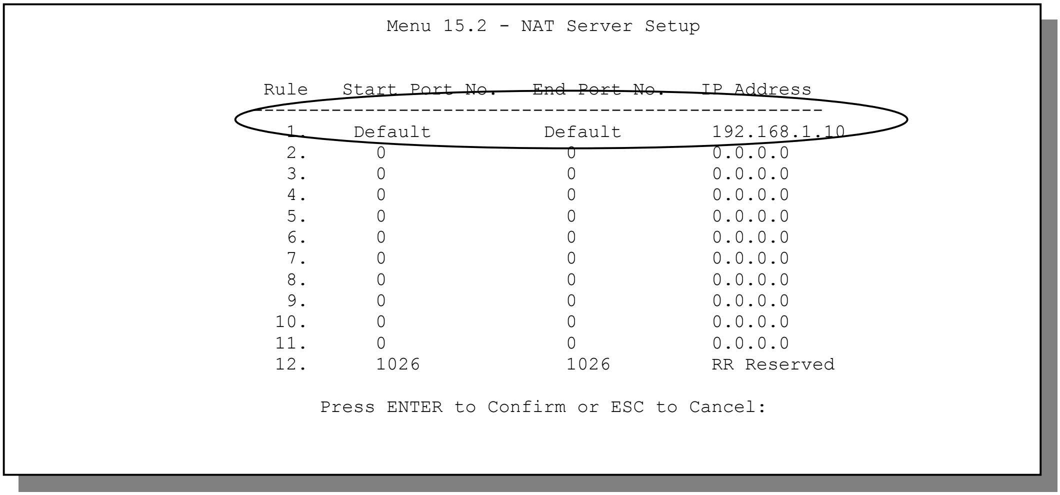


Figure 12-14 NAT Example 2

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.



```
                    Menu 15.2 - 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.      1026             1026         RR Reserved

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

Figure 12-15 Menu 15.2: Specifying an Inside Server

12.5.3 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 uni-directional as follows.

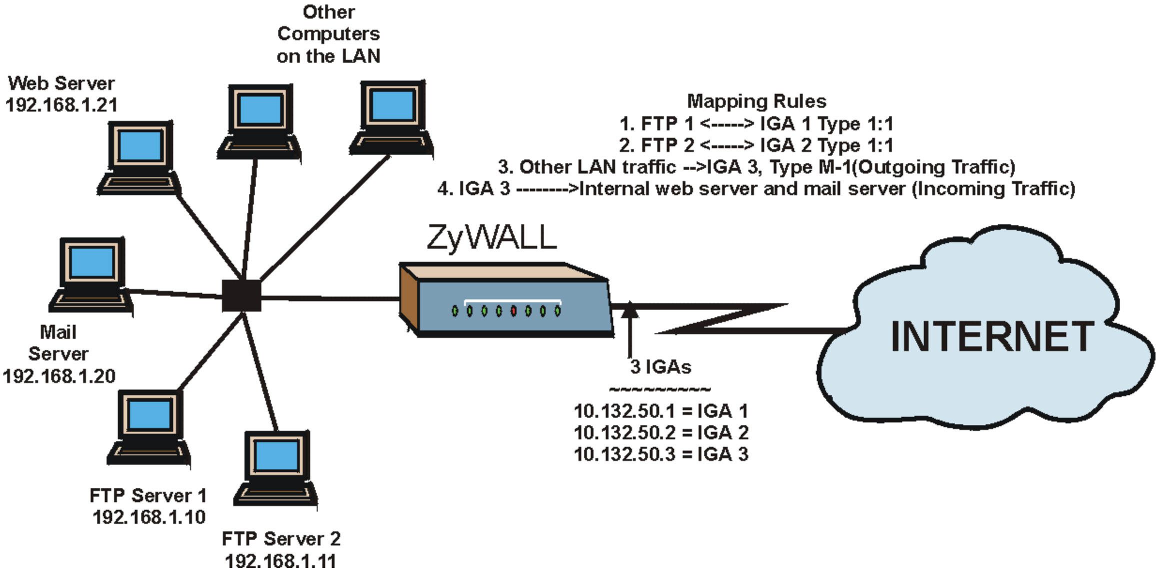
Rule 1. Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 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).

Rule 3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 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:



Other Computers on the LAN
Web Server 192.168.1.21
Mapping Rules
1. FTP 1 <-----> IGA 1 Type 1:1
2. FTP 2 <-----> IGA 2 Type 1:1
3. Other LAN traffic -->IGA 3, Type M-1(Outgoing Traffic)
4. IGA 3 -------->Internal web server and mail server (Incoming Traffic)
ZyWALL
INTERNET
Mail Server 192.168.1.20
3 IGAs
~~~~~~~~~~
10.132.50.1 = IGA 1
10.132.50.2 = IGA 2
10.132.50.3 = IGA 3
FTP Server 1 192.168.1.10
FTP Server 2 192.168.1.11

Figure 12-16 NAT Example 3

Step 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 **Network Address Translation** field (in menu 4 or menu 11.3) in *Figure 12-17*.

Step 2. Then enter 15 from the main menu.

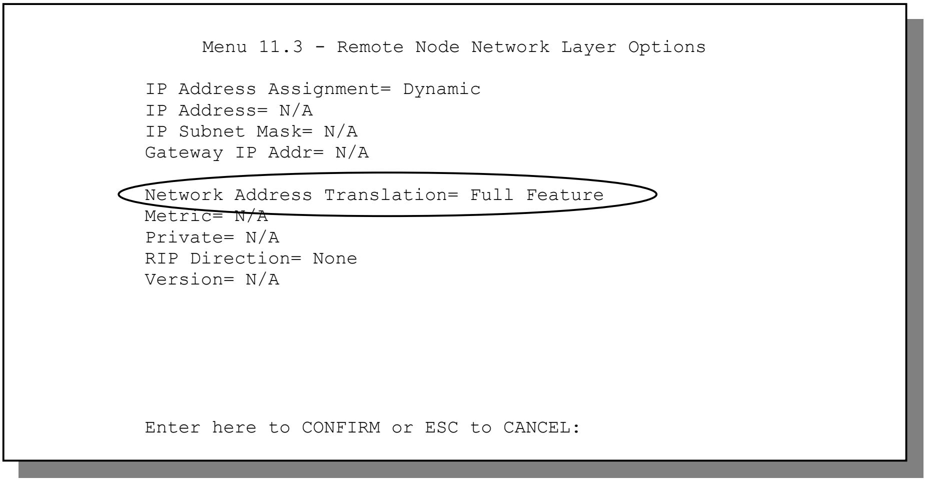
Step 3. Enter 1 to configure the Address Mapping Sets.

Step 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.

Step 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 12-18).*

Step 6. Repeat the previous step for rules 2 to 4 as outlined above.

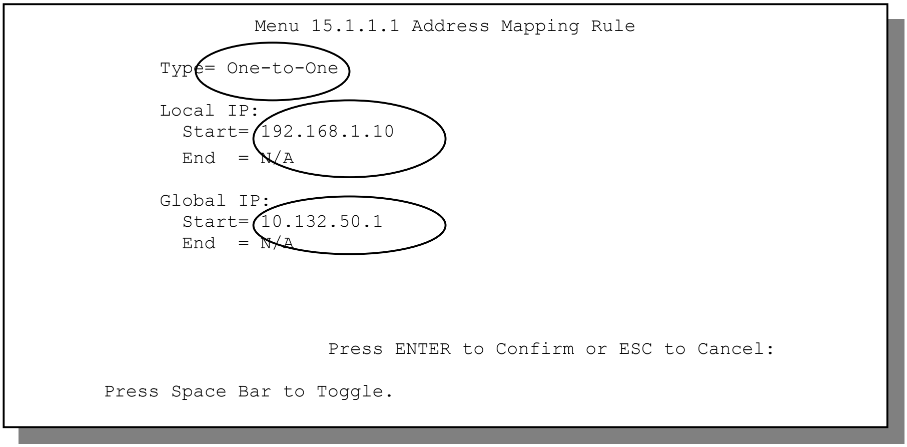
Step 7. When finished, menu 15.1.1 should look like as shown in *Figure 12-19.*
~~~~~~~~~~



```
          Menu 11.3 - Remote Node Network Layer Options

     IP Address Assignment= Dynamic
     IP Address= N/A
     IP Subnet Mask= N/A
     Gateway IP Addr= N/A

     Network Address Translation= Full Feature
     Metric= N/A
     Private= N/A
     RIP Direction= None
     Version= N/A




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

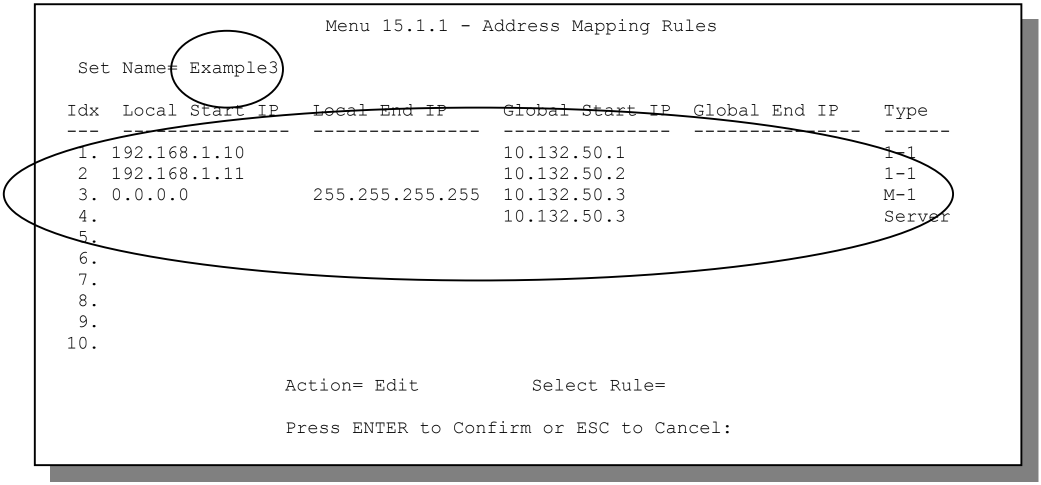
Figure 12-17 Example 3: Menu 11.3

The following figure shows how to configure the first rule.



```
                  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



                          Press ENTER to Confirm or ESC to Cancel:

     Press Space Bar to Toggle.
```

Figure 12-18 Example 3: Menu 15.1.1.1



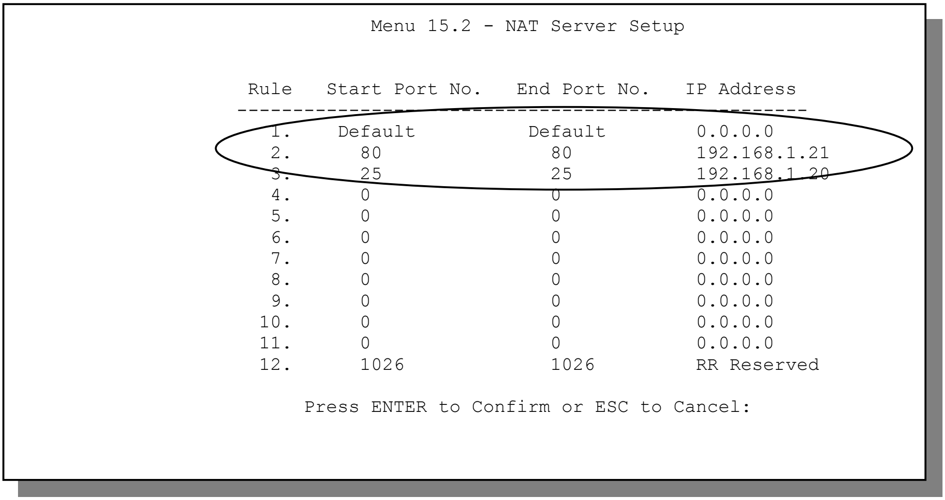
```
                          Menu 15.1.1 - Address Mapping Rules

   Set Name= Example3

  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= Edit          Select Rule=

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

Figure 12-19 Example 3: Final Menu 15.1.1

Now configure the IGA3 to map to our web server and mail server on the LAN.

Step 8. Enter 15 from the main menu.

Step 9. Now enter 2 from this menu and configure it as shown in *Figure 12-20*.



```
                         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.        1026             1026         RR Reserved

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

Figure 12-20 Example 3: Menu 15.2

12.5.4 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-One-to-One** mapping as port numbers do *not* change for **Many-One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

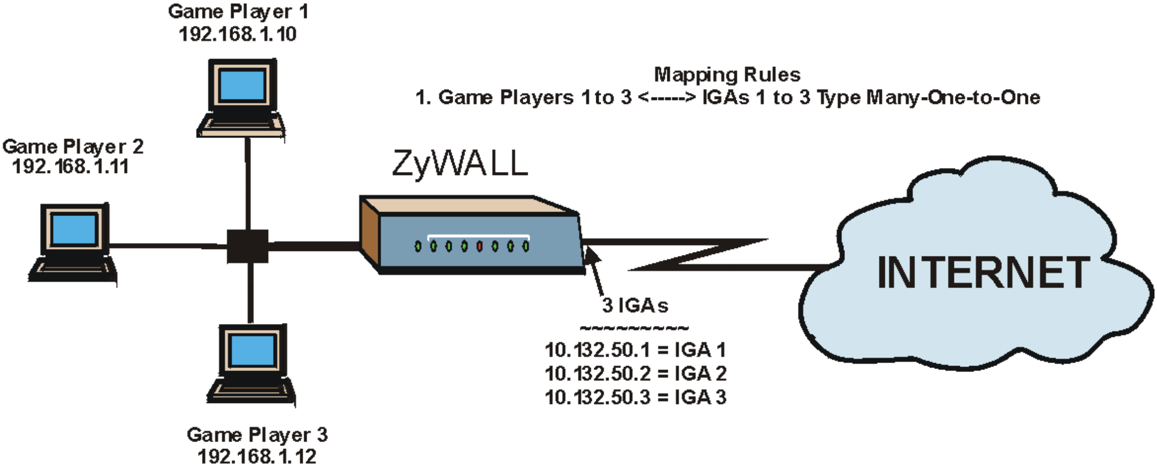
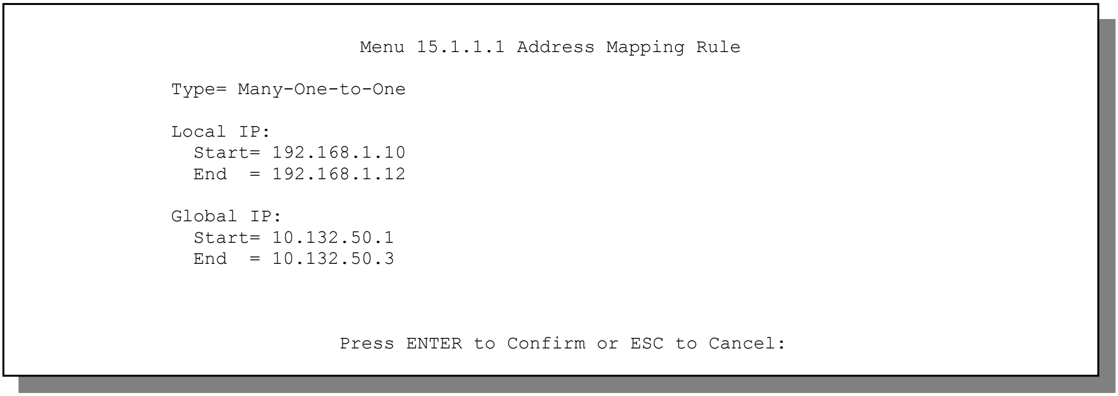


Figure 12-21 NAT Example 4

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-One-to-One **mapping types.**

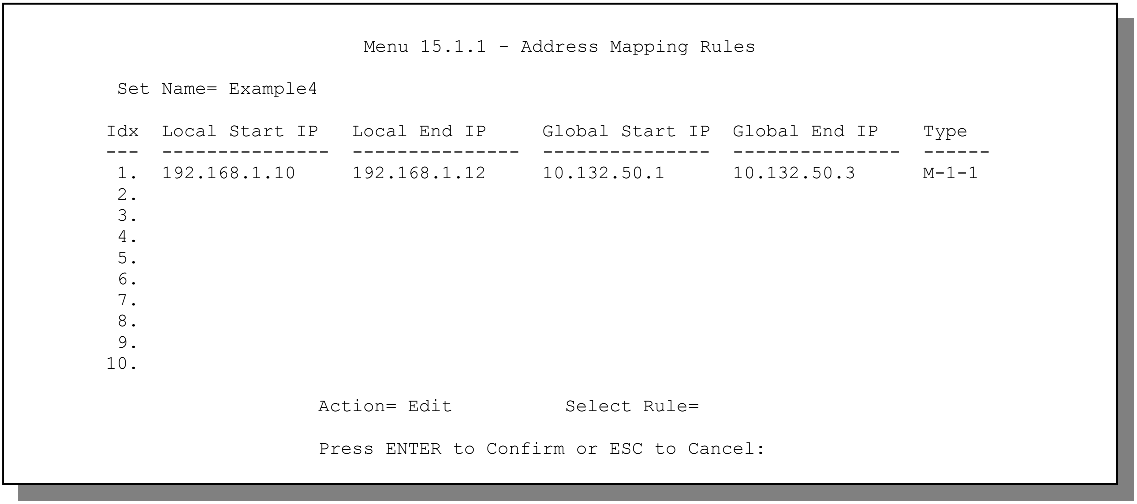
Follow the steps outlined in example 3 above to configure these two menus as follows.



```
                         Menu 15.1.1.1 Address Mapping Rule

          Type= Many-One-to-One

          Local IP:
            Start= 192.168.1.10
            End  = 192.168.1.12

          Global IP:
            Start= 10.132.50.1
            End  = 10.132.50.3



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

Figure 12-22 Example 4: Menu 15.1.1.1: Address Mapping Rule

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.



```
                              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-1-1
          2.
          3.
          4.
          5.
          6.
          7.
          8.
          9.
         10.

                            Action= Edit          Select Rule=

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

Figure 12-23 Example 4: Menu 15.1.1: Address Mapping Rules

12.6 Trigger Port Forwarding

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

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

12.6.1 Trigger Port Forwarding Process

The following is an example of trigger port forwarding.

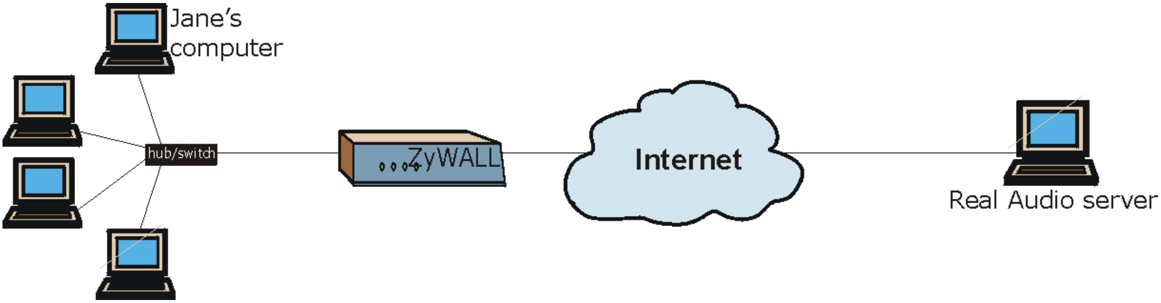


Figure 12-24 Trigger Port Forwarding Process: Example

1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the ZyWALL to record Jane's computer IP address. The ZyWALL associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The ZyWALL forwards the traffic to Jane's computer IP address.

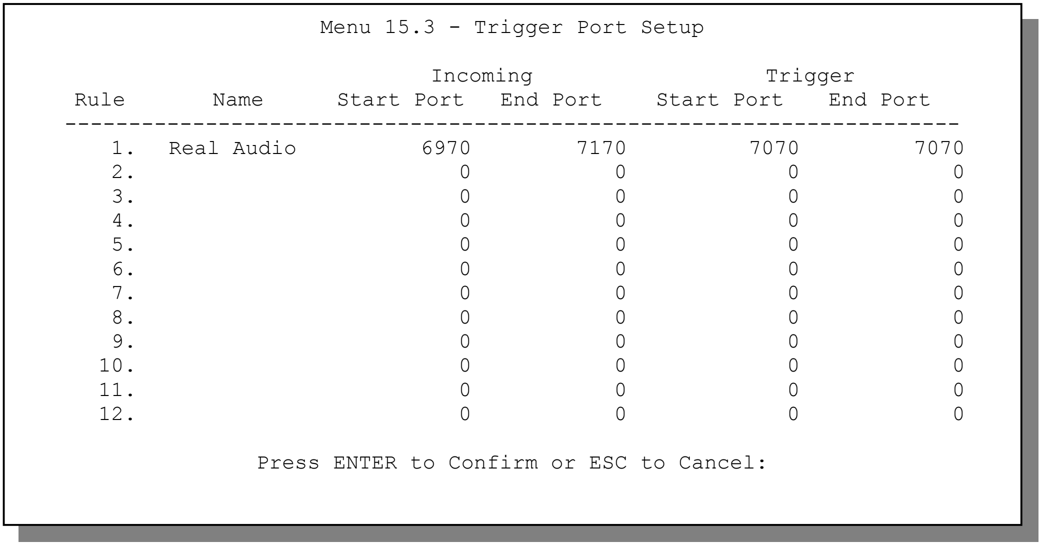
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyWALL times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

12.6.2 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is going coming from inside the ZyWALL and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

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

Enter 3 in menu 15 to display **Menu 15.3 — Trigger Port Setup**, shown next.



```
                        Menu 15.3 - Trigger Port Setup

                                  Incoming                  Trigger
     Rule       Name      Start Port   End Port    Start Port   End Port
    ----------------------------------------------------------------------
       1.   Real Audio          6970       7170          7070       7070
       2.                          0          0             0          0
       3.                          0          0             0          0
       4.                          0          0             0          0
       5.                          0          0             0          0
       6.                          0          0             0          0
       7.                          0          0             0          0
       8.                          0          0             0          0
       9.                          0          0             0          0
      10.                          0          0             0          0
      11.                          0          0             0          0
      12.                          0          0             0          0

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

Figure 12-25 Menu 15.3—Trigger Port Setup

Table 12-8 Menu 15.3—Trigger Port Setup Description

FIELD	DESCRIPTION	EXAMPLE
Rule	This is the rule index number.	1
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.	Real Audio
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	6970
End Port	Enter a port number or the ending port number in a range of port numbers.	7170
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	7070
End Port	Enter a port number or the ending port number in a range of port numbers.	7070
Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

Part IV:

Firewall and Content Filters

This part introduces firewalls in general and the ZyWALL firewall. It also explains custom ports and gives example firewall rules and an overview of content filtering.

Chapter 13 Firewalls

This chapter gives some background information on firewalls and explains how to get started with the ZyWALL firewall.

13.1 What Is a Firewall?

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.

13.2 Types of Firewalls

There are three main types of firewalls:

1. Packet Filtering Firewalls
2. Application-level Firewalls
3. Stateful Inspection Firewalls

13.2.1 Packet Filtering Firewalls

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

13.2.2 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:

i. 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.

ii. 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.

13.2.3 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 13.5* for more information on Stateful Inspection.

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

13.3 Introduction to ZyXEL's Firewall

The ZyWALL 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 ZyWALL's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyWALL 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 ZyWALL also has packet-filtering capabilities.

The ZyWALL is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The ZyWALL has one Ethernet WAN port and one Ethernet LAN port, which are used to physically separate the network into two areas.

❑ The WAN (Wide Area Network) port attaches to the broadband modem (cable or ADSL) connecting 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 the remote host is authorized to use a specific service.

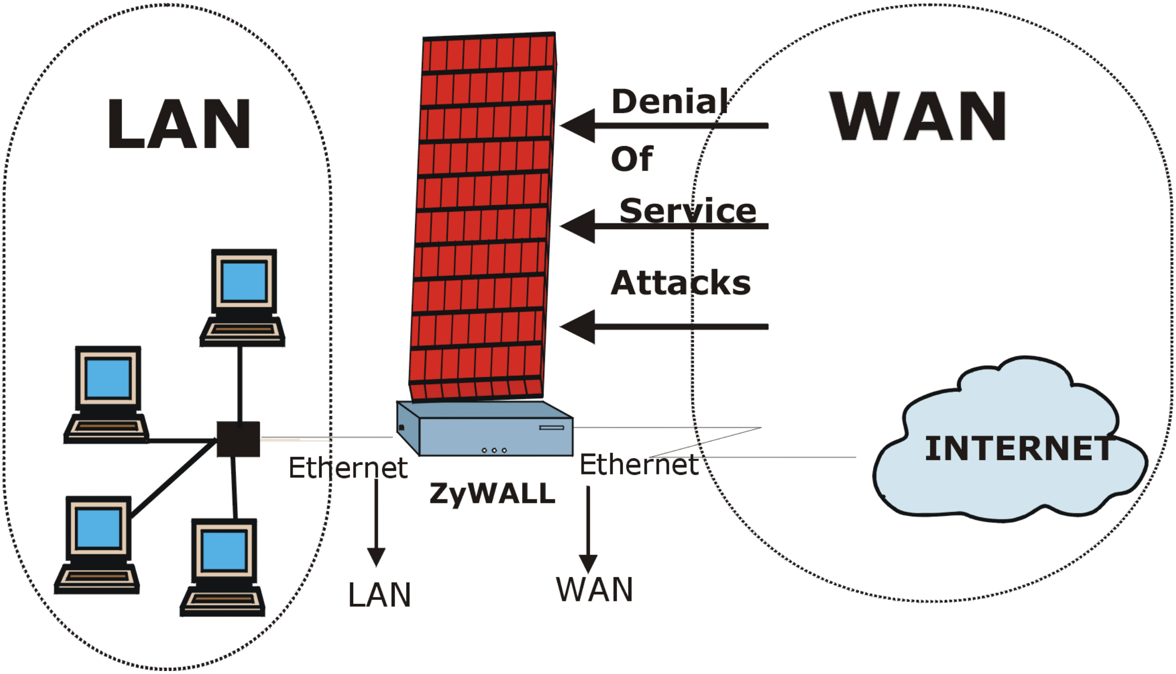


Figure 13-1 ZyWALL Firewall Application

13.4 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 ZyWALL is pre-configured to automatically detect and thwart all known DoS attacks.

13.4.1 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 13-1 Common IP Ports

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

13.4.2 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.

1. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

    1-a 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.

    1-b Teardrop attack exploits weaknesses in the reassembly 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.

2. 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.

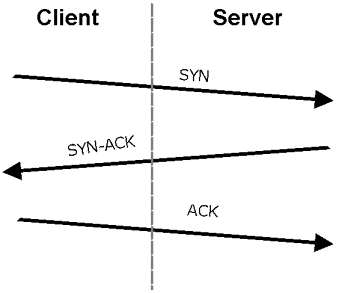


Figure 13-2 Three-Way Handshake

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.

2-a **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.

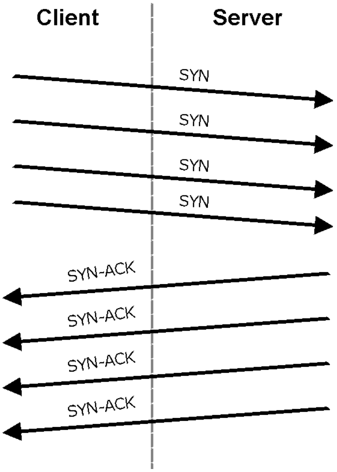


Figure 13-3 SYN Flood

2-b 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.

3. 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.

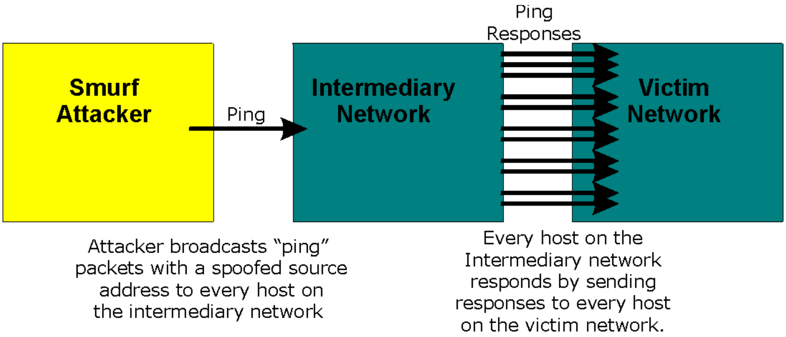

Ping
Responses
Smurf
Attacker
Ping
Intermediary
Network
Victim
Network
Attacker broadcasts "ping" packets with a spoofed source address to every host on the intermediary network
Every host on the Intermediary network responds by sending responses to every host on the victim network.

Figure 13-4 Smurf Attack

❑ ICMP Vulnerability

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

Table 13-2 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- ❑ Illegal Commands (NetBIOS and SMTP)

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

Table 13-3 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

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

Table 13-4 Legal SMTP Commands

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

- ❑ 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.

4. 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 ZyWALL blocks all IP Spoofing attempts.

13.5 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 ZyWALL uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyWALL’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.

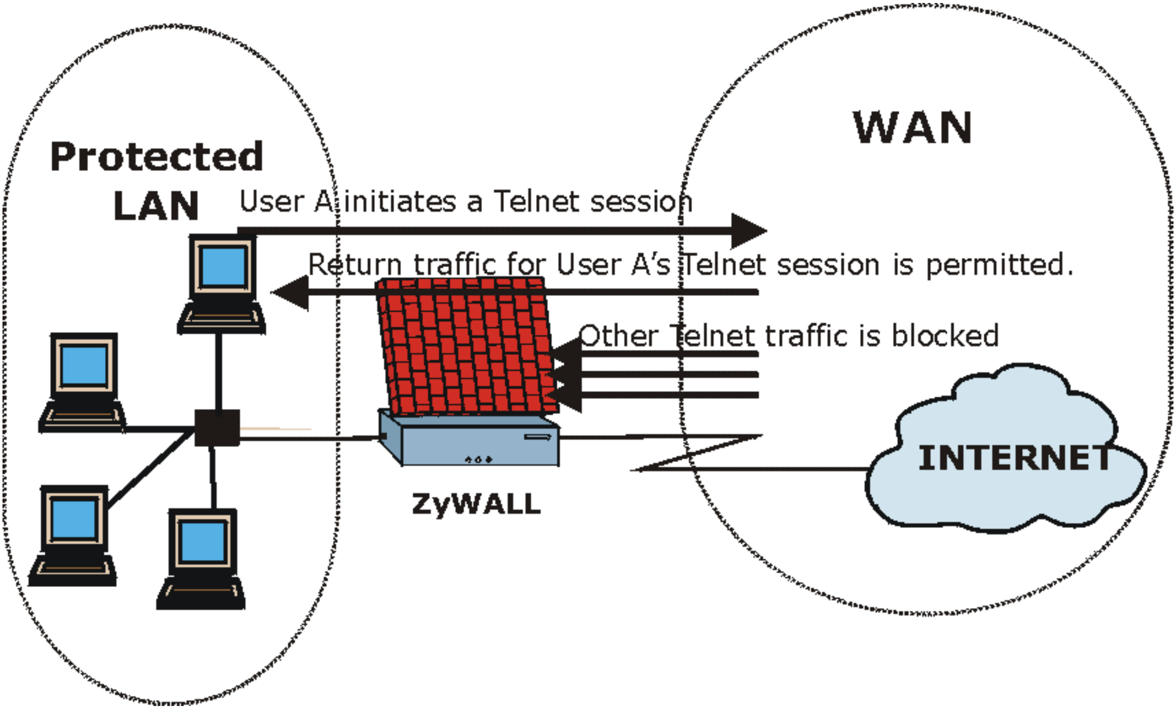

Protected
LAN
User A initiates a Telnet session
Return traffic for User A's Telnet session is permitted.
Other Telnet traffic is blocked
WAN
INTERNET
ZyWALL

Figure 13-5 Stateful Inspection

The previous figure shows the ZyWALL'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.

13.5.1 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 16-3*) determines 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.

13.5.2 Stateful Inspection and the ZyWALL

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

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

ii. Allow certain types of traffic from the Internet to specific hosts on the LAN.

iii. Allow access to a Web server to everyone but competitors.

iv. 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.

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 ZyWALL itself (as with the "virtual connections" created for UDP and ICMP).

13.5.3 TCP Security

The ZyWALL 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 ZyWALL 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).

13.5.4 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 ZyWALL 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.

13.5.5 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 ZyWALL 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.

13.6 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via SMT or web configurator.
2. Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.
3. Limit who can telnet into your router.
4. 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.
5. 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.
6. Protect against IP spoofing by making sure the firewall is active.

7. Keep the firewall in a secured (locked) room.

13.6.1 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.

1. 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!
2. 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.
3. Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
4. Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
5. 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.
6. 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.
7. 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 #.
8. 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.
9. If you use "chat rooms" or IRC sessions, be careful with any information you reveal to strangers.
10. 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.
11. 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.

13.7 Packet Filtering Vs Firewall

Below are some comparisons between the ZyWALL's filtering and firewall functions.

13.7.1 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.

When To Use Filtering

1. To block/allow LAN packets by their MAC addresses.
2. To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
3. 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 cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. To block/allow IP trace route.

13.7.2 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.

When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. 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.

3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.

4. The firewall performs better than filtering if you need to check many rules.

5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.

6. 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 14
Introducing the ZyWALL Firewall

This chapter shows you how to get started with the ZyWALL firewall.

14.1 Remote Management and the Firewall

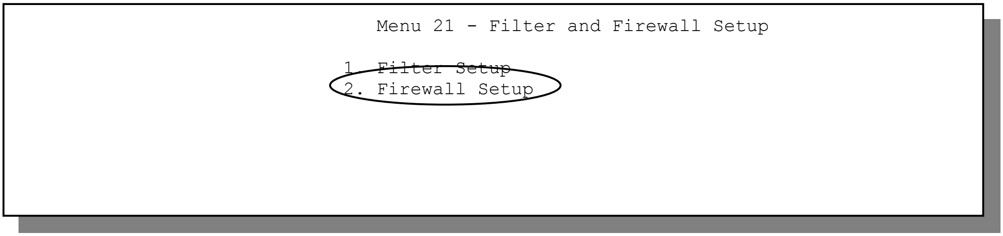
When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the *Remote Management* chapter for details on remote management.

14.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyWALL 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. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to the appendix of firewall CLI commands.

14.3 Using ZyWALL SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next**.**

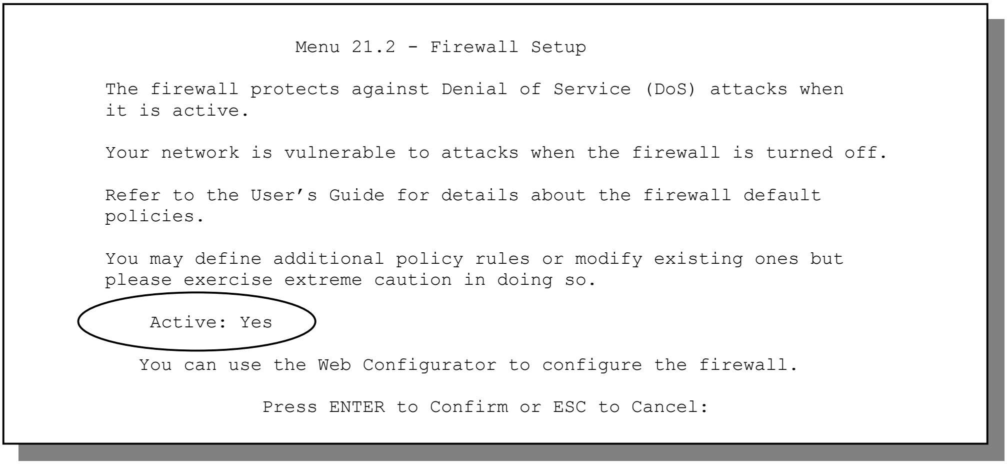


```
                          Menu 21 - Filter and Firewall Setup

                        1. Filter Setup
                        2. Firewall Setup
```

Figure 14-1 Menu 21: Filter and Firewall Setup

14.3.1 Activating the Firewall

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. Use the web configurator to configure firewall rules. This screen varies by ZyWALL model.



```
                       Menu 21.2 - Firewall Setup

         The firewall protects against Denial of Service (DoS) attacks when
         it is active.

         Your network is vulnerable to attacks when the firewall is turned off.

         Refer to the User's Guide for details about the firewall default
         policies.

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

             Active: Yes

            You can use the Web Configurator to configure the firewall.

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

Figure 14-2 Menu 21.2: Firewall Setup

Configure the firewall rules using the web configurator or CLI commands.

Chapter 15
Using the ZyWALL Web Configurator

This chapter shows you how to configure your firewall with the web configurator.

15.1 Web Configurator Login and Main Menu Screens

Use the ZyWALL web configurator, to configure your firewall. To get started, follow the steps shown next.

Step 1. Launch your web browser and enter 192.168.1.1 as the URL.

Step 2. Enter "1234" (default) as the password and click **Login**. If a password appears automatically, just click **Login**. You should see a screen asking you to change your password (highly recommended).

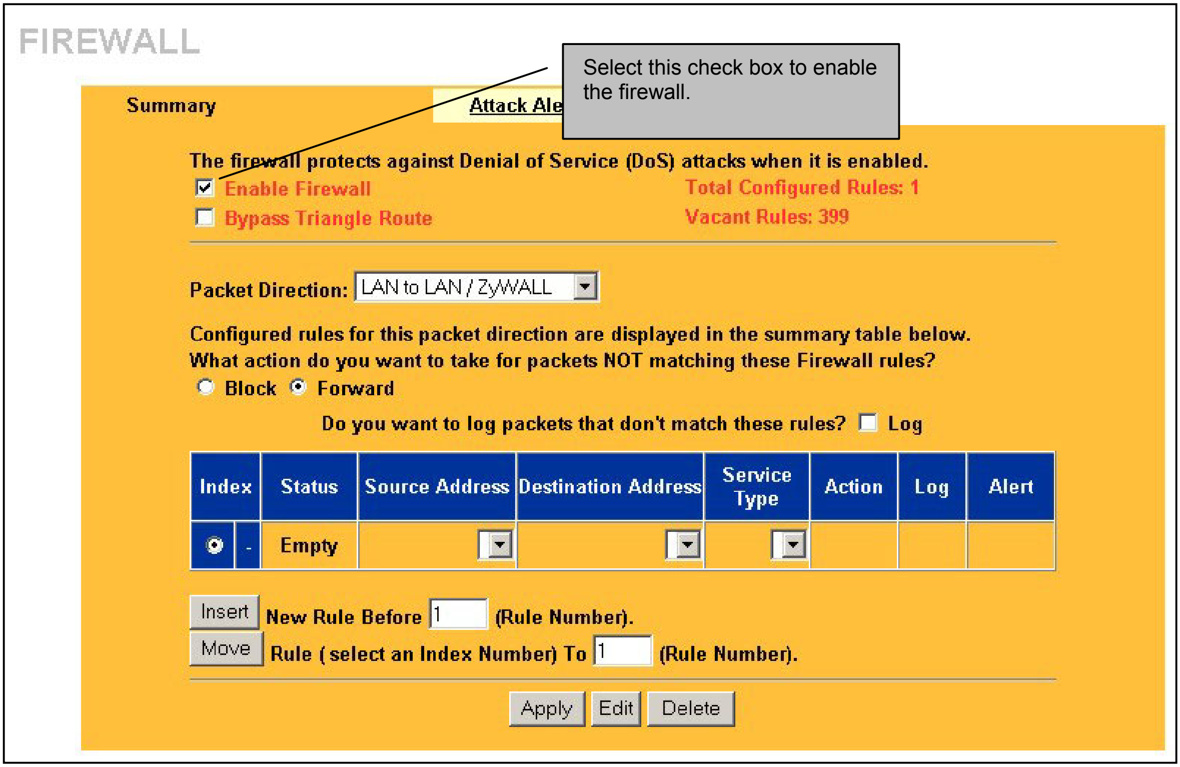
Step 3. Either enter a new password (and retype it to confirm) and click **Login** or click **Ignore** to display the **MAIN MENU** screen.

Use the Help icon in the web configurator for explanations of the fields.

If you forget your password, refer to the *Resetting the ZyWALL* section to see how to reset the default configuration file.

15.2 Enabling the Firewall

Click **Advanced**, **Firewall** and then the **Summary** tab. Enable (or activate) the firewall by clicking the **Enable Firewall** check box as seen in the following screen.



The firewall protects against Denial of Service (DoS) attacks when it is enabled.

☑ Enable Firewall

□ Bypass Triangle Route

Total Configured Rules: 1

Vacant Rules: 399

Packet Direction: LAN to LAN / ZyWALL

Configured rules for this packet direction are displayed in the summary table below.
What action do you want to take for packets NOT matching these Firewall rules?

○ Block ● Forward

Do you want to log packets that don't match these rules? □ Log

Index		Status	Source Address	Destination Address	Service Type	Action	Log	Alert
●	-	Empty						

Insert New Rule Before 1 (Rule Number).

Move Rule (select an Index Number) To 1 (Rule Number).

Figure 15-1 Enabling the Firewall (ZyWALL 100)

15.2.1 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 **Attack Alert** screen *(Figure 15-2* - check the **Generate alert when attack detected** checkbox) or when a rule is matched in the **Rule Config** screen (see *Figure 16-4)*. When an event generates an alert, a message is immediately sent to an e-mail account specified by you. Enter the complete e-mail address to which alert messages will be sent in the **E-mail Alerts To** field and schedule times for sending alerts in the **Log Timer** fields in the **E-mail** screen (following screen).

15.3 Attack Alert

Attack alerts are the first defense against DOS attacks. In the **Attack Alert** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the ZyWALL 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.

15.3.1 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 normal small offices with ADSL bandwidth. Factors influencing choices for threshold values are:

1. The maximum number of opened sessions.
2. The minimum capacity of server backlog in your LAN network.
3. The CPU power of servers in your LAN network.
4. Network bandwidth.
5. 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.

15.3.2 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 13-2*). For UDP, "half-open" means that the firewall has detected no return traffic.

The ZyWALL 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 ZyWALL starts deleting half-open sessions as required to accommodate new connection requests. The ZyWALL 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 ZyWALL starts deleting half-open sessions as required to accommodate new connection requests. The ZyWALL 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.

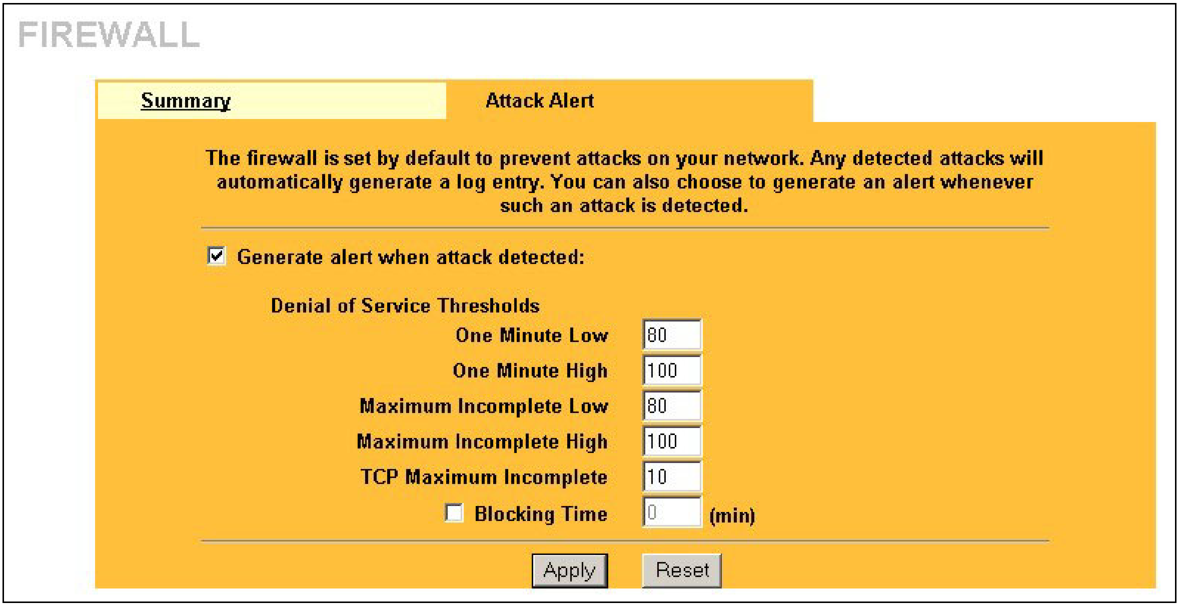
TCP Maximum Incomplete and Blocking Time

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 ZyWALL starts deleting half-open sessions according to one of the following methods:

1. If the **Blocking Time** timeout is 0 (the default), then the ZyWALL 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.
2. If the **Blocking Time** timeout is greater than 0, then the ZyWALL blocks all new connection requests to the host giving the server time to handle the present connections. The ZyWALL continues to block all new connection requests until the **Blocking Time** expires.

The ZyWALL also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click the **Attack Alert** tab to bring up the next screen.



FIREWALL

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 0 (min)

Figure 15-2 Attack Alert

The following table describes the fields in this screen.

Table 15-1 Attack Alert

FIELD	DESCRIPTION	DEFAULT VALUES
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected. See the chapter on logs for more information on logs and alerts.	
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 ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.

Table 15-1 Attack Alert

FIELD	DESCRIPTION	DEFAULT VALUES
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 ZyWALL deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the ZyWALL to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
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 ZyWALL deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum** I**ncomplete Low** number.	100 existing half-open sessions. The above values causes the ZyWALL to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
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 250. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	10 existing half-open TCP sessions.

Table 15-1 Attack Alert

FIELD	DESCRIPTION	DEFAULT VALUES
Blocking Time	When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you check **Blocking Time** any new sessions will be blocked for the length of time you specify in the next field (min) 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.	Select this check box to specify a number in minutes (min) text box.
(min)	Enter the length of **Blocking Time** in minutes.	0
When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to exit this screen without saving, or **Help** for online HTML help on fields in this screen.		

Chapter 16
Creating Custom Rules

This chapter contains instructions for defining both Local Network and Internet rules. DMZ applies to the ZyWALL 100.

16.1 Rules Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ZyWALL
- LAN to WAN
- LAN to DMZ
- WAN to LAN
- WAN to WAN/ZyWALL
- WAN to DMZ
- DMZ to LAN
- DMZ to WAN
- DMZ to DMZ/ZyWALL

DMZ is not available on all models.

By default, the ZyWALL’s stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ZyWALL

  This allows computers on the LAN to manage the ZyWALL and communicate between networks or subnets connected to the LAN interface.

- LAN to WAN
- LAN to DMZ
- WAN to DMZ
- DMZ to WAN

By default, the ZyWALL’s stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/ZyWALL

  This prevents computers on the WAN from using the ZyWALL as a gateway to communicate with other computers on the WAN and/or managing the ZyWALL.

- DMZ to LAN
- DMZ to DMZ/ZyWALL

This prevents computers on the DMZ from communicating between networks or subnets connected to the DMZ interface and/or managing the ZyWALL.

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

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 ZyWALL's default rules.

16.2 Rule Logic Overview

Study these points carefully before configuring rules.

16.2.1 Rule Checklist

1. 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."
2. Is the intent of the rule to forward or block traffic?
3. What direction of traffic does the rule apply to (refer to *16.1*)?
4. What IP services will be affected?
5. What computers on the LAN or DMZ are to be affected (if any)?
6. 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.

16.2.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

1. 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?
2. 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?
3. 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.
4. Does this rule conflict with any existing rules?

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.

16.2.3 Key Fields For Configuring Rules

Action

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

"Block" means the firewall silently discards the packet.

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 16.5* for more information on predefined services.

Source Address

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

Destination Address

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

16.3 Connection Direction Examples

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN. Rules for the DMZ work in a similar fashion.

LAN to LAN/ZyWALL, WAN to WAN/ZyWALL and DMZ to DMZ/ZyWALL rules apply to packets coming in on the associated interface (LAN, WAN, or DMZ respectively). LAN to LAN/ZyWALL means policies for LAN-to-ZyWALL (the policies for managing the ZyWALL through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN).
Similarly, WAN to WAN/ZyWALL and DMZ to DMZ/ZyWALL polices apply in the same way to the WAN and DMZ ports.

16.3.1 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. See the following figure.

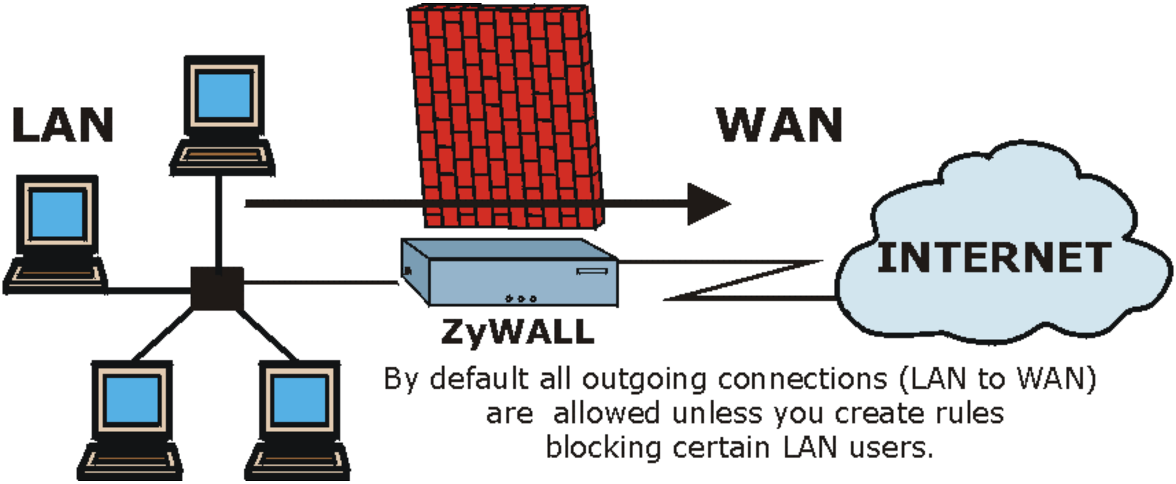

LAN
WAN
INTERNET
ZyWALL
By default all outgoing connections (LAN to WAN)
are allowed unless you create rules
blocking certain LAN users.

Figure 16-1 LAN to WAN Traffic

16.3.2 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.

See the following figure.

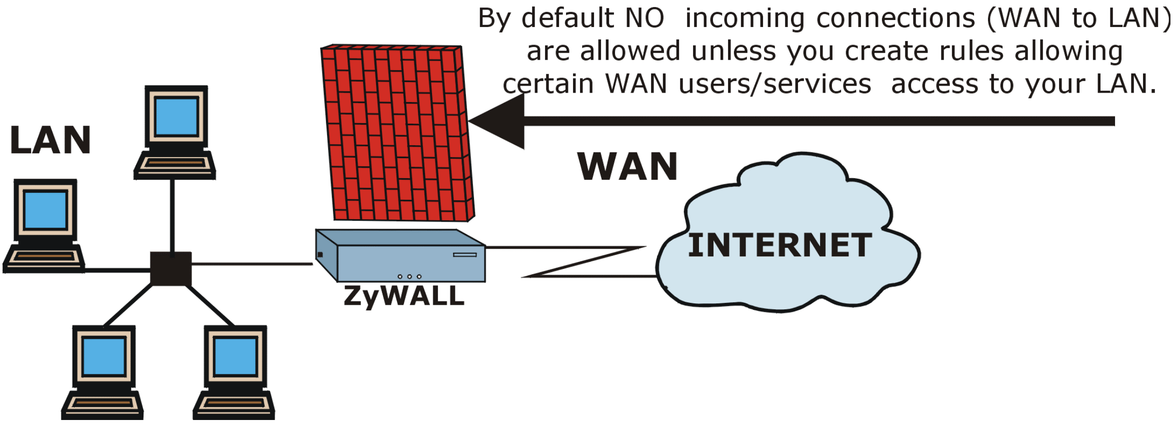
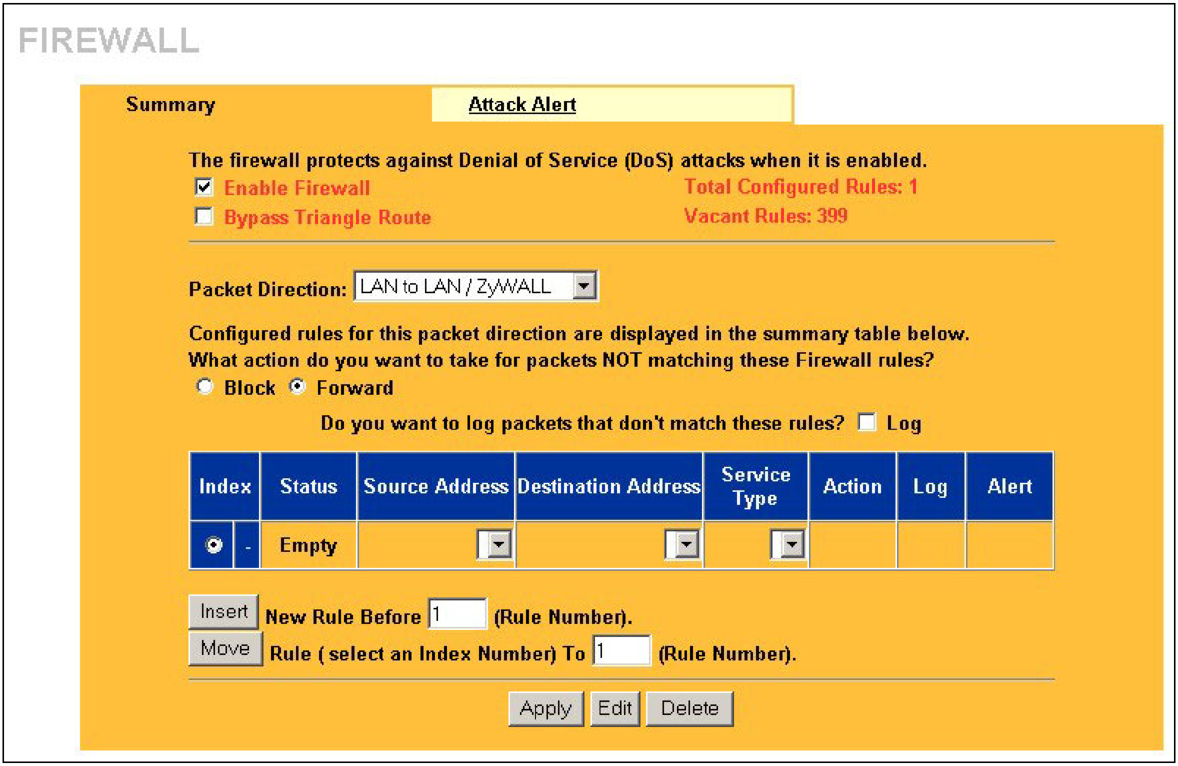

By default NO incoming connections (WAN to LAN) are allowed unless you create rules allowing certain WAN users/services access to your LAN.
LAN
WAN
INTERNET
ZyWALL

Figure 16-2 WAN to LAN Traffic

16.4 Rule Summary

Click **Advanced**, **Firewall** and the **Summary** tab to display the following screen. This screen is a summary of the existing rules. Note the order in which the rules are listed.

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



FIREWALL

Summary | Attack Alert

The firewall protects against Denial of Service (DoS) attacks when it is enabled.

☑ Enable Firewall — Total Configured Rules: 1

□ Bypass Triangle Route — Vacant Rules: 399

Packet Direction: LAN to LAN / ZyWALL

Configured rules for this packet direction are displayed in the summary table below.
What action do you want to take for packets NOT matching these Firewall rules?

○ Block ● Forward

Do you want to log packets that don't match these rules? □ Log

Index		Status	Source Address	Destination Address	Service Type	Action	Log	Alert
●	-	Empty						

New Rule Before 1 (Rule Number).

Rule (select an Index Number) To 1 (Rule Number).

Figure 16-3 Firewall Rules Summary: First Screen (ZyWALL100)

The following table describes the fields in the firewall summary screen.

Table 16-1 Firewall Rules Summary: First Screen

FIELD	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the ZyWALL firewall ignore the use of triangle route topology on the network. See the appendices for more on triangle route topology.
Total Configured Rules	This read-only number is the total number of rules that have been configured for the ZyWALL (the combined total for all packet directions). The ZyWALL allows you to configure up to 30 firewall rules total.

Table 16-1 Firewall Rules Summary: First Screen

FIELD	DESCRIPTION
Vacant Rules	This read-only number is the number of rules that can still be configured for the ZyWALL (the combined total available for all packet directions).
Packet Direction	Use the drop-down list box to select a direction of travel of packets (**LAN to LAN/ZyWALL**, **LAN to WAN**, **LAN to DMZ**, **WAN to WAN/ZyWALL**, **WAN to LAN**, **WAN to DMZ, DMZ to DMZ/ZyWALL**, **DMZ to LAN** or **DMZ to WAN**) for which you want to configure firewall rules.
Block Forward	Use the option buttons to select whether to **Block** (discard) or **Forward** (allow the passage of) packets that are traveling in the selected direction.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.	
Index	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.
Status	This field displays whether a firewall is turned on (**Active**) or not (**Inactive**). Rules that have not been configured display **Empty**.
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any.
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any.
Service Type	This drop-down list box displays the services to which this firewall rule applies. Please note that a blank service type is equivalent to Any. See *Table 16-2* for more information.
Action	This is the specified action for that rule, either **Block** or **Forward**. Note that **Block** means the firewall silently discards the packet.
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**).
Alert	This field tells you whether this rule generates an alert (**Yes**) or not (**No**) when the rule is matched.

Table 16-1 Firewall Rules Summary: First Screen

FIELD	DESCRIPTION
Insert	Type the index number for where you want to put a rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. Click **Insert** to display this screen and refer to the following table for information on the fields.
Move	Select a rule’s Index option button and type a number for where you want to put that rule. Click **Move** to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Rule to (Rule Number)	Click a rule's option button and type the number for where you want to put that rule.
Click **Apply** to save your changes to the ZyWALL. Click **Edit** to create or edit a rule. Click **Delete** to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action. Click **Help** for online HTML help on fields in this screen	

16.5 Predefined Services

The **Available Services** list box in the **Rule Config**(uration) screen (see *Figure 16-4*) displays all predefined services that the ZyWALL 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 services may also be configured using the **Custom Ports** function discussed later.

Table 16-2 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 16-2 Predefined Services

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)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.

Table 16-2 Predefined Services

SERVICE	DESCRIPTION
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.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.

Table 16-2 Predefined Services

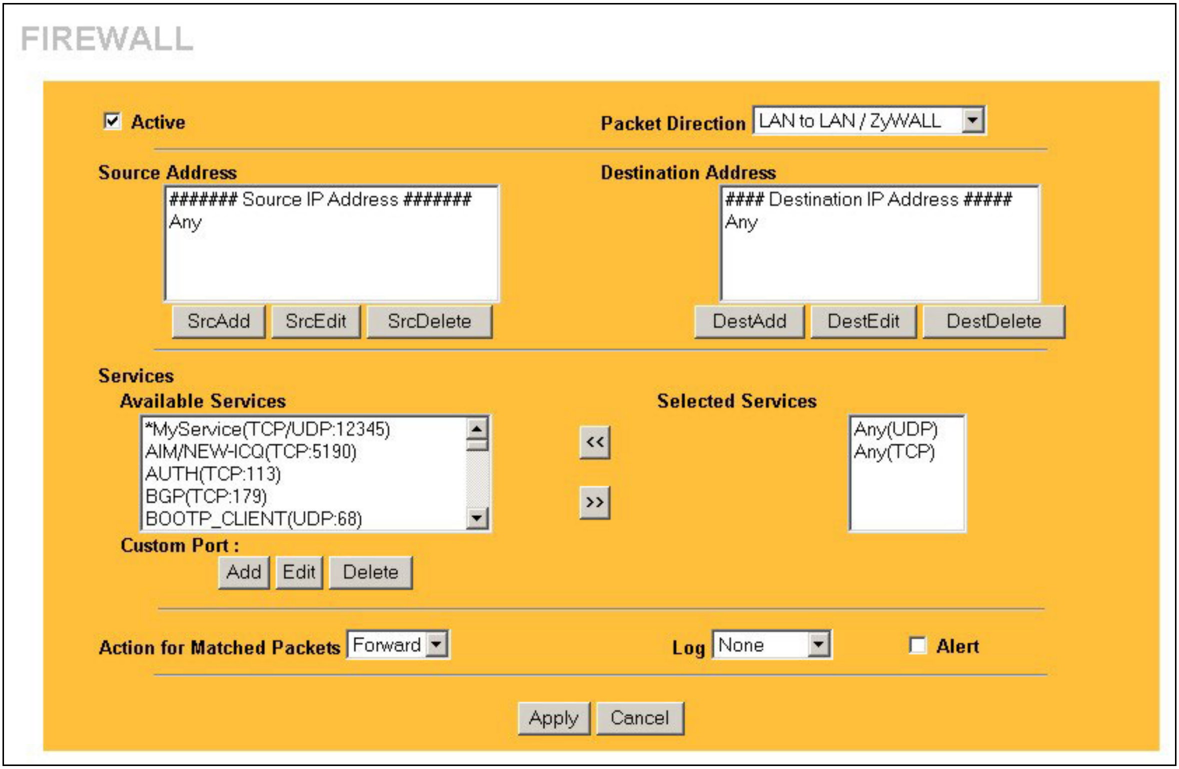
SERVICE	DESCRIPTION
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users 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.

16.5.1 Creating/Editing Firewall Rules

Follow these directions to create a new rule.

Step 1. In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

Step 2. Click **Insert** to display this screen and refer to the following table for information on the fields.



FIREWALL

☑ Active

Packet Direction: LAN to LAN / ZyWALL

Source Address

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

Destination Address

Destination IP Address
Any

Services

Available Services

*MyService(TCP/UDP:12345)
AIM/NEW-ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)
BOOTP_CLIENT(UDP:68)

Selected Services

Any(UDP)
Any(TCP)

Custom Port :

Action for Matched Packets: Forward

Log: None

□ Alert

Figure 16-4 Creating/Editing A Firewall Rule (ZyWALL100)

Table 16-3 Creating/Editing A Firewall Rule

FIELD	DESCRIPTION	OPTIONS
Active	Check the **Active** check box to have the ZyWALL use this rule. Leave it unchecked if you do not want the ZyWALL to use the rule after you apply it	

Table 16-3 Creating/Editing A Firewall Rule

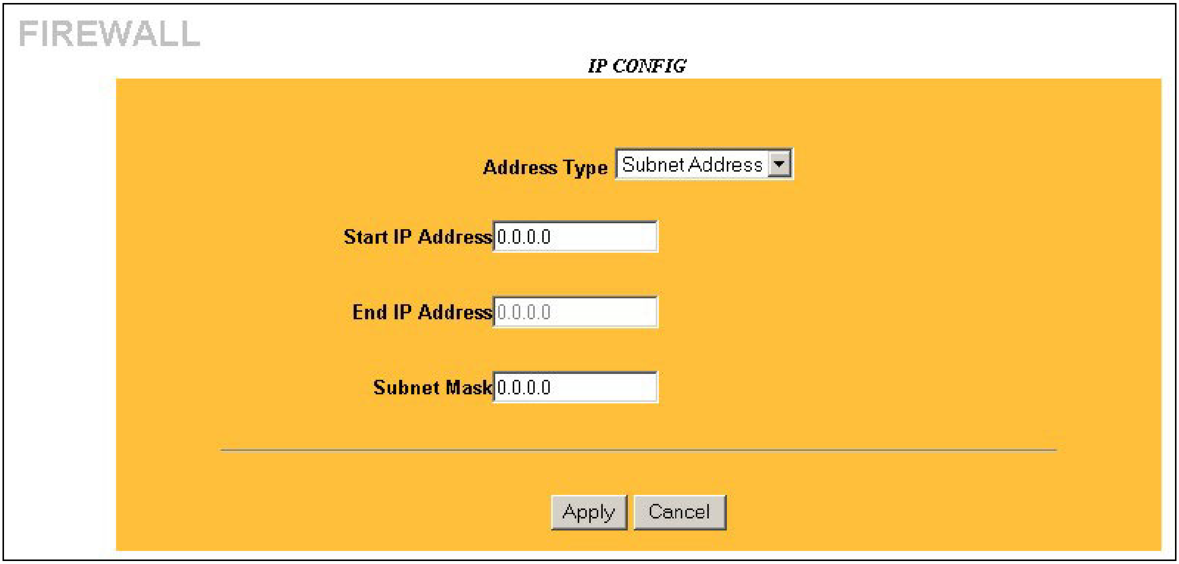
FIELD	DESCRIPTION	OPTIONS
Packet Direction	Use the drop-down list box to select the direction of packet travel to which you want to apply this firewall rule.	**LAN to LAN/ZyWALL** **LAN to WAN** **LAN to DMZ** **WAN to WAN/ZyWALL** **WAN to LAN** **WAN to DMZ** **DMZ to DMZ/ZyWALL** **DMZ to LAN** **DMZ to WAN**
Source Address	Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one. Please see the next section for more information on adding and editing source addresses.	**SrcAdd** **SrcEdit** **SrcDelete**
Destination Address	Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one. Please see the following section on adding and editing destination addresses.	**DestAdd** **DestEdit** **DestDelete**
Services Available/Selected Services	Please see *Table 16-2* for more information on services available. Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**.	**>>** **<<**
Custom Port		
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.	
Edit	Select a custom service (denoted by an "*") from the Available Services list and click this button to edit the service.	
Delete	Select a custom service (denoted by an "*") from the Available Services list and click this button to remove the service.	
Action for Matched Packets	Should packets that match this rule be blocked or forwarded? Make your choice from the drop down list box. Note that **Block** means the firewall silently discards the packet.	**Block** **Forward**

Table 16-3 Creating/Editing A Firewall Rule

FIELD	DESCRIPTION	OPTIONS
Log	This field determines if a log is created for packets that match the rule, don't match the rule, both or no log is created.	**Match** **Not Match** **Both** **None**
Alert	Check the **Alert** check box to determine that this rule generates an alert when the rule is matched.	
When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to exit this screen without saving, or **Help** for online HTML help on fields in this screen.		

16.5.2 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.



Address Type: Subnet Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Figure 16-5 Adding/Editing Source and Destination Addresses

Table 16-4 Adding/Editing Source and Destination Addresses

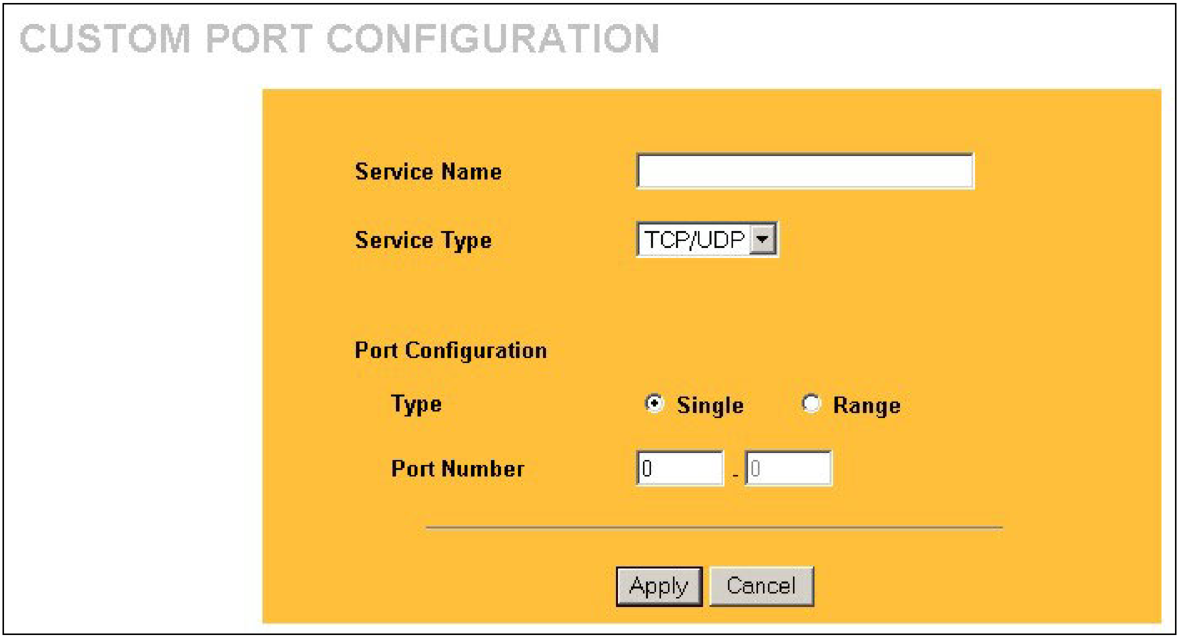
FIELD	DESCRIPTION	OPTIONS
Address Type	Do you want your rule to apply to packets with a particular (single) IP address, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop down list box	**Single Address** **Range Address** **Subnet Address** **Any Address**
Start IP Address	Enter the single IP address or the starting IP address in a range here.	
End IP Address	Enter the ending IP address in a range here.	
Subnet Mask	Enter the subnet mask here, if applicable.	
When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to exit this screen without saving, or **Help** for online HTML help on fields in this screen.		

16.6 Custom Ports

Configure customized ports for services not predefined by the ZyWALL (see *section 16.5* for a list of predefined services). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

16.7 Creating/Editing A Custom Port

Click the **Add** button under **Custom Port** while editing a firewall to configure a custom port. This displays the following screen.



CUSTOM PORT CONFIGURATION

Service Name

Service Type: TCP/UDP

Port Configuration

Type: ● Single ○ Range

Port Number: 0 - 0

Figure 16-6 Creating/Editing A Custom Port

The next table describes the fields in this screen.

Table 16-5 Creating/Editing A Custom Port

FIELD	DESCRIPTION	OPTIONS
Service Name	Enter a unique name for your custom port.	
Service Type	Choose the IP port (**TCP**, **UDP** or **Both**) that defines your customized port from the drop down list box.	**TCP** **UDP** **Both**
Port Configuration Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.	**Single** **Range**
Port Number	Enter a single port number or the range of port numbers that define your customized service.	
When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to exit this screen without saving, or **Help** for online HTML help on fields in this screen.		

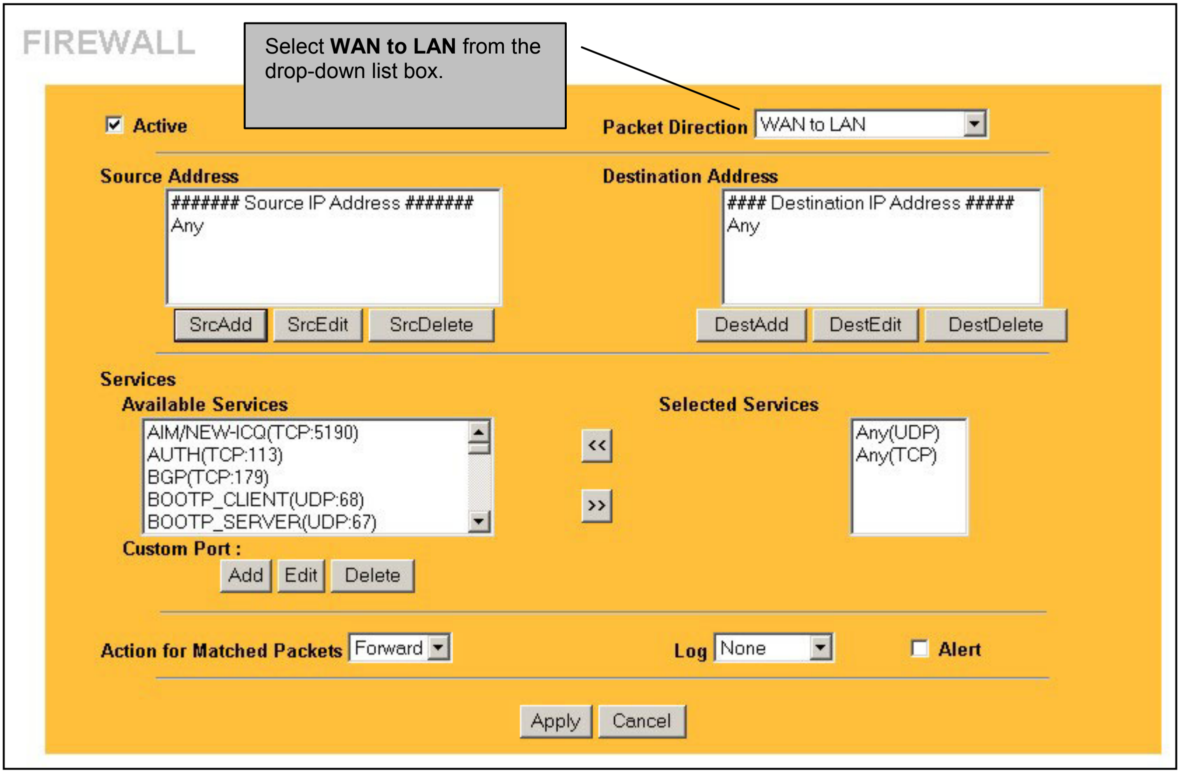
16.8 Example Firewall Rule

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

Step 1. Click the **Firewall** link and then the **Summary** tab.

Step 2. In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

Step 3. Click **Insert** to display the firewall rule configuration screen.



Select **WAN to LAN** from the drop-down list box.

FIREWALL

☑ Active

Packet Direction: WAN to LAN

Source Address

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

Destination Address

Destination IP Address
Any

Services

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

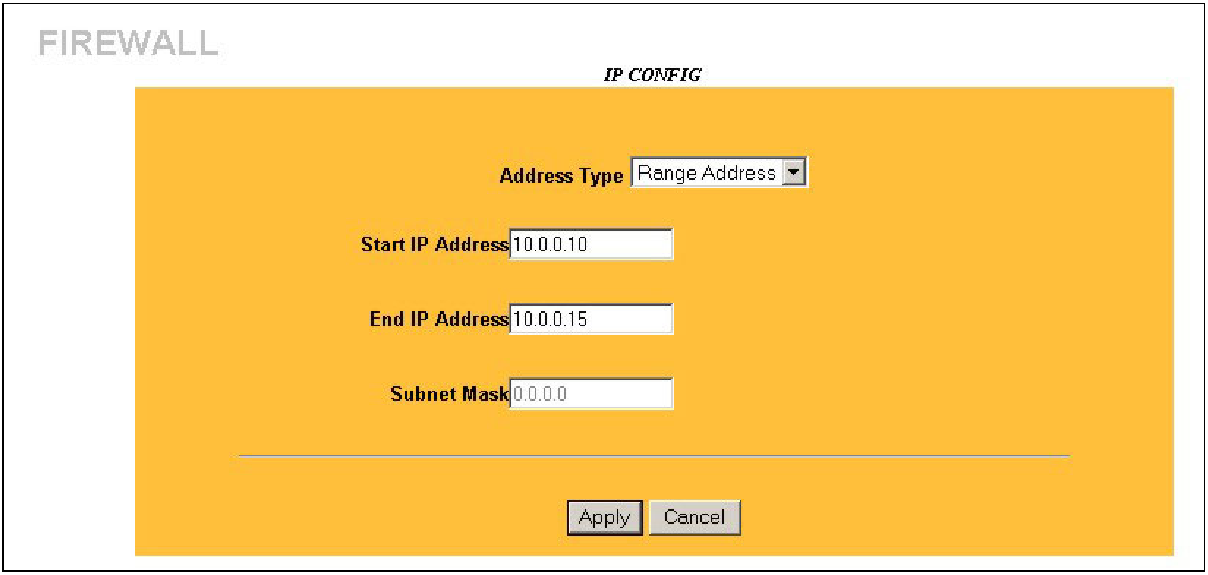
☐ Alert

Figure 16-7 Firewall Rule Configuration Screen (ZyWALL100)

Step 4. Click **Any** in the Source Address box and then click **ScrDelete**.

Step 5. Click **ScrAdd** under the Source Address box.

Step 6. Configure the **Firewall IP Config** screen as follows and click **Apply**.



FIREWALL

IP CONFIG

Address Type: Range Address

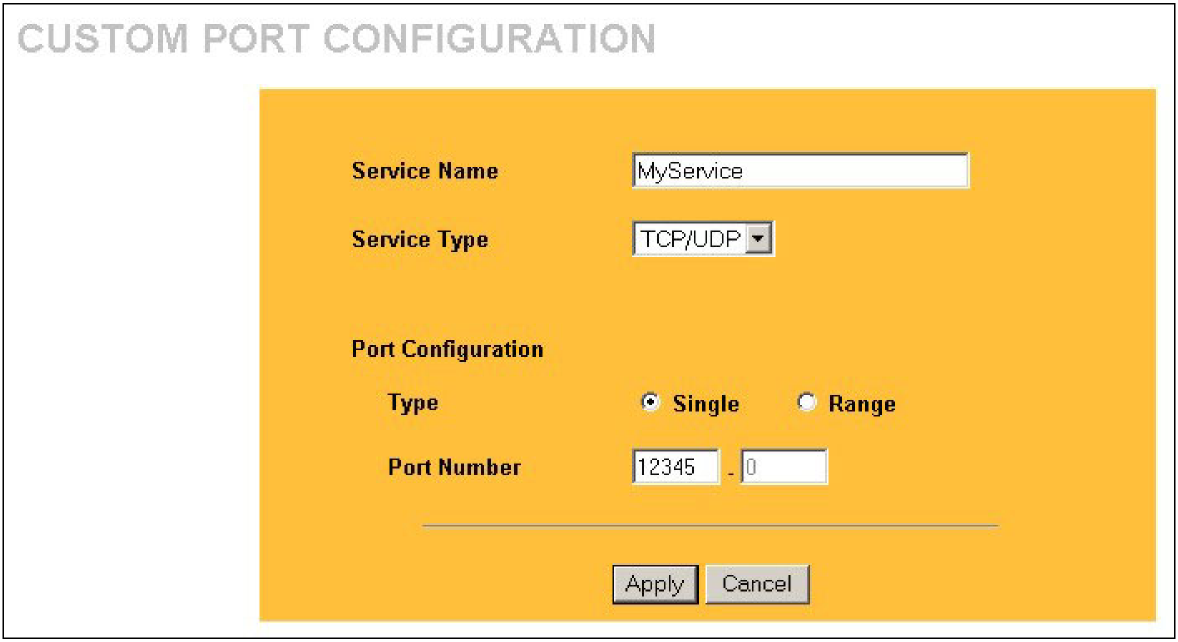
Start IP Address: 10.0.0.10

End IP Address: 10.0.0.15

Subnet Mask: 0.0.0.0

Figure 16-8 Firewall IP Config Screen

Step 7. In the firewall rule configuration screen, click **Add** under **Custom Port** to open the **Custom Port Configuration** screen. Configure it as follows and click **Apply**.



CUSTOM PORT CONFIGURATION

Service Name: MyService

Service Type: TCP/UDP

Port Configuration

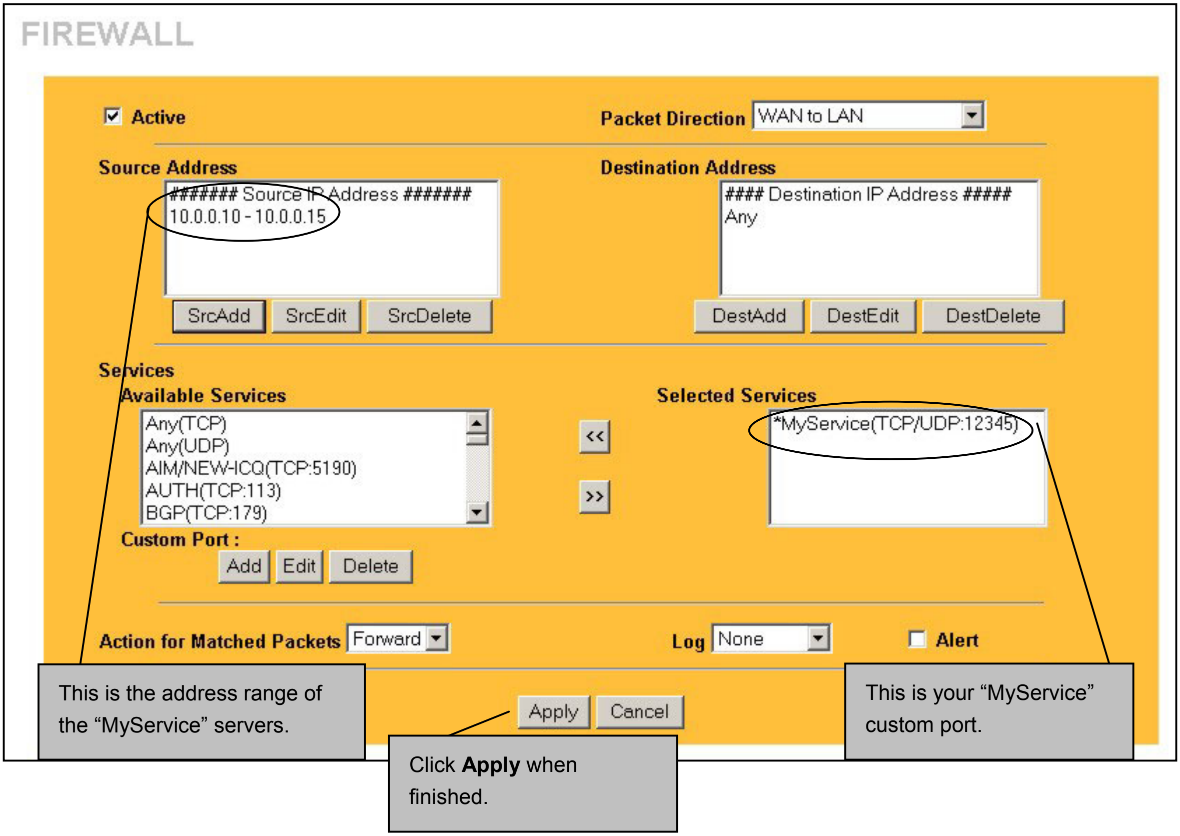
Type: ● Single ○ Range

Port Number: 12345 - 0

Figure 16-9 Custom Port for MyService

Step 8. The firewall rule configuration screen displays, use the arrows between **Available Services** and **Selected Services** to configure it as follows. Click **Apply** when you are done.

Custom ports 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 custom port.**



FIREWALL

☑ Active

Packet Direction: WAN to LAN

Source Address

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

Destination Address

Destination IP Address
Any

Services

Available Services

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

Selected Services

*MyService(TCP/UDP:12345)

Action for Matched Packets: Forward

Log: None

□ Alert

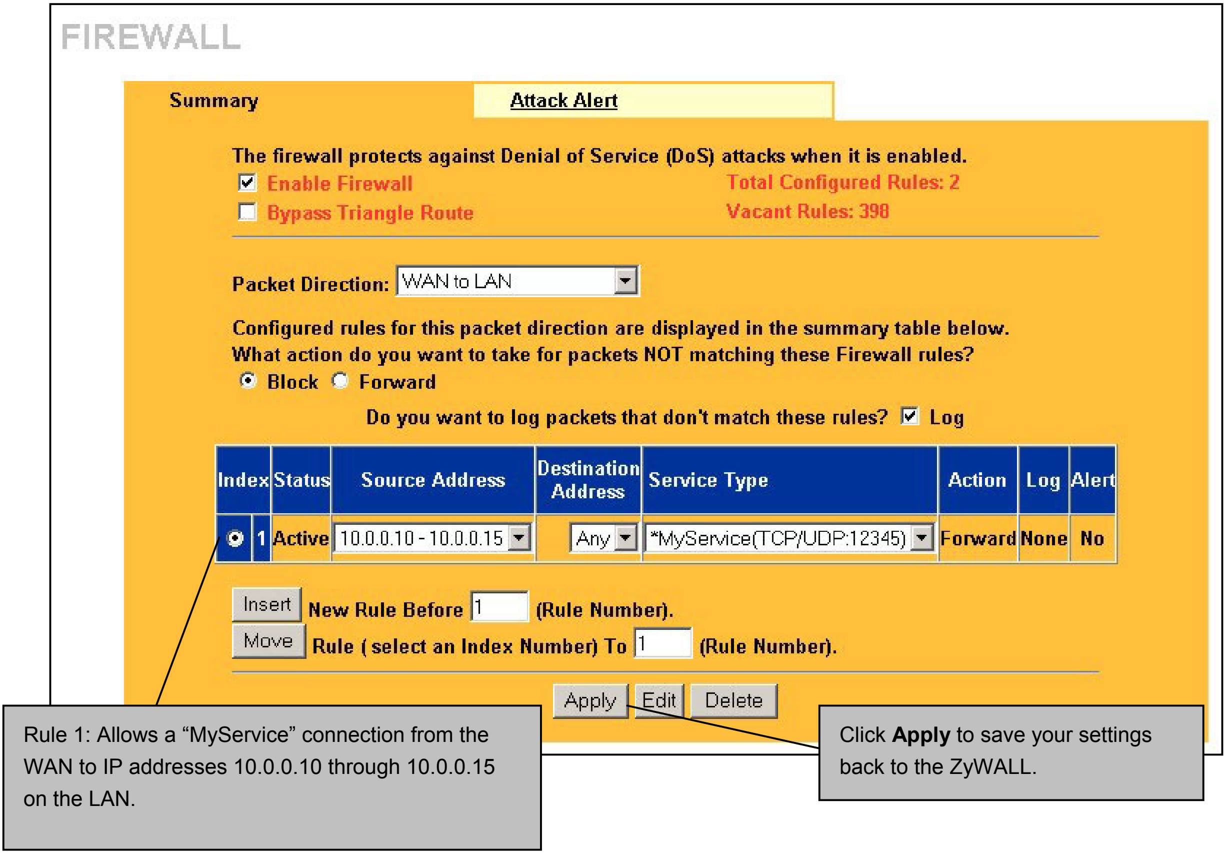
This is the address range of the “MyService” servers.

This is your “MyService” custom port.

Click **Apply** when finished.

Figure 16-10 MyService Rule Configuration (ZyWALL100)

Step 9. On completing the configuration procedure for this Internet firewall rule, the **Rule Summary** screen should look like the following. Remember to click **Apply** when you have finished configuring your rule(s) to save your settings back to the ZyWALL.



FIREWALL

The firewall protects against Denial of Service (DoS) attacks when it is enabled.

☑ Enable Firewall

□ Bypass Triangle Route

Total Configured Rules: 2

Vacant Rules: 398

Packet Direction: WAN to LAN

Configured rules for this packet direction are displayed in the summary table below.

What action do you want to take for packets NOT matching these Firewall rules?

● Block ○ Forward

Do you want to log packets that don't match these rules? ☑ Log

Index		Status	Source Address	Destination Address	Service Type	Action	Log	Alert
●	1	Active	10.0.0.10 - 10.0.0.15	Any	*MyService(TCP/UDP:12345)	Forward	None	No

Insert New Rule Before 1 (Rule Number).

Move Rule (select an Index Number) To 1 (Rule Number).

Rule 1: Allows a “MyService” connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

Click **Apply** to save your settings back to the ZyWALL.

Figure 16-11 Example 3: Rule Summary (ZyWALL100)

Chapter 17
Content Filtering

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

Internet content filtering allows schools and businesses to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URLs and should not be confused with packet filtering via SMT menu 21.1. To access these functions, from the **Main Menu**, click **Advanced**, then **Content Filter** to expand the Content Filter menus.

17.1 Categories

17.1.1 Restrict Web Features

The ZyWALL can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

17.1.2 Filter List

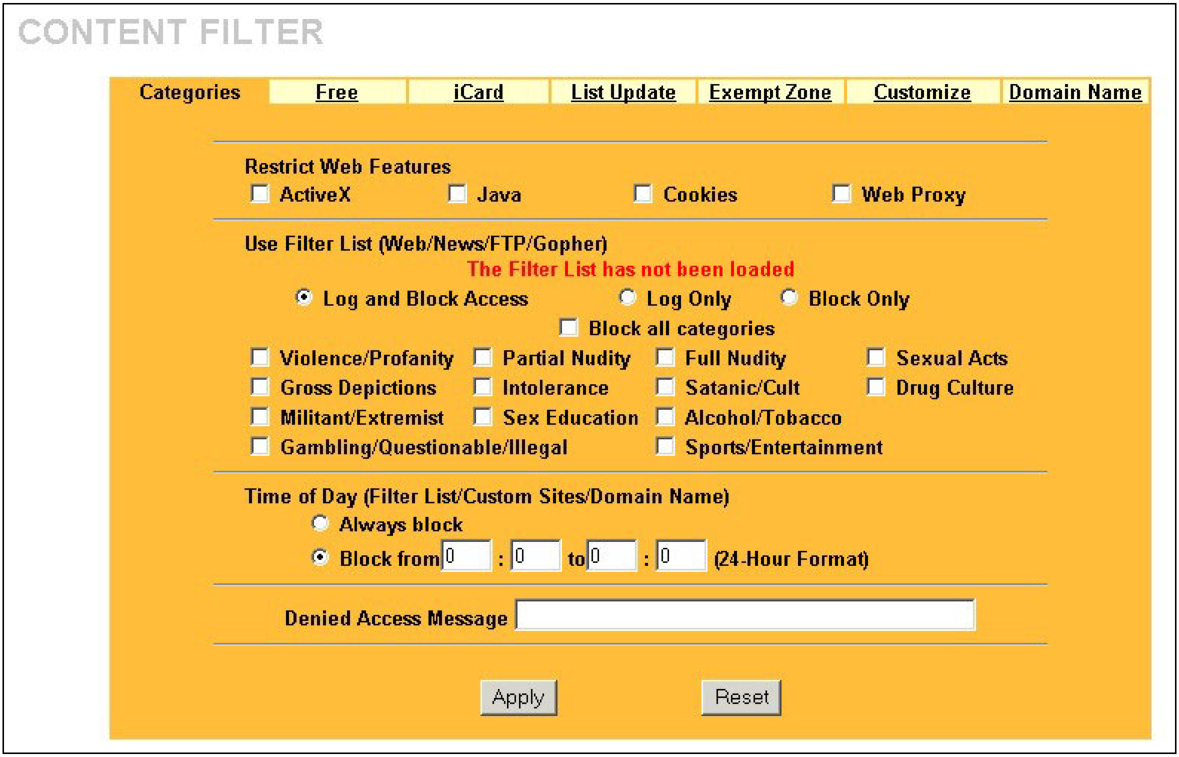
You can select categories, such as pornography or racial intolerance, to block or monitor from a pre-defined list. There is a period of free use of the list when you register the ZyWALL. After this period, you must subscribe to the list periodically.

17.1.3 Days and Times

The ZyWALL also allows you to define time periods and days during which content filtering should be enabled.

17.1.4 Configure Categories

Click **Content** on the navigation panel, and then the **Categories** tab to open the following screen.



CONTENT FILTER

Restrict Web Features

□ ActiveX □ Java □ Cookies □ Web Proxy

Use Filter List (Web/News/FTP/Gopher)

The Filter List has not been loaded

● Log and Block Access ○ Log Only ○ Block Only

□ Block all categories

□ Violence/Profanity □ Partial Nudity □ Full Nudity □ Sexual Acts

□ Gross Depictions □ Intolerance □ Satanic/Cult □ Drug Culture

□ Militant/Extremist □ Sex Education □ Alcohol/Tobacco

□ Gambling/Questionable/Illegal □ Sports/Entertainment

Time of Day (Filter List/Custom Sites/Domain Name)

○ Always block

● Block from 0 : 0 to 0 : 0 (24-Hour Format)

Denied Access Message

Figure 17-1Content Filter: Categories

Table 17-1 Content Filter: Categories

LABEL	DESCRIPTION
Restricted Web Features Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.	
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.

Table 17-1 Content Filter: Categories

LABEL	DESCRIPTION
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Use Filter List (Web/News/FTP/Gopher) You will see the message "The Filter List has not been loaded" if you have not yet downloaded the filter list or your subscription has expired.	
Log and Block Access	Click this option button to record attempts to access prohibited sites (as defined below) and prevent users from accessing these sites.
Log Only	Click this option button to just log user attempts to access prohibited sites (as defined below).
Block Only	Click this option button to prevent users from accessing prohibited sites (as defined below), but have no record made of attempts to access these sites.
Block all categories	Select this box to restrict access to all site categories listed below.
Violence/ Profanity	Selecting this category excludes pictures or text exposing extreme cruelty, or physical or emotional acts against any animal or person, which are primarily intended to hurt or inflict pain. Obscene words, phrases, and profanity are defined as text that uses, but is not limited to, George Carlin's seven censored words more often than once every 50 messages (Newsgroups) or once a page (Web sites).
Partial Nudity	Selecting this category excludes pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia.
Full Nudity	Selecting this category excludes pictures exposing any or all portions of the human genitalia.
Sexual Acts	Selecting this category excludes pictures or text exposing anyone or anything involved in explicit sexual acts and or lewd and lascivious behavior. Also includes phone sex ads, dating services, and adult personals, CD-ROM's and videos.

Table 17-1 Content Filter: Categories

LABEL	DESCRIPTION
Gross Depictions	Selecting this category excludes pictures or descriptive text of anyone or anything which are crudely vulgar or grossly deficient in civility or behavior, or which show scatological impropriety. Includes such depictions as maiming, bloody figures, or indecent depiction of bodily functions.
Intolerance	Selecting this category excludes pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Also includes intolerant jokes or slurs.
Satanic/Cult	Selecting this category excludes pictures or text advocating devil worship, an affinity for evil or wickedness, or the advocacy to join a cult. A cult is defined as a closed society headed by a single individual where loyalty is demanded and leaving is punishable.
Drug Culture	Selecting this category excludes pictures or text advocating the illegal use of drugs for entertainment. Includes substances used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This would exclude currently illegal drugs legally prescribed for medicinal purposes.
Militant/ Extremist	Selecting this category excludes pictures or text advocating extremely aggressive and combative behaviors, or advocacy of unlawful political measures. Topics include groups that advocate violence as a means to achieve their goals. Includes "how to" information on weapons making, ammunition making or the making or use of pyrotechnics materials. Also includes the use of weapons for unlawful reasons.
Sex Education	Selecting this category excludes pictures or text advocating the proper use of contraceptives. In addition, this category will include discussion sites on discussing diseases with a partner, pregnancy and respecting boundaries. Excluded from this category are commercial sites wishing to sell sexual paraphernalia.
Alcohol/Tobacco	Selecting this category excludes pictures or text advocating the sale, consumption, or production of alcoholic beverages and tobacco products.
Gambling/ Questionable/ Illegal	Selecting this category excludes pictures or text advocating materials or activities of a dubious nature which may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone's phone lines without permission) and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, on-line sports or financial betting, including non-monetary dares.

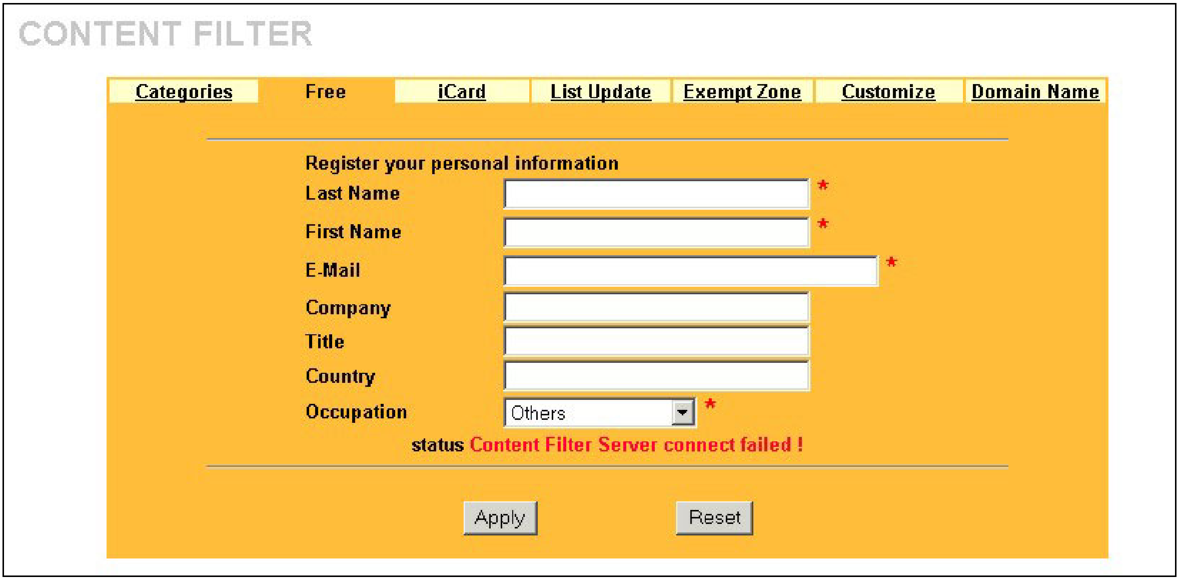
Table 17-1 Content Filter: Categories

LABEL	DESCRIPTION
Sports/ Entertainment	Selecting this category excludes pictures or text of leisure, sports, or other similar sites not considered applicable to the primary business function.
Time of Day (Filter List/Custom Sites/Domain Name) Time of Day allows the administrator to define time periods content filtering is enabled. Time of Day restrictions only apply to the Filter List (sites checked above), Customized sites and Keywords. Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected.	
Always Block	Click this option button to have content filtering always active with Time of Day limitations not enforced. This is enabled by default.
Block from	Click this option button to have content filtering only active during the time interval specified. Enter the time period, in 24-hour format, during which content filtering will be enforced.
Denied Access Message	Enter a message to be displayed when a user tries to access a restricted web site.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

17.2 Free

Click **Content** on the navigation panel, and then the **Free** tab to open the following screen.

Use this screen to register the ZyWALL. Registering the ZyWALL allows you to install and activate the Content Filter List, and to receive a free subscription to updated Content Filter Lists for a limited period. You may register your ZyWALL for the initial free subscription in this page by filling in your personal information in the fields and then clicking **Apply**. You must fill in all required fields (denoted by an asterisk).



CONTENT FILTER

Register your personal information

Last Name *

First Name *

E-Mail *

Company

Title

Country

Occupation: Others *

status Content Filter Server connect failed !

Figure 17-2 Content Filter: Free

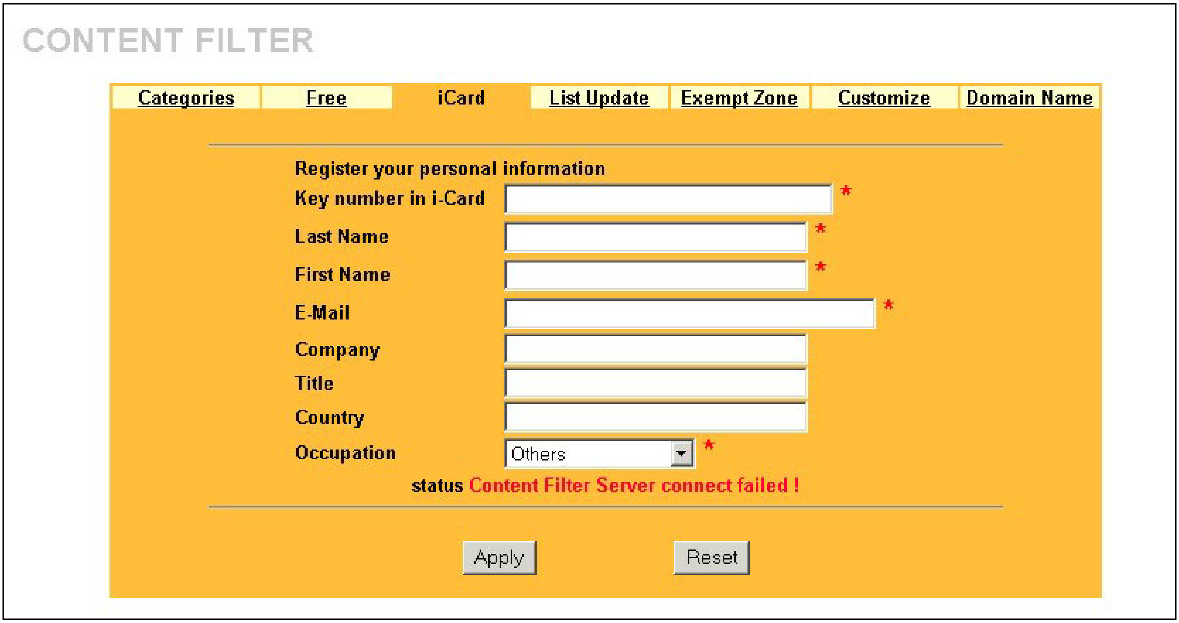
Table 17-2 Content Filter: Free

LABEL	DESCRIPTION
Last Name	Type your last name. You may enter up to 31 characters. This is a required field.
First Name	Type your first name. You may enter up to 31 characters. This is a required field.
E-mail	Type your e-mail address. You may enter up to 40 characters. This is a required field.
Company	Type the name of your company. You may enter up to 31 characters.
Title	Type your job title. You may enter up to 31 characters.
Country	Type your country name. You may enter up to 31 characters.
Occupation	Select the industry you work in from this drop-down list box. This is a required field.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

17.3 iCard

Click **Content** on the navigation panel, and then the **iCard** tab to open the following screen.

Use this screen to register the ZyWALL. Registering the ZyWALL allows you to install and activate the Content Filter List and to receive a free subscription to updated Content Filter Lists for a limited period. When the initial free subscription period expires, update your subscription in this page by filling in your personal information in the fields as shown, and then click Apply. You must fill in all required fields (marked with an asterisk).



Register your personal information

Key number in i-Card	*
Last Name	*
First Name	*
E-Mail	*
Company	
Title	
Country	
Occupation	Others *

status Content Filter Server connect failed !

Figure 17-3 Content Filter: iCard

Table 17-3 Content Filter: iCard

LABEL	DESCRIPTION
Key number in I-Card	Type the key from your subscription card (required field).
Last Name	Type your last name. You may enter up to 31 characters (required field).
First Name	Type your first name. You may enter up to 31 characters (required field).

Table 17-3 Content Filter: iCard

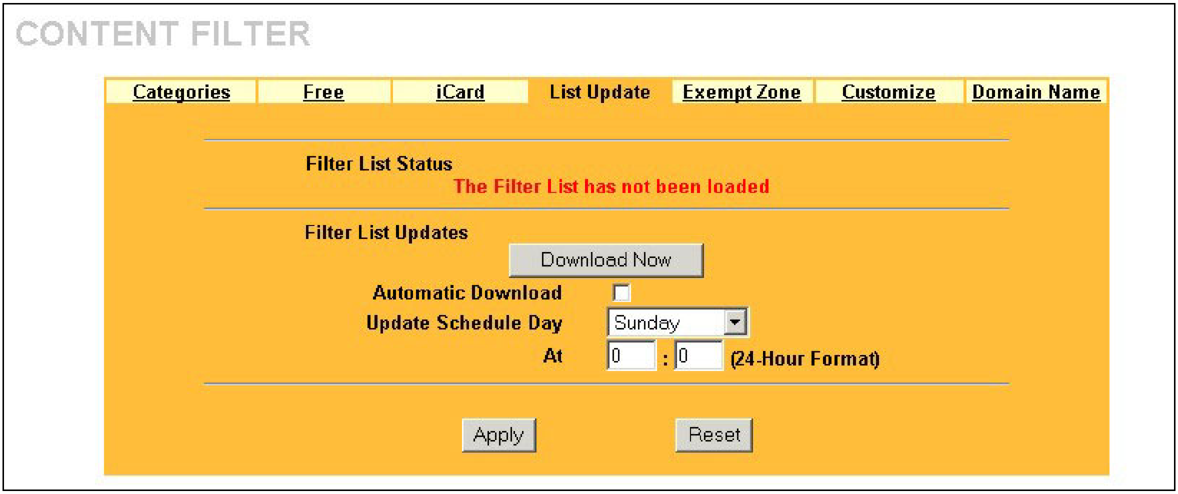
LABEL	DESCRIPTION
E-mail	Type your e-mail address. You may enter up to 40 characters (required field).
Company	Type the name of your company. You may enter up to 31 characters.
Title	Type your job title. You may enter up to 31 characters.
Country	Type your country name. You may enter up to 31 characters.
Occupation	Select the industry you work in from this drop-down list box (required field).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

17.4 List Update

Click **Content** on the navigation panel, and then the **List Update** tab to open the following screen.

The "The Filter List has not been loaded" message displays if you have not yet downloaded the filter list or your subscription has expired.

Content on the Internet is constantly changing, so the content filter list should be updated on a weekly basis.



CONTENT FILTER

Filter List Status

The Filter List has not been loaded

Filter List Updates

Automatic Download □

Update Schedule Day: Sunday

At: 0 : 0 (24-Hour Format)

Figure 17-4 Content Filter: List Update

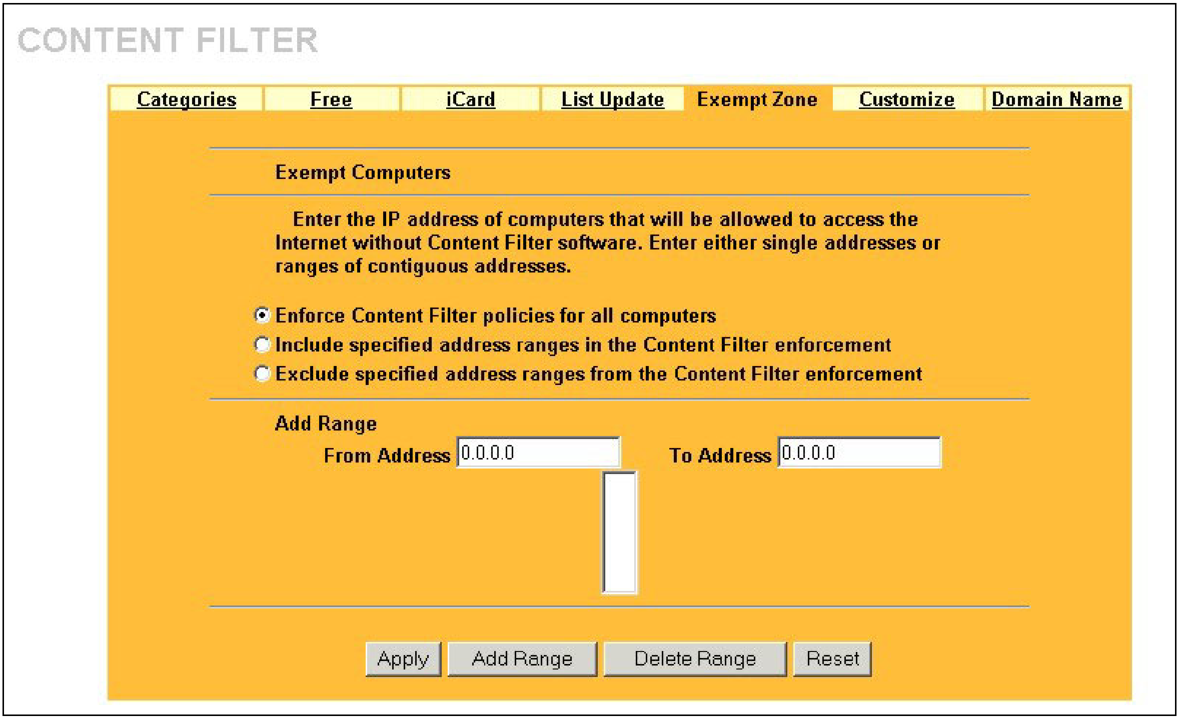
Table 17-4 Content Filter: List Update

LABEL	DESCRIPTION
Download Now	Click **Download Now** to download and install a new Content Filter List. This process may take a couple of minutes, depending on Internet traffic conditions and requires a current subscription to the Content Filter List. It is a good idea to download new lists when LAN access to the Internet is at a minimum.
Automatic Download	Select this check box to enable automatic weekly downloads of the Content Filter List.
Update Schedule Day	Select the day of the week, from the drop-down menu, that the new list should be retrieved. A current subscription to the Content Filter List updates is required.
At	Type the time in 24-hour format when the new Content Filter List should be retrieved. It is a good idea to choose a day and time when LAN traffic to the Internet is at a minimum.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

17.5 Exempt Computers

Click **Content** on the navigation panel, and then the **Exempt Zone** tab to open the following screen.

Use this screen to include or exclude a range of users on the LAN from content filtering.



CONTENT FILTER

Exempt Computers

Enter the IP address of computers that will be allowed to access the Internet without Content Filter software. Enter either single addresses or ranges of contiguous addresses.

● Enforce Content Filter policies for all computers
○ Include specified address ranges in the Content Filter enforcement
○ Exclude specified address ranges from the Content Filter enforcement

Add Range

From Address 0.0.0.0 To Address 0.0.0.0

Figure 17-5 Content Filter: Exempt Zone

Table 17-5 Content Filter: Exempt Zone

LABEL	DESCRIPTION
Enforce Content Filter policies for all computers	Select to have all users on your LAN follow Content Filter policies (default).
Include specified address ranges in the Content Filter enforcement	Select to have a specific range of users on your LAN follow Content Filter policies.

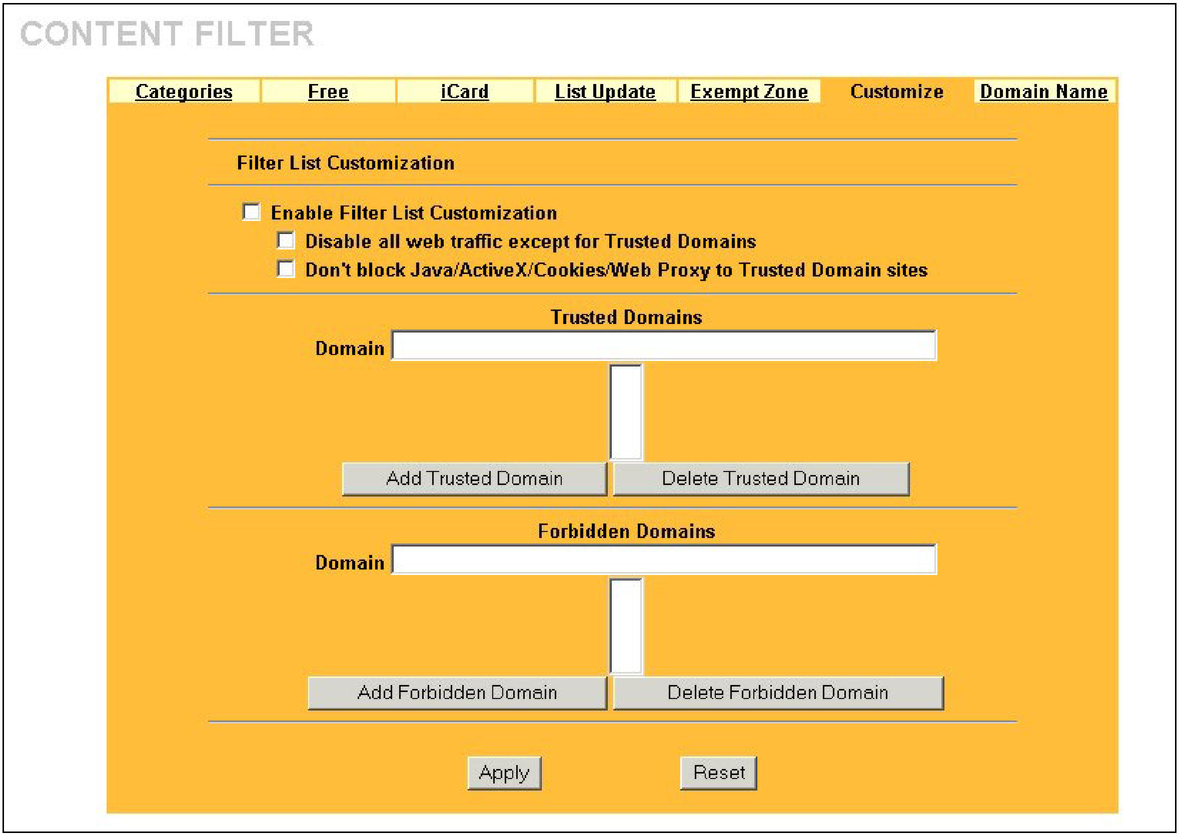
Table 17-5 Content Filter: Exempt Zone

LABEL	DESCRIPTION
Exclude specified address ranges from the Content Filter enforcement	Select to exempt a specific range of users on your LAN from Content Filter policies.
Add Range	Fill in the two fields below if you selected one of the last two options above.
From Address	Type the beginning IP address of the specific range of users on your LAN.
To Address	Type the ending IP address of the specific range of users on your LAN, then click **Add Range**.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Add Range	Click **Add Range** after you have filled in the From Address and To Address fields above.
Delete Range	Click **Delete Range** after you select the range of addresses you wish to delete.
Reset	Click **Reset** to begin configuring this screen afresh.

17.6 Customizing

Click **Content** on the navigation panel, and then the **Customize** tab to open the following screen.

Use this screen to customize the content filter list by adding or removing specific sites from the filter list.



CONTENT FILTER

Filter List Customization

☐ Enable Filter List Customization

☐ Disable all web traffic except for Trusted Domains

☐ Don't block Java/ActiveX/Cookies/Web Proxy to Trusted Domain sites

Trusted Domains

Domain

Forbidden Domains

Domain

Figure 17-6 Content Filter: Customize

Table 17-6 Content Filter: Customize

LABEL	DESCRIPTION
Filter List Customization Make sure the **Enable Filter List Customization** check box is selected to make this feature available. Add or remove sites from the Filter List to customize the Content Filter List.	
Enable Filter List Customization	Select this check box to allow **Trusted Domain** web sites and block **Forbidden Domain** web sites. Content Filter List Customization may be enabled and disabled without re-entering all site names. Sites also do not have to be re-entered when the Content Filter List is updated each week.

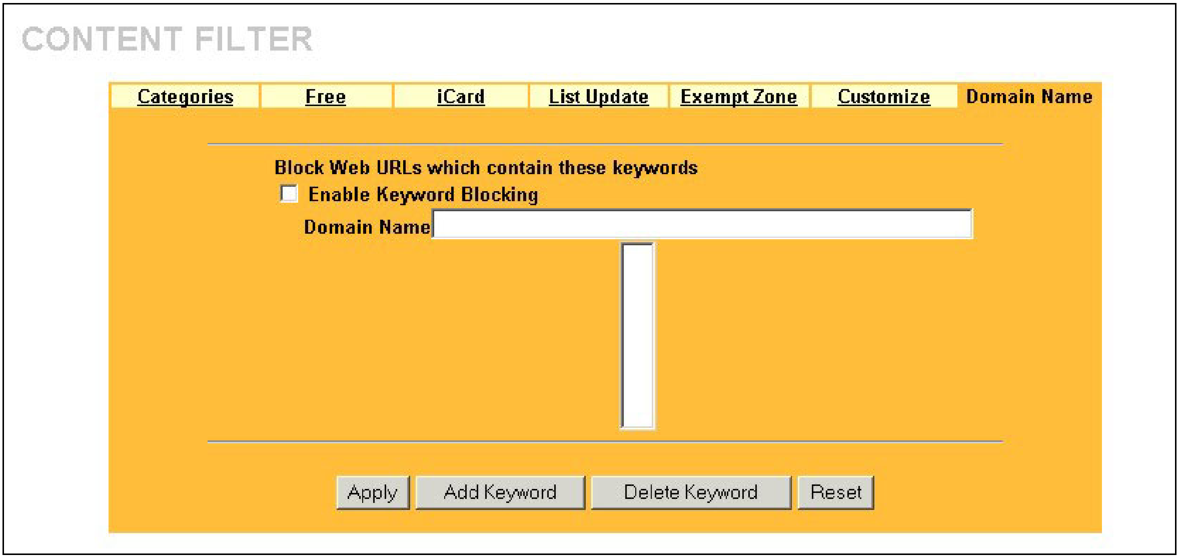
Table 17-6 Content Filter: Customize

LABEL	DESCRIPTION
Disable all web traffic except for Trusted Domains	When this box is selected, ZyWALL only allows Web access to sites on the **Trusted Domains** list. If **Trusted Domains** are chosen carefully, this is the most effective way to block objectionable material.
Don't block Java/ActiveX/Cookies/Web Proxy to Trusted Domains sites	When this box is selected, ZyWALL will permit Java, ActiveX and Cookies from sites on the **Trusted Domains** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Add or delete a Trusted Domain to the Content Filter List. Up to 32 entries are supported in this list.	
Domain	Enter host names such as "www.good-site.com" into this text field. Do not enter the complete URL of the site - that is, do not include "http://". All subdomains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", etc.
Add Trusted Domain	Click **Add Trusted Domain** when you have finished adding the host name in the text field above.
Delete Trusted Domain	Select a domain name from the Trusted Domain list, and then click **Delete Trusted Domain** to delete it from that list.
Forbidden Domains Sites that are not objectionable (not in the Content Filter List), but are considered inappropriate may be blocked by adding them to the Forbidden Domains list. Up to 32 entries are supported in this list.	
Domain	Enter its host name, such as "www.bad-site.com" into this text field. Do not enter the complete URL of the site - that is, do not include "http://". All subdomains are also blocked.
Add Forbidden Domain	Click **Add Forbidden Domain** when you have finished adding the host name in the text field above.
Delete Forbidden Domain	Select a domain name from the **Forbidden Domain** list, and then click **Delete Forbidden Domain** to delete it from that list.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

17.7 Domain Name

Click **Content** on the navigation panel, and then the **Domain Name** tab to open the following screen.

Use this screen to configure the ZyWALL to block Web sites containing keywords in their URLs. For example, if you enable the keyword "bad", the ZyWALL blocks all sites containing this keyword, for example, the ZyWALL blocks URL http://www.website.com/bad.html, even if it is not included in the Filter List. This functions as a second line of defense against objectionable material.



Block Web URLs which contain these keywords

□ Enable Keyword Blocking

Domain Name

Figure 17-7 Content Filter: Domain Name

Table 17-7 Content Filter: Domain Name

LABEL	DESCRIPTION
Enable Keyword Blocking	Select this check box to enable this feature.
Domain Name	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.
Apply	Click **Apply** to save your changes back to the ZyWALL.

Table 17-7 Content Filter: Domain Name

LABEL	DESCRIPTION
Add Keyword	Click **Add Keyword** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the Content Filter is blocking this request.
Delete Keyword	Highlight a keyword in the lower box and click **Delete Keyword** to remove it. The keyword disappears from the text box after you click **Apply**.
Reset	Click **Reset** to begin configuring this screen afresh.

Part V:

Logs, Filter Configuration, and SNMP Configuration

This part provides information and configuration instructions for the logs, filters, and SNMP.

Chapter 18
Centralized Logs

This chapter contains information about configuring general log settings and viewing the ZyWALL's logs. Refer to the appendices for example log message explanations and how to view the logs via the SMT command interface.

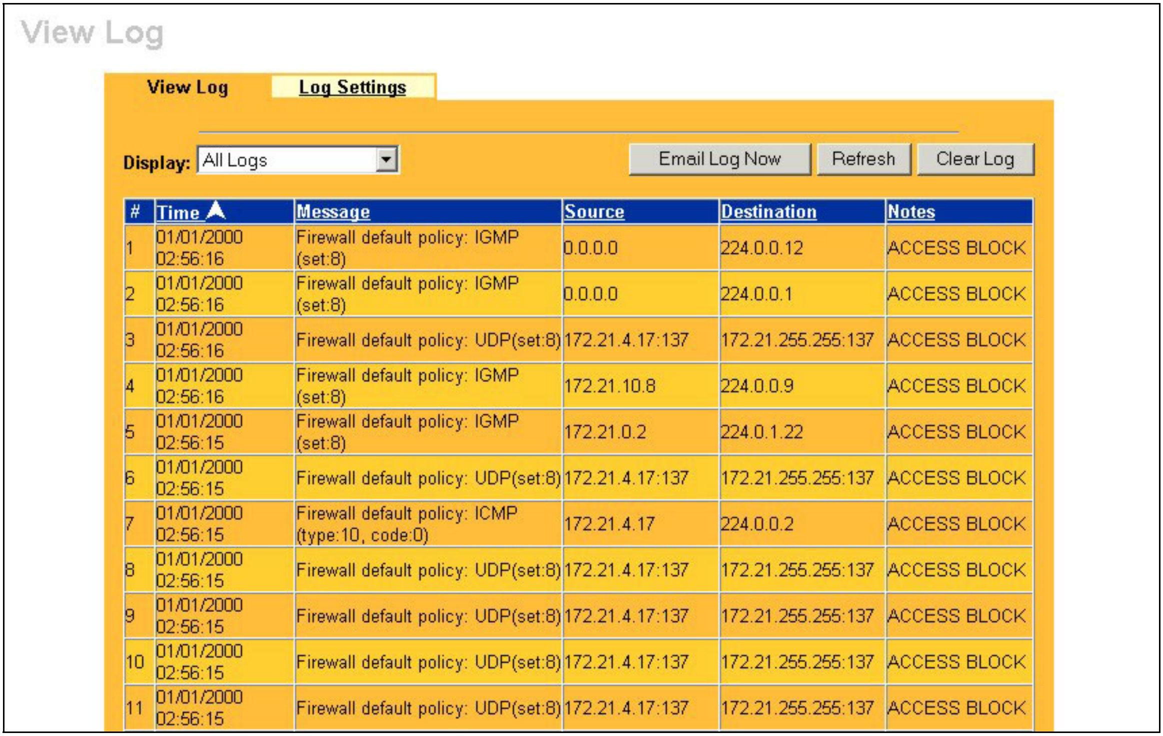
18.1 View Log

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

Click the **Advanced** and then **Logs** links in the navigation panel to open the **View Log** screen.

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see *section 18.2*). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

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



Display: All Logs

#	Time	Message	Source	Destination	Notes
1	01/01/2000 02:56:16	Firewall default policy: IGMP (set:8)	0.0.0.0	224.0.0.12	ACCESS BLOCK
2	01/01/2000 02:56:16	Firewall default policy: IGMP (set:8)	0.0.0.0	224.0.0.1	ACCESS BLOCK
3	01/01/2000 02:56:16	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
4	01/01/2000 02:56:16	Firewall default policy: IGMP (set:8)	172.21.10.8	224.0.0.9	ACCESS BLOCK
5	01/01/2000 02:56:15	Firewall default policy: IGMP (set:8)	172.21.0.2	224.0.1.22	ACCESS BLOCK
6	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
7	01/01/2000 02:56:15	Firewall default policy: ICMP (type:10, code:0)	172.21.4.17	224.0.0.2	ACCESS BLOCK
8	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
9	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
10	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
11	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK

Figure 18-1 View Log

Table 18-1 View Log

FIELD	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see *section 18.2*) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the ZyWALL’s time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.

Table 18-1 View Log

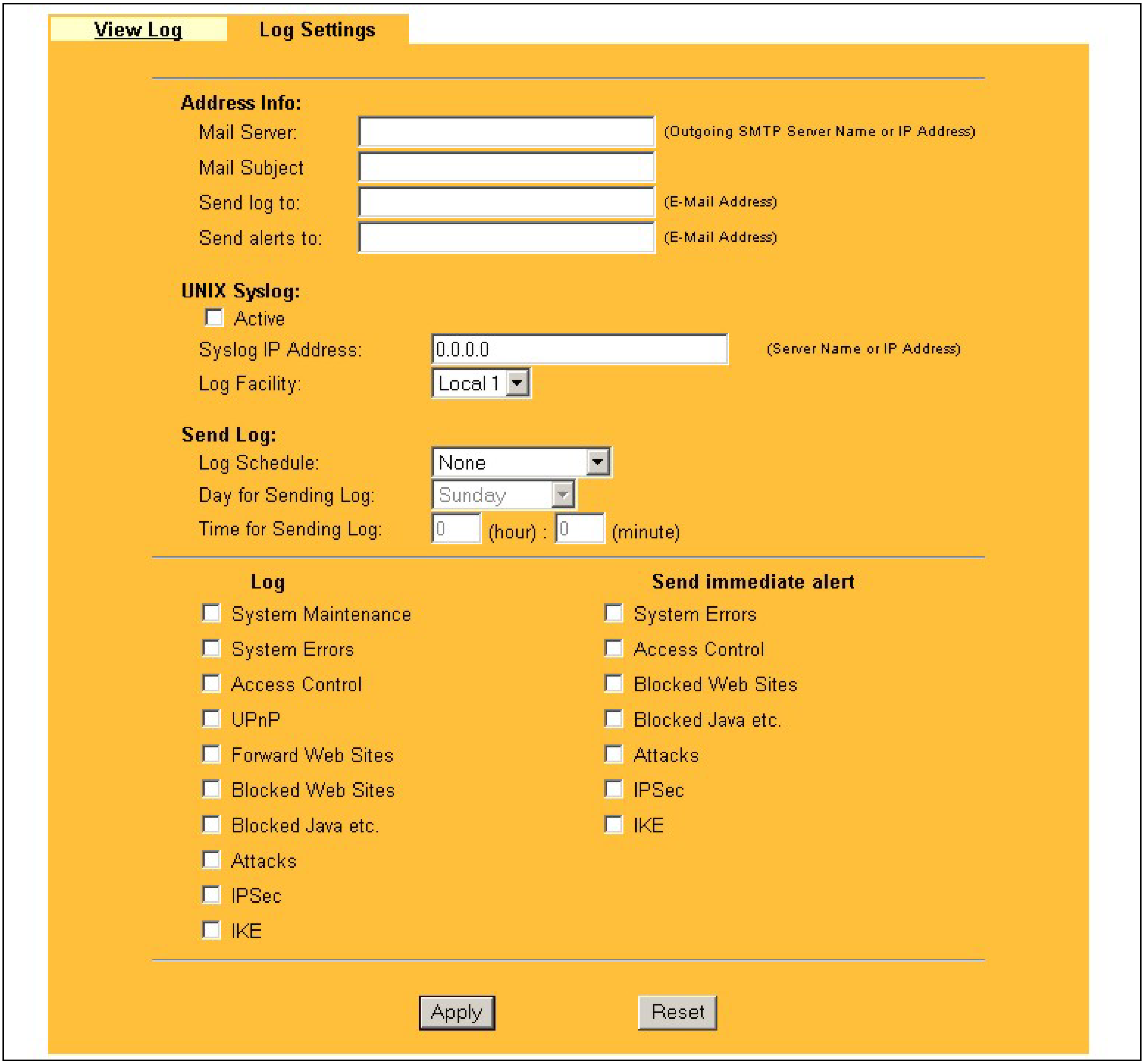
FIELD	DESCRIPTION
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**, see *section 18.2*).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

18.2 Log Settings

You can configure the ZyWALL's general log settings in one location.

Click the **Advanced**, and then **Logs** links on the navigation panel and then the **Log Settings** tab to open the **Log Settings** screen.

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



Address Info:

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject

Send log to: (E-Mail Address)

Send alerts to: (E-Mail Address)

UNIX Syslog:

□ Active

Syslog IP Address: 0.0.0.0 (Server Name or IP Address)

Log Facility: Local 1

Send Log:

Log Schedule: None

Day for Sending Log: Sunday

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

Log	Send immediate alert
□ System Maintenance	□ System Errors
□ System Errors	□ Access Control
□ Access Control	□ Blocked Web Sites
□ UPnP	□ Blocked Java etc.
□ Forward Web Sites	□ Attacks
□ Blocked Web Sites	□ IPSec
□ Blocked Java etc.	□ IKE
□ Attacks	
□ IPSec	
□ IKE	

Figure 18-2 Log Settings

Table 18-2 Log Settings Screen

FIELD	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.
Send Log To	The ZyWALL sends logs to the e-mail address specified in this field. If this field is left blank, the ZyWALL does not send logs via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyWALL sends.
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the e-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via e-mail.
UNIX Syslog	UNIX syslog sends a log to an external UNIX server used to store logs.
Active	Click **Active** to enable UNIX syslog.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to your UNIX manual for more information.
Send Log	

Table 18-2 Log Settings Screen

FIELD	DESCRIPTION
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • **Daily** • **Weekly** • **Hourly** • **When the Log is Full** • **None.** If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select a log category for which you want the ZyWALL to send immediately e-mail alerts.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 19
Filter Configuration

This chapter shows you how to create and apply filters.

19.1 About Filtering

Your ZyWALL 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. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

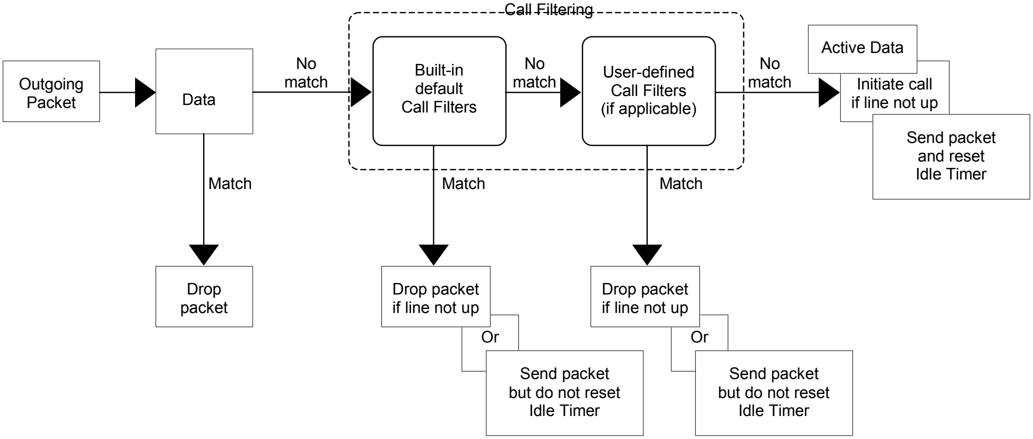

Call Filtering
Outgoing Packet
Data
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset Idle Timer
Drop packet if line not up
Or
Send packet but do not reset Idle Timer

Figure 19-1 Outgoing Packet Filtering Process

For incoming packets, your ZyWALL applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

19.1.1 The Filter Structure of the ZyWALL

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 ZyWALL 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 19-7* for the logic flow when executing an IP filter.

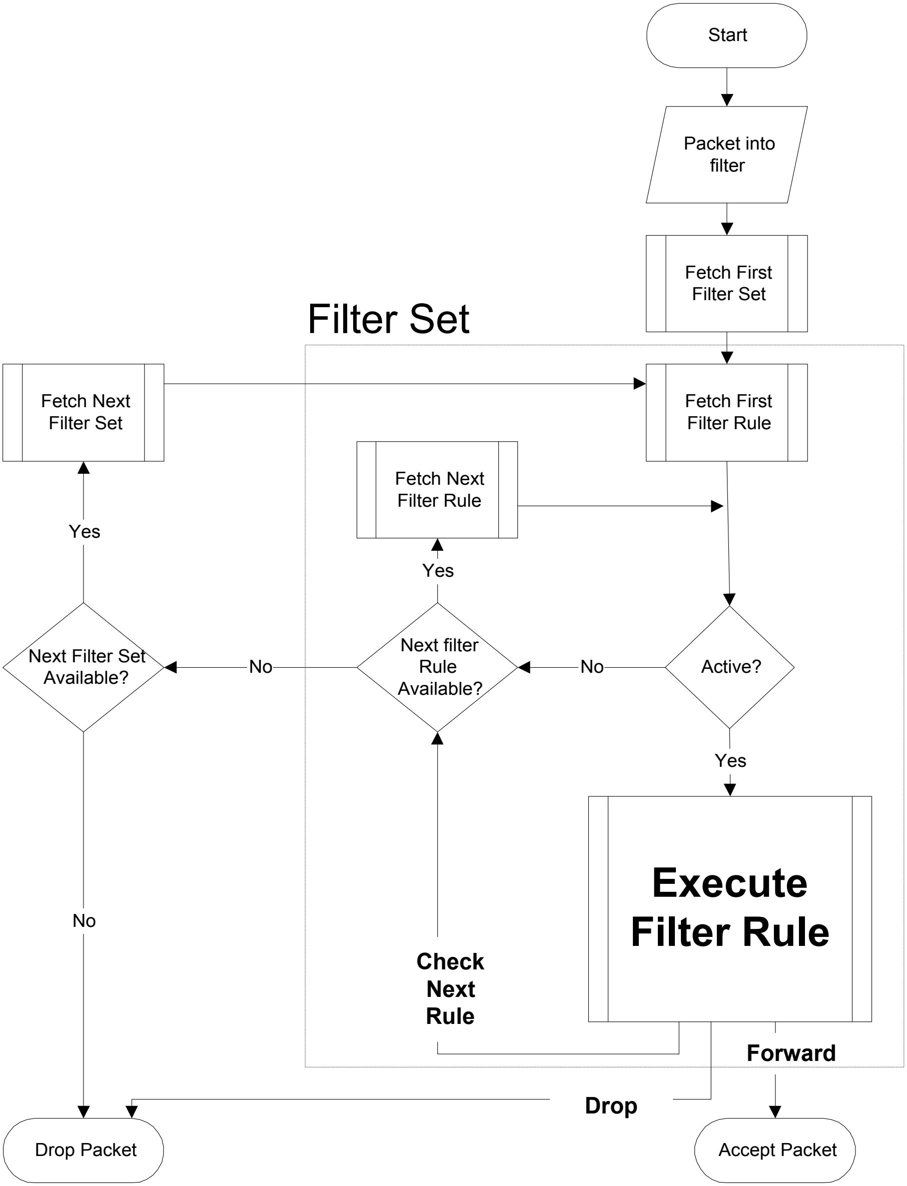


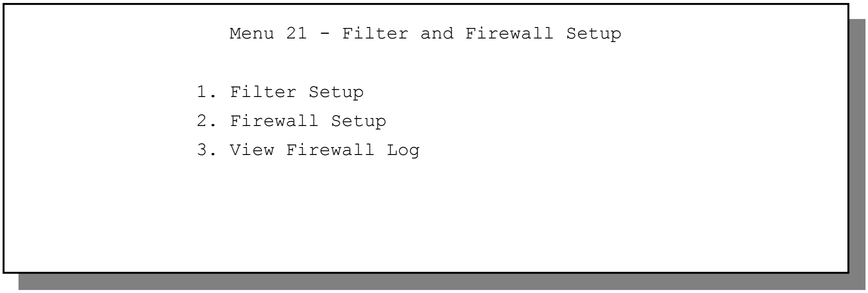
Figure 19-2 Filter Rule Process

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.

19.2 Configuring a Filter Set

The ZyWALL includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

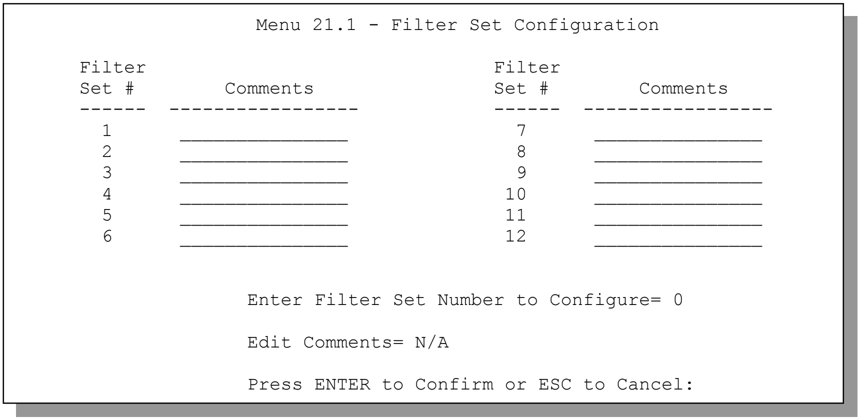
Step 1. Enter 21 in the main menu to open menu 21.



```
                    Menu 21 - Filter and Firewall Setup

                 1. Filter Setup
                 2. Firewall Setup
                 3. View Firewall Log
```

Figure 19-4 Menu 21: Filter and Firewall Setup

Step 2. Enter 1 to bring up the following menu.



```
                    Menu 21.1 - Filter Set Configuration

      Filter                                 Filter
      Set #        Comments                  Set #        Comments
      ------  -----------------              ------  -----------------
        1      _______________                 7      _______________
        2      _______________                 8      _______________
        3      _______________                 9      _______________
        4      _______________                10      _______________
        5      _______________                11      _______________
        6      _______________                12      _______________

                      Enter Filter Set Number to Configure= 0

                      Edit Comments= N/A

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

Figure 19-5 Menu 21.1: Filter Set Configuration

Step 3. Select the filter set you wish to configure (1-12) and press [ENTER].

Step 4. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

Table 19-1 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 19-2 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.

19.2.1 Configuring a Filter Rule

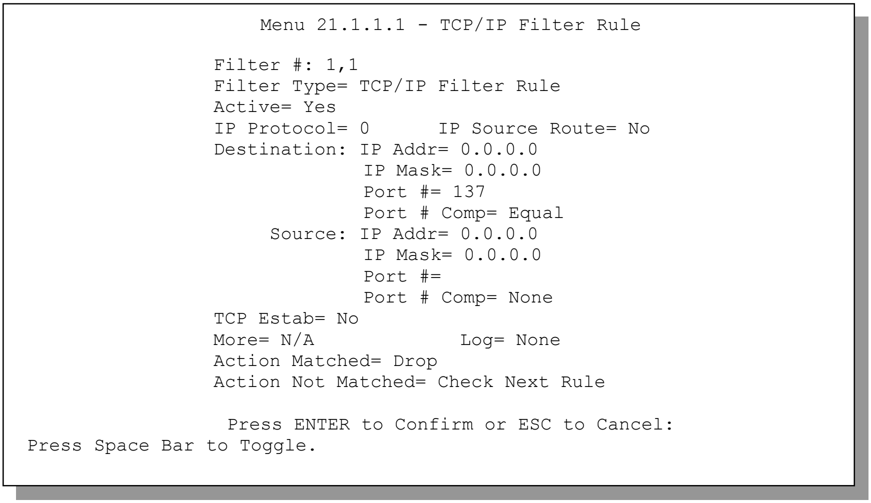
To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

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 ZyWALL will warn you and will not allow you to save.

19.2.2 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 21.1.1.1 - TCP/IP Filter Rule**, as shown next.



```
                     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= No
                 More= N/A             Log= None
                 Action Matched= Drop
                 Action Not Matched= Check Next Rule

                  Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 19-6 Menu 21.1.1.1: TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 19-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
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

Table 19-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
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
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**

Table 19-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
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 21.1.1.1 - 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 21.1.1 - Filter Rules Summary**.		

The following figure illustrates the logic flow of an IP filter.

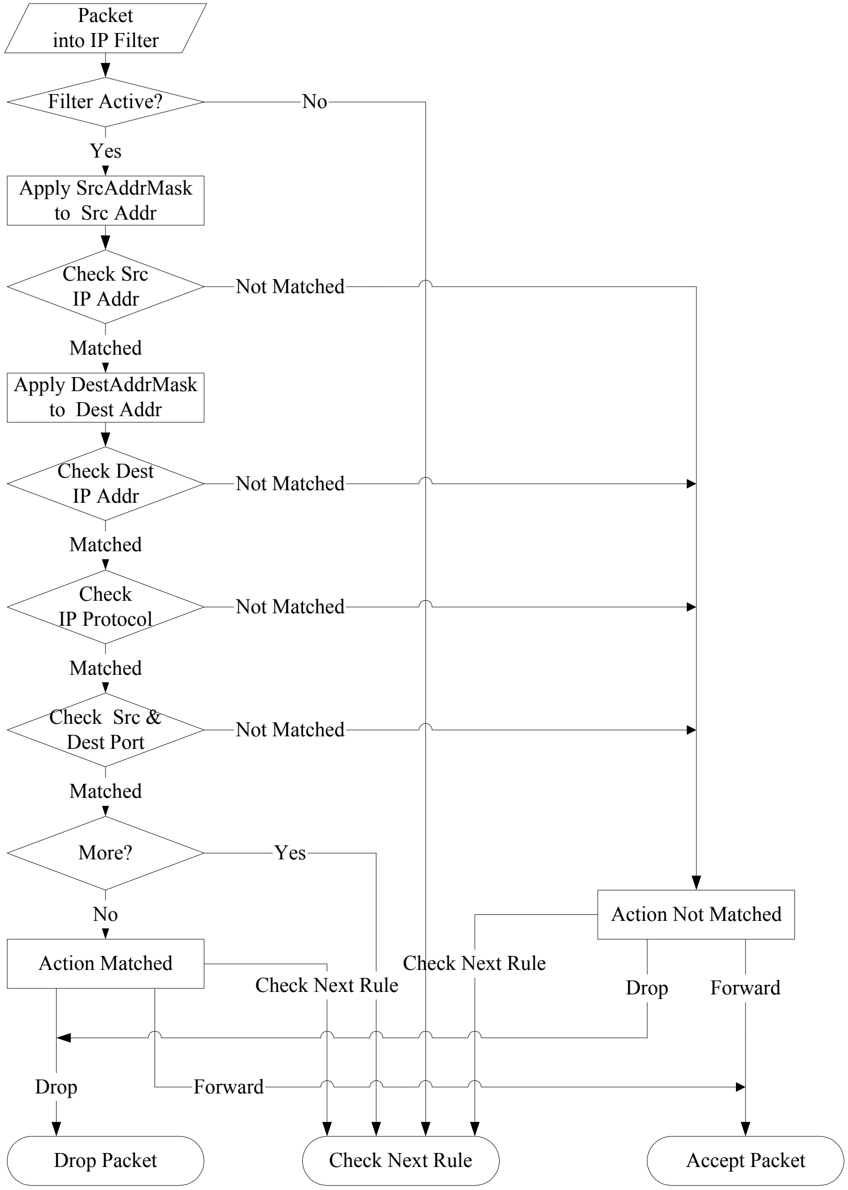


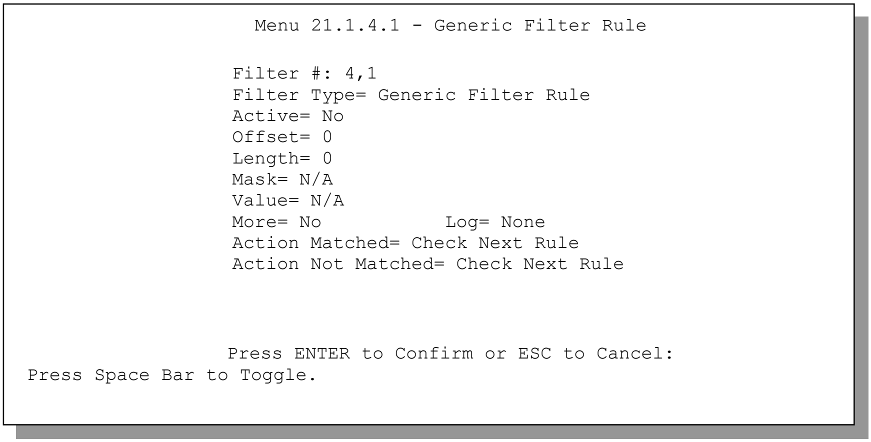
Figure 19-7 Executing an IP Filter

19.2.3 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 ZyWALL 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 ZyWALL 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 21.1.4.1 and press [ENTER] to open Generic Filter Rule, as shown below.



```
                      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:
Press Space Bar to Toggle.
```

Figure 19-8 Menu 21.1.4.1: Generic Filter Rule

The following table describes the fields in the Generic Filter Rule menu.

Table 19-4 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.	
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 21.4.1.1 - 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 21.1.1 - Filter Rules Summary**.		

19.3 Example Filter

Let’s look at an example to block outside users from telnetting into the ZyWALL. Please see our included disk for more example filters.

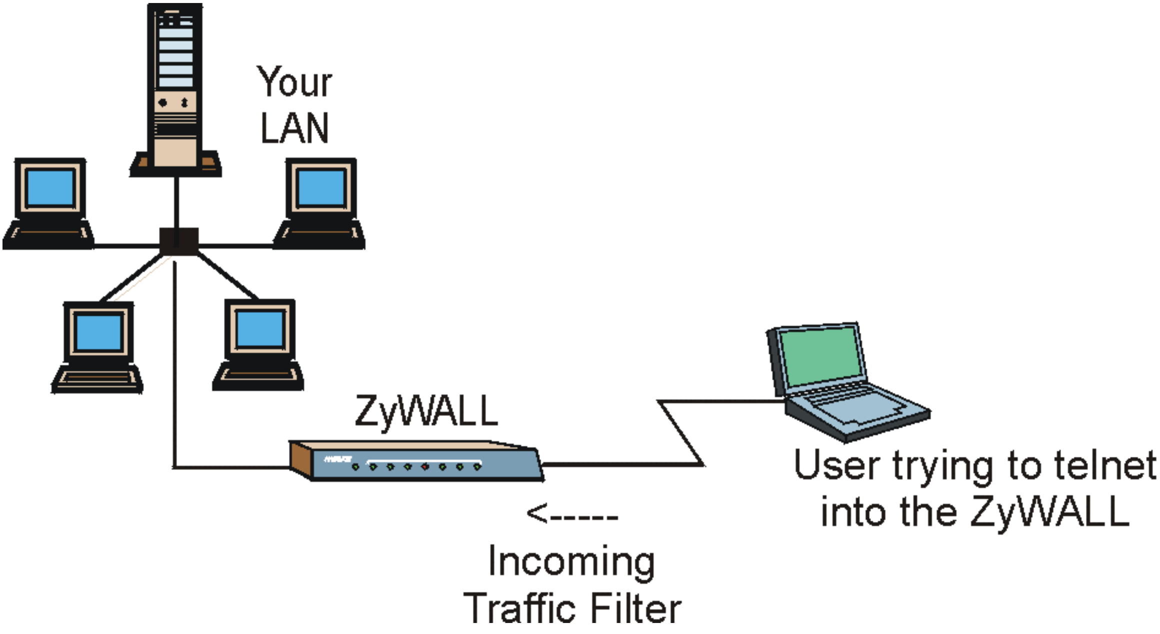


Figure 19-9 Telnet Filter Example

Step 1. Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.

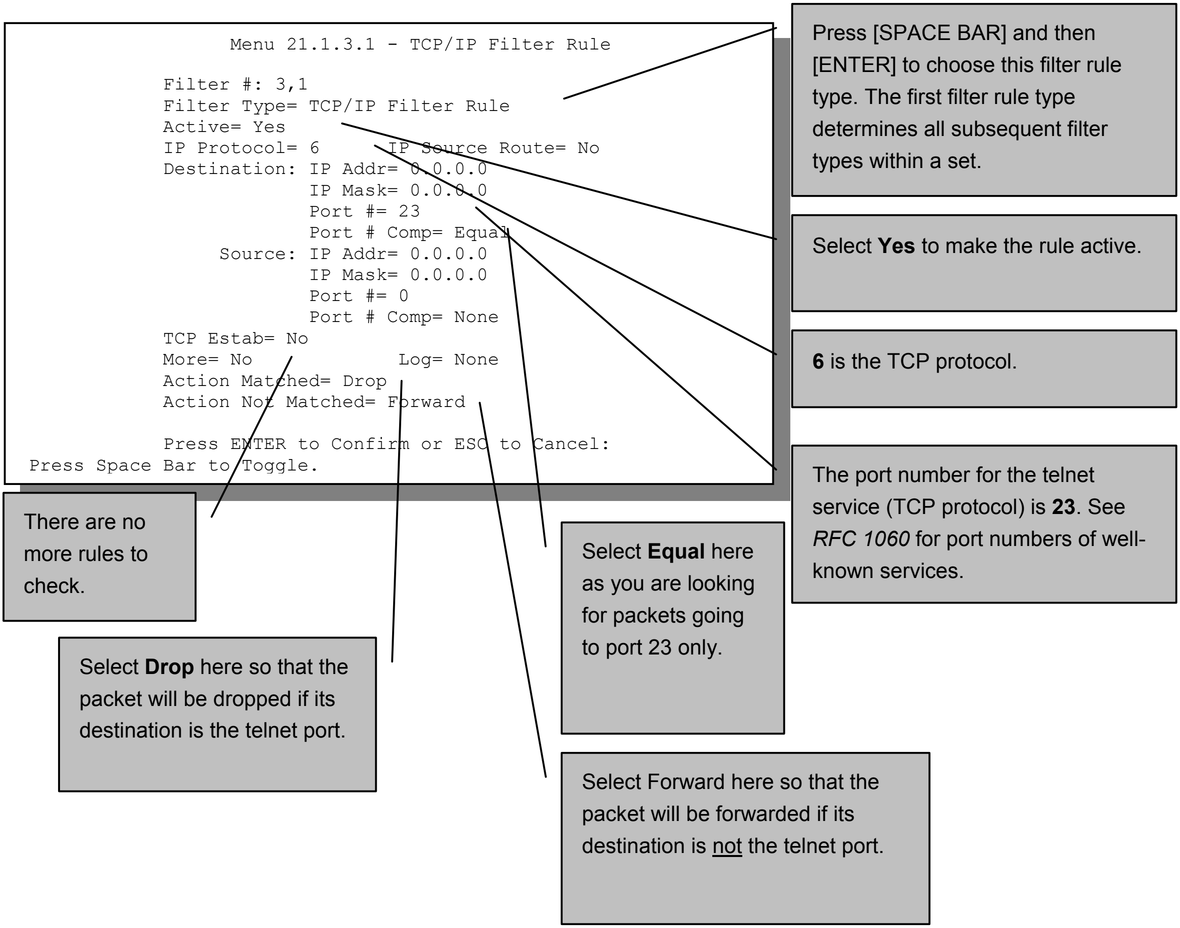
Step 2. Enter 1 to open **Menu 21.1 - Filter Set Configuration**.

Step 3. Enter the index of the filter set you wish to configure (say 3) and press [ENTER].

Step 4. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.

Step 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.



```
                  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.
```

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.

Select **Yes** to make the rule active.

6 is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

Select **Equal** here as you are looking for packets going to port 23 only.

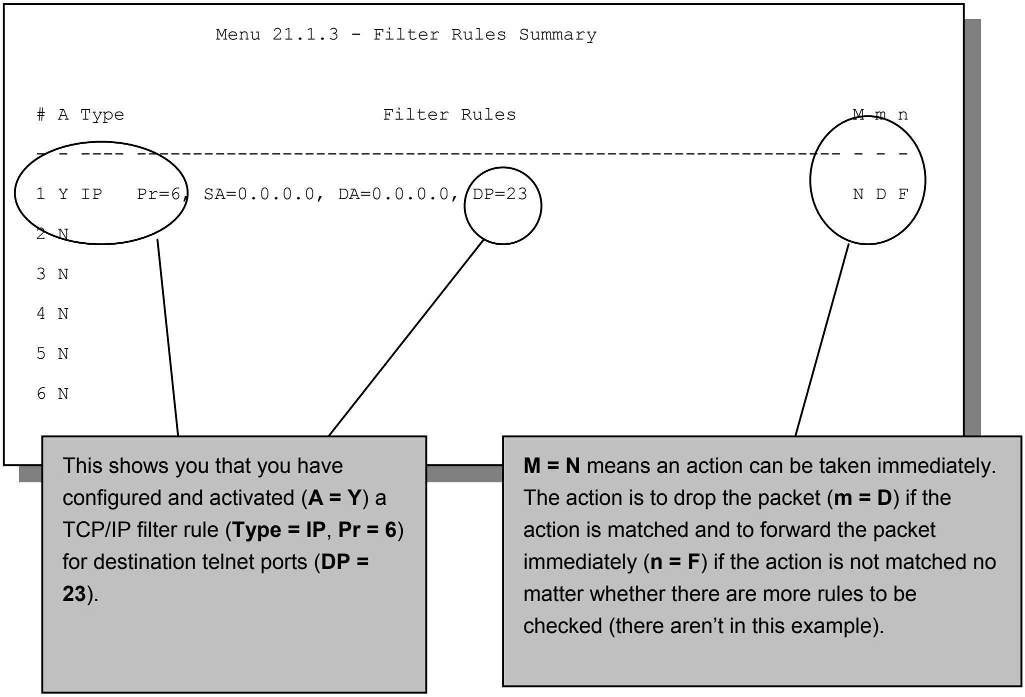
Select Forward here so that the packet will be forwarded if its destination is not the telnet port.

There are no more rules to check.

Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Figure 19-10 Example Filter: Menu 21.1.3.1

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.



```
                  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
```

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).

Figure 19-11 Example Filter Rules Summary: Menu 21.1.3

After you've created the filter set, you must apply it.

Step 1. Enter 11 from the main menu to go to menu 11.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].

Step 3. This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in *Figure 19-15*.

Step 4. Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

19.4 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 ZyWALL 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 ZyWALL 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.

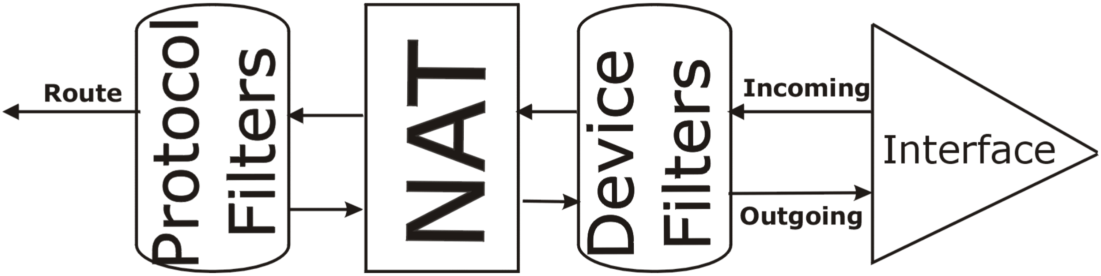


Figure 19-12 Protocol and Device Filter Sets

19.5 Firewall

Firewall configuration is discussed in the *firewall* chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

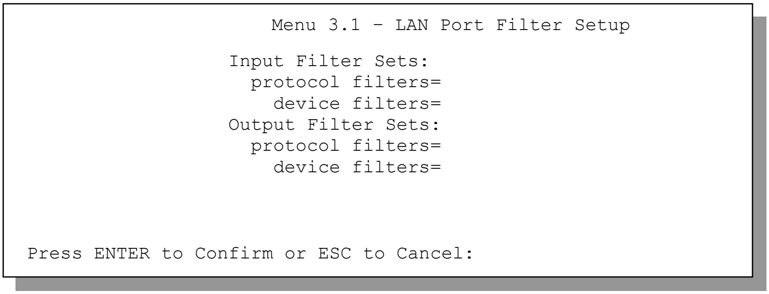
19.6 Applying a Filter and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

If you do not activate the firewall, it is advisable to apply filters.

19.6.1 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. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

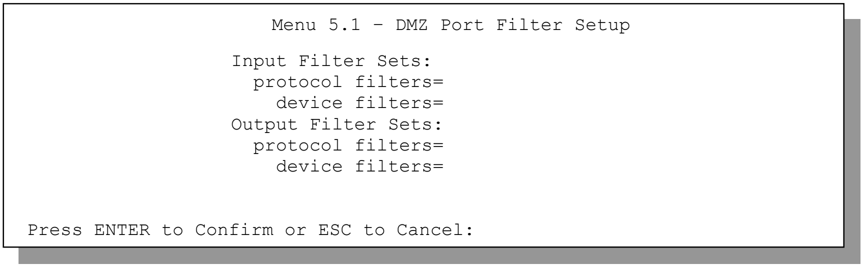


```
                       Menu 3.1 - LAN Port Filter Setup

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



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

Figure 19-13 Filtering LAN Traffic

19.6.2 DMZ Filters

DMZ traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 5.1 (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. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections. The DMZ port is not available on all models.

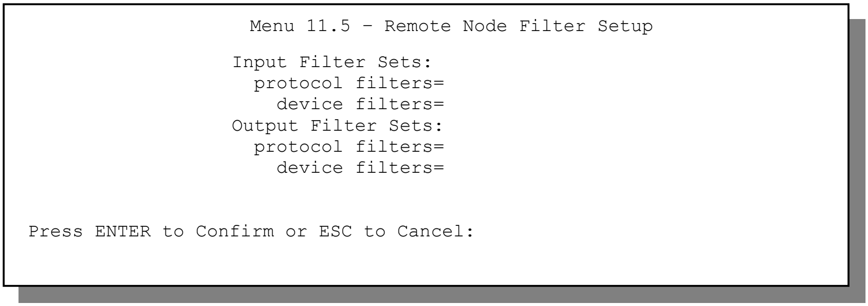


```
                        Menu 5.1 - DMZ Port Filter Setup

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


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

Figure 19-14Filtering DMZ Traffic

19.6.3 Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) 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. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.



```
                      Menu 11.5 - Remote Node Filter Setup

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


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

Figure 19-15 Filtering Remote Node Traffic

Chapter 20
SNMP Configuration

This chapter explains SNMP configuration menu 22.

SNMP is only available if TCP/IP is configured.

20.1 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 ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

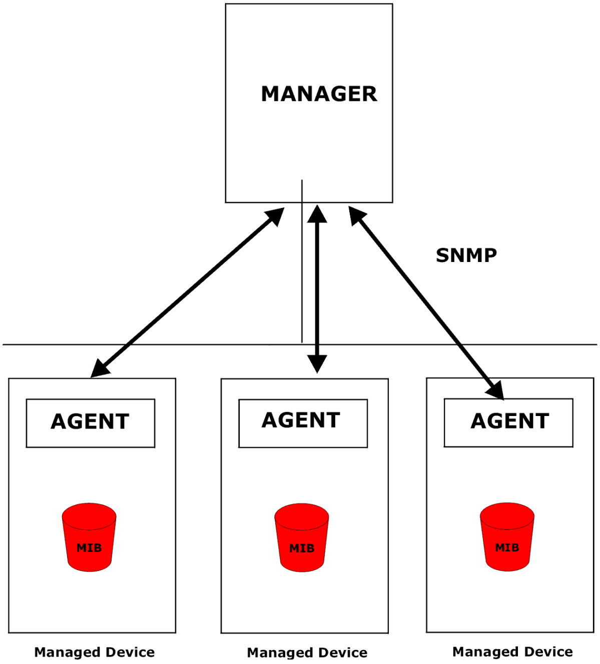


Figure 20-1 SNMP Management Model

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

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

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

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

- Get - Allows the manager to retrieve an object variable from the agent.

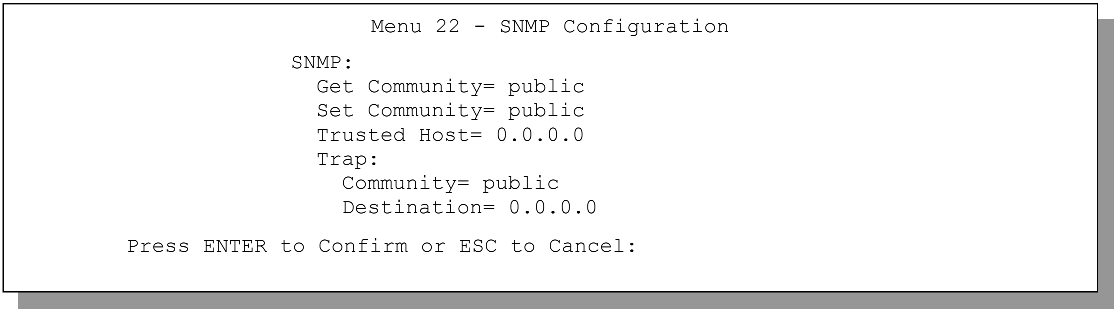
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values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

20.2 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

20.3 SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The “community” for **Get**, **Set** and **Trap** fields is SNMP terminology for password.



```
                             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:
```

Figure 20-2 Menu 22: SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 20-1 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Get Community	Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station.	**Public**

Table 20-1 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.	**Public**
Trusted Host	If you enter a trusted host, your ZyWALL will only respond to SNMP messages from this address. A blank (default) field means your ZyWALL will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap Community	Type the Trap community, which is the password sent with each trap to the SNMP manager.	**Public**
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

20.4 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs:

Table 20-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

Part VI:

System Information and Diagnosis and Firmware and Configuration File Maintenance

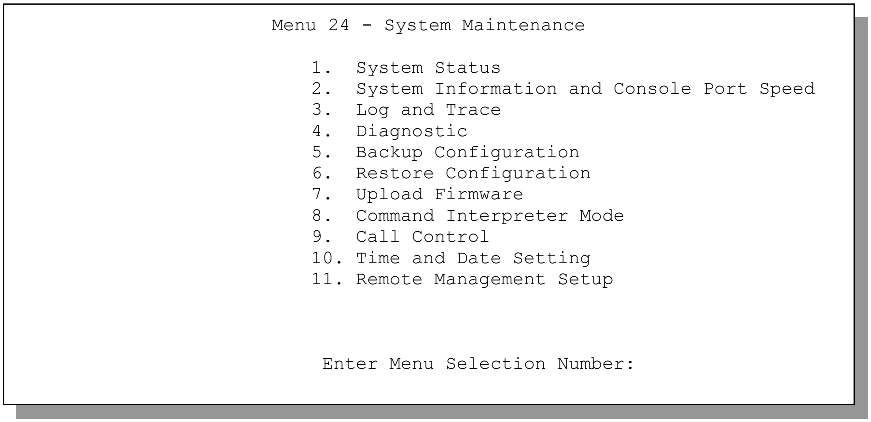
This part provides information on system information and diagnosis and maintaining the firmware and configuration files.

Chapter 21
System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24.4. DMZ applies to the ZyWALL 100. Wireless LAN and dial-backup apply to the ZyWALL 100 and 10W (see Table 1-1 Model Specific Features).

This chapter covers the diagnostic tools that help you to maintain your ZyWALL. These tools include updates on system status, port status and log and trace capabilities.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown below.



```
                        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:
```

Figure 21-1 Menu 24: System Maintenance

21.1 System Status

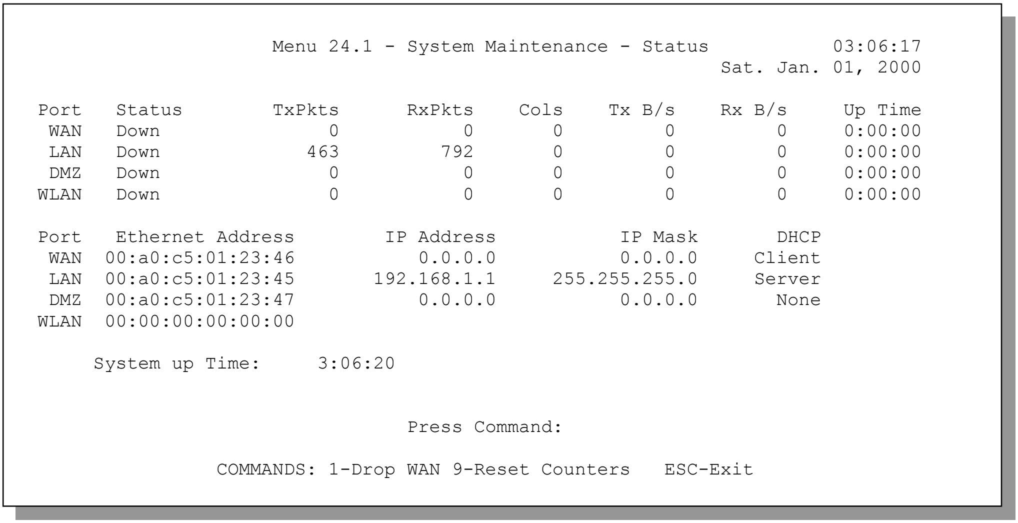
The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your ZyWALL. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

Step 1. Enter number 24 to go to **Menu 24 - System Maintenance**.

Step 2. In this menu, enter 1 to open System Maintenance - Status.

Step 3. There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.



```
                        Menu 24.1 - System Maintenance - Status           03:06:17
                                                                Sat. Jan. 01, 2000

   Port   Status          TxPkts      RxPkts    Cols     Tx B/s     Rx B/s     Up Time
    WAN   Down                 0           0       0          0          0     0:00:00
    LAN   Down               463         792       0          0          0     0:00:00
    DMZ   Down                 0           0       0          0          0     0:00:00
   WLAN   Down                 0           0       0          0          0     0:00:00

   Port   Ethernet Address          IP Address           IP Mask       DHCP
    WAN  00:a0:c5:01:23:46             0.0.0.0           0.0.0.0     Client
    LAN  00:a0:c5:01:23:45         192.168.1.1     255.255.255.0     Server
    DMZ  00:a0:c5:01:23:47             0.0.0.0           0.0.0.0       None
   WLAN  00:00:00:00:00:00

        System up Time:     3:06:20


                                    Press Command:

                   COMMANDS: 1-Drop WAN 9-Reset Counters   ESC-Exit
```

Figure 21-2 Menu 24.1: System Maintenance: Status (ZyWALL 100)

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 21-1 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	Identifies a port (WAN, LAN, DMZ or WLAN) on the ZyWALL. DMZ not available on all models.
Status	Shows the port speed and duplex setting if you're using **Ethernet Encapsulation** and **Down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using **PPPoE Encapsulation**.
TxPkts	The number of transmitted packets on this port.
RxPkts	The number of received packets on this port.

Table 21-1 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Cols	The number of collisions on this port.
Tx B/s	Shows the transmission speed in Bytes per second on this port.
Rx B/s	Shows the reception speed in Bytes per second on this port.
Up Time	Total amount of time the line has been up.
Ethernet Address	The Ethernet address of the port listed on the left.
IP Address	The IP address of the port listed on the left.
IP Mask	The IP mask of the port listed on the left.
DHCP	The DHCP setting of the port listed on the left.
System up Time	The total time the ZyWALL has been on.
ZyNOS F/W Version	The ZyNOS Firmware version and the date created.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

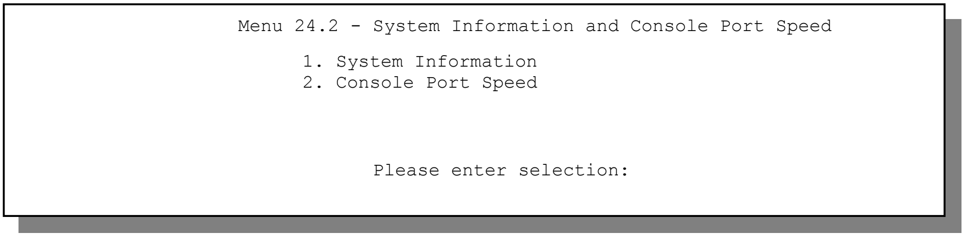
21.2 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

Step 1. Enter 24 to go to **Menu 24 – System Maintenance**.

Step 2. Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.

Step 3. From this menu you have two choices as shown in the next figure:

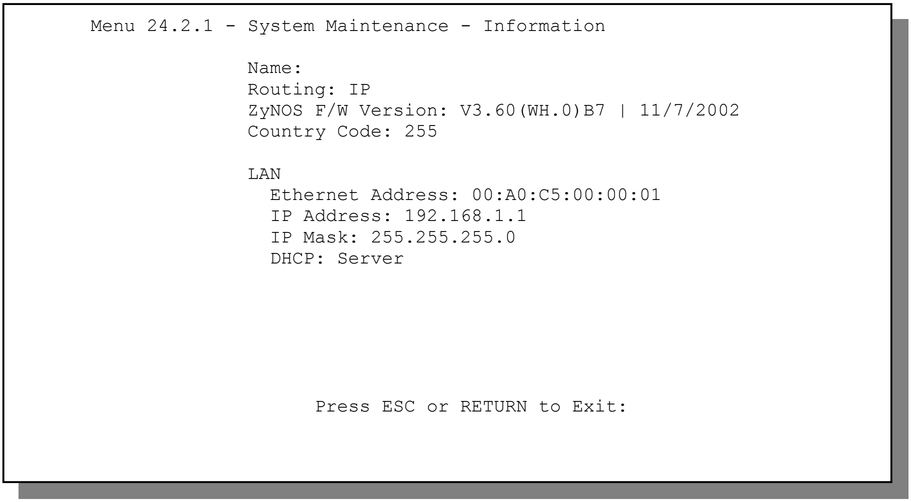


```
          Menu 24.2 - System Information and Console Port Speed

               1. System Information
               2. Console Port Speed



                      Please enter selection:
```

Figure 21-3 Menu 24.2: System Information and Console Port Speed

21.2.1 System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.



```
        Menu 24.2.1 - System Maintenance - Information

                      Name:
                      Routing: IP
                      ZyNOS F/W Version: V3.60(WH.0)B7 | 11/7/2002
                      Country Code: 255

                      LAN
                        Ethernet Address: 00:A0:C5:00:00:01
                        IP Address: 192.168.1.1
                        IP Mask: 255.255.255.0
                        DHCP: Server






                            Press ESC or RETURN to Exit:
```

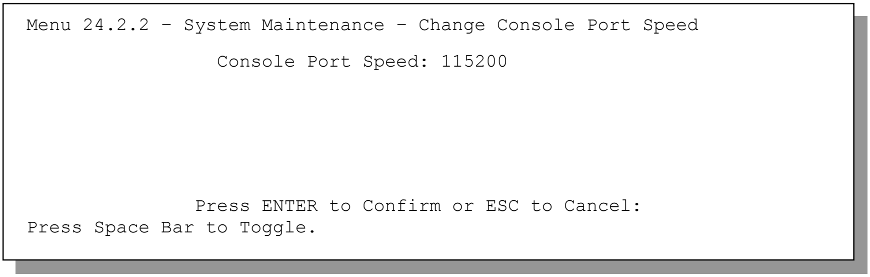
Figure 21-4 Menu 24.2.1: System Maintenance: Information (ZyWALL 10W)

Table 21-2 Fields in System Maintenance: Information

FIELD	DESCRIPTION
Name	This is the ZyWALL's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the version of ZyXEL's Network Operating System software.
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) address of your ZyWALL.
IP Address	This is the IP address of the ZyWALL in dotted decimal notation.
IP Mask	This shows the IP mask of the ZyWALL.
DHCP	This field shows the DHCP setting of the ZyWALL.
When finished viewing, press [ESC] or [ENTER] to exit.	

21.2.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your ZyWALL supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown next.



```
Menu 24.2.2 – System Maintenance – Change Console Port Speed

                 Console Port Speed: 115200






               Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 21-5 Menu 24.2.2: System Maintenance: Change Console Port Speed

21.3 Log and Trace

There are two logging facilities in the ZyWALL. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

21.3.1 Viewing Error Log

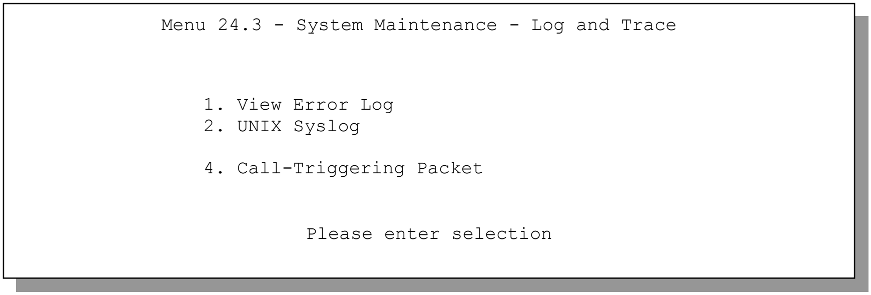
The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

Step 1. Select option 24 from the main menu to open **Menu 24 - System Maintenance**.

Step 2. From menu 24, select option 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.

Step 3. Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

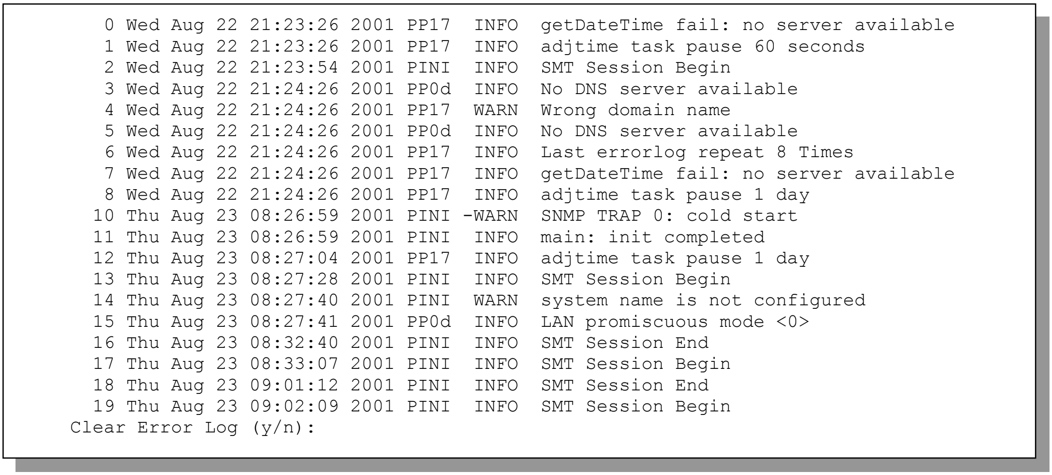
After the ZyWALL finishes displaying, you will have the option to clear the error log.



```
                Menu 24.3 - System Maintenance - Log and Trace



                    1. View Error Log
                    2. UNIX Syslog

                    4. Call-Triggering Packet


                             Please enter selection
```

Figure 21-6 Menu 24.3: System Maintenance: Log and Trace

Examples of typical error and information messages are presented in the following figure.

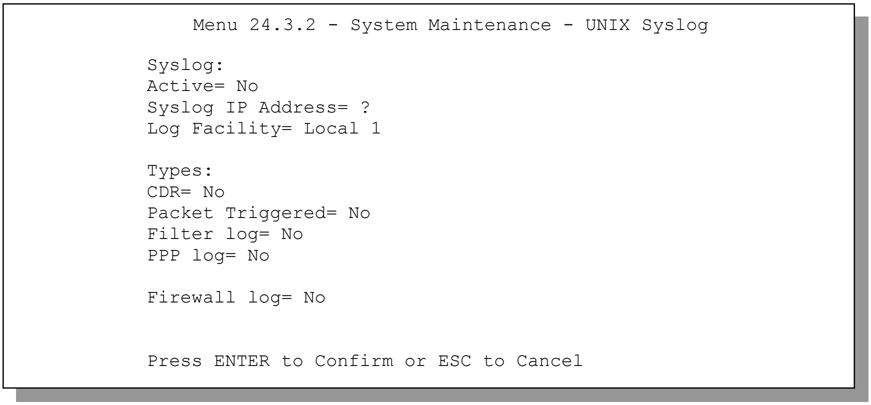


```
     0 Wed Aug 22 21:23:26 2001 PP17  INFO  getDateTime fail: no server available
     1 Wed Aug 22 21:23:26 2001 PP17  INFO  adjtime task pause 60 seconds
     2 Wed Aug 22 21:23:54 2001 PINI  INFO  SMT Session Begin
     3 Wed Aug 22 21:24:26 2001 PP0d  INFO  No DNS server available
     4 Wed Aug 22 21:24:26 2001 PP17  WARN  Wrong domain name
     5 Wed Aug 22 21:24:26 2001 PP0d  INFO  No DNS server available
     6 Wed Aug 22 21:24:26 2001 PP17  INFO  Last errorlog repeat 8 Times
     7 Wed Aug 22 21:24:26 2001 PP17  INFO  getDateTime fail: no server available
     8 Wed Aug 22 21:24:26 2001 PP17  INFO  adjtime task pause 1 day
    10 Thu Aug 23 08:26:59 2001 PINI -WARN  SNMP TRAP 0: cold start
    11 Thu Aug 23 08:26:59 2001 PINI  INFO  main: init completed
    12 Thu Aug 23 08:27:04 2001 PP17  INFO  adjtime task pause 1 day
    13 Thu Aug 23 08:27:28 2001 PINI  INFO  SMT Session Begin
    14 Thu Aug 23 08:27:40 2001 PINI  WARN  system name is not configured
    15 Thu Aug 23 08:27:41 2001 PP0d  INFO  LAN promiscuous mode <0>
    16 Thu Aug 23 08:32:40 2001 PINI  INFO  SMT Session End
    17 Thu Aug 23 08:33:07 2001 PINI  INFO  SMT Session Begin
    18 Thu Aug 23 09:01:12 2001 PINI  INFO  SMT Session End
    19 Thu Aug 23 09:02:09 2001 PINI  INFO  SMT Session Begin
   Clear Error Log (y/n):
```

Figure 21-7 Examples of Error and Information Messages

21.3.2 UNIX Syslog

The ZyWALL uses the UNIX 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.



```
                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
```

Figure 21-8 Menu 24.3.2: System Maintenance: UNIX Syslog (ZyWALL 100)

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 21-3 System Maintenance Menu Syslog Parameters

PARAMETER	DESCRIPTION
UNIX 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 your UNIX manual for more details.
Types:	
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** (Menu 21.x.x) are logged when this field is set to **Yes**.

Table 21-3 System Maintenance Menu Syslog Parameters

PARAMETER	DESCRIPTION
PPP log	PPP events are logged when this field is set to **Yes**.
Firewall log	When set to **Yes**, the ZyWALL sends the firewall log to a syslog server.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your ZyWALL sends five types of syslog messages. Some examples (not all ZyWALL specific) of these syslog messages with their message formats are shown next:

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.)
                L02      Tunnel 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
```

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=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f707172
7374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

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
```

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
```

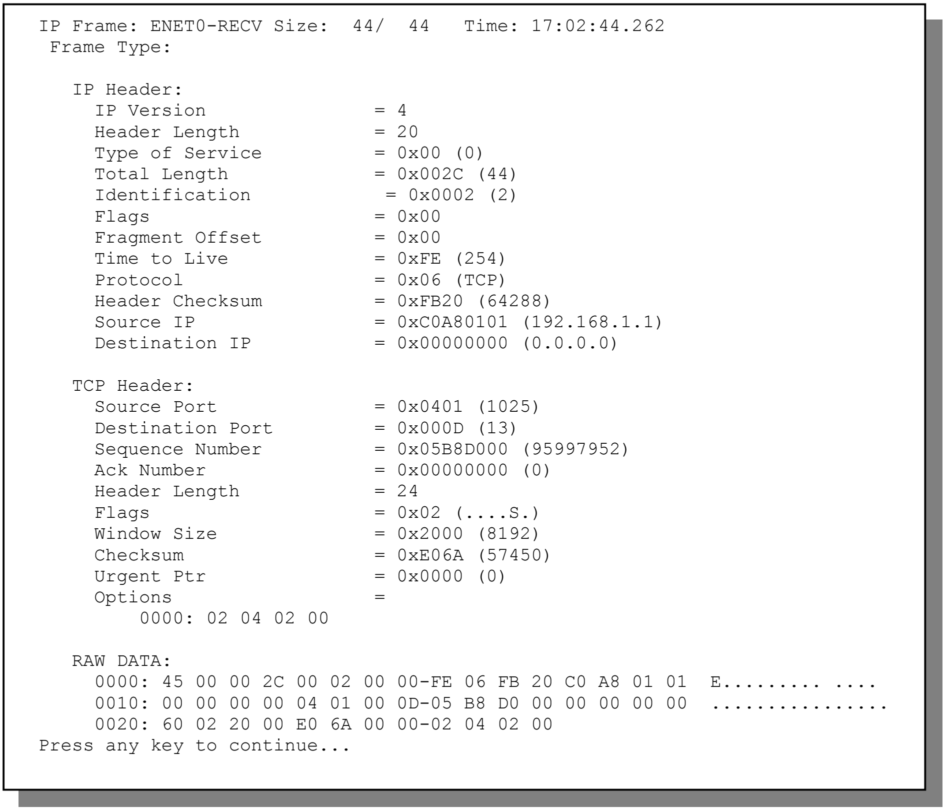
5. Firewall log

Firewall Log Message Format

```
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol (“TCP”,”UDP”,”ICMP”, ”IGMP”, ”GRE”, ”ESP”)
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-2000       11:48:41 Local1.Notice    192.168.10.10    RAS: FW 172.21.1.80     :137  -
>172.21.1.80     :137  |UDP|default permit:<2,0>|B
08-01-2000       11:48:41 Local1.Notice    192.168.10.10    RAS: FW 192.168.77.88   :520  -
>192.168.77.88   :520  |UDP|default permit:<2,0>|B
08-01-2000       11:48:39 Local1.Notice    192.168.10.10    RAS: FW 172.21.1.50     ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-2000       11:48:39 Local1.Notice    192.168.10.10    RAS: FW 172.21.1.25     ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
```

21.3.3 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.



```
IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
 Frame Type:

   IP Header:
     IP Version                = 4
     Header Length             = 20
     Type of Service           = 0x00 (0)
     Total Length              = 0x002C (44)
     Identification             = 0x0002 (2)
     Flags                     = 0x00
     Fragment Offset           = 0x00
     Time to Live              = 0xFE (254)
     Protocol                  = 0x06 (TCP)
     Header Checksum           = 0xFB20 (64288)
     Source IP                 = 0xC0A80101 (192.168.1.1)
     Destination IP            = 0x00000000 (0.0.0.0)

   TCP Header:
     Source Port               = 0x0401 (1025)
     Destination Port          = 0x000D (13)
     Sequence Number           = 0x05B8D000 (95997952)
     Ack Number                = 0x00000000 (0)
     Header Length             = 24
     Flags                     = 0x02 (....S.)
     Window Size               = 0x2000 (8192)
     Checksum                  = 0xE06A (57450)
     Urgent Ptr                = 0x0000 (0)
     Options                   =
         0000: 02 04 02 00

   RAW DATA:
     0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E......... ....
     0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00  ................
     0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...
```

Figure 21-9 Call-Triggering Packet Example

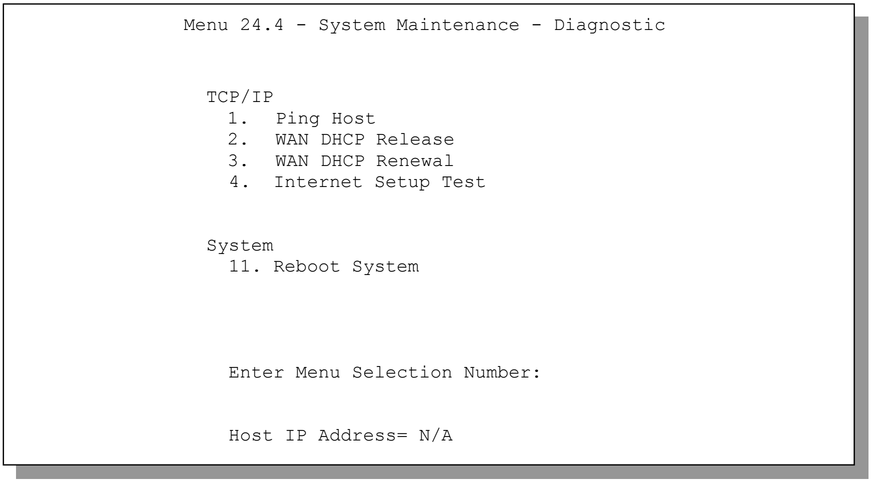
21.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyWALL 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 next.

Follow the procedure below to get to **Menu 24.4 - System Maintenance – Diagnostic.**

Step 1. From the main menu, select option 24 to open **Menu 24 - System Maintenance**.

Step 2. From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.



```
                Menu 24.4 - System Maintenance - Diagnostic


                  TCP/IP
                    1.  Ping Host
                    2.  WAN DHCP Release
                    3.  WAN DHCP Renewal
                    4.  Internet Setup Test


                  System
                    11. Reboot System




                    Enter Menu Selection Number:


                    Host IP Address= N/A
```

Figure 21-10 Menu 24.4: System Maintenance: Diagnostic

21.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 21-11*. LAN DHCP has already been discussed. The ZyWALL can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

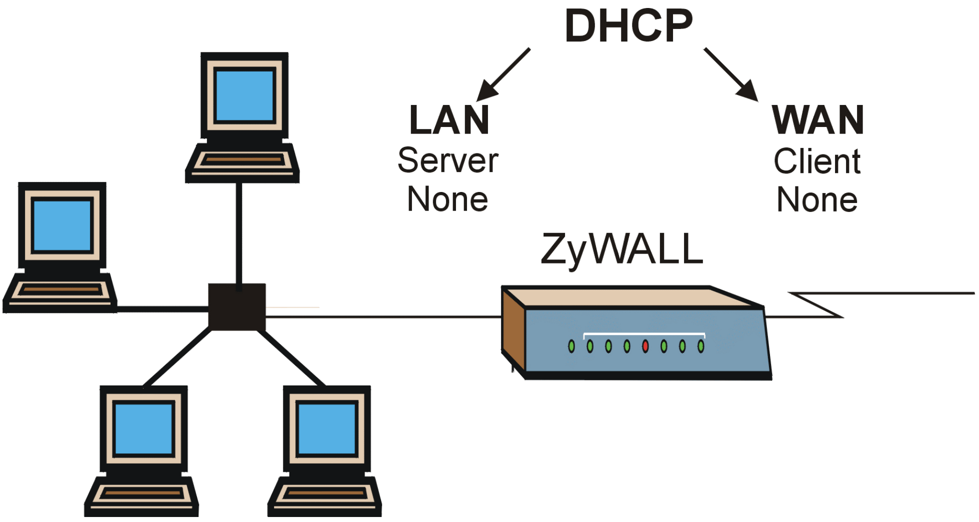


Figure 21-11 WAN & LAN DHCP

The following table describes the diagnostic tests available in menu 24.4 for your ZyWALL and associated connections.

Table 21-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the **Host IP Address** field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.
Internet Setup Test	Enter 4 to test the Internet setup. You can also test the Internet setup in **Menu 4 - Internet Access**. Please refer to the *Internet Access* chapter for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation.
Reboot System	Enter 11 to reboot the ZyWALL.
Host IP Address=	If you entered 1 in **Ping Host**, then enter the IP address of the computer you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	

Chapter 22
Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

22.1 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 ZyWALL's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyWALL.

```
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 ZyWALL 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 ZyWALL and the external filename refers to the filename not on the ZyWALL, 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 22-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyWALL. Uploading the rom-0 file replaces the entire ROM file system, including your ZyWALL 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 ZyWALL.	*.bin

22.2 Backup Configuration

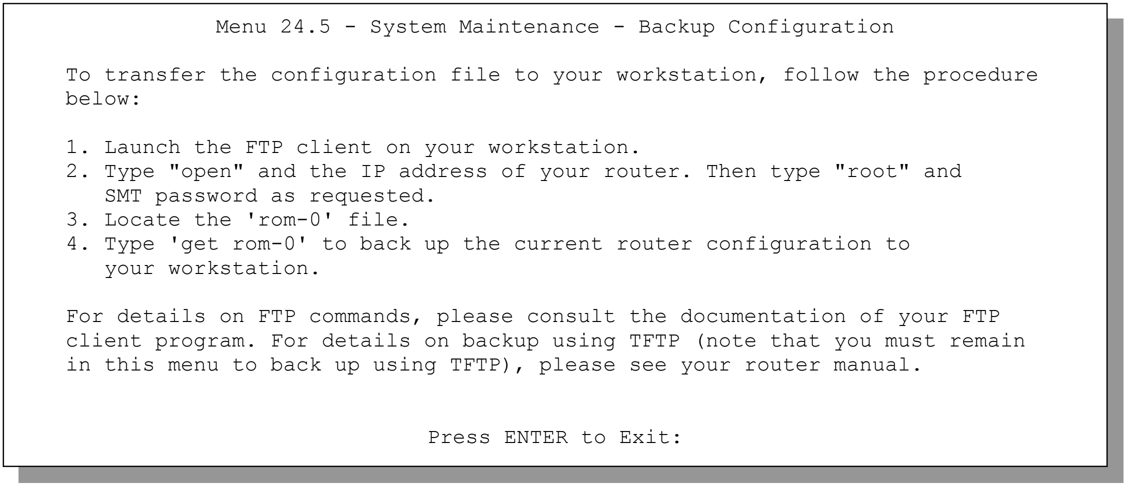
The ZyWALL displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current ZyWALL configuration to your computer. Backup is highly recommended once your ZyWALL 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 ZyWALL to the computer, while upload means from your computer to the ZyWALL.

22.2.1 Backup Configuration

Follow the instructions as shown in the next screen.



```
                Menu 24.5 - System Maintenance - 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:
```

Figure 22-1 Telnet into Menu 24.5

22.2.2 Using the FTP Command from the Command Line

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyWALL.

Step 3. Press [ENTER] when prompted for a username.

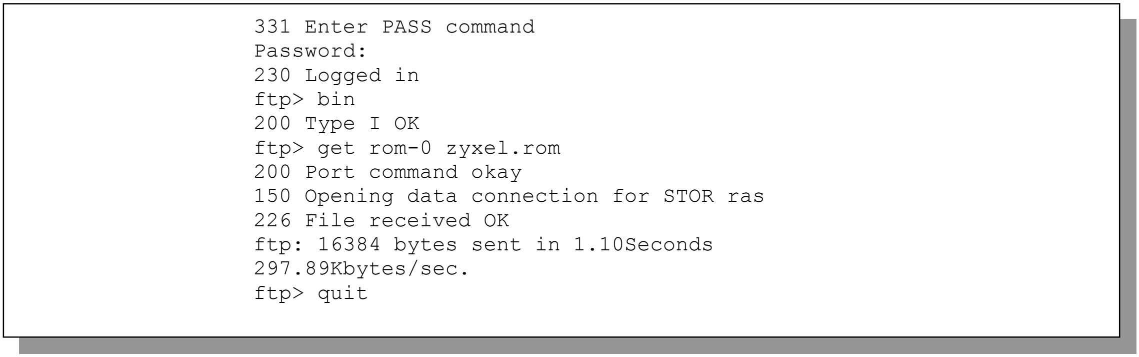
Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Use “get” to transfer files from the ZyWALL to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

Step 7. Enter “quit” to exit the ftp prompt.

22.2.3 Example of FTP Commands from the Command Line



```
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
```

Figure 22-2 FTP Session Example

22.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 22-2 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.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

22.2.5 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

1. The firewall is active (turn the firewall off in menu 21.2 or create a firewall rule to allow access from the WAN).
2. You have disabled Telnet service in menu 24.11.
3. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
4. The IP you entered in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyWALL will disconnect the Telnet session immediately.
5. You have an SMT console session running.

22.2.6 Backup Configuration Using TFTP

The ZyWALL 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.

Step 1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 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.

Step 4. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyWALL 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 ZyWALL to the computer and “binary” to set binary transfer mode.

22.2.7 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 ZyWALL IP address, "get" transfers the file source on the ZyWALL (rom-0, name of the configuration file on the ZyWALL) to the file destination on the computer and renames it config.rom.

22.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 22-3 General Commands for GUI-based TFTP Clients

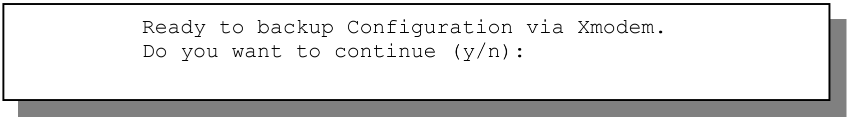
COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyWALL. 192.168.1.1 is the ZyWALL's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyWALL and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyWALL. 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.

Refer to *section 22.2.5* to read about configurations that disallow TFTP and FTP over WAN.

22.2.9 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.

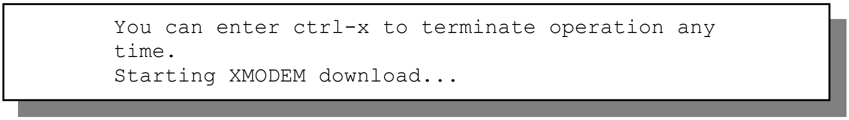
Step 1. Display menu 24.5 and enter "y" at the following screen.



```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 22-3 System Maintenance: Backup Configuration

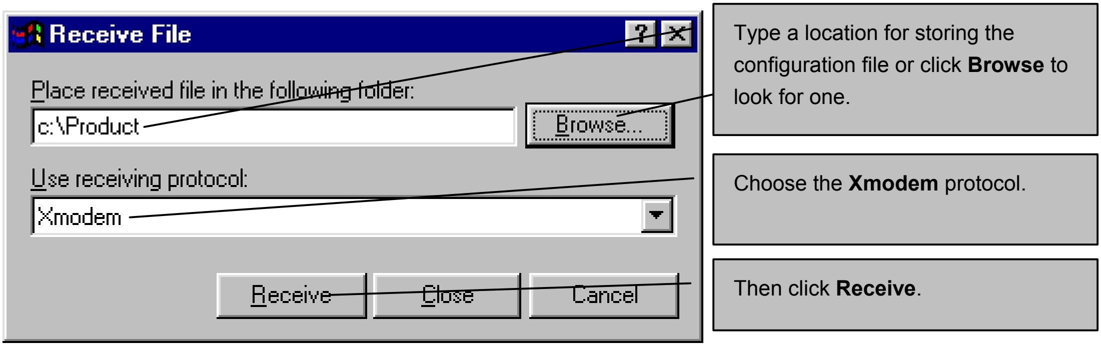
Step 2. The following screen indicates that the Xmodem download has started.



```
You can enter ctrl-x to terminate operation any
time.
Starting XMODEM download...
```

Figure 22-4 System Maintenance: Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.



Receive File

Place received file in the following folder: c:\Product

Use receiving protocol: Xmodem

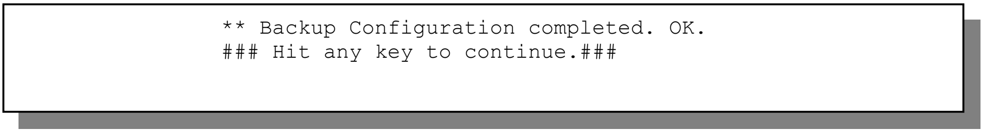
Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

Figure 22-5 Backup Configuration Example

Step 4. After a successful backup you will see the following screen. Press any key to return to the SMT menu.



```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

Figure 22-6 Successful Backup Confirmation Screen

22.3 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.

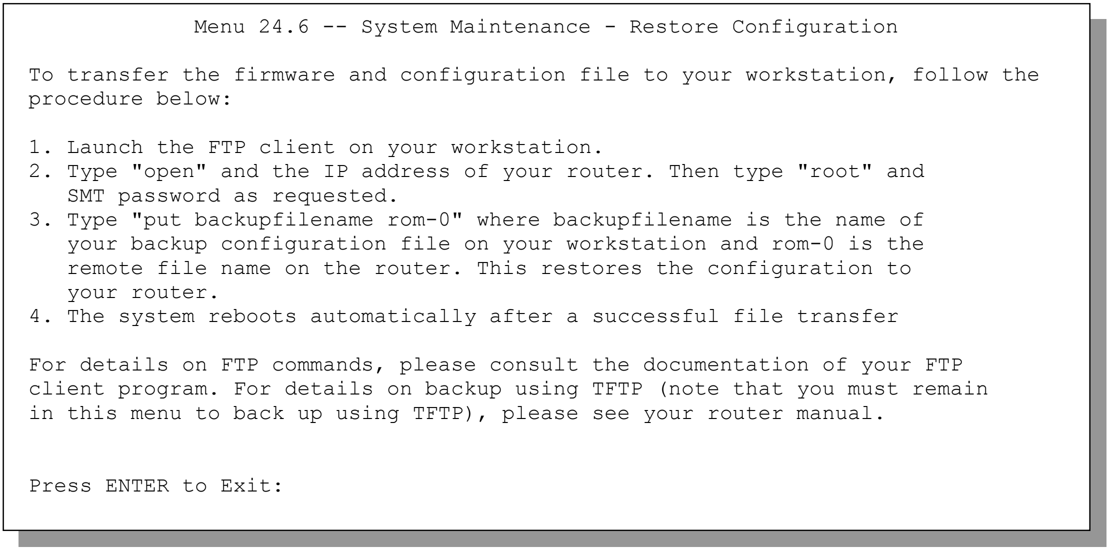
FTP is the preferred method for restoring your current computer configuration to your ZyWALL since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL. When the Restore Configuration process is complete, the ZyWALL will automatically restart.

22.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.



```
                 Menu 24.6 -- System Maintenance - Restore Configuration

 To transfer the firmware and 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. Type "put backupfilename rom-0" where backupfilename is the name of
    your backup configuration file on your workstation and rom-0 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 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:
```

Figure 22-7 Telnet into Menu 24.6

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyWALL.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is “1234”).

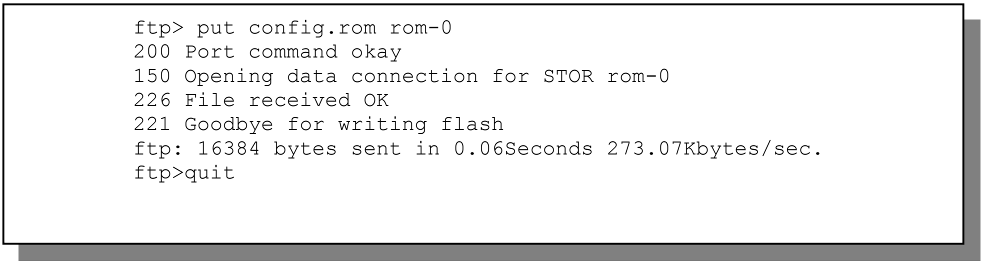
Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Find the “rom” file (on your computer) that you want to restore to your ZyWALL.

Step 7. Use “put” to transfer files from the ZyWALL to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the ZyWALL. See earlier in this chapter for more information on filename conventions.

Step 8. Enter “quit” to exit the ftp prompt. The ZyWALL will automatically restart after a successful restore process.

22.3.2 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
```

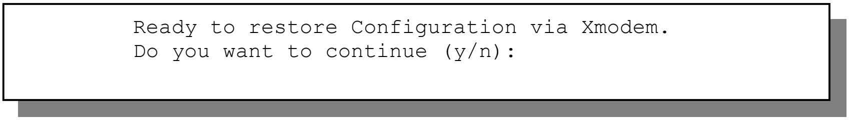
Figure 22-8 Restore Using FTP Session Example

Refer to *section 22.2.5* to read about configurations that disallow TFTP and FTP over WAN.

22.3.3 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.

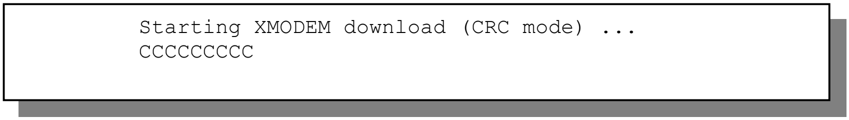
Step 1. Display menu 24.6 and enter "y" at the following screen.



```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 22-9 System Maintenance: Restore Configuration

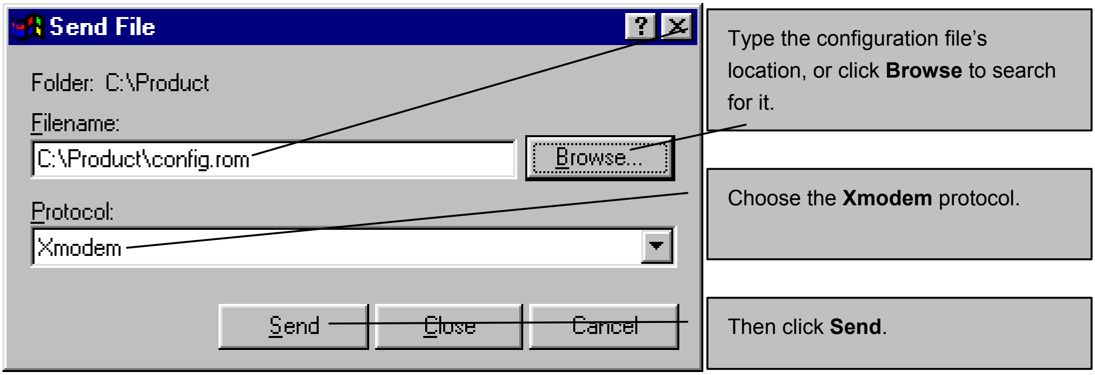
Step 2. The following screen indicates that the Xmodem download has started.



```
Starting XMODEM download (CRC mode) ...
CCCCCCCCC
```

Figure 22-10 System Maintenance: Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.



Folder: C:\Product

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

Figure 22-11 Restore Configuration Example

Step 4. After a successful restoration you will see the following screen. Press any key to restart the ZyWALL and return to the SMT menu.

```
              Save to ROM
              Hit any key to start system reboot.
```

Figure 22-12 Successful Restoration Confirmation Screen

22.4 Uploading Firmware and Configuration Files

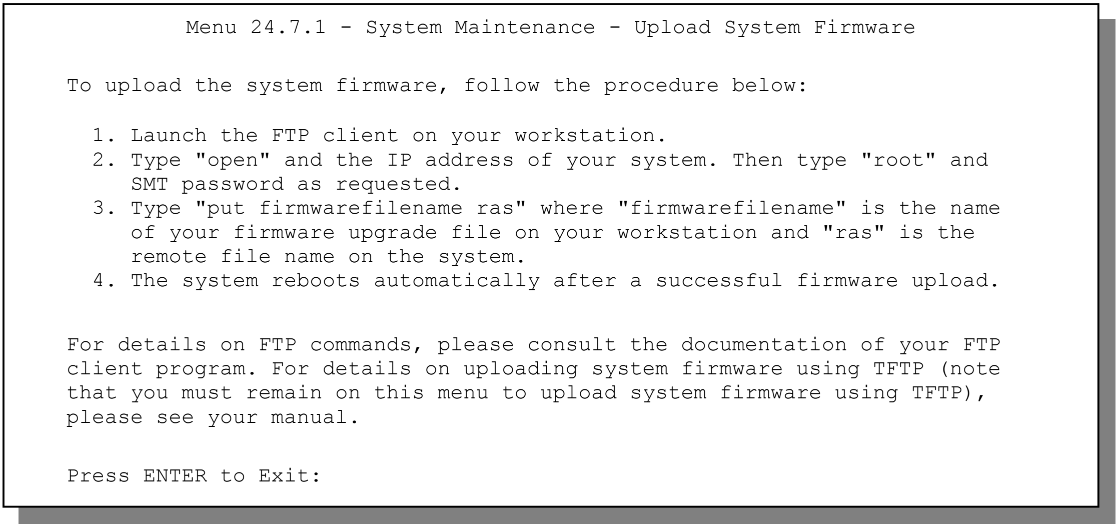
This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

WARNING!
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL.

22.4.1 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 ZyWALL, you will see the following screens for uploading firmware and the configuration file using FTP.

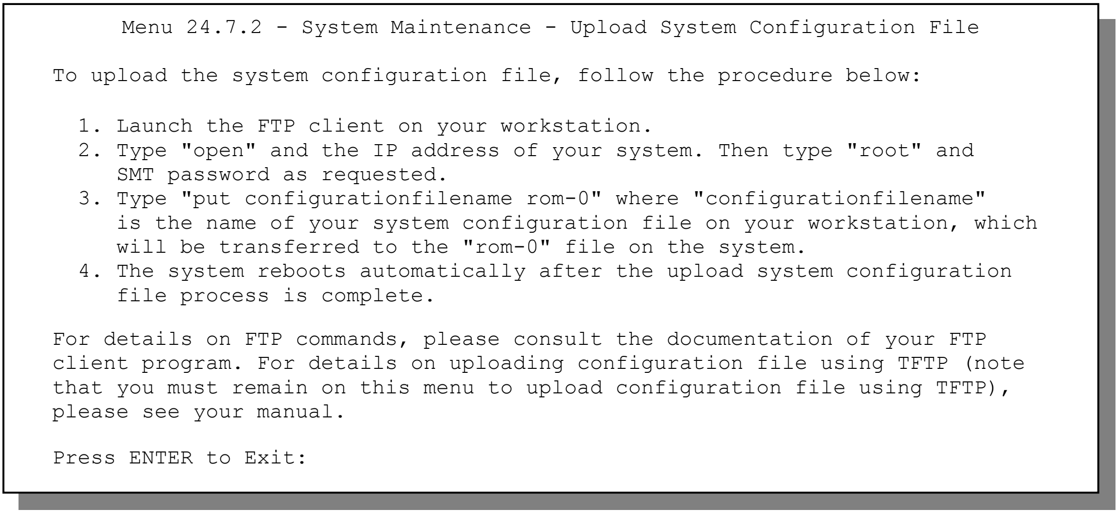


```
            Menu 24.7.1 - System Maintenance - Upload System Firmware

     To upload the system firmware, follow the procedure below:

       1. Launch the FTP client on your workstation.
       2. Type "open" and the IP address of your system. Then type "root" and
          SMT password as requested.
       3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
          of your firmware upgrade file on your workstation and "ras" is the
          remote file name on the system.
       4. The system reboots automatically after a successful firmware upload.


     For details on FTP commands, please consult the documentation of your FTP
     client program. For details on uploading system firmware using TFTP (note
     that you must remain on this menu to upload system firmware using TFTP),
     please see your manual.

     Press ENTER to Exit:
```

Figure 22-13 Telnet Into Menu 24.7.1: Upload System Firmware

22.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.



```
      Menu 24.7.2 - System Maintenance - Upload System Configuration File

  To upload the system configuration file, follow the procedure below:

    1. Launch the FTP client on your workstation.
    2. Type "open" and the IP address of your system. Then type "root" and
       SMT password as requested.
    3. Type "put configurationfilename rom-0" where "configurationfilename"
       is the name of your system configuration file on your workstation, which
       will be transferred to the "rom-0" file on the system.
    4. The system reboots automatically after the upload system configuration
       file process is complete.

  For details on FTP commands, please consult the documentation of your FTP
  client program. For details on uploading configuration file using TFTP (note
  that you must remain on this menu to upload configuration file using TFTP),
  please see your manual.

  Press ENTER to Exit:
```

Figure 22-14 Telnet Into Menu 24.7.2: System Maintenance

To upload the firmware and the configuration file, follow these examples

22.4.3 FTP File Upload Command from the DOS Prompt Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyWALL.

Step 3. Press [ENTER] when prompted for a username.

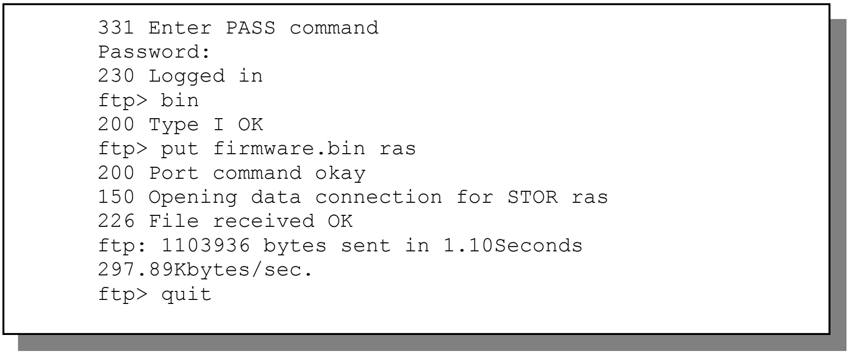
Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Use “put” to transfer files from the computer to the ZyWALL, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyWALL and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyWALL and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

Step 7. Enter “quit” to exit the ftp prompt.

22.4.4 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
```

Figure 22-15 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 22.2.5* to read about configurations that disallow TFTP and FTP over WAN.

22.4.5 TFTP File Upload

The ZyWALL 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.

Step 1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 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.

Step 4. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the ZyWALL 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 ZyWALL to the computer, “put” the other way around, and “binary” to set binary transfer mode.

22.4.6 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 ZyWALL’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyWALL).

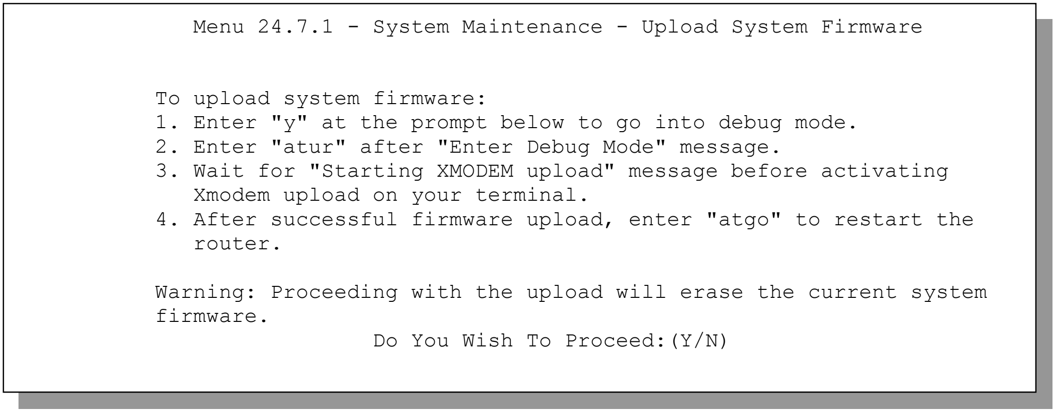
Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

22.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyWALL. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyWALL 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.

22.4.8 Uploading Firmware File Via Console Port

Step 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.



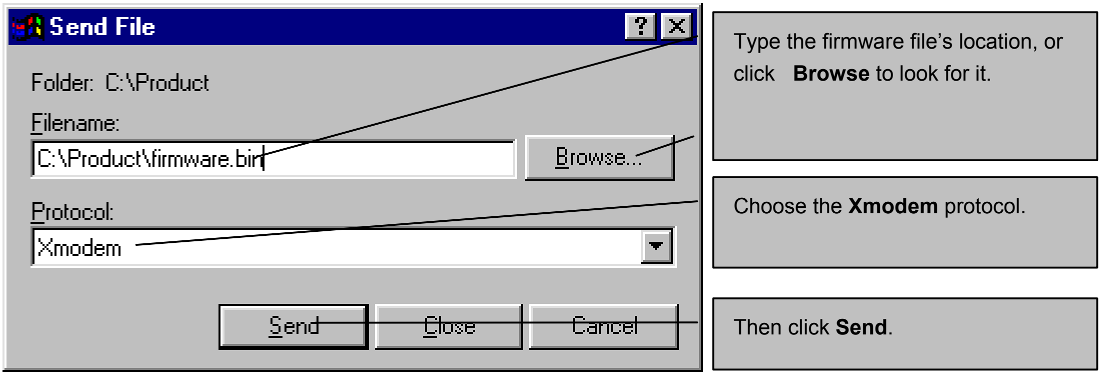
```
              Menu 24.7.1 - System Maintenance - Upload System Firmware


           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)
```

Figure 22-16 Menu 24.7.1 as seen using the Console Port

Step 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.

22.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.



Folder: C:\Product

Filename: C:\Product\firmware.bin

Protocol: Xmodem

Type the firmware file's location, or click **Browse** to look for it.

Choose the **Xmodem** protocol.

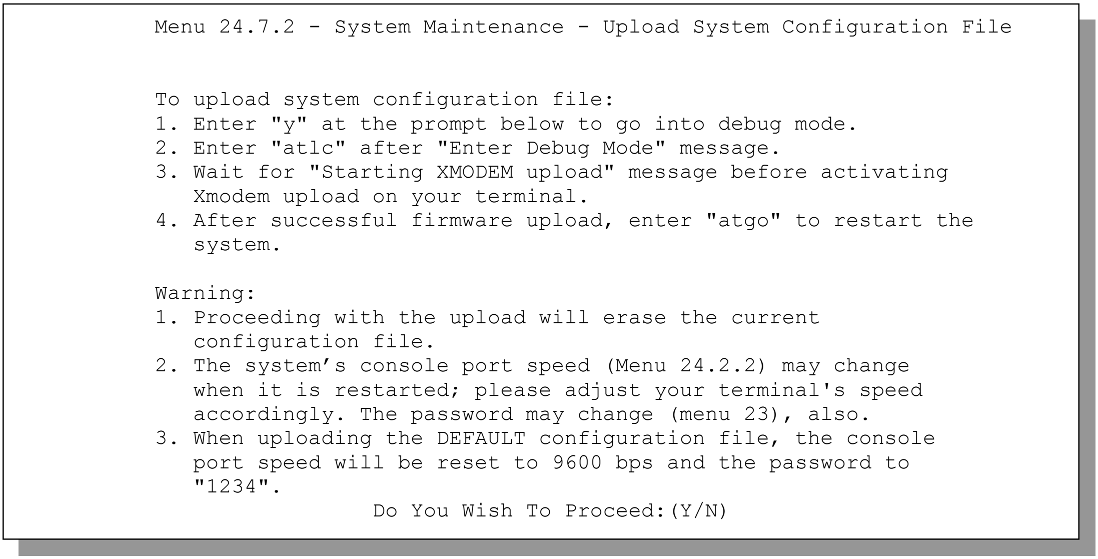
Then click **Send**.

Figure 22-17 Example Xmodem Upload

After the firmware upload process has completed, the ZyWALL will automatically restart.

22.4.10 Uploading Configuration File Via Console Port

Step 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.



```
            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)
```

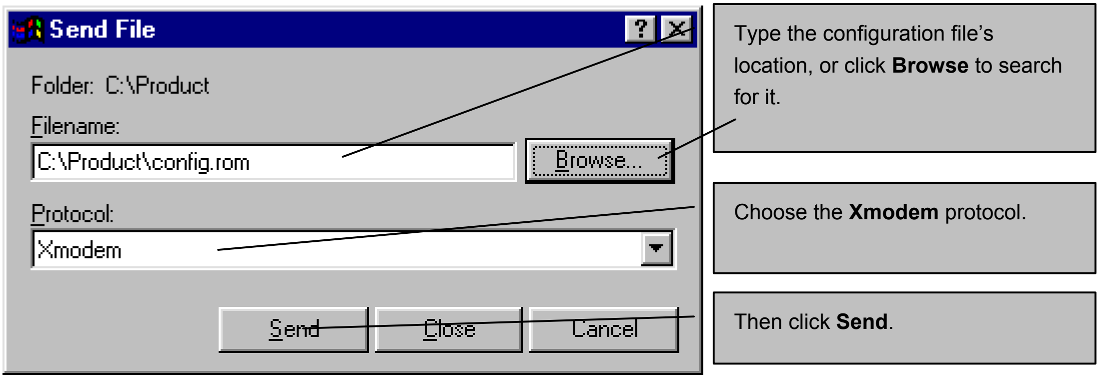
Figure 22-18 Menu 24.7.2 as seen using the Console Port

Step 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.

Step 3. Enter “atgo” to restart the ZyWALL.

22.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.



Folder: C:\Product

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

Figure 22-19 Example Xmodem Upload

After the configuration upload process has completed, restart the ZyWALL by entering “atgo”.

Part VII:

System Maintenance and Information and Remote Management

This part provides information on the system maintenance and information functions and how to configure remote management.

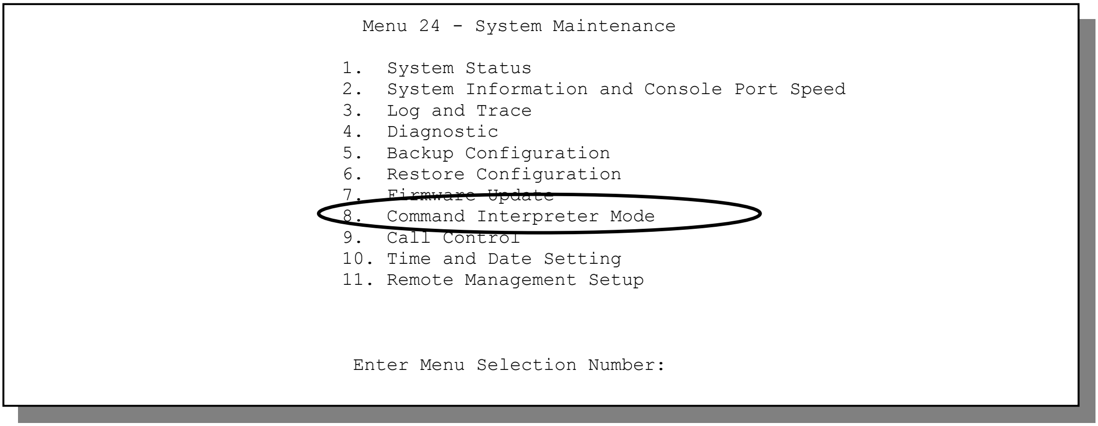
Chapter 23
System Maintenance & Information

This chapter leads you through SMT menus 24.8 to 24.10. The Real Time Chip (RTC) applies to the ZyWALL 100, 50 and 10W.

23.1 Command Interpreter Mode

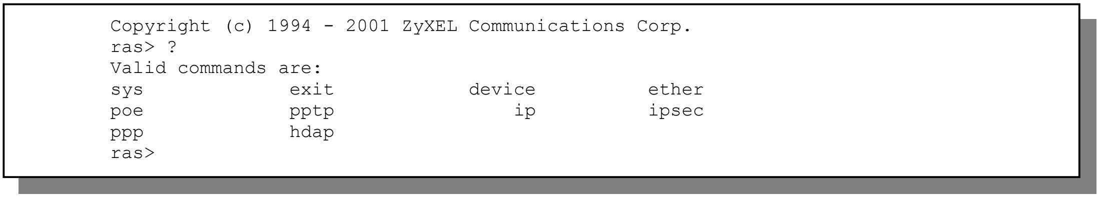
The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or zyxel.com for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**. Type `exit` to return to the SMT main menu when finished.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.



```
                              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:
```

Figure 23-1 Command Mode in Menu 24



```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
poe             pptp                ip          ipsec
ppp             hdap
ras>
```

Figure 23-2 Valid Commands

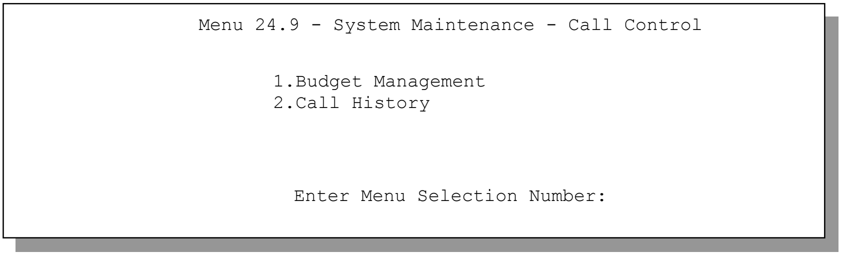
23.2 Call Control Support

The ZyWALL provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyWALL within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

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.

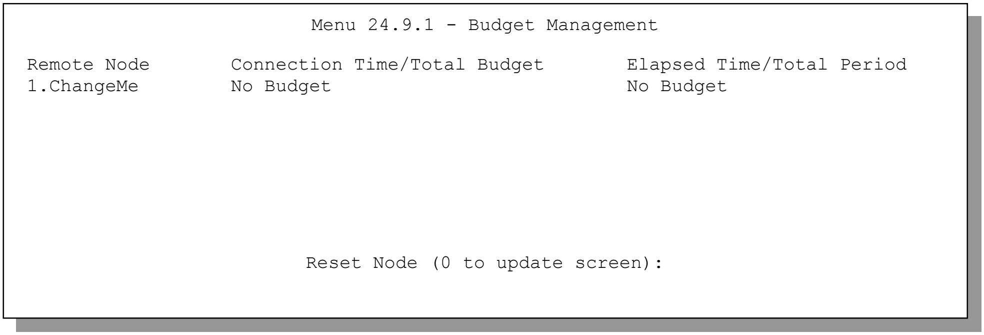


```
                 Menu 24.9 - System Maintenance - Call Control


                        1.Budget Management
                        2.Call History




                          Enter Menu Selection Number:
```

Figure 23-3 Call Control

23.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.



```
                          Menu 24.9.1 - Budget Management

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










                          Reset Node (0 to update screen):
```

Figure 23-4 Budget Management

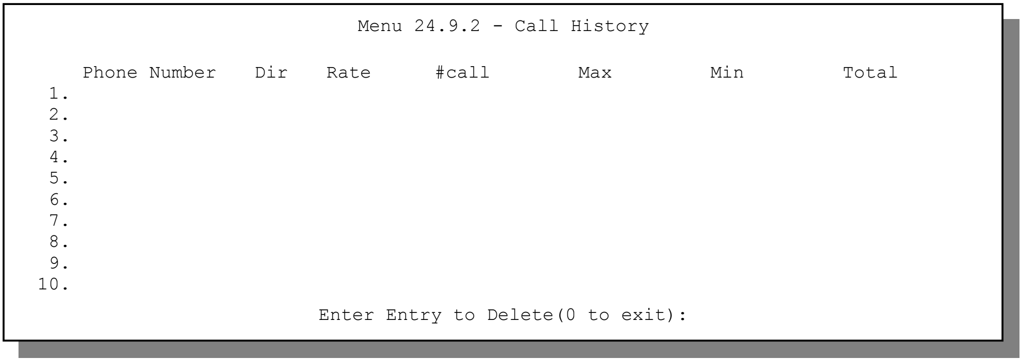
The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes 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 23-1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
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).	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 (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1-hour time period has lapsed.
Enter “0” to update the screen or press [ESC] to return to the previous screen.		

23.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.



```
                              Menu 24.9.2 - 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):
```

Figure 23-5 Call History

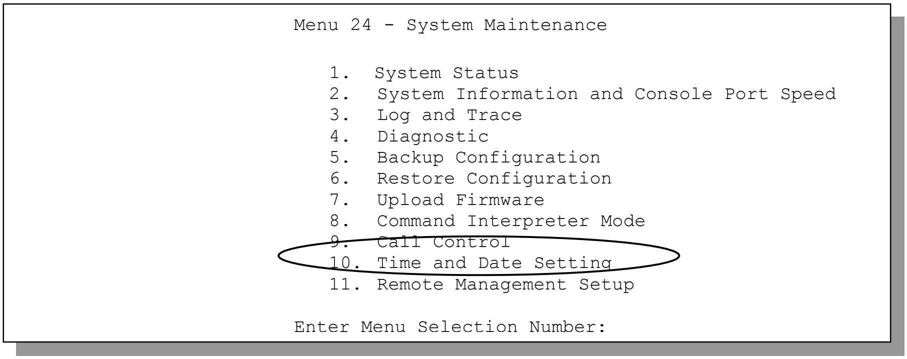
Table 23-2 Call History Fields

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
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.	

23.3 Time and Date Setting

The Real Time Chip (RTC) keeps track of the time and date (Not available on all models). 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 ZyWALL. Menu 24.10 allows you to update the time and date settings of your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs.

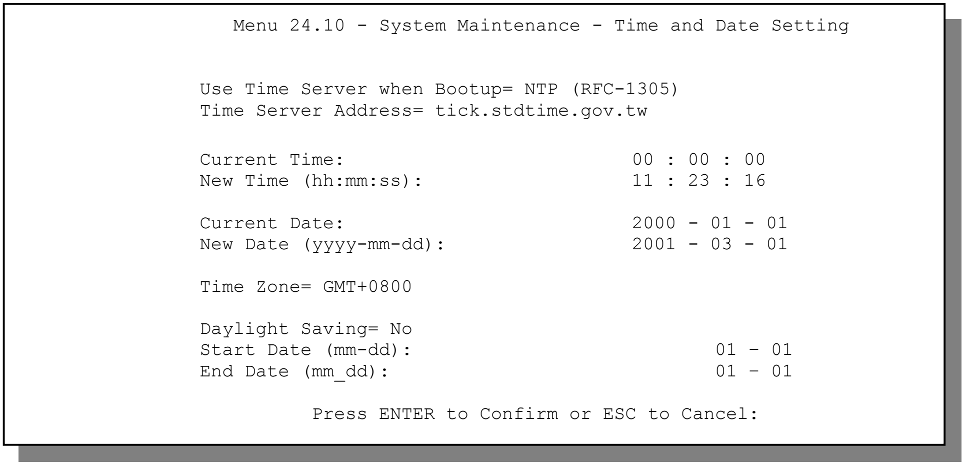
Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.



```
                        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:
```

Figure 23-6 Menu 24: System Maintenance

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your ZyWALL as shown in the following screen.



```
                  Menu 24.10 - System Maintenance - Time and Date Setting


               Use Time Server when Bootup= NTP (RFC-1305)
               Time Server Address= tick.stdtime.gov.tw

               Current Time:                        00 : 00 : 00
               New Time (hh:mm:ss):                 11 : 23 : 16

               Current Date:                        2000 - 01 - 01
               New Date (yyyy-mm-dd):               2001 - 03 - 01

               Time Zone= GMT+0800

               Daylight Saving= No
               Start Date (mm-dd):                         01 – 01
               End Date (mm_dd):                           01 – 01

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

Figure 23-7 Menu 24.10 System Maintenance: Time and Date Setting

Table 23-3 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 ZyWALL. 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 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.

Table 23-3 Time and Date Setting Fields

FIELD	DESCRIPTION
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose **Yes**.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Yes** in the **Daylight Saving** field.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Yes** in the **Daylight Saving** field.
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.	

23.3.1 Resetting the Time

The ZyWALL resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the ZyWALL starts up, if there is a timeserver configured in menu 24.10.

iii. 24-hour intervals after starting.

Chapter 24
Remote Management

This chapter covers remote management found in SMT menu 24.11.

24.1 Remote Management and the Firewall

When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

24.2 Telnet

The only way to configure the ZyWALL for remote management is through an SMT session using the console port. Once your ZyWALL is configured, you can use telnet to configure it remotely as shown next.

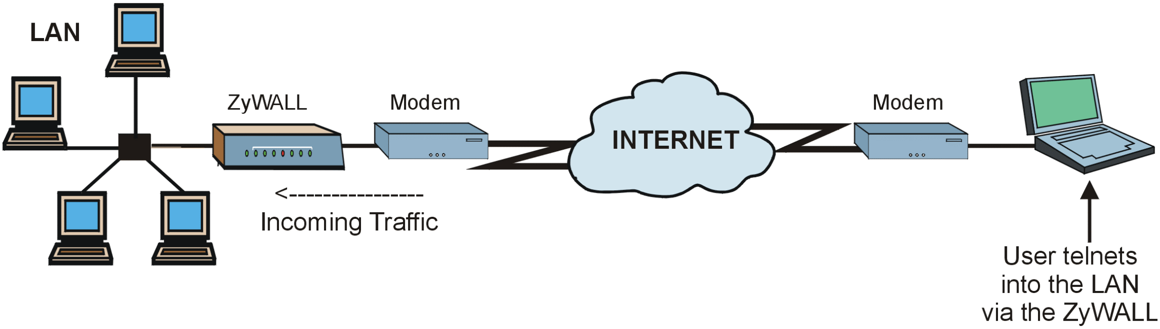


Figure 24-1 Telnet Configuration on a TCP/IP Network

24.3 FTP

You can upload and download the ZyWALL's firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

24.4 Web

You can use the ZyWALL's embedded web configurator for configuration and file management. See the *Using the ZyWALL Web Configurator* chapter for an introduction to the web configurator.

24.5 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. Refer to the *SNMP* chapter for more information.

24.6 DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for example, the IP address of www.zyxel.com is 204.217.0.2. Refer to the *Internet Access* chapter for more information.

24.7 Remote Management

Remote management control is for managing Telnet, Web and FTP services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your ZyWALL from a remote location via:

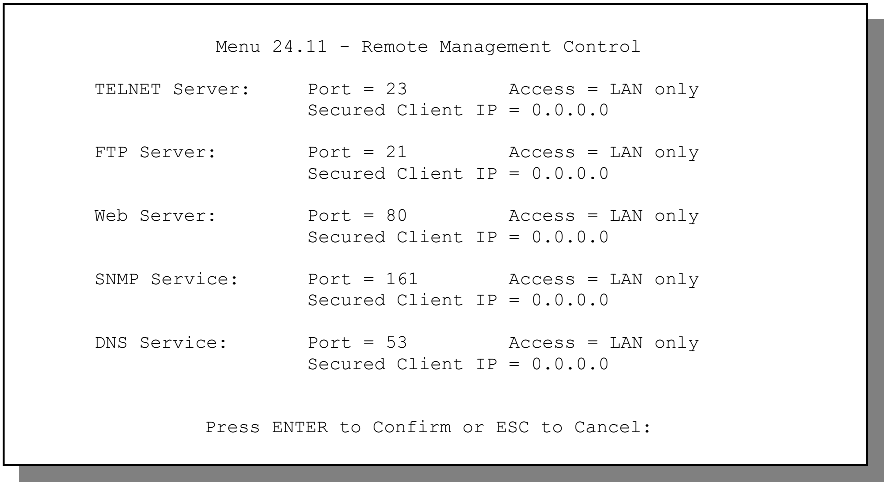
- Internet (WAN only)
- ALL (LAN and WAN)

- LAN only,
- Neither (Disable).

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**.



```
                   Menu 24.11 - Remote Management Control

         TELNET Server:     Port = 23         Access = LAN only
                            Secured Client IP = 0.0.0.0

         FTP Server:        Port = 21         Access = LAN only
                            Secured Client IP = 0.0.0.0

         Web Server:        Port = 80         Access = LAN only
                            Secured Client IP = 0.0.0.0

         SNMP Service:      Port = 161        Access = LAN only
                            Secured Client IP = 0.0.0.0

         DNS Service:       Port = 53         Access = LAN only
                            Secured Client IP = 0.0.0.0


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

Figure 24-2 Menu 24.11 – Remote Management Control

Table 24-1 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a service that you may use to remotely manage the ZyWALL.	
Server Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	23
Server Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.	**LAN Only** (default)

Table 24-1 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyWALL. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
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.		

24.7.1 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 **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
6. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

24.8 Remote Management and NAT

When NAT is enabled:

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

24.9 System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or telnet/web/FTP connections. Your ZyWALL automatically logs you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Part VIII:

Bandwidth Management

This part provides information on the functions and configuration of Bandwidth Management.

Chapter 25
Bandwidth Management

This chapter describes the functions and configuration of bandwidth management. Bandwidth management applies to the ZyWALL 100.

25.1 Introduction

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the ZyWALL forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1000kbps if the broadband device connected to the WAN port has an upstream speed of 1000kbps. All configuration screens display measurements in kbps (kilobits per second), but this *User's Guide* also uses Mbps (megabits per second) for brevity's sake.

25.2 Bandwidth Classes and Filters

Use bandwidth classes and child-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or child-class) based on a specific application and/or subnet. Use the **Class Configuration** tab (see *section 25.8.3*) to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure child-classes with filters for any classes that you configure without filters. The ZyWALL leaves the bandwidth budget allocated and unused for a class that does not have a filter itself or child-classes with filters. View your configured bandwidth classes and child-classes in the **Class Setup** tab (see *section 25.8.2* for details).

The total of the configured bandwidth budgets for child-classes cannot exceed the configured bandwidth budget speed of the parent class.

25.3 Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

25.4 Bandwidth Management Usage Examples

These examples show bandwidth management allotments on a WAN interface that is configured for 10Mbps.

25.4.1 Application-based Bandwidth Management Example

The bandwidth classes in the following example are based solely on application. Each bandwidth class (VoIP, Web, FTP, E-mail and Video) is allotted 2 Mbps.

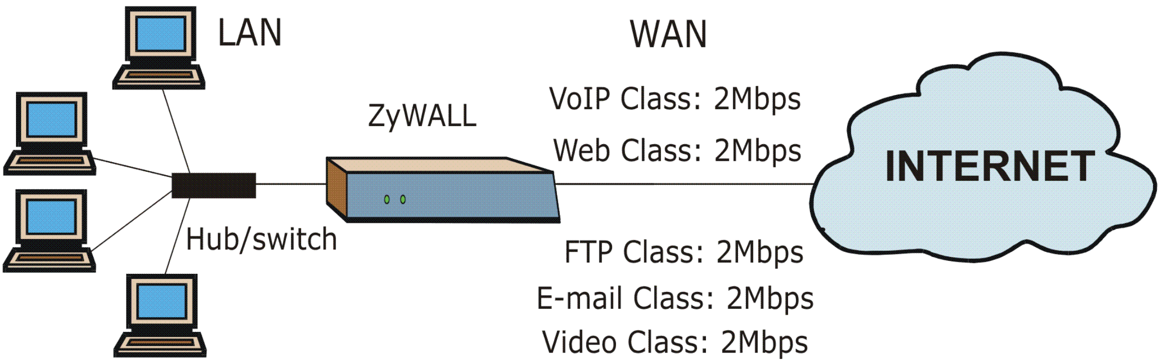


Figure 25-1 Application-based Bandwidth Management Example

25.4.2 Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based solely on LAN subnets. Each bandwidth class (Subnet A and Subnet B) is allotted 5 Mbps.

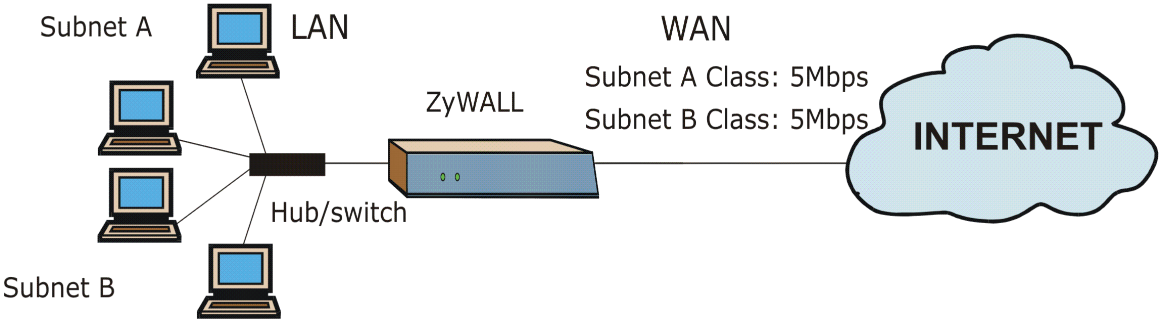


Figure 25-2 Subnet-based Bandwidth Management Example

25.4.3 Application and Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based on LAN subnets and applications (specific applications in each subnet are allotted bandwidth).

Table 25-1 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	1 Mbps	1 Mbps
Web	1 Mbps	1 Mbps
FTP	1 Mbps	1 Mbps
E-mail	1 Mbps	1 Mbps
Video	1 Mbps	1 Mbps

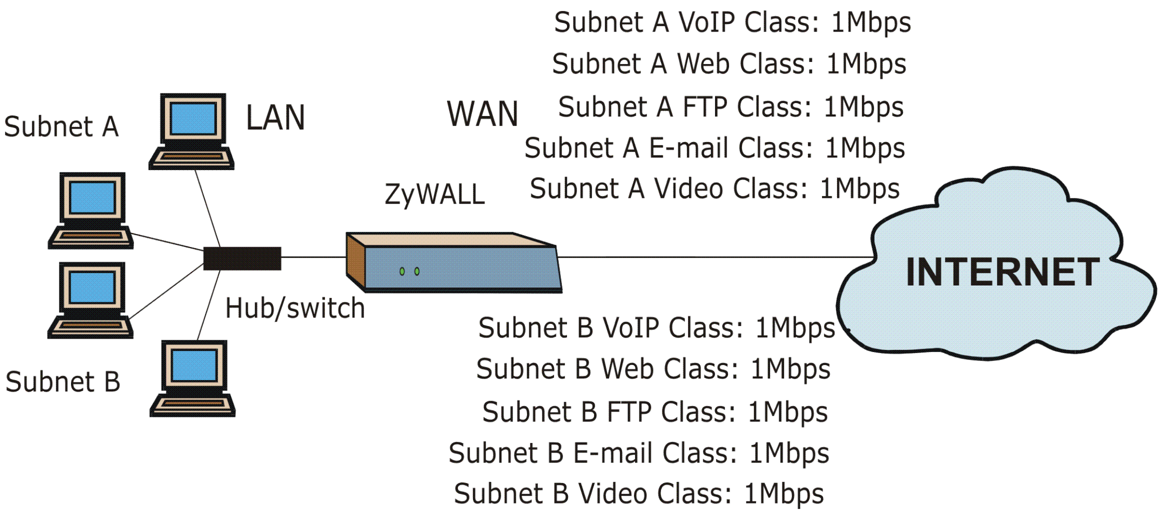

Subnet A VoIP Class: 1Mbps
Subnet A Web Class: 1Mbps
Subnet A FTP Class: 1Mbps
Subnet A E-mail Class: 1Mbps
Subnet A Video Class: 1Mbps
Subnet A
LAN
WAN
ZyWALL
INTERNET
Hub/switch
Subnet B
Subnet B VoIP Class: 1Mbps
Subnet B Web Class: 1Mbps
Subnet B FTP Class: 1Mbps
Subnet B E-mail Class: 1Mbps
Subnet B Video Class: 1Mbps

Figure 25-3 Application and Subnet-based Bandwidth Management Example

25.5 Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The ZyWALL has two types of scheduler: fairness-based and priority-based.

25.5.1 Priority-based Scheduler

With the priority-based scheduler, the ZyWALL forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

25.5.2 Fairness-based Scheduler

The ZyWALL divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

25.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see *Figure 25-7*) allows the ZyWALL to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyWALL first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the ZyWALL divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the ZyWALL gives extra bandwidth to that class.

When multiple classes require more bandwidth, the ZyWALL gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The ZyWALL distributes the available bandwidth equally among classes with the same priority level.

25.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

Do the following three steps to configure the ZyWALL to allow bandwidth for traffic that is not defined in a bandwidth filter.

Step 1. Leave some of the interface's bandwidth unbudgeted.

Step 2. Do not enable the interface's **Maximize Bandwidth Usage** option.

Step 3. Do not enable bandwidth borrowing on the child-classes that have the root class as their parent (see *section 25.7*).

25.6.2 Maximize Bandwidth Usage Example

Here is an example of a ZyWALL that has maximize bandwidth usage enabled on an interface. The first figure shows each bandwidth class's bandwidth budget and priority. The classes are set up based on subnets. The interface is set to 10 Mbps. Each subnet is allocated 2 Mbps. The unbudgeted 2 Mbps allows traffic not defined in one of the bandwidth filters to go out when you do not select the maximize bandwidth option.

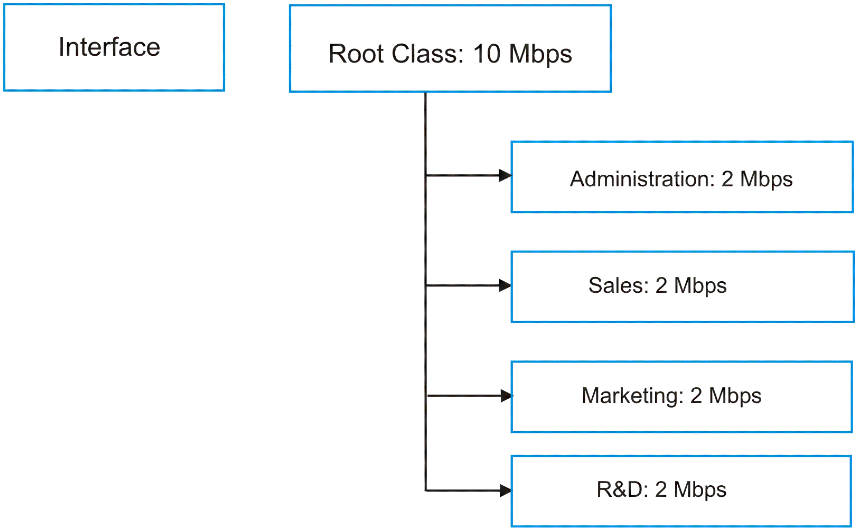


Figure 25-4 Bandwidth Allotment Example

The following figure shows the bandwidth usage with the maximize bandwidth usage option enabled. The ZyWALL divides up the unbudgeted 2 Mbps among the classes that require more bandwidth. If the administration department only uses 1 Mbps of the budgeted 2 Mbps, the ZyWALL also divides the remaining 1 Mbps among the classes that require more bandwidth. Therefore, the ZyWALL divides a total of 3 Mbps total of unbudgeted and unused bandwidth among the classes that require more bandwidth.

In this case, suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1 Mbps of its budgeted 2 Mbps.
- Sales and Marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1.5 Mbps or more of extra bandwidth, the ZyWALL divides the total 3 Mbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1.5 Mbps extra to each for a total of 3.5 Mbps for each) because they both have the highest priority level.
- R&D requires more bandwidth but only gets its budgeted 2 Mbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.
- The ZyWALL does not send any traffic that is not defined in the bandwidth filters because all of the unbudgeted bandwidth goes to the classes that need it.

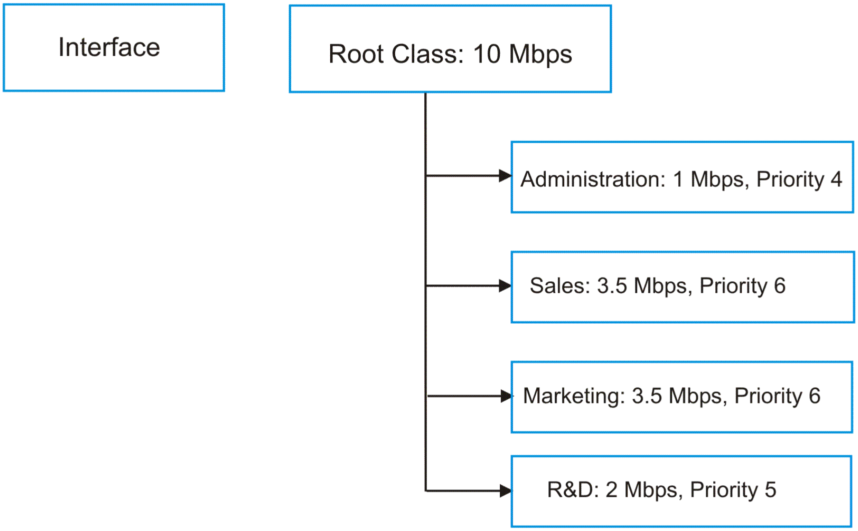

Interface
Root Class: 10 Mbps
Administration: 1 Mbps, Priority 4
Sales: 3.5 Mbps, Priority 6
Marketing: 3.5 Mbps, Priority 6
R&D: 2 Mbps, Priority 5

Figure 25-5 Maximize Bandwidth Usage Example

25.7 Bandwidth Borrowing

Bandwidth borrowing allows a child-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows bandwidth classes to borrow any unused or unbudgeted bandwidth on the whole interface.

Enable bandwidth borrowing on a child-class to allow the child-class to use its parent class's unused bandwidth. A parent class's unused bandwidth is given to the highest priority child-class first. The child-class can also borrow bandwidth from a higher parent class (grandparent class) if the child-class's parent class is also configured to borrow bandwidth from its parent class. This can go on for as many levels as are configured to borrow bandwidth from their parent class (see *section 25.7.1*).

The total of the bandwidth allotments for child-classes cannot exceed the bandwidth allotment of their parent class. The ZyWALL uses the scheduler to divide a parent class's unused bandwidth among the child-classes.

25.7.1 Bandwidth Borrowing Example

Here is an example of bandwidth management with classes configured for bandwidth borrowing. The classes are set up based on departments and individuals within certain departments.

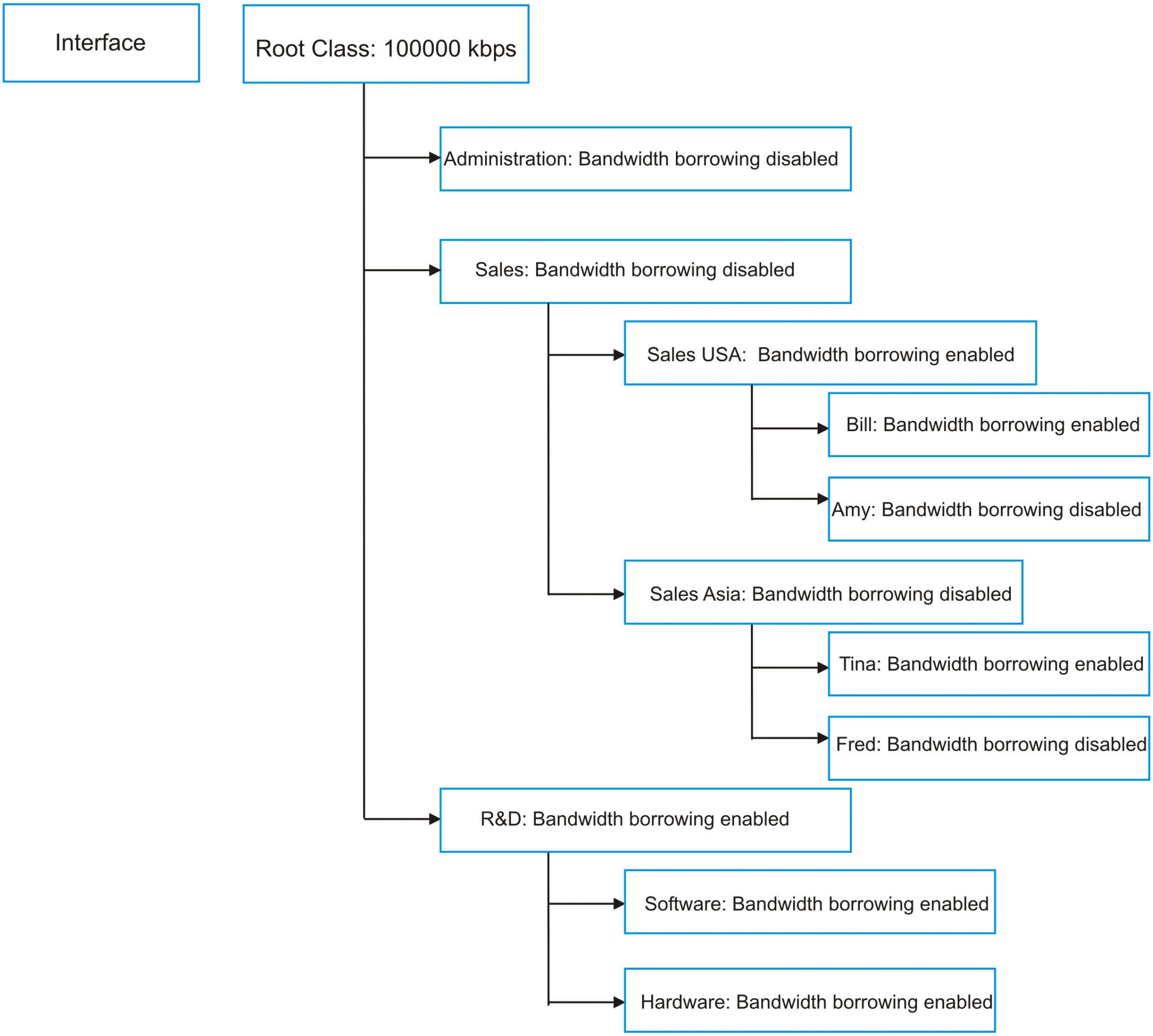

Interface
Root Class: 100000 kbps
Administration: Bandwidth borrowing disabled
Sales: Bandwidth borrowing disabled
Sales USA: Bandwidth borrowing enabled
Bill: Bandwidth borrowing enabled
Amy: Bandwidth borrowing disabled
Sales Asia: Bandwidth borrowing disabled
Tina: Bandwidth borrowing enabled
Fred: Bandwidth borrowing disabled
R&D: Bandwidth borrowing enabled
Software: Bandwidth borrowing enabled
Hardware: Bandwidth borrowing enabled

Figure 25-6 Bandwidth Borrowing Example

- The Bill class can borrow unused bandwidth from the Sales USA class because the Bill class has bandwidth borrowing enabled.
- The Bill class can also borrow unused bandwidth from the Sales class because the Sales USA class also has bandwidth borrowing enabled.

- The Bill class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.
- The Amy class cannot borrow unused bandwidth from the Sales USA class because the Amy class has bandwidth borrowing disabled.
- The R&D Software and Hardware classes can both borrow unused bandwidth from the R&D class because the R&D Software and Hardware classes both have bandwidth borrowing enabled.
- The R&D Software and Hardware classes can also borrow unused bandwidth from the Root class because the R&D class also has bandwidth borrowing enabled.

25.7.2 Maximize Bandwidth Usage With Bandwidth Borrowing

If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual child-classes), the ZyWALL functions as follows.

1. The ZyWALL sends traffic according to each bandwidth class's bandwidth budget.
2. The ZyWALL assigns a parent class's unused bandwidth to its child-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The ZyWALL gives priority to bandwidth child-classes of higher priority and treats bandwidth classes of the same priority equally.
3. The ZyWALL assigns any remaining unused or unbudgeted bandwidth on the interface to any bandwidth class that requires it. The ZyWALL gives priority to bandwidth classes of higher priority and treats bandwidth classes of the same level equally.
4. The ZyWALL assigns any remaining unbudgeted bandwidth to traffic that does not match any of the bandwidth classes.

25.8 Bandwidth Management Setup

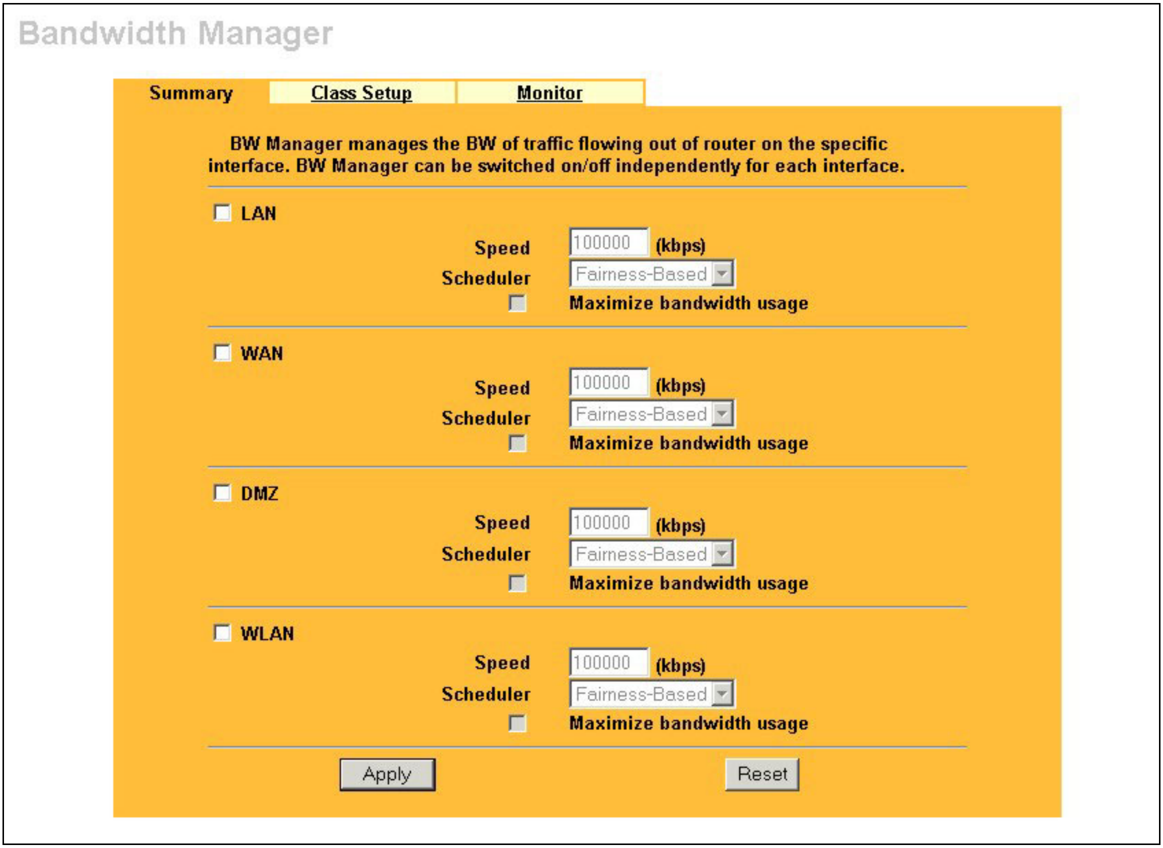
Use the web configurator to access the bandwidth management screens (refer to the chapter on using the ZyWALL web configurator).

Click **Advanced** and then **BW Manager** to access the bandwidth management configuration screens.

25.8.1 Bandwidth Manager Summary

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface in the bandwidth manager's **Summary** tab.

Click **Advanced**, **BW Manager**, and then **Summary** to open the screen shown next.



Bandwidth Manager

BW Manager manages the BW of traffic flowing out of router on the specific interface. BW Manager can be switched on/off independently for each interface.

□ LAN

Speed 100000 (kbps)
Scheduler Fairness-Based
□ Maximize bandwidth usage

□ WAN

Speed 100000 (kbps)
Scheduler Fairness-Based
□ Maximize bandwidth usage

□ DMZ

Speed 100000 (kbps)
Scheduler Fairness-Based
□ Maximize bandwidth usage

□ WLAN

Speed 100000 (kbps)
Scheduler Fairness-Based
□ Maximize bandwidth usage

Figure 25-7 Bandwidth Manager: Summary

Table 25-2 Bandwidth Manager: Summary

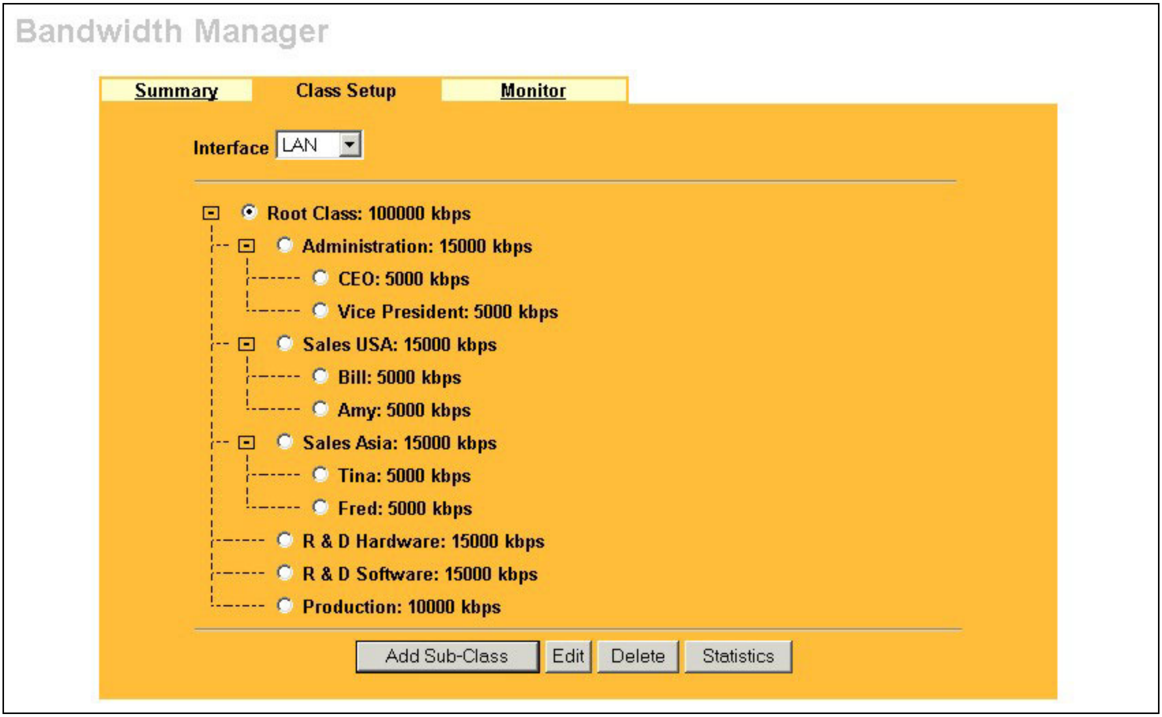
FIELD	DESCRIPTION
LAN WAN DMZ WLAN	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Not all interfaces are available on every ZyWALL.
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class (see *section 25.8.2*). The recommendation is to set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1000 kbps if the broadband device connected to the WAN port has an upstream speed of 1000 kbps.
Scheduler	Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow. Select **Priority-Based** to give preference to bandwidth classes with higher priorities. Select **Fairness-Based** to treat all bandwidth classes equally. See *section 25.5*.
Maximize Bandwidth Usage	Select this check box to have the ZyWALL divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see *section 25.6.1*) or you want to limit the speed of this interface (see the **Speed** field description).
Click **Apply** to save your changes back to the ZyWALL. Click **Reset** to begin configuring this screen afresh.	

25.8.2 Bandwidth Manager Class Setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-" to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see *section 25.8.1* to configure the speed of the interface). Configure child-class layers for the root class.

Click **Advanced**, **BW Manager**, and then the **Class Setup** tab to go to the screen shown next (with example classes).

The example reserves 15 Mbps of unbudgeted bandwidth for traffic that is not defined in the bandwidth filters (see *section 25.6.1*). The Administration, Sales USA and Sales Asia bandwidth classes each have bigger bandwidth budgets than the total of the budgets of their child-classes. The child-classes can borrow the extra bandwidth as long as they have bandwidth borrowing enabled (see *section 25.7*).



Bandwidth Manager

Summary | Class Setup | Monitor

Interface LAN

- ● Root Class: 100000 kbps
  - ○ Administration: 15000 kbps
    - ○ CEO: 5000 kbps
    - ○ Vice President: 5000 kbps
  - ○ Sales USA: 15000 kbps
    - ○ Bill: 5000 kbps
    - ○ Amy: 5000 kbps
  - ○ Sales Asia: 15000 kbps
    - ○ Tina: 5000 kbps
    - ○ Fred: 5000 kbps
  - ○ R & D Hardware: 15000 kbps
  - ○ R & D Software: 15000 kbps
  - ○ Production: 10000 kbps

Figure 25-8 Bandwidth Manager: Class Setup

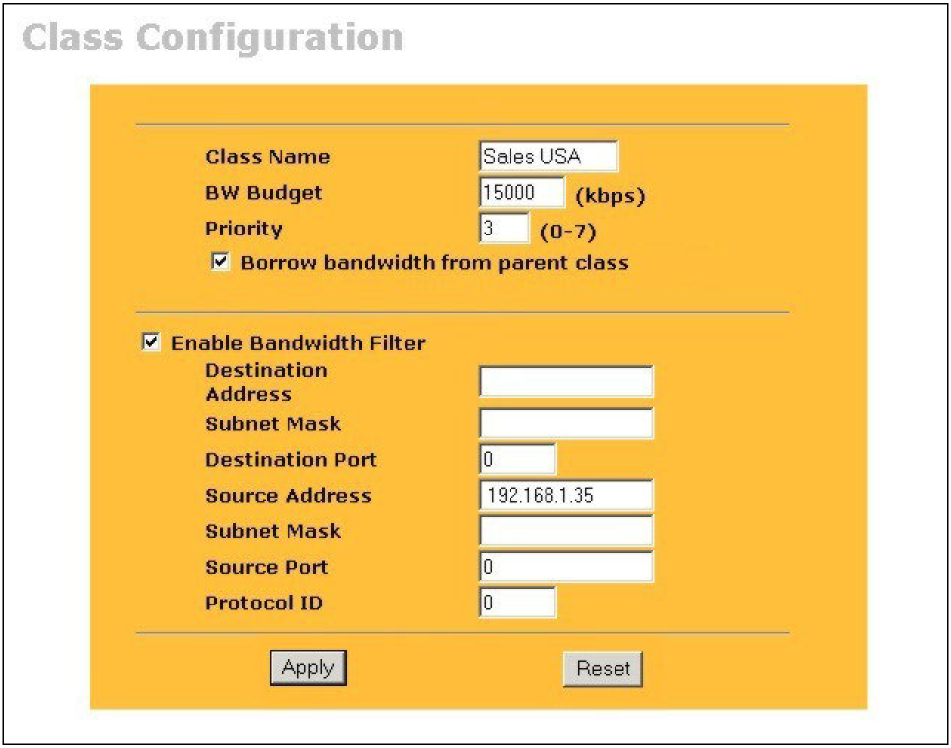
Table 25-3 Bandwidth Manager: Class Setup

FIELD	DESCRIPTION
Interface	Select an interface from the drop-down list box for which you wish to set up classes.
Add Sub-Class	Click **Add Child-class** to add a child-class.
Edit	Click **Edit** to configure the selected class. You cannot edit the root class.
Delete	Click **Delete** to delete the class and all its child-classes. You cannot delete the root class.
Statistics	Click **Statistics** to display the status of the selected class.

25.8.3 Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Configuration** screen. You must use the **Bandwidth Manager Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

Click **Advanced**, **BW Manager**, and then the **Class Setup** tab. Click the **Add Child-Class** button to open the following screen.



Class Configuration

Class Name: Sales USA
BW Budget: 15000 (kbps)
Priority: 3 (0-7)
☑ Borrow bandwidth from parent class

☑ Enable Bandwidth Filter
Destination Address:
Subnet Mask:
Destination Port: 0
Source Address: 192.168.1.35
Subnet Mask:
Source Port: 0
Protocol ID: 0

Figure 25-9 Bandwidth Manager: Class Configuration

Table 25-4 Bandwidth Manager: Class Configuration

FIELD	DESCRIPTION
Class Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.

Table 25-4 Bandwidth Manager: Class Configuration

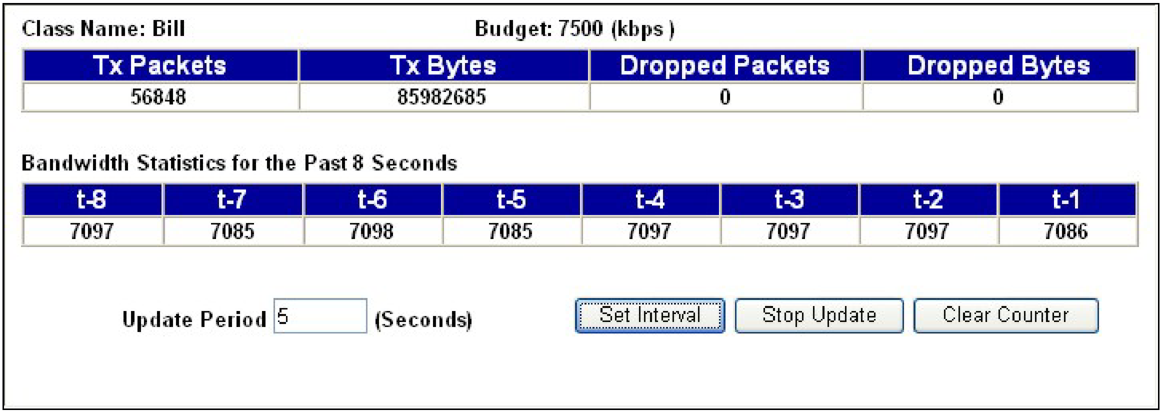
FIELD	DESCRIPTION
BW Budget (kbps)	Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class.
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Borrow bandwidth from parent class	Select this option to allow a child-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget. Bandwidth borrowing is governed by the priority of the child-classes. That is, a child-class with the highest priority (7) is the first to borrow bandwidth from its parent class. Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types (see *25.6.1*) or you want to set the interface's speed to match what the next device in network can handle (see the **Speed** field description in *Table 25-2*).
Enable Bandwidth Filter	Select **Enable Bandwidth Filter** to have the ZyWALL use this bandwidth filter when it performs bandwidth management. You must enter a value in at least one of the following fields (other than the **Subnet Mask** fields which are only available when you enter the destination or source IP address).
Destination Address	Enter the destination IP address in dotted decimal notation.
Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination Address**. Refer to the appendices for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See the chapter on creating custom firewall rules for a table of services and port numbers.
Source Address	Enter the source IP address.
Subnet Mask	Enter the source subnet mask. This field is N/A if you do not specify a **Source Address**. Refer to the appendices for more information on IP subnetting.
Source Port	Enter the port number of the source. See the following table for some common services and port numbers.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.
Click **Apply** to save your changes back to the ZyWALL. Click **Reset** to begin configuring this screen afresh.	

Table 25-5Services 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

25.8.4 Bandwidth Management Statistics

Use the **Bandwidth Management Statistics** screen to view network performance information. Click the **Statistics** button in the **Class Setup** screen to open the **Statistics** screen.



Class Name: Bill

Budget: 7500 (kbps)

Tx Packets	Tx Bytes	Dropped Packets	Dropped Bytes
56848	85982685	0	0

Bandwidth Statistics for the Past 8 Seconds

t-8	t-7	t-6	t-5	t-4	t-3	t-2	t-1
7097	7085	7098	7085	7097	7097	7097	7086

Update Period 5 (Seconds)

Figure 25-10 Bandwidth Management Statistics

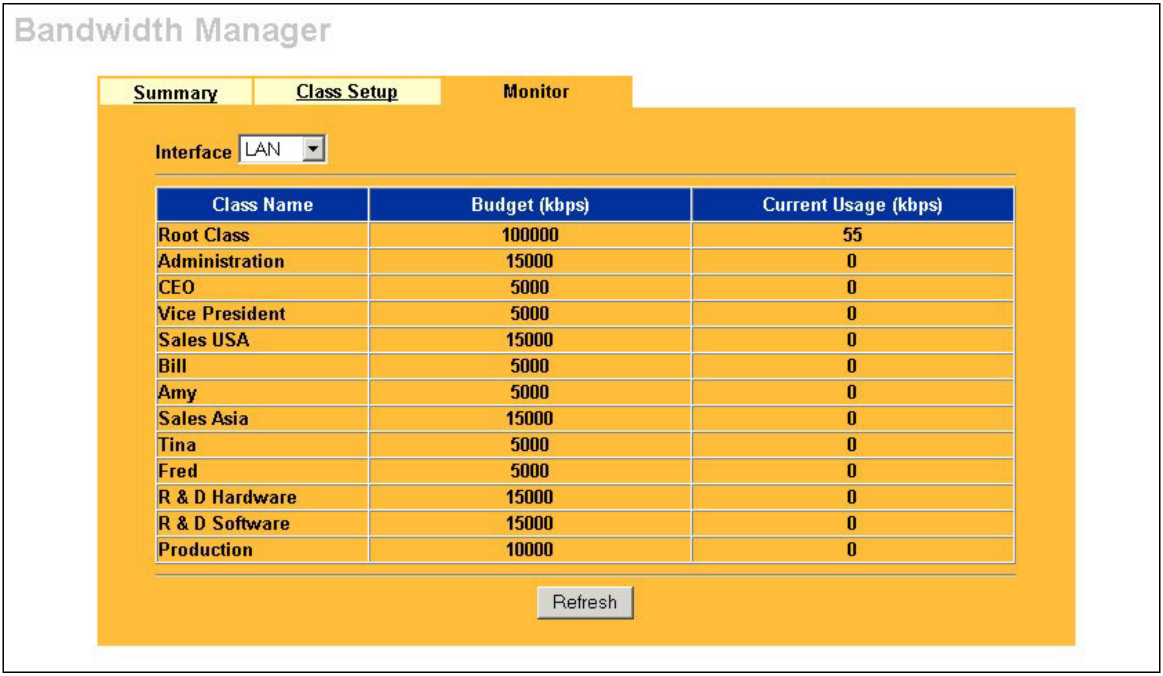
Table 25-6 Bandwidth Management Statistics

FIELD	DESCRIPTION
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
TX Bytes	This field displays the total number of bytes transmitted.
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago.	
Update Period (seconds)	Enter the time interval in seconds to define how often the information should be refreshed.
Set Interval	Click **Set Interval** to apply the new update period you entered in the **Update Period** field above.
Stop Update	Click **Stop Update** to stop the browser from refreshing bandwidth management statistics.
Clear Counter	Click **Clear Counter** to clear all of the bandwidth management statistics.

25.8.5 Bandwidth Manager Monitor

Use the **Bandwidth Manager Monitor** screen to view the device's bandwidth usage and allotments.

Click **Advanced**, **BW Manager**, and then the **Monitor** tab to open the following screen.



Interface LAN

Class Name	Budget (kbps)	Current Usage (kbps)
Root Class	100000	55
Administration	15000	0
CEO	5000	0
Vice President	5000	0
Sales USA	15000	0
Bill	5000	0
Amy	5000	0
Sales Asia	15000	0
Tina	5000	0
Fred	5000	0
R & D Hardware	15000	0
R & D Software	15000	0
Production	10000	0

Figure 25-11 Bandwidth Manager Monitor

Table 25-7 Bandwidth Manager Monitor

FIELD	DESCRIPTION
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.
Class Name	This field displays the name of the class.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Current Usage (kbps)	This field displays the amount of bandwidth that each class is using.
Click **Refresh** to update the page.	

Part IX:

IP Policy Routing, Call Scheduling and VPN/IPSec

This part provides information on how to configure IP Policy Routing, call scheduling and VPN/IPSec.

Chapter 26
IP Policy Routing

This chapter covers setting and applying policies used for IP routing. IP Policy Routing applies to the ZyWALL 100.

26.1 Introduction

Traditionally, routing is based on the destination address only and the ZyWALL takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. This feature is not available on all models.

26.2 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or ToS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

26.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, ToS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

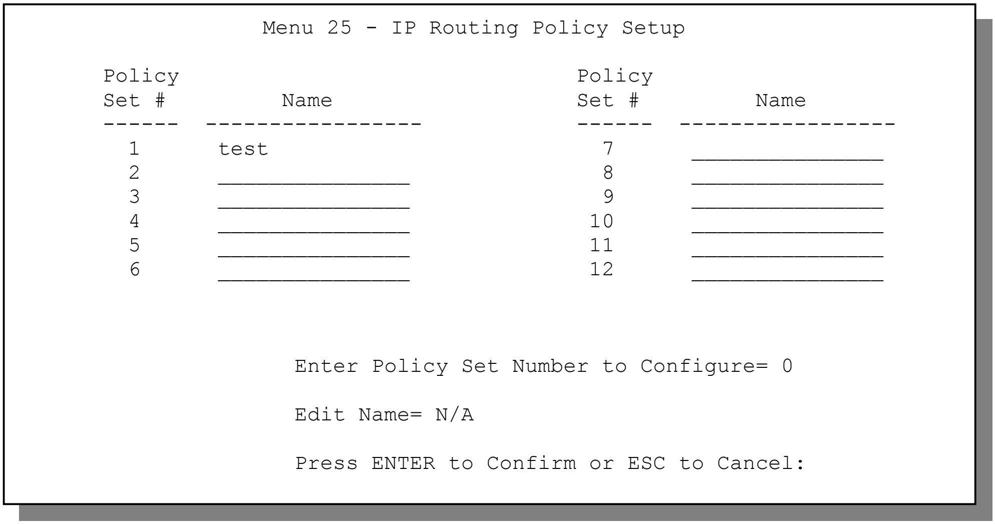
The actions that can be taken include:

- Routing the packet to a different gateway (and hence the outgoing interface).
- Setting the ToS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

26.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.



```
                    Menu 25 - IP Routing Policy Setup

       Policy                               Policy
       Set #         Name                   Set #         Name
       ------  -----------------            ------  -----------------
         1      test                          7      _______________
         2      _______________               8      _______________
         3      _______________               9      _______________
         4      _______________              10      _______________
         5      _______________              11      _______________
         6      _______________              12      _______________


                      Enter Policy Set Number to Configure= 0

                      Edit Name= N/A

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

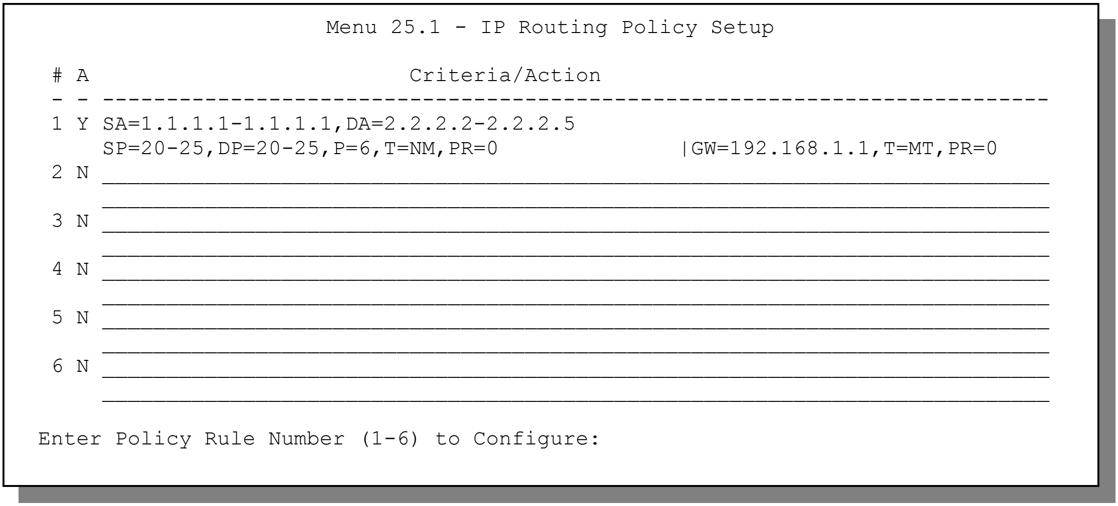
Figure 26-2 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

Step 1. Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup.**

Step 2. Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator “|” means the action is taken on criteria matched and separator “=” means the action is taken on criteria not matched.



```
                      Menu 25.1 - IP Routing Policy Setup

 # A                        Criteria/Action
 - - --------------------------------------------------------------------------
 1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
     SP=20-25,DP=20-25,P=6,T=NM,PR=0              |GW=192.168.1.1,T=MT,PR=0
 2 N __________________________________________________________________________
     __________________________________________________________________________
 3 N __________________________________________________________________________
     __________________________________________________________________________
 4 N __________________________________________________________________________
     __________________________________________________________________________
 5 N __________________________________________________________________________
     __________________________________________________________________________
 6 N __________________________________________________________________________
     __________________________________________________________________________

Enter Policy Rule Number (1-6) to Configure:
```

Figure 26-4 Menu 25.1: Sample IP Routing Policy Setup

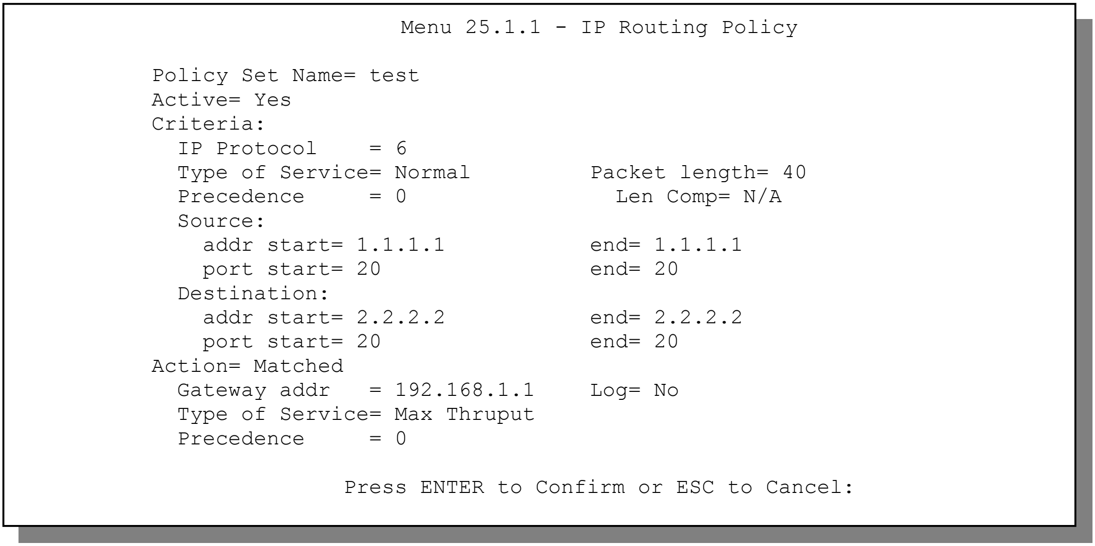
Table 26-1 IP Routing Policy Setup

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17…)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address

Table 26-1 IP Routing Policy Setup

ABBREVIATION	MEANING
T	Outgoing Type of service
P	Outgoing Precedence
Service NM	Normal
MD	Minimum Delay
MT	Maximum Throughput
MR	Maximum Reliability
MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.



```
                              Menu 25.1.1 - IP Routing Policy

           Policy Set Name= test
           Active= Yes
           Criteria:
             IP Protocol    = 6
             Type of Service= Normal         Packet length= 40
             Precedence     = 0                Len Comp= N/A
             Source:
               addr start= 1.1.1.1           end= 1.1.1.1
               port start= 20                end= 20
             Destination:
               addr start= 2.2.2.2           end= 2.2.2.2
               port start= 20                end= 20
           Action= Matched
             Gateway addr   = 192.168.1.1    Log= No
             Type of Service= Max Thruput
             Precedence     = 0

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

Figure 26-5 IP Routing Policy

Table 26-2 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in **Menu 25 – IP Routing Policy Setup**.

Table 26-2 IP Routing Policy

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the policy.
Criteria	
IP Protocol	Enter a number that represents an IP layer 4 protocol, for example, UDP=17, TCP=6, ICMP=1 and Don't care=0.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the ZYWALL if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **No Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are 0 to 7 or **No Change**.
Log	Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed.

Table 26-2 IP Routing Policy

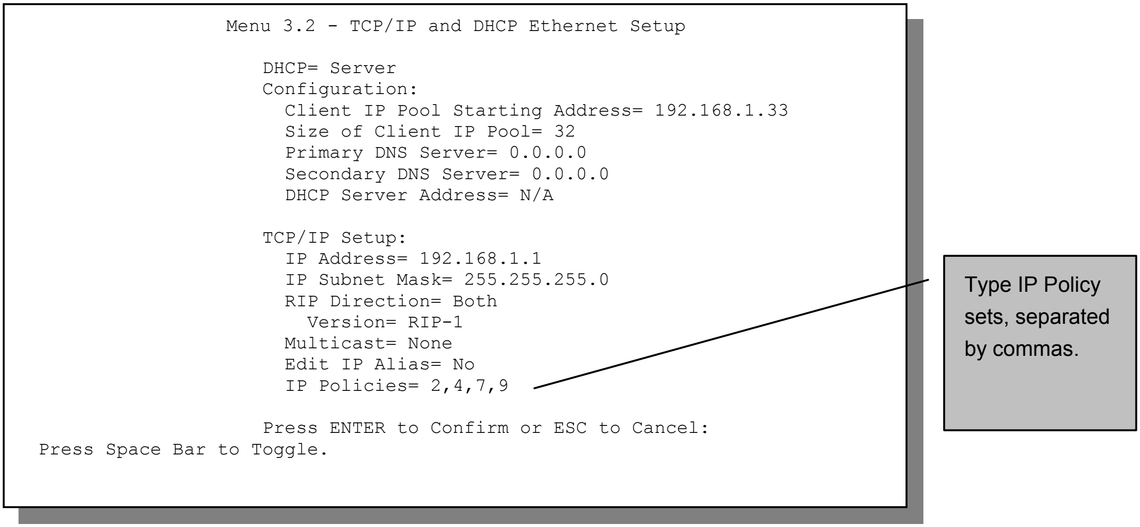
FIELD	DESCRIPTION
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

26.5 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

26.5.1 Ethernet IP Policies

From **Menu 3 – Ethernet Setup**, type 2 to go to **Menu 3.2 – TCP/IP and DHCP Ethernet Setup**. You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.



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

                       DHCP= Server
                       Configuration:
                         Client IP Pool Starting Address= 192.168.1.33
                         Size of Client IP Pool= 32
                         Primary DNS Server= 0.0.0.0
                         Secondary DNS Server= 0.0.0.0
                         DHCP Server Address= N/A

                       TCP/IP Setup:
                         IP Address= 192.168.1.1
                         IP Subnet Mask= 255.255.255.0
                         RIP Direction= Both
                           Version= RIP-1
                         Multicast= None
                         Edit IP Alias= No
                         IP Policies= 2,4,7,9

                       Press ENTER to Confirm or ESC to Cancel:
   Press Space Bar to Toggle.
```

Type IP Policy sets, separated by commas.

Figure 26-6 Menu 3.2: TCP/IP and DHCP Ethernet Setup

26.6 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

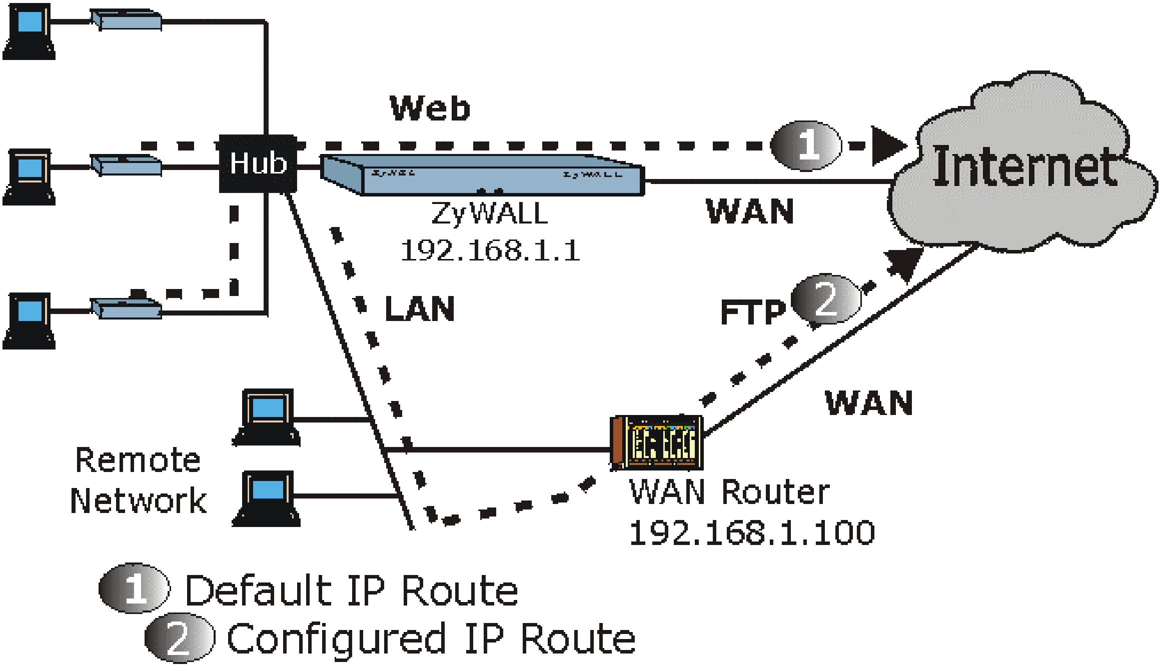
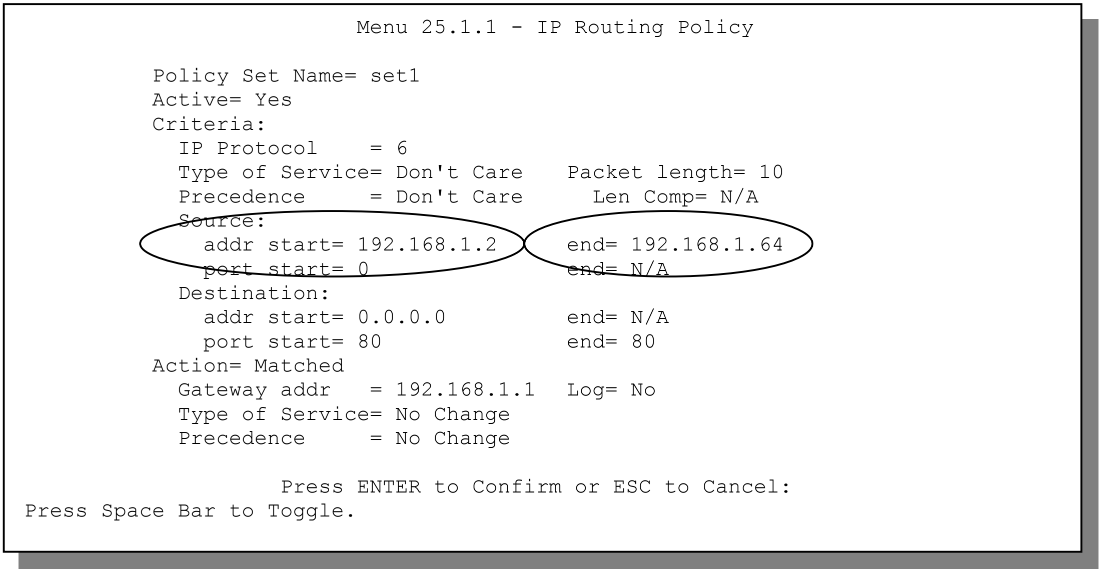


Figure 26-7 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the ZyWALL, follow the steps as shown next.

Step 1. Create a routing policy set in menu 25.

Step 2. Create a rule for this set in **Menu 25.1.1 - IP Routing Policy** as shown next.



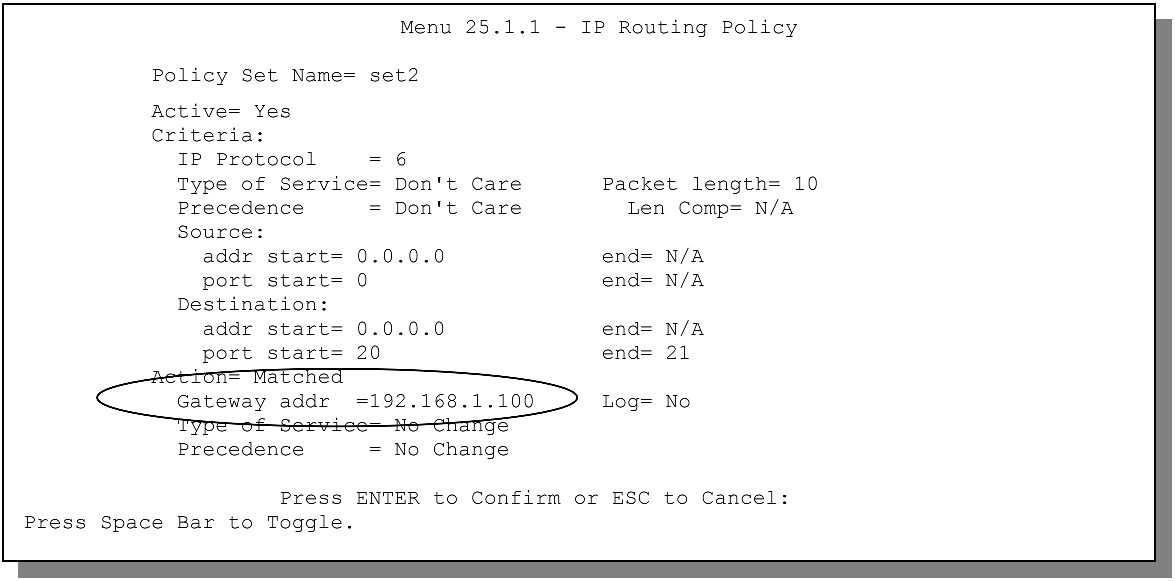
```
                           Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set1
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care   Packet length= 10
            Precedence     = Don't Care     Len Comp= N/A
            Source:
              addr start= 192.168.1.2     end= 192.168.1.64
              port start= 0               end= N/A
            Destination:
              addr start= 0.0.0.0         end= N/A
              port start= 80              end= 80
          Action= Matched
            Gateway addr   = 192.168.1.1  Log= No
            Type of Service= No Change
            Precedence     = No Change

                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 26-8 IP Routing Policy Example

Step 3. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 4. Create another policy set in menu 25.

Step 5. Create a rule in menu 25.1.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

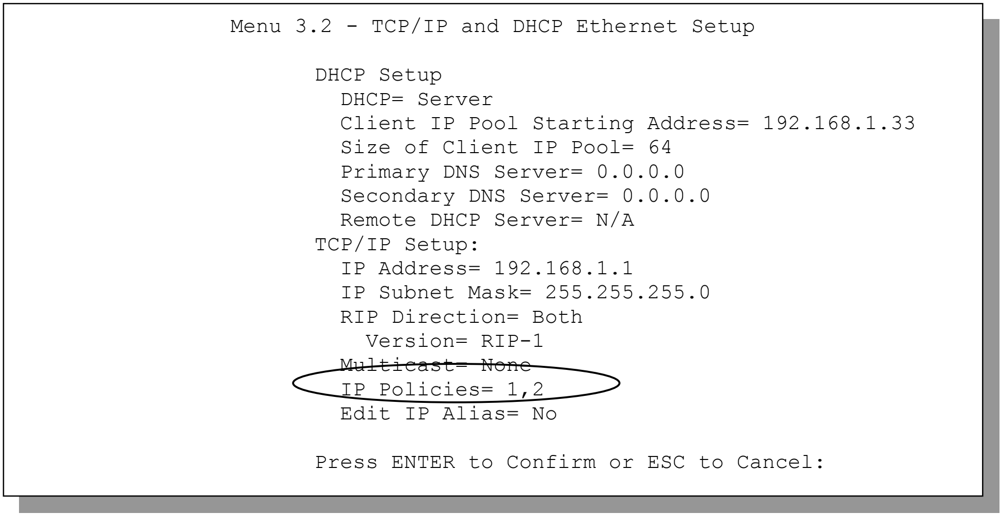


```
                              Menu 25.1.1 - IP Routing Policy

           Policy Set Name= set2

           Active= Yes
           Criteria:
             IP Protocol    = 6
             Type of Service= Don't Care      Packet length= 10
             Precedence     = Don't Care        Len Comp= N/A
             Source:
               addr start= 0.0.0.0            end= N/A
               port start= 0                  end= N/A
             Destination:
               addr start= 0.0.0.0            end= N/A
               port start= 20                 end= 21
           Action= Matched
             Gateway addr  =192.168.1.100     Log= No
             Type of Service= No Change
             Precedence     = No Change

                     Press ENTER to Confirm or ESC to Cancel:
 Press Space Bar to Toggle.
```

Figure 26-9 IP Routing Policy

Step 6. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 7. Apply both policy sets in menu 3.2 as shown next.



```
                     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= 64
                              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
                              Multicast= None
                              IP Policies= 1,2
                              Edit IP Alias= No

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

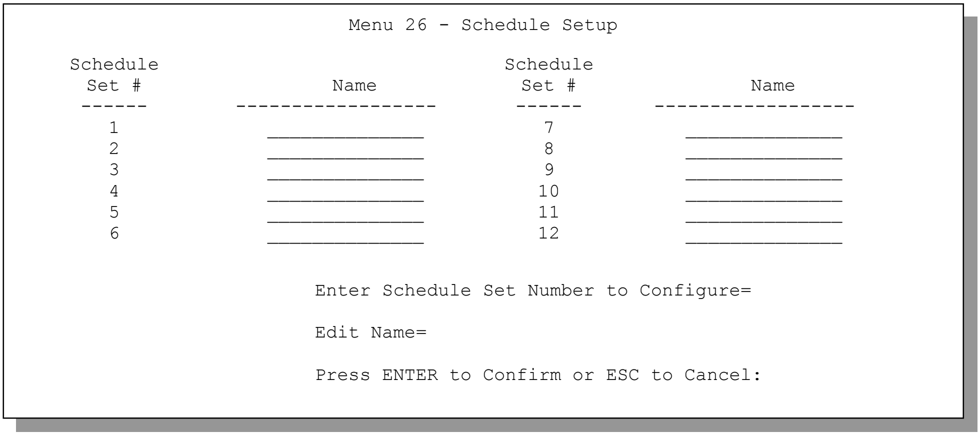
Figure 26-10 Applying IP Policies

Chapter 27
Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

27.1 Introduction

The call scheduling feature allows the ZyWALL 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.



```
                          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=

                        Edit Name=

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

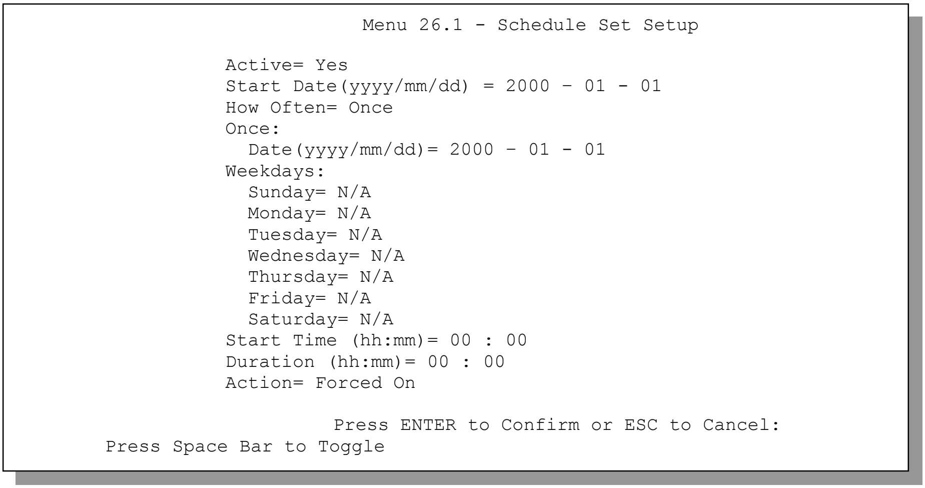
Figure 27-1 Menu 26 - Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node, then set 1 will take precedence over set 2, 3 and 4 as the ZyWALL, 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.

To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] or [DEL] in the Edit Name field.

To set up 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.



```
                         Menu 26.1 - Schedule Set Setup

                 Active= Yes
                 Start Date(yyyy/mm/dd) = 2000 - 01 - 01
                 How Often= Once
                 Once:
                   Date(yyyy/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:
      Press Space Bar to Toggle
```

Figure 27-2 Schedule Set Setup

If a connection has been already established, your ZyWALL 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**.

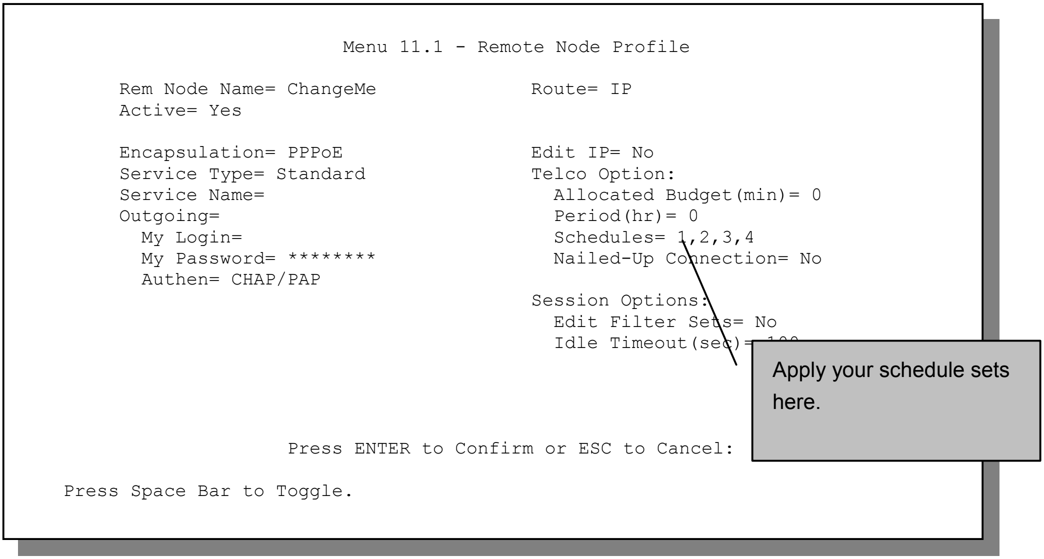
Table 27-1Schedule Set Setup Fields

FIELD	DESCRIPTION	OPTIONS
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.	**Yes** **No**
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 [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** **Weekly**

Table 27-1Schedule Set Setup Fields

FIELD	DESCRIPTION	OPTIONS
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.	
Weekday: 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].	**Yes** **No** **N/A**
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.	
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.	**Forced On** **Forced Down** **Enable Dial-On-Demand** **Disable Dial-On-Demand**
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.		

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. Press [SPACE BAR] and then [ENTER] to select **PPPoE** in the **Encapsulation** field to make the schedule sets field available as shown next.

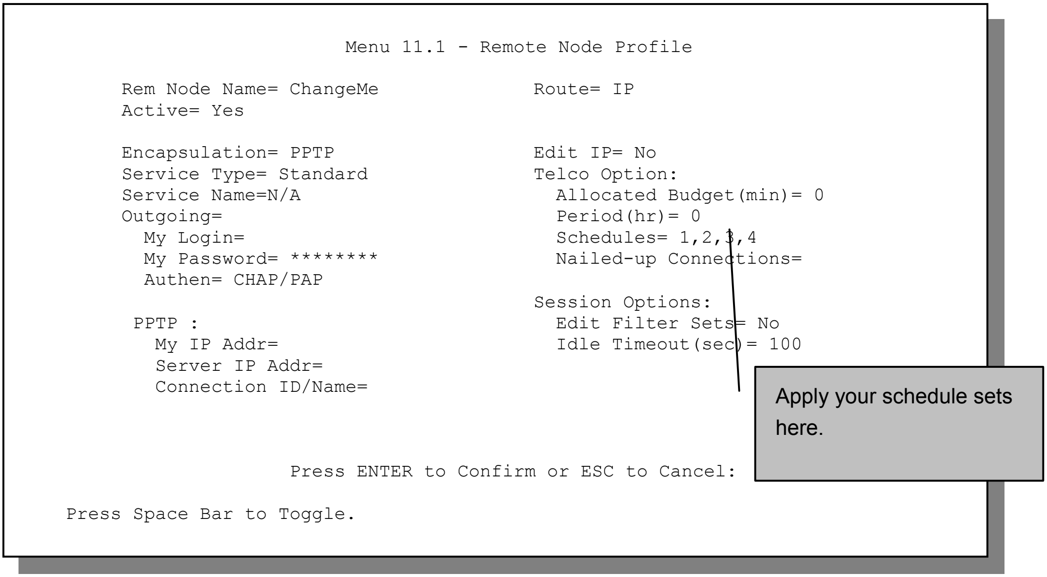


```
                         Menu 11.1 - Remote Node Profile

      Rem Node Name= ChangeMe              Route= IP
      Active= Yes

      Encapsulation= PPPoE                 Edit IP= No
      Service Type= Standard               Telco Option:
      Service Name=                          Allocated Budget(min)= 0
      Outgoing=                              Period(hr)= 0
        My Login=                            Schedules= 1,2,3,4
        My Password= ********                Nailed-Up Connection= No
        Authen= CHAP/PAP
                                           Session Options:
                                             Edit Filter Sets= No
                                             Idle Timeout(sec)= 100




                      Press ENTER to Confirm or ESC to Cancel:

   Press Space Bar to Toggle.
```

Apply your schedule sets here.

Figure 27-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).



```
                       Menu 11.1 - Remote Node Profile

     Rem Node Name= ChangeMe              Route= IP
     Active= Yes

     Encapsulation= PPTP                  Edit IP= No
     Service Type= Standard               Telco Option:
     Service Name=N/A                       Allocated Budget(min)= 0
     Outgoing=                              Period(hr)= 0
       My Login=                            Schedules= 1,2,3,4
       My Password= ********                Nailed-up Connections=
       Authen= CHAP/PAP
                                          Session Options:
      PPTP :                                Edit Filter Sets= No
        My IP Addr=                         Idle Timeout(sec)= 100
        Server IP Addr=
        Connection ID/Name=


                    Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Apply your schedule sets here.

Figure 27-4 Applying Schedule Set(s) to a Remote Node (PPTP)

Chapter 28
Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

28.1 Introduction

28.1.1 VPN

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.

28.1.2 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.

28.1.3 Security Association

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

28.1.4 Other Terminology

- **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.

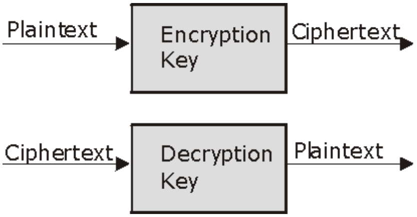


Figure 28-1 Encryption and Decryption

- **Data Confidentiality**

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

- **Data Integrity**

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

- **Data Origin Authentication**

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

28.1.5 VPN Applications

The ZyWALL 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.

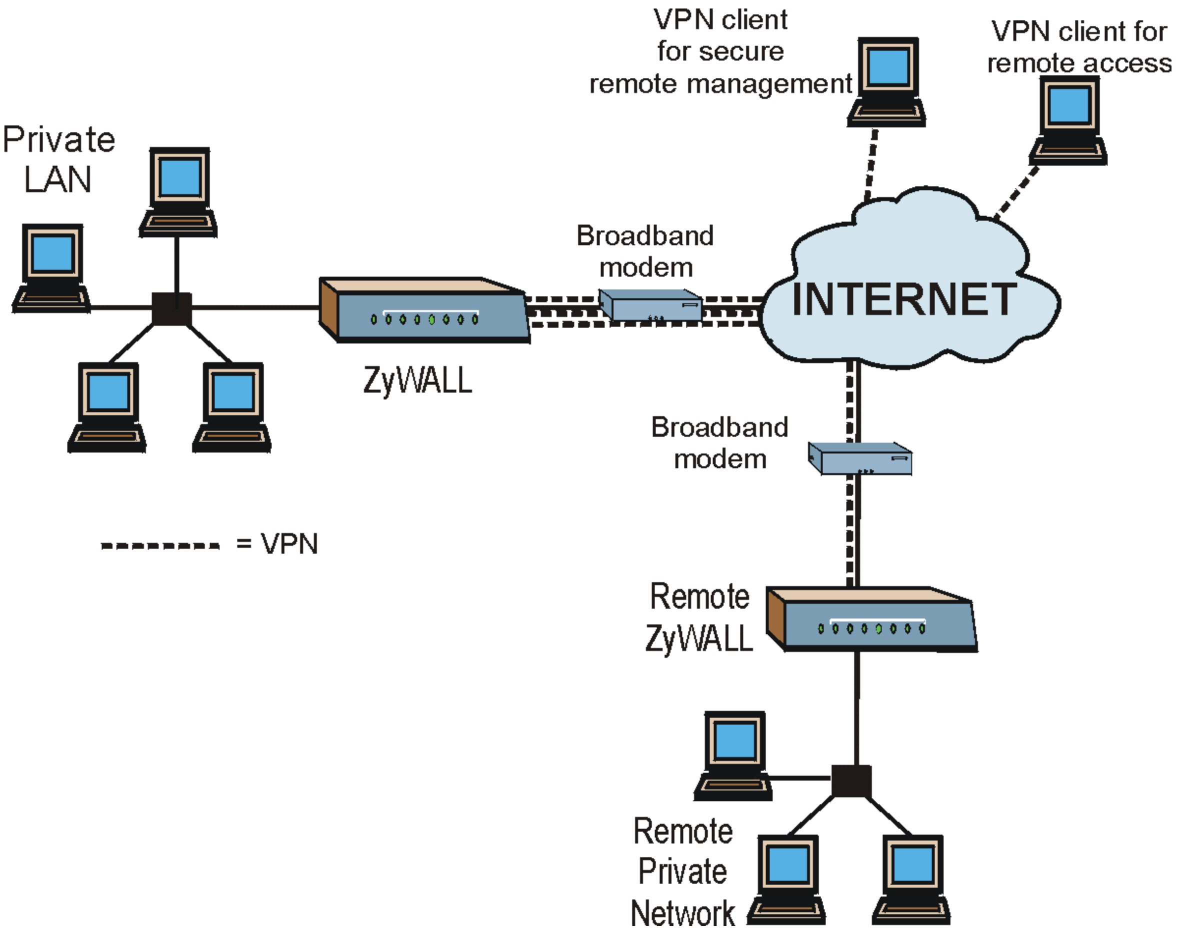


Figure 28-2 VPN Application

28.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

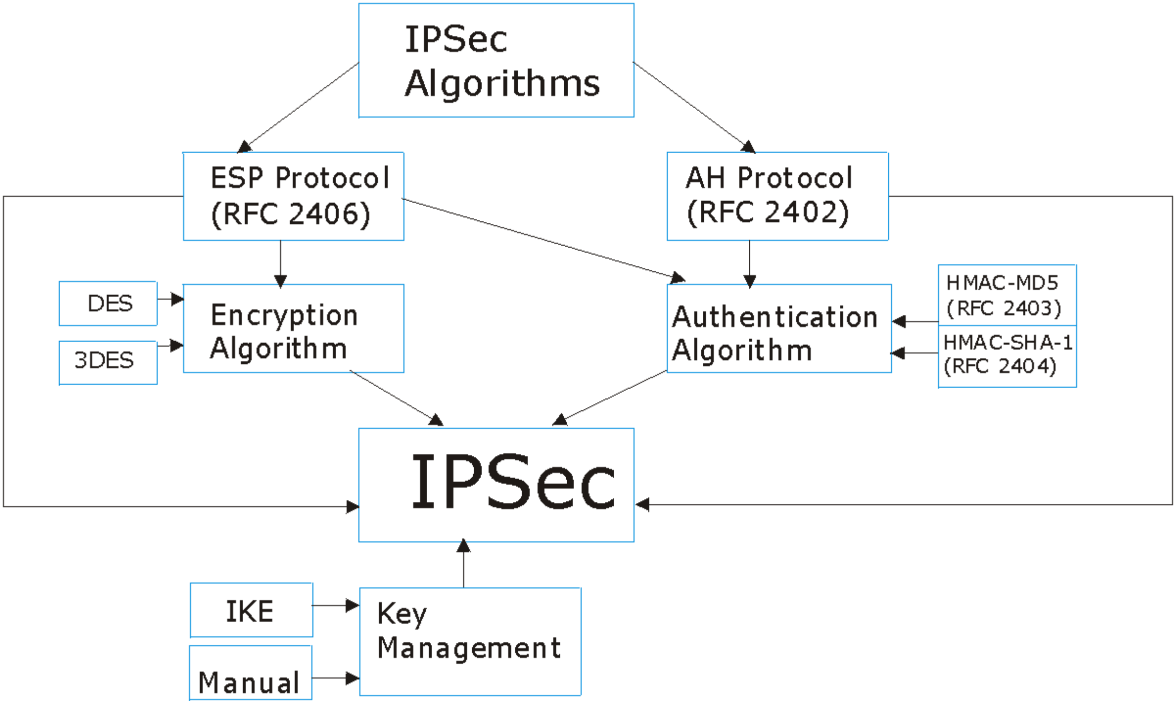


Figure 28-3 IPSec Architecture

28.2.1 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 29.2* for more information.

28.2.2 Key Management

Key Management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN. Please see *sections 29.5* and *29.6* for more information.

28.3 Encapsulation

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

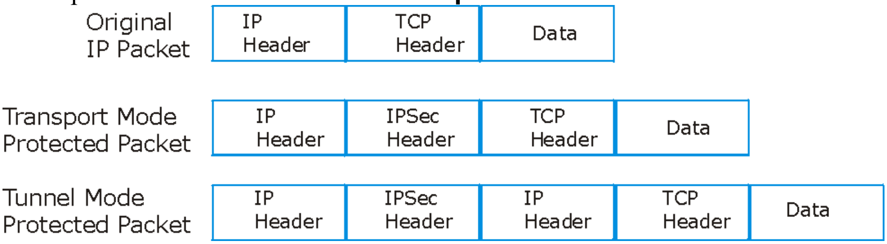


Figure 28-4 Transport and Tunnel Mode IPSec Encapsulation

28.3.1 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.

28.3.2 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.

28.4 IPSec and NAT

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

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.

Table 28-1 VPN and NAT

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

Chapter 29
VPN/IPSec Setup

This chapter introduces the VPN SMT menus. See the Logs chapter and the appendices for information on IPSec logs.

29.1 VPN/IPSec Setup

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.

This is an overview of the VPN menu tree.

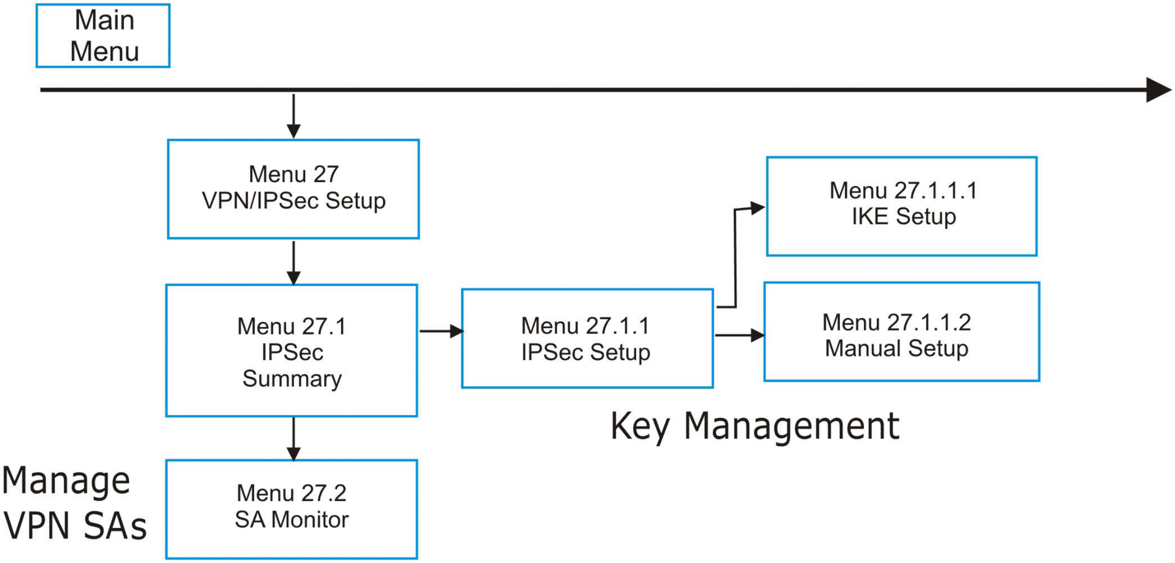
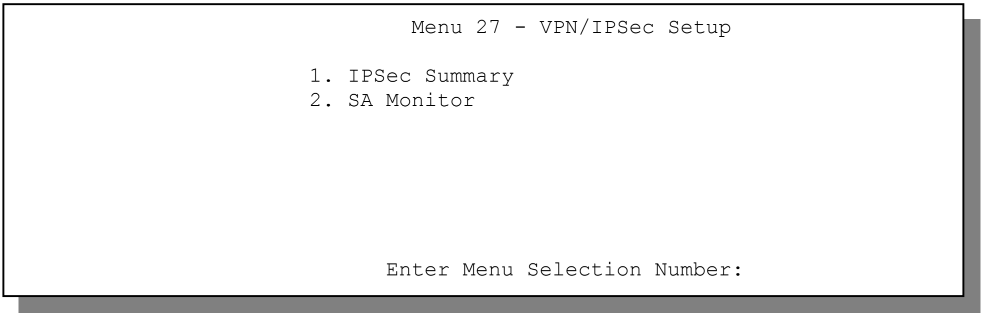


Figure 29-1 VPN SMT Menu Tree

From the main menu, enter 27 to display the first VPN menu (shown next).



```
                    Menu 27 - VPN/IPSec Setup

                1. IPSec Summary
                2. SA Monitor






                   Enter Menu Selection Number:
```

Figure 29-2 Menu 27: VPN/IPSec Setup

29.2 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.

29.2.1 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.

29.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of 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 29-1 AH and ESP

ESP	AH
Select **DES** for minimal security and **3DES** for maximum. Select **NULL** to set up a tunnel without encryption.	Select **MD5** for minimal security and **SHA-1** for maximum security.
DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet 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.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

29.3 IPSec Summary

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.

The following figure helps explain the main fields in menu 27.1.

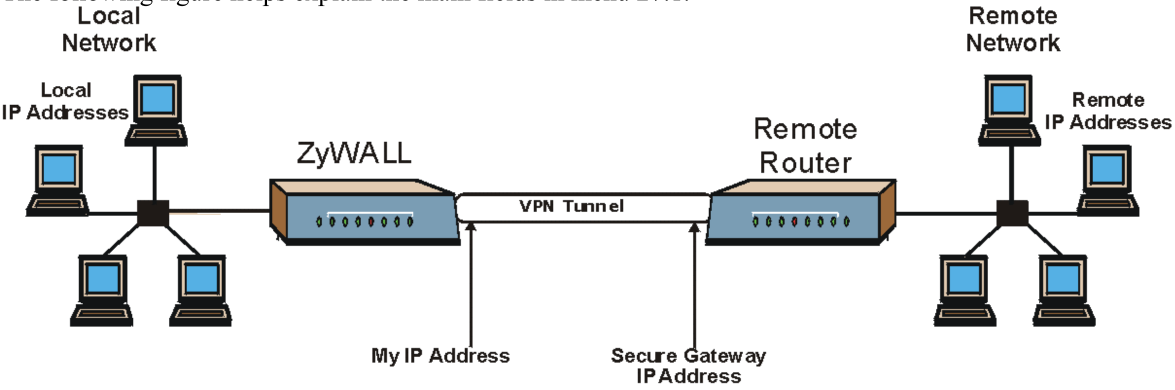


Figure 29-3 IPSec Summary Fields

Local and remote IP addresses must be static.

29.3.1 Keep Alive

A tunnel with no outbound or inbound traffic is "idle" and stays connected until the IPSec SA lifetime period expires (see *section 29.5*). The ZyWALL automatically renegotiates the IPSec SA if there is traffic when the

IPSec SA lifetime period expires. If there is no traffic when the IPSec SA lifetime period expires, the tunnel is dropped and will have to be renegotiated the next time that someone attempts to send traffic, unless you enable keep alive.

Keep alive allows you to set the ZyWALL to automatically renegotiate the IPSec SA at the end of the IPSec SA lifetime, even if there is no traffic. Both IPSec routers must have a ZyWALL-compatible keep alive enabled in order for this feature to work.

When there is outbound traffic with no inbound traffic, the ZyWALL automatically drops the tunnel after two minutes.

29.3.2 ID Type and Content

The ZyWALL identifies an individual SA by its type of ID and the contents of its ID.

With aggressive negotiation mode (see *section 29.5.2*), the ZyWALL can distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic IP addresses. For example, telecommuters can use separate passwords to simultaneously connect to the ZyWALL from IPSec routers with dynamic IP addresses.

With main mode (see *section 29.5.2*), 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 29-2 Local Fields

LOCAL ID TYPE=	CONTENT=
IP	N/A, do not enter anything.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyWALL.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyWALL.
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 29-3 Peer Fields

LOCAL ID TYPE=	CONTENT=
IP	N/A, do not enter anything.
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 Addr** field below.	

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel. The two ZyWALLs in this example can complete negotiation and establish a VPN tunnel.

Table 29-4 Matching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
Local ID type: IP	Local ID type: IP
Local ID content: N/A	Local ID content: N/A
Local IP address: 1.1.1.1	Local IP address: 1.1.1.2
Peer ID type: IP	Peer ID type: IP
Peer ID content: N/A	Peer ID content: N/A
Peer IP address: 1.1.1.2	Peer IP address: 1.1.1.1

The two ZyWALLs in this example cannot complete their negotiation because ZyWALL B's **Local ID type** is **IP**, but ZyWALL A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 29-5 Mismatching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
Local ID type: IP	**Local ID type: IP**
Local ID content: N/A	Local ID content: N/A
Local IP address: 1.1.1.1	Local IP address: 1.1.1.2
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A
Peer IP address: 1.1.1.2	Peer IP address: 1.1.1.1

29.3.3 My IP Address

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

29.3.4 Secure Gateway Address

Secure Gateway Addr 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 Addr** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Addr** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Addr** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyWALL 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).

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 in the **Secure Gateway Addr** field. 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. See the following table for an example configuration.

You can configure multiple SAs to simultaneously connect through the same secure gateway. In this case, you must configure the SAs to have the same **Negotiation Mode** and **Pre-Shared Key** (**Menu 27.1.1.1 IKE Setup**).

Table 29-6 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.

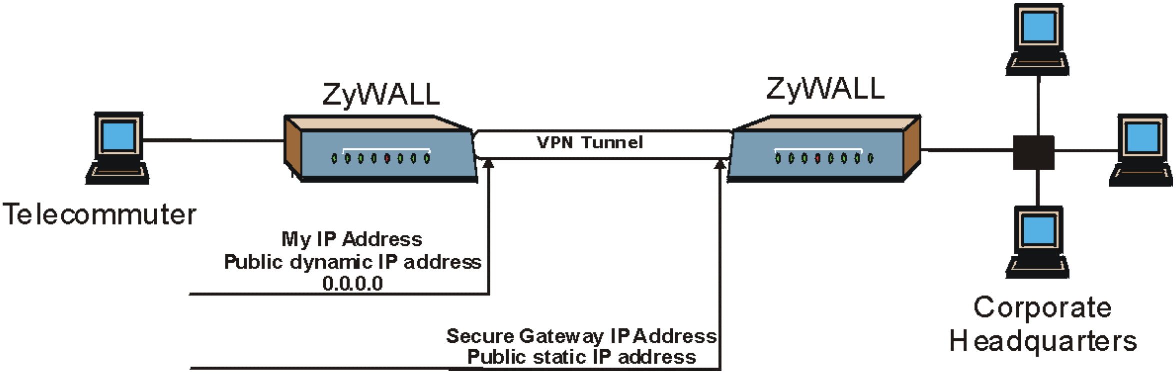


Figure 29-4 Telecommuter's ZyWALL Configuration

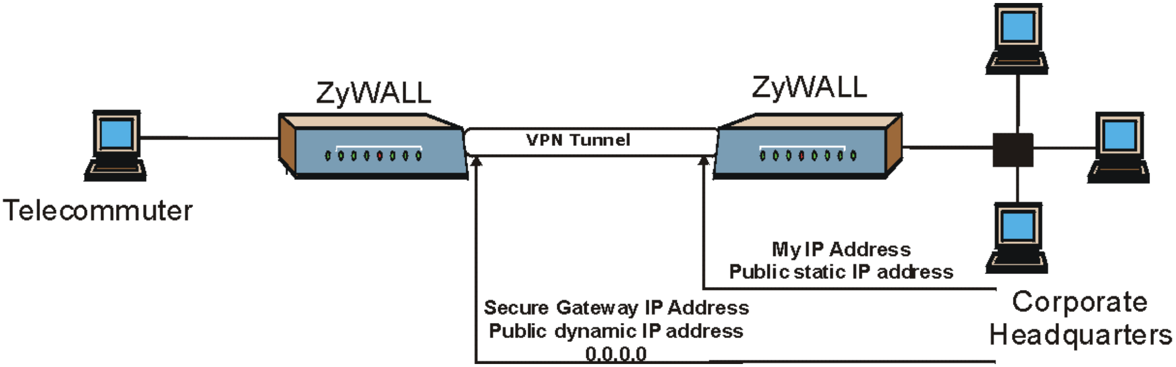
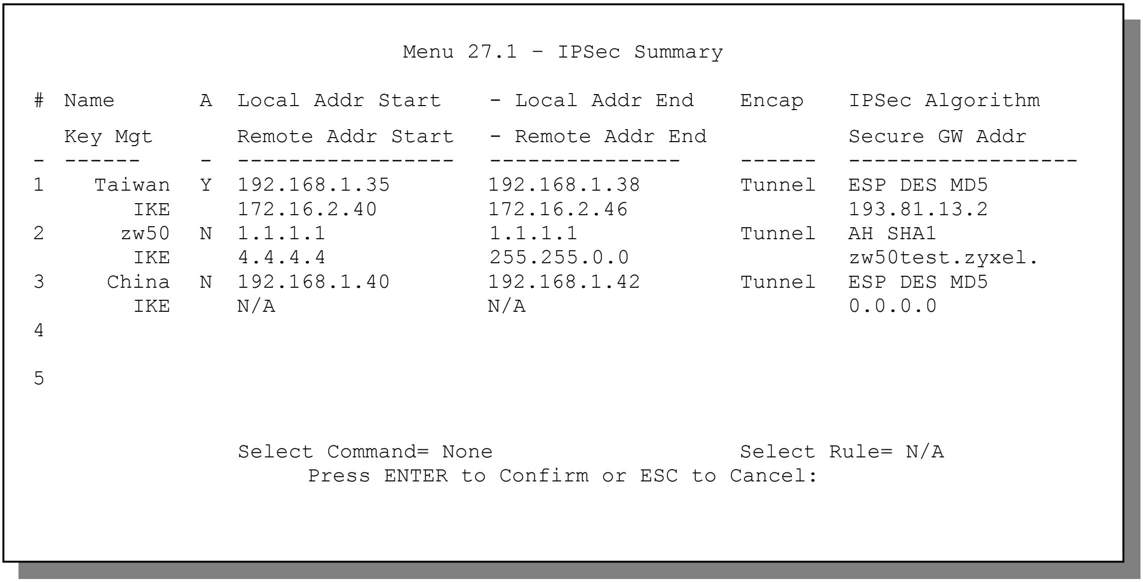


Figure 29-5 Headquarters ZyWALL Configuration

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

A ZyWALL with Secure Gateway Address **set to 0.0.0.0 can receive multiple VPN connection requests using the same VPN rule at the same time.**



```
                          Menu 27.1 - IPSec Summary

 #  Name       A  Local Addr Start    - Local Addr End    Encap    IPSec Algorithm

    Key Mgt       Remote Addr Start   - Remote Addr End            Secure GW Addr
 -  ------     -  -----------------   ---------------     ------   ------------------
 1    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
 2      zw50   N  1.1.1.1             1.1.1.1             Tunnel   AH SHA1
         IKE      4.4.4.4             255.255.0.0                  zw50test.zyxel.
 3     China   N  192.168.1.40        192.168.1.42        Tunnel   ESP DES MD5
         IKE      N/A                 N/A                          0.0.0.0
 4

 5



                  Select Command= None                    Select Rule= N/A
                       Press ENTER to Confirm or ESC to Cancel:
```

Figure 29-6 Menu 27.1: IPSec Summary

Table 29-7 Menu 27.1: IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
#	This is the VPN policy index number.	1
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.	Taiwan
A	**Y** signifies that this VPN rule is active.	**Y**

Table 29-7 Menu 27.1: IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
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 ZyWALL. 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 ZyWALL. 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 ZyWALL.	192.168.1.35
Local Addr End	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 ZyWALL. 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 ZyWALL.	192.168.1.38
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.	**Tunnel**
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 ZyWALL'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.	**ESP DES MD5**
Key Mgt	This field displays the SA's type of key management, (**IKE** or **Manual**).	**IKE**

Table 29-7 Menu 27.1: IPSec Summary

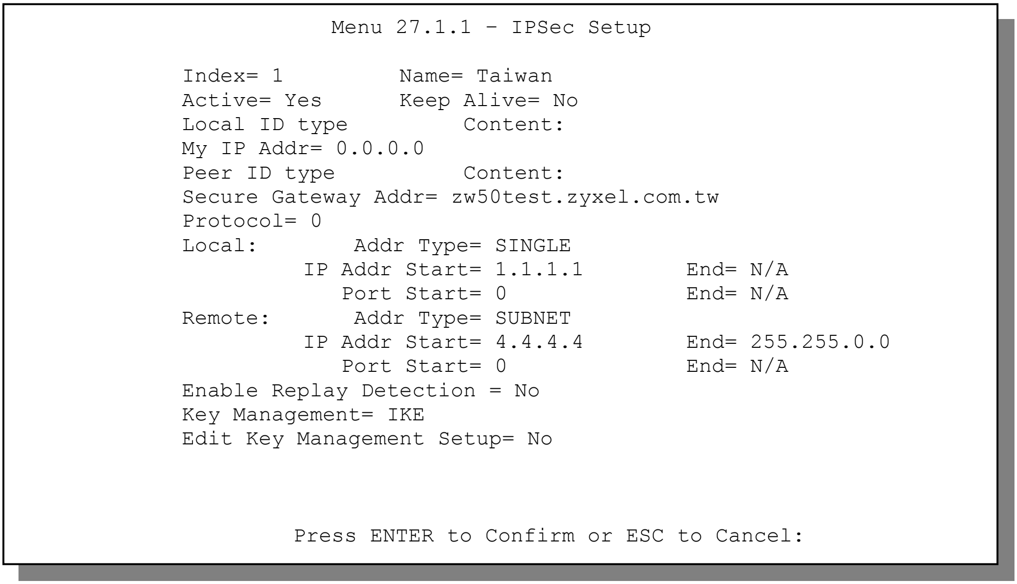
FIELD	DESCRIPTION	EXAMPLE
Remote Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this 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.	172.16.2.40
Remote Addr End	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 Addr** field in SMT 27.1.1 to 0.0.0.0.	172.16.2.46
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 Addr** field in SMT 27.1.1 to 0.0.0.0.	193.81.13.2

Table 29-7 Menu 27.1: IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, Delete or **Go To** 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. Use **Go To Rule** to view the page where your desired rule is listed. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).	**None**
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].	3
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.		

29.4 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.



```
            Menu 27.1.1 - IPSec Setup

Index= 1         Name= Taiwan
Active= Yes      Keep Alive= No
Local ID type         Content:
My IP Addr= 0.0.0.0
Peer ID type          Content:
Secure Gateway Addr= zw50test.zyxel.com.tw
Protocol= 0
Local:       Addr Type= SINGLE
         IP Addr Start= 1.1.1.1        End= N/A
            Port Start= 0              End= N/A
Remote:      Addr Type= SUBNET
         IP Addr Start= 4.4.4.4        End= 255.255.0.0
            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:
```

Figure 29-7 Menu 27.1.1: IPSec Setup

You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.

Table 29-8 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Index	This is the VPN rule index number you selected in the previous menu.	**1**
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**.	Taiwan
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.	**Yes**

Table 29-8 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Keep Alive	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to have the ZyWALL 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.	**No**
Local ID Type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. Select **IP** to identify this ZyWALL by its IP address. Select **DNS** to identify this ZyWALL by a domain name. Select **E-mail** to identify this ZyWALL by an e-mail address.	
Content	This field is **N/A** when you select **IP** in the **Local ID Type** field (the ZyWALL uses the IP address in the **My IP Addr** field. When you select **DNS** in the **Local ID Type** field, type a domain name (up to 31 characters) by which to identify this ZyWALL. 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 ZyWALL. 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 ZyWALL. The ZyWALL 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.	0.0.0.0
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.	

Table 29-8 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Content	This field is **N/A** when you select **IP** in the **Peer ID Type** field (the ZyWALL uses the IP address in the **Secure Gateway Addr** 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 Addr** field below.	
Secure Gateway Addr	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). See section *29.3.4* for more details.	Zw50test.com.tw
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.	0
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	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.	**SINGLE**
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the LAN behind your ZyWALL. 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 ZyWALL. When the **Addr Type** is configured to **SUBNET**, this is a (static) IP address on the LAN behind your ZyWALL.	192.168.1.35

Table 29-8 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
End	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 ZyWALL. When the **Addr Type** field is configured to **SUBNET**, this is a subnet mask on the LAN behind your ZyWALL.	192.168.1.38
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	0
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.	N/A
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 Addr** 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.	**SUBNET**
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 Addr** field to 0.0.0.0.	4.4.4.4

Table 29-8 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
End	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 Addr** field to 0.0.0.0.	255.255.0.0
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.	0
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.	**No**
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.	**IKE**
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**.	**No**
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.		

29.5 IKE Setup

To edit this menu, the **Key Management** field **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**.

29.5.1 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.

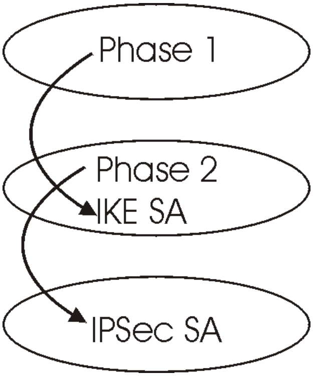


Figure 29-8 Two Phases to Set Up the IPSec SA

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 29.5.5*. 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 ZyWALL automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyWALL 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.

29.5.2 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.

29.5.3 Pre-Shared Key

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.

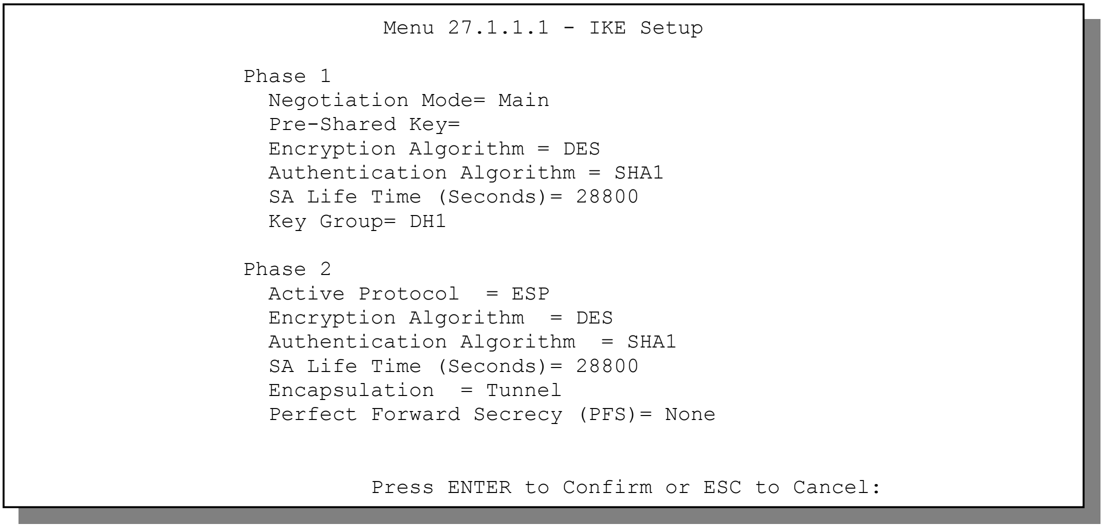
29.5.4 Diffie-Hellman (DH) Key Groups

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.

29.5.5 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 ZyWALL. 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).



```
                              Menu 27.1.1.1 - IKE Setup

                   Phase 1
                     Negotiation Mode= Main
                     Pre-Shared Key=
                     Encryption Algorithm = DES
                     Authentication Algorithm = SHA1
                     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:
```

Figure 29-9 Menu 27.1.1.1: IKE Setup

Table 29-9 Menu 27.1.1.1: IKE Setup

FIELD	DESCRIPTION	EXAMPLE
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.	**Main**
Pre-Shared Key	ZyWALL 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. Multiple SAs connecting through a secure gateway must have the same pre-shared key.	
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. ZyWALL **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.	**DES**

Table 29-9 Menu 27.1.1.1: IKE Setup

FIELD	DESCRIPTION	EXAMPLE
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. ZyWALL **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].	**DES**
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].	**SHA1**
SA Life Time (Seconds)	Define the length of time before an IKE Security Association 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.	28800 (default)
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.	**DH1**
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.	**ESP**
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.	**DES**
Authentication Algorithm	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].	**MD5**
SA Life Time (Seconds)	Define the length of time before an IPSec Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).	28800 (default)
Encapsulation	Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these.	**Tunnel**

Table 29-9 Menu 27.1.1.1: IKE Setup

FIELD	DESCRIPTION	EXAMPLE
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).	**None**
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.		

29.6 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.

29.6.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. These parameters have been discussed earlier.

Table 29-10 Active Protocol: Encapsulation and Security Protocol

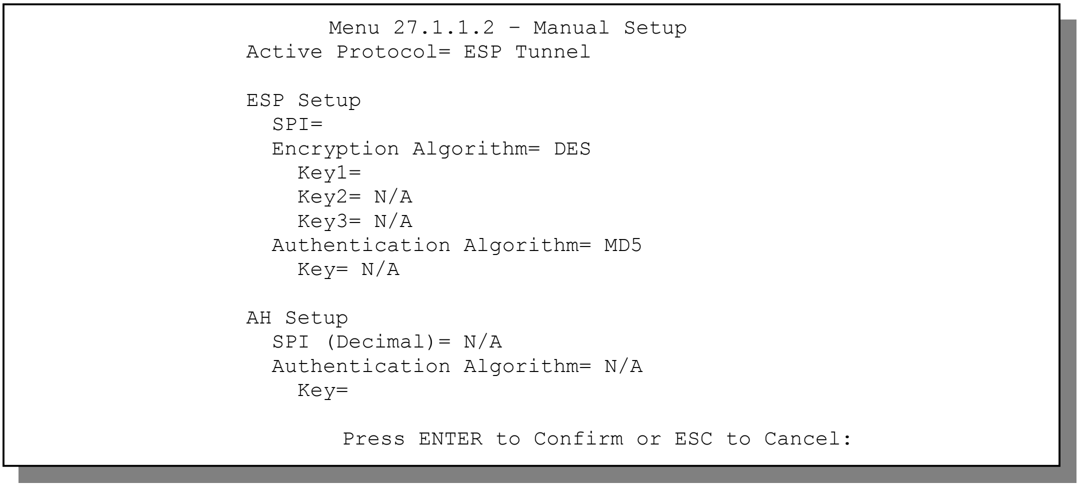
MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

29.6.2 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.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

To edit this menu, move the cursor to the **Edit Manual 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**.



```
                   Menu 27.1.1.2 - Manual Setup
             Active Protocol= ESP Tunnel

             ESP Setup
               SPI=
               Encryption Algorithm= DES
                 Key1=
                 Key2= N/A
                 Key3= N/A
               Authentication Algorithm= MD5
                 Key= N/A

             AH Setup
               SPI (Decimal)= N/A
               Authentication Algorithm= N/A
                 Key=

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

Figure 29-10 Menu 27.1.1.2: Manual Setup

Table 29-11 Menu 27.1.1.2: Manual Setup

FIELD	DESCRIPTION	EXAMPLE
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 Tunnel**
ESP Setup	The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**.	
SPI	The **SPI** must be unique and from one to four integers ("0" to "9").	1234
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.	**DES**
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**.	89abcde
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	

Table 29-11 Menu 27.1.1.2: Manual Setup

FIELD	DESCRIPTION	EXAMPLE
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].	**MD5**
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.	123456789abcde
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.	**N/A**
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].	**N/A**
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.	**N/A**
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 30
SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

30.1 Introduction

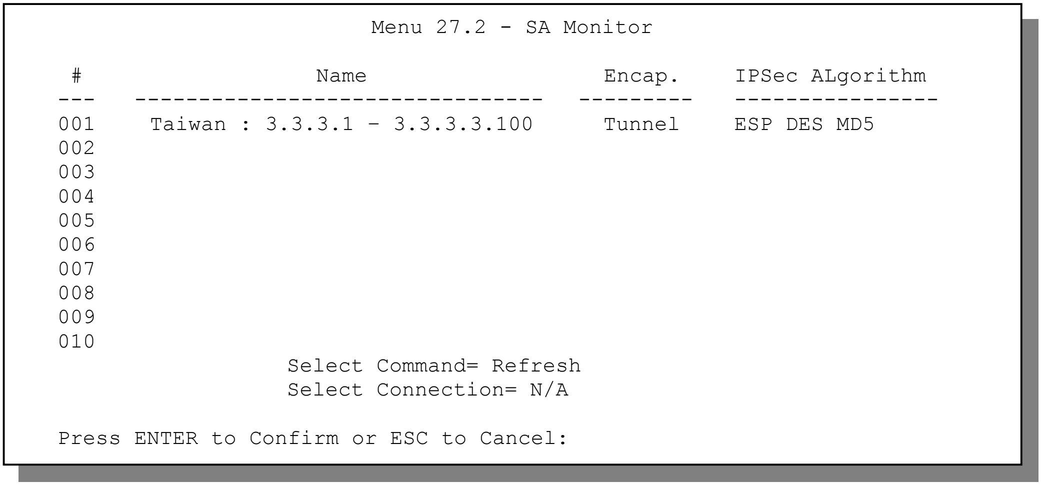
A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

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 *section 29.3.1* on keep alive to have the ZyWALL renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

30.2 Using SA Monitor

1. Use the **Refresh** function to display active VPN connections.
2. Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.



```
                          Menu 27.2 - SA Monitor

   #                  Name                      Encap.     IPSec ALgorithm
  ---   --------------------------------   ---------   ----------------
  001    Taiwan : 3.3.3.1 - 3.3.3.3.100      Tunnel     ESP DES MD5
  002
  003
  004
  005
  006
  007
  008
  009
  010
                    Select Command= Refresh
                    Select Connection= N/A

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

Figure 30-1 Menu 27.2: SA Monitor

Table 30-1 Menu 27.2: SA Monitor

FIELD	DESCRIPTION	EXAMPLE
#	This is the security association 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.	**Taiwan**
Encap.	This field displays **Tunnel** mode or **Transport** mode. See previous for discussion.	**Tunnel**
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 ZyWALL processing requirements and communications latency (delay).	**ESP DES MD5**
Select Command	Press [SPACE BAR] to choose from **Refresh**, **Disconnect**, **None**, **Next Page**, or **Previous Page** 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 **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).	**Refresh**
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].	**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.		

Part X:

Troubleshooting

This part provides possible remedies for potential problems.

Chapter 31 Troubleshooting

This chapter covers potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem. Please see our included disk for further information. DMZ applies to the ZyWALL 100.

31.1 Problems Starting Up the ZyWALL

Table 31-1 Troubleshooting the Start-Up of your ZyWALL

<table>
<tr><th>PROBLEM</th><th colspan="2">CORRECTIVE ACTION</th></tr>
<tr><td rowspan="3">None of the LEDs turn on when you turn on the ZyWALL.</td><td colspan="2">Make sure that you have the power cord connected to the ZyWALL and plugged in.</td></tr>
<tr><td colspan="2">Replace the fuse if it is burnt out.</td></tr>
<tr><td colspan="2">If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</td></tr>
<tr><td rowspan="4">Cannot access the ZyWALL via the console port.</td><td colspan="2">1. Check to see if the ZyWALL is connected to your computer’s console port.</td></tr>
<tr><td rowspan="3">2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:</td><td>VT100 terminal emulation</td></tr>
<tr><td>9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.</td></tr>
<tr><td>No parity, 8 data bits, 1 stop bit, data flow set to none.</td></tr>
</table>

31.2 Problems with the LAN Interface

Table 31-2 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL from the LAN.	Check your Ethernet cable type and connections. Refer to the *Rear Panel and Connections* section for LAN connection instructions.
	Make sure your NIC (Network Interface Card) is installed and functioning properly.
Cannot ping any computer on the LAN.	Check the 10M/100M LAN LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your ZyWALL and hub or the station.
	Verify that the IP address and the subnet mask of the ZyWALL and the computers are on the same subnet.

31.3 Problems with the DMZ Interface

The DMZ interface is not available on all models.

Table 31-3 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access servers on the DMZ from the LAN.	Check your Ethernet cable type and connections. Refer to the *Rear Panel and Connections* section for DMZ connection instructions.
	Make sure the NIC on the LAN computer and the NIC on the DMZ server are installed and functioning properly.
	Verify that the IP address of the DMZ port and the LAN port are on separate subnets.
	Make sure that NAT is configured for your DMZ servers in menus 15.1 and 15.2.
Cannot ping any computer on the DMZ.	Check the 10M/100M DMZ LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your ZyWALL and hub or the station.
	Verify that the IP address and the subnet mask of the ZyWALL and the servers are on the same subnet.

31.4 Problems with the WAN Interface

Table 31-4 Troubleshooting the WAN interface

PROBLEM	CORRECTIVE ACTION
Cannot get WAN IP from the ISP.	The WAN IP is provided when the ISP recognizes the user as an authorized user after verifying the MAC address, Host Name or User ID. Find out the verification method used by your ISP.
	If the ISP checks the LAN MAC Address, tell the ISP the WAN MAC address of the ZyWALL. The WAN MAC can be obtained from menu 24.1. In case the ISP does not allow you to use a new MAC, you can clone the MAC from the LAN as the WAN MAC and send it to the ISP using **Menu 2 - WAN Setup**. It is recommended that you configure this menu even if your ISP presently does not require MAC address authentication.
	If the ISP checks the Host Name, enter host name in the **System Name** field in **Menu 1 - General Setup** when you connect the ZyWALL to a cable/ads modem.
	If the ISP checks the User ID, make sure that you have entered the correct **Service Type**, user name (in the **My Login** field) and password (in the **My Password** field) in **Menu 4 - Internet Access Setup**.
Can’t connect to a remote node or ISP.	Check menu 24.1 to verify the line status. If the line is down, contact your service provider.

31.5 Problems with Internet Access

Table 31-5 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
Cannot access the Internet.	Connect your cable/DSL modem with the ZyWALL using appropriate cable. Check with the manufacturer of your cable/DSL device about your cable requirement because some devices may require crossover cable and others a regular straight-through cable.
	Verify your settings in menu 3.2 and menu 4.

31.6 Problems with the Password

Table 31-6 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL.	The Password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	Use the Reset button to restore the factory default configuration file. This will restore all of the factory defaults including the password. See *the Resetting the ZyWALL* section for details.

31.7 Problems with Remote Management

Table 31-7 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL from the LAN or WAN.	Refer to the Remote Management Limitations section for scenarios when remote management may not be possible.
	When NAT is enabled: ➢ Use the ZyWALL's WAN IP address when configuring from the WAN. ➢ Use the ZyWALL's LAN IP address when configuring from the LAN.
	Refer to the *Problems with the LAN Interface* section for instructions on checking your LAN connection.
	Refer to the Problems with the WAN Interface section for instructions on checking your WAN connection.

Part XI:

General Appendices

This part provides background information about setting up your computer's IP address, triangle route, how functions are related, wireless LAN, 802.1x, PPPoE, PPTP, hardware specifications, Universal Plug and Play, IP subnetting, safety warnings and how to change a ZyWALL 100 Fuse.

Appendix A
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.

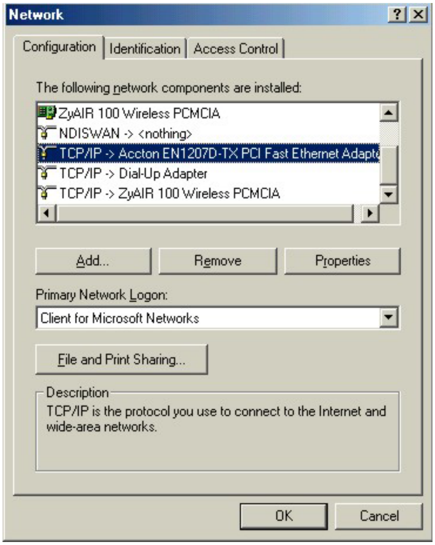
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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 ZyWALL's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.



The following network components are installed:

ZyAIR 100 Wireless PCMCIA
NDISWAN -> <nothing>
TCP/IP -> Accton EN1207D-TX PCI Fast Ethernet Adapte
TCP/IP -> Dial-Up Adapter
TCP/IP -> ZyAIR 100 Wireless PCMCIA

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

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:

a. In the **Network** window, click **Add**.

b. Select **Adapter** and then click **Add**.

c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a. In the **Network** window, click **Add**.

b. Select **Protocol** and then click **Add**.

c. Select **Microsoft** from the list of **manufacturers**.

d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

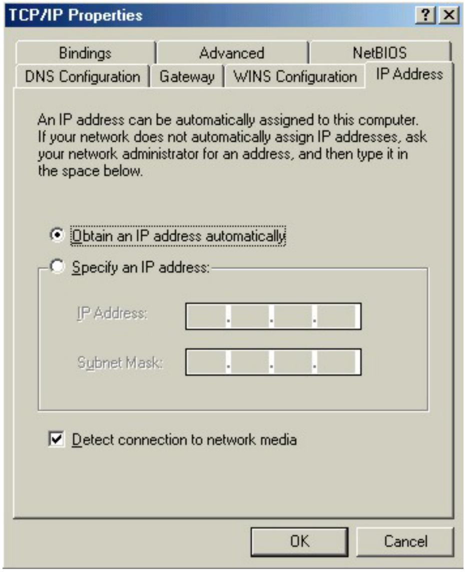
e. Restart your computer so the changes you made take effect.

In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

1. 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.



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

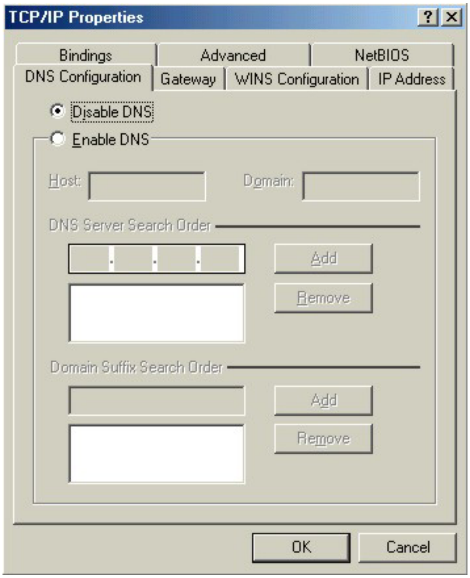
○ Specify an IP address:

☑ Detect connection to network media

2. 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).



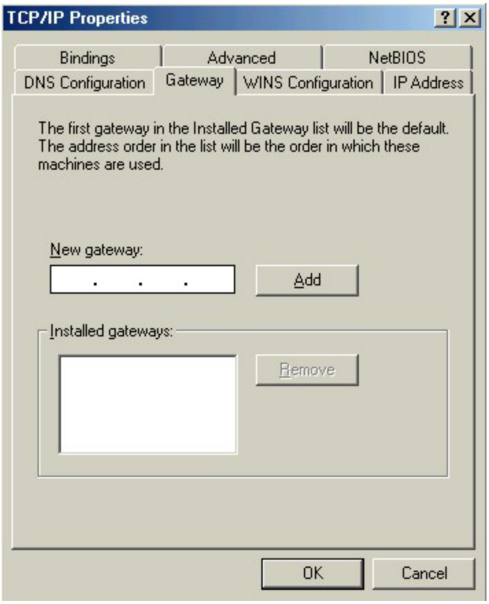
● Disable DNS

○ Enable DNS

3. 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**.



The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

4. Click **OK** to save and close the **TCP/IP Properties** window.

5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

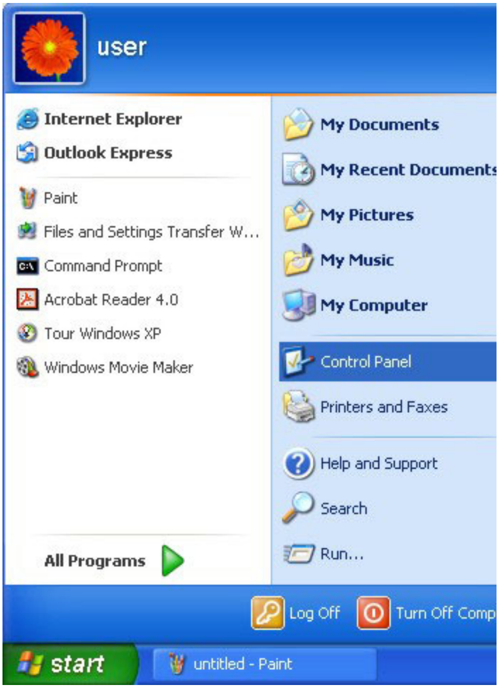
6. Turn on your ZyWALL and restart your computer when prompted.

Verifying Your Computer's IP Address

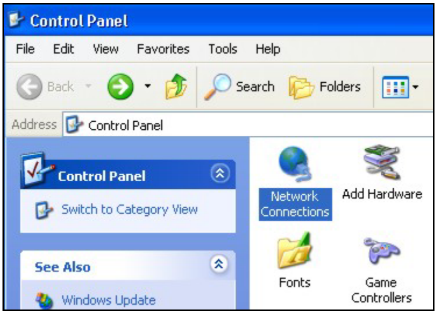
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

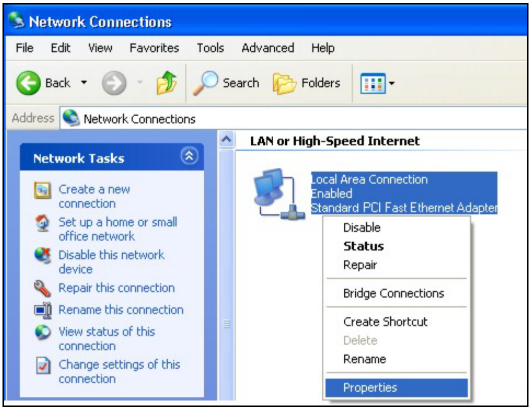
1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.



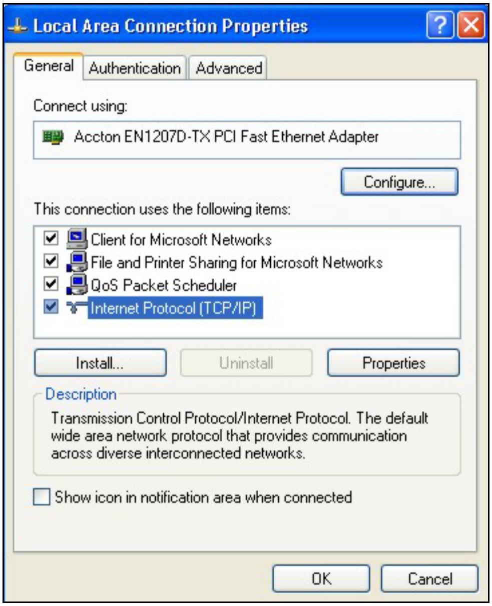
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.



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



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

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

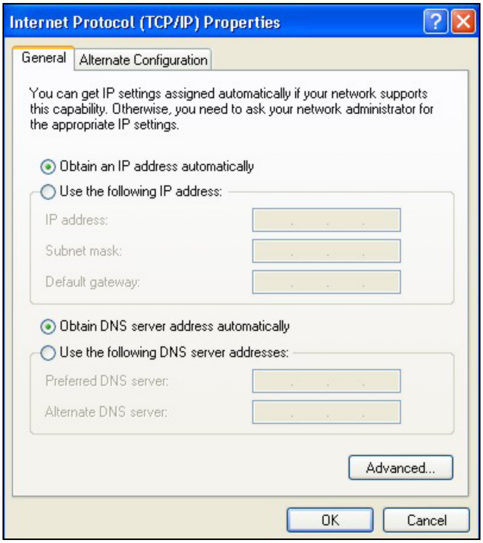
☐ Show icon in notification area when connected

5. The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

   -If you have a dynamic IP address click **Obtain an IP address automatically**.

   -If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

   Click **Advanced**.



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 Settin**gs 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.

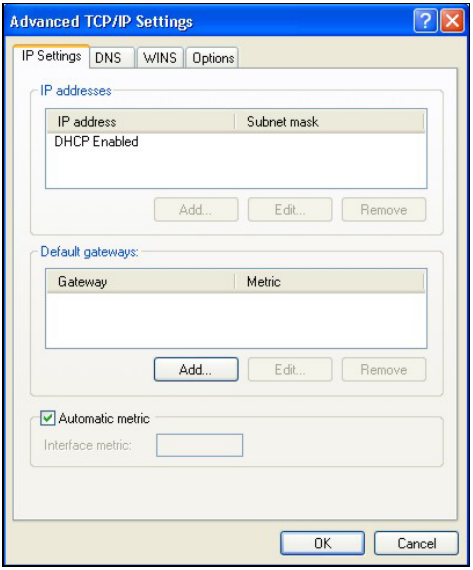
   -Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

   -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.



Advanced TCP/IP Settings

IP addresses

IP address	Subnet mask
DHCP Enabled	

Default gateways:

Gateway	Metric

☑ Automatic metric

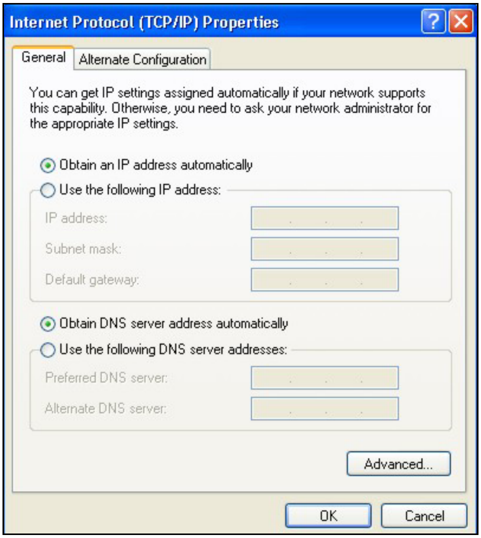
Interface metric:

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.



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

10. Turn on your ZyWALL and restart your computer (if prompted).

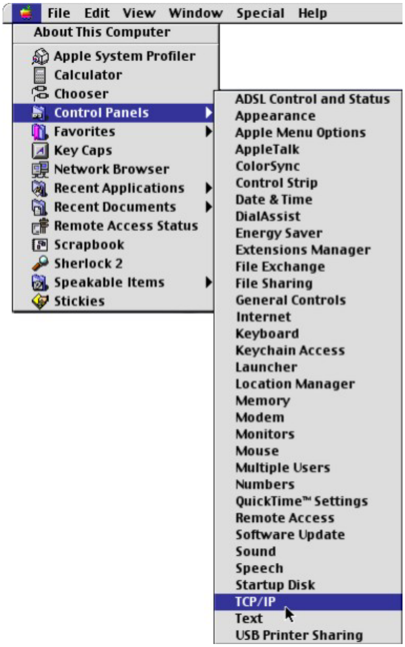
Verifying Your Computer’s IP Address

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

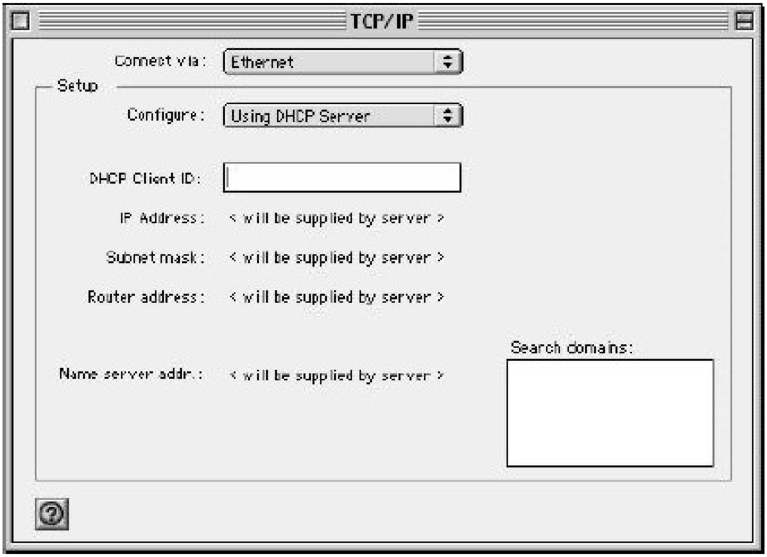
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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



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



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 ZyWALL in the **Router address** box.

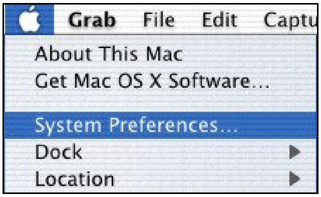
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your ZyWALL and restart your computer (if prompted).

Verifying Your Computer’s IP Address

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.

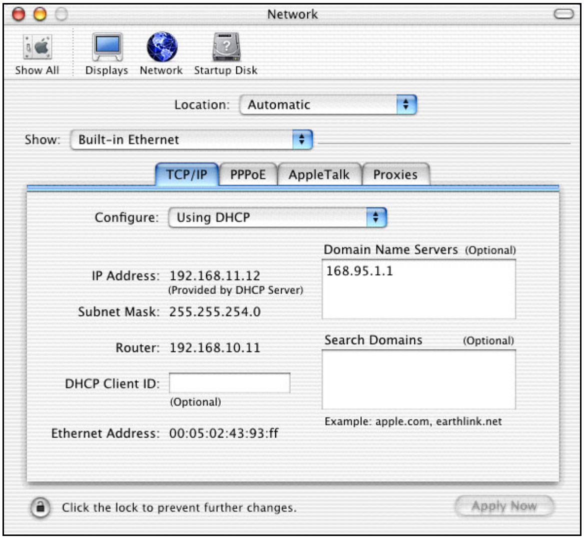


2. Click **Network** in the icon bar.

   - Select **Automatic** from the **Location** list.

   - Select **Built-in Ethernet** from the **Show** list.

   - Click the **TCP/IP** tab.



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.

3. For dynamically assigned settings, select **Using DHCP** 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 ZyWALL in the **Router address** box.

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

6. Turn on your ZyWALL and restart your computer (if prompted).

Verifying Your Computer's IP Address

Check your TCP/IP properties in the **Network** window.

Appendix B
Triangle Route

The Ideal Setup

When the firewall is on, your ZyWALL acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the ZyWALL to protect your LAN against attacks.

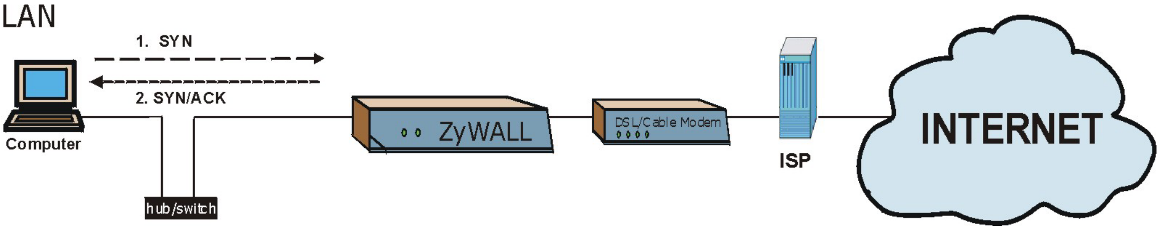


Diagram B-1 Ideal Setup

The "Triangle Route" Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the "triangle route" problem may occur. The steps below describe the "triangle route" problem.

Step 1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

Step 2. The ZyWALL reroutes the SYN packet through Gateway **B** on the LAN to the WAN.

Step 3. The reply from the WAN goes directly to the computer on the LAN without going through the ZyWALL.

As a result, the ZyWALL resets the connection, as the connection has not been acknowledged.

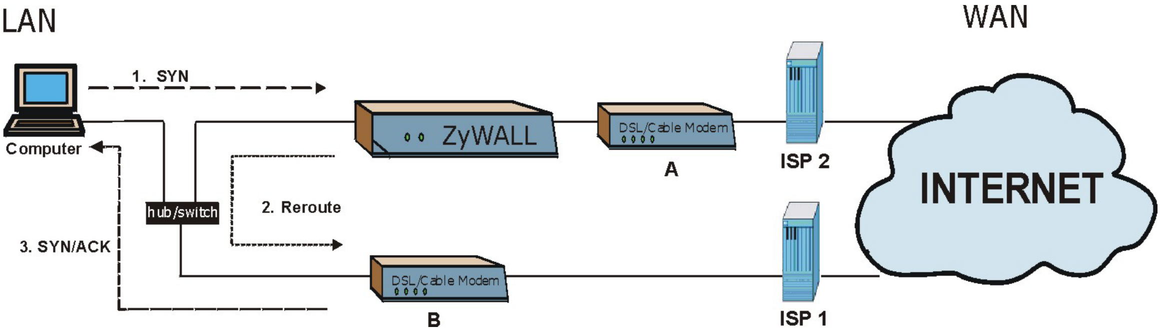


Diagram B-2 "Triangle Route" Problem

The "Triangle Route" Solutions

This section presents you two solutions to the "triangle route" problem.

IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyWALL supports up to three logical LAN interfaces with the ZyWALL being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the ZyWALL to your LAN. The following steps describe such a scenario.

Step 1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

Step 2. The ZyWALL reroutes the packet to Gateway **B** which is in Subnet 2.

Step 3. The reply from WAN goes through the ZyWALL to the computer on the LAN in Subnet 1.

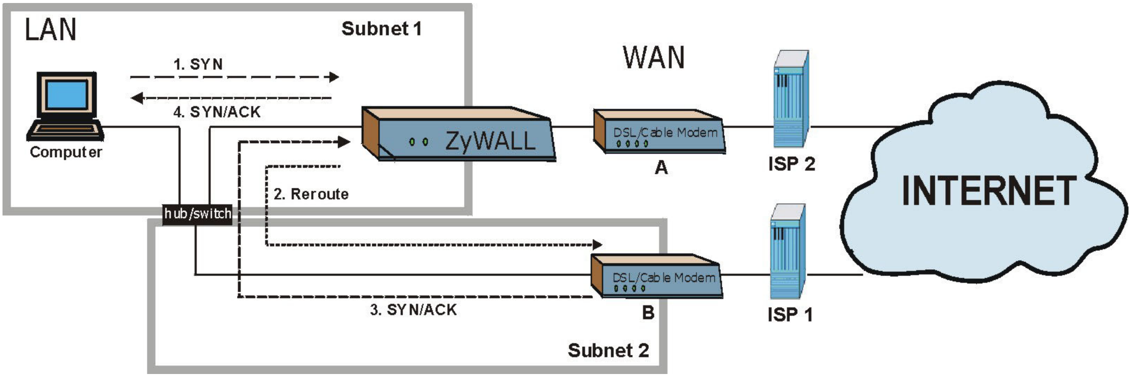


Diagram B-3 IP Alias

Gateways on the WAN Side

A second solution to the "triangle route" problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your ZyWALL to your LAN. Therefore your LAN is protected.

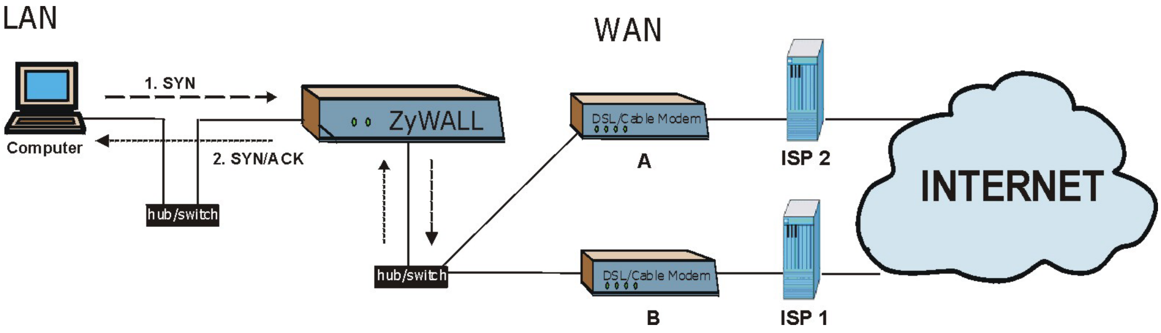


Diagram B-4 Gateways on the WAN Side

Appendix C
The Big Picture

The following figure gives an overview of how filtering, the firewall, VPN and NAT are related.

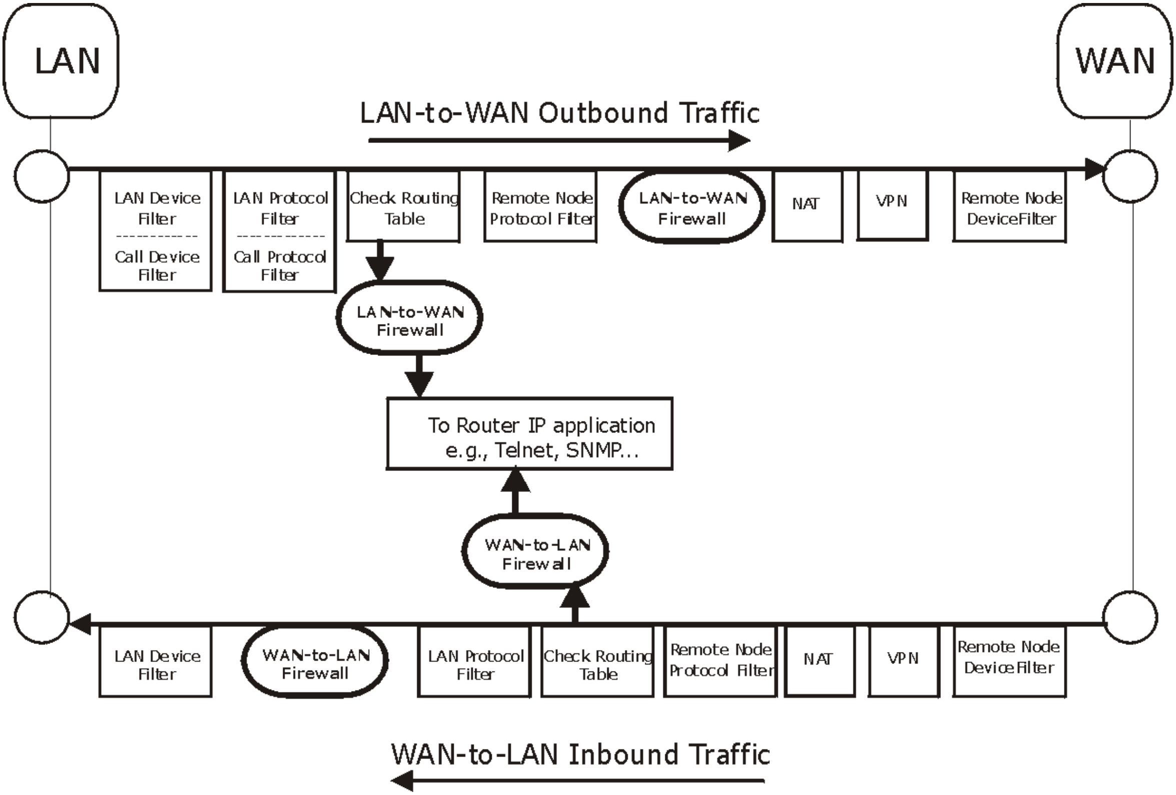


Diagram C-1 Big Picture— Filtering, Firewall, VPN and NAT

Appendix D
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area. WLAN is not available on all models.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

1. It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.
4. It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".
5. It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits. On September 16, 1999, the 802.11b provided much higher data rates of up to 11Mbps, while maintaining the 802.11 protocol.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). See the following diagram of an example of an Ad-hoc wireless LAN.

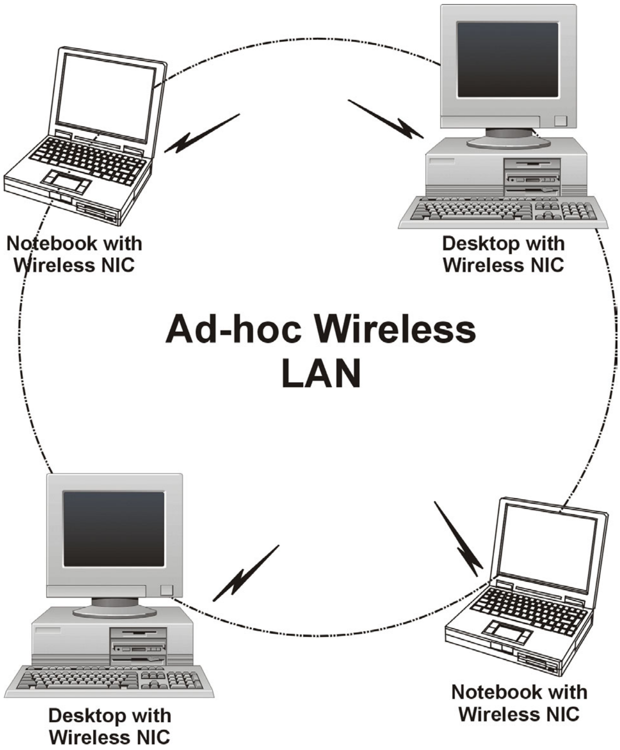

Notebook with Wireless NIC
Desktop with Wireless NIC
Ad-hoc Wireless LAN
Desktop with Wireless NIC
Notebook with Wireless NIC

Diagram D-1 Peer-to-Peer Communication in an Ad-hoc Network

Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple Access Points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple Access Points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the Access Point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between Access Points and seamless campus-wide coverage is possible.

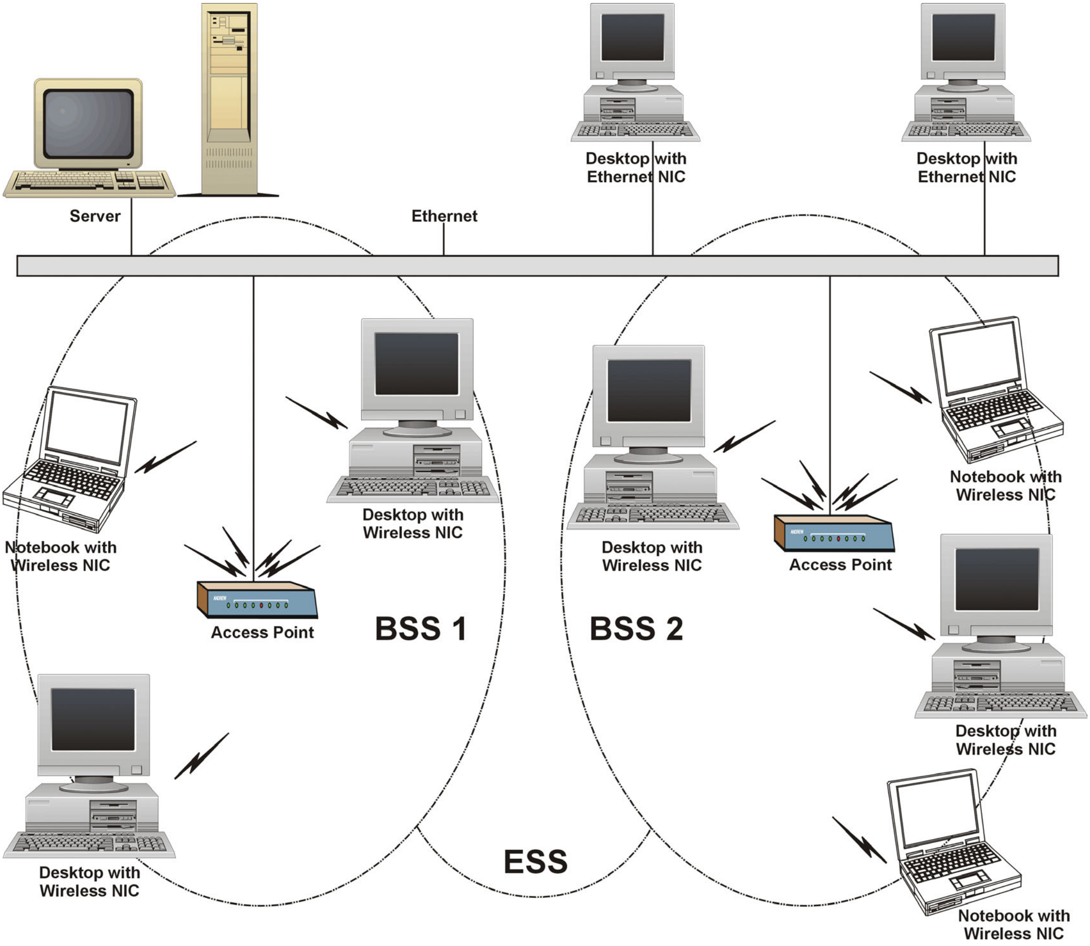

Server
Ethernet
Desktop with Ethernet NIC
Desktop with Ethernet NIC
Notebook with Wireless NIC
Desktop with Wireless NIC
Access Point
BSS 1
Desktop with Wireless NIC
Desktop with Wireless NIC
Access Point
BSS 2
Notebook with Wireless NIC
Desktop with Wireless NIC
ESS
Notebook with Wireless NIC

Diagram D-2 ESS Provides Campus-Wide Coverage

Appendix E
Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

IEEE 802.1x

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

Advantages of the IEEE 802.1x

- User based identification that allows for roaming.

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

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

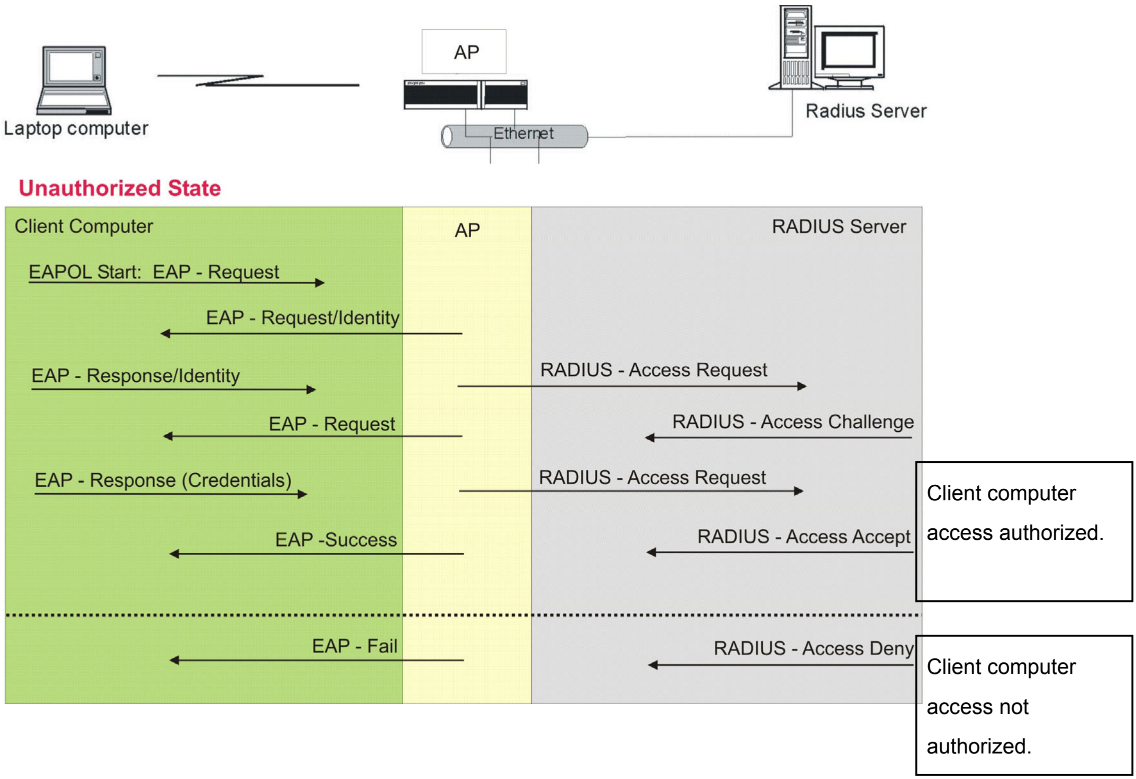


Diagram E-1 Sequences for EAP MD5–Challenge Authentication

Appendix F PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit), which connects to a DSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN & ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

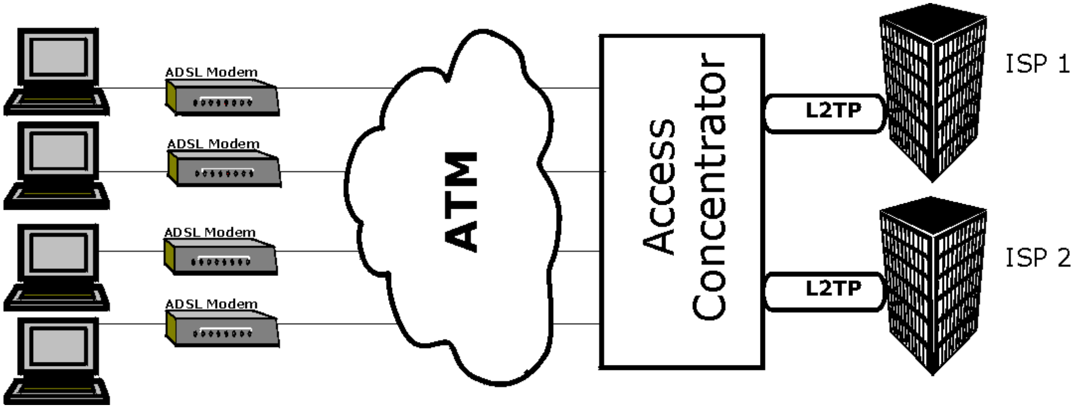


Diagram F-1 Single-PC per Modem Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

ZyWALL as a PPPoE Client

When using the ZyWALL as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

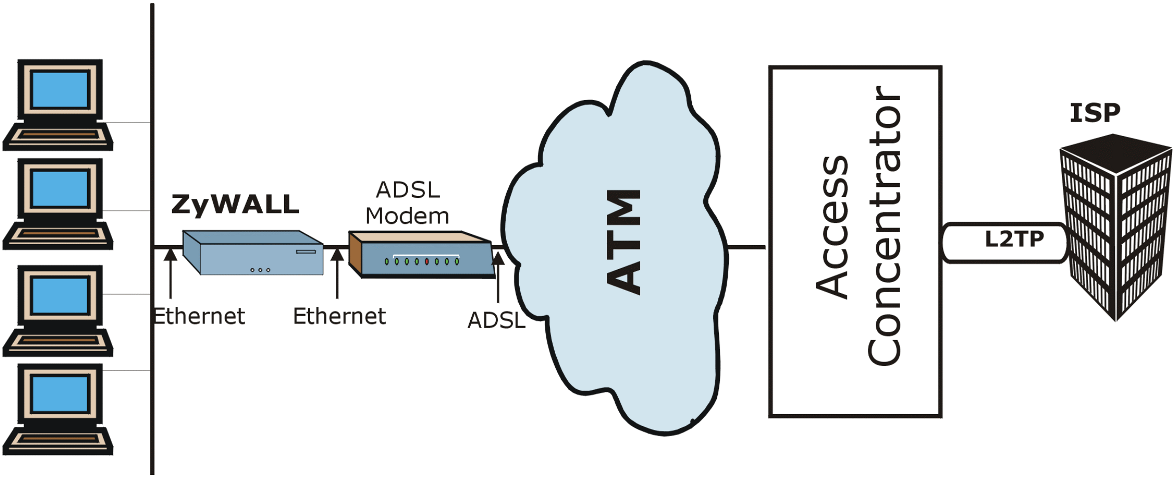


Diagram F-2 ZyWALL as a PPPoE Client

Appendix G
PPTP

What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

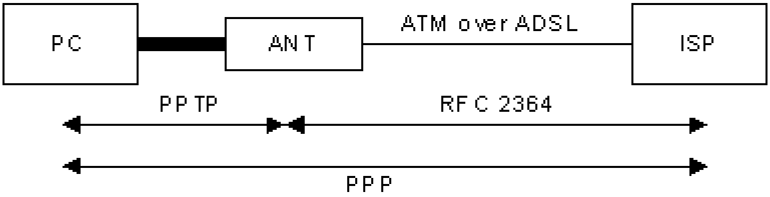


Diagram G-1 Transport PPP frames over Ethernet

PPTP and the ZyWALL

When the ZyWALL is deployed in such a setup, it appears as a PC to the ANT.

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the ZyWALL's Internet connection. In NAT mode, the ZyWALL is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The ZyWALL initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

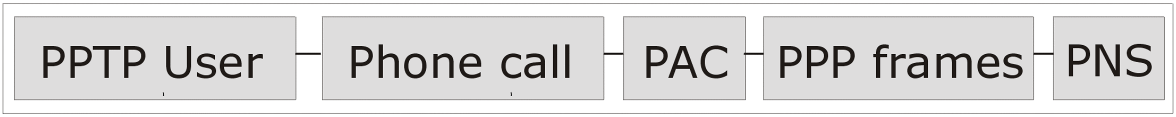


Diagram G-2 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, and hence the ZyWALL, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP connections

Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

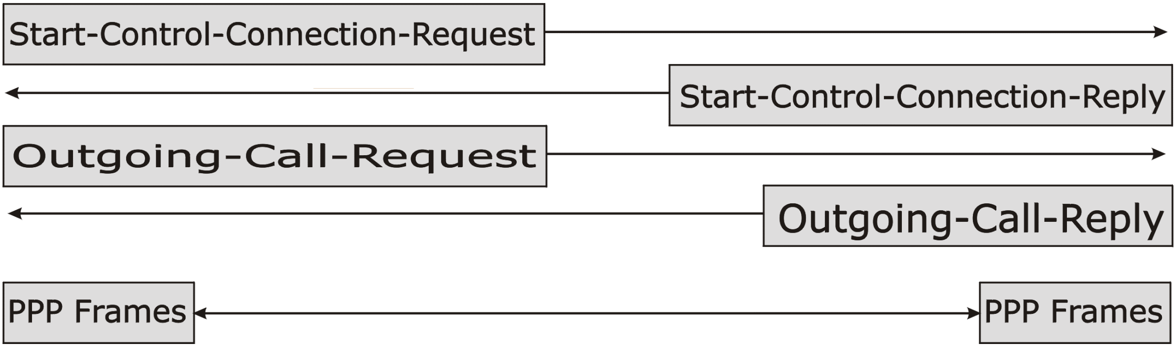

Start-Control-Connection-Request
Start-Control-Connection-Reply
Outgoing-Call-Request
Outgoing-Call-Reply
PPP Frames
PPP Frames

Diagram G-3 Example Message Exchange between PC and an ANT

PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix H
Hardware Specifications

Chart H-1 General Specifications

Power Specification (ZyWALL 100)	100-240 VAC, 50/60Hz
Power Specification (ZyWALL 10,10W, 50)	I/P AC 120V / 60Hz; O/P DC 12V 1200 mA
Power Consumption (ZyWALL 100)	16 Watts maximum
Power Current (ZyWALL 100)	1.9 Amps
Fuse Rating (ZyWALL 100)	0.5 Amps, 250 VAC
MTBF	100000 hrs (Mean Time Between Failures)
Operation Temperature	0º C ~ 40º C
Ethernet Specification for WAN (Not on all models)	10/100Mbps Half / Full Auto-negotiation
Ethernet Specification for WAN (Not on all models)	10Mbps Half / Full Auto-negotiation
Ethernet Specification for DMZ (Not on all models)	10/100Mbps Half / Full Auto-negotiation
Ethernet Specification for LAN	10/100Mbps Half / Full Auto-negotiation

Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The ZyWALL is DCE when you connect a computer to the console port. The ZyWALL is DTE when you connect a modem to the dial backup port.

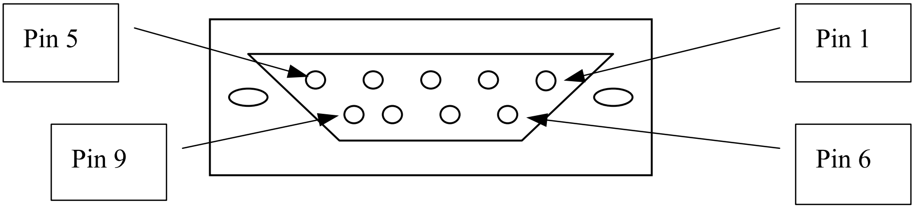


Diagram H-1 Console/Dial Backup Port Pin Layouts [1]

Chart H-2 Console/Dial Backup Port Pin Assignments

CONSOLE Port RS – 232 (Female) DB-9F	DIAL BACKUP RS – 232 (Male) DB-9M (Not on all models)
Pin 1 = NON Pin 2 = DCE-TXD Pin 3 = DCE –RXD Pin 4 = DCE –DSR Pin 5 = GND Pin 6 = DCE –DTR Pin 7 = DCE –CTS Pin 8 = DCE –RTS PIN 9 = NON	Pin 1 = NON Pin 2 = DTE-RXD Pin 3 = DTE-TXD Pin 4 = DTE-DTR Pin 5 = GND Pin 6 = DTE-DSR Pin 7 = DTE-RTS Pin 8 = DTE-CTS PIN 9 = NON.
The CON/AUX port also has these pin assignments. The CON/AUX switch changes the setting in the firmware only and does not change the CON/AUX port's pin assignments.	ZyWALLs with a CON/AUX port also have a 9-pin adaptor for the console cable with these pin assignments on the male end.

[1] Products without flow control only use pins 2,3 and 5.

Chart H-3 Ethernet Cable Pin Assignments

WAN/LAN/DMZ Ethernet Cable Pin Layout: Straight-Through				Crossover			
(Switch)		(Adapter)		(Switch)		(Switch)	
1	IRD +	1	OTD +	1	IRD +	1	IRD +
2	IRD -	2	OTD -	2	IRD -	2	IRD -
3	OTD +	3	IRD +	3	OTD +	3	OTD +
6	OTD -	6	IRD -	6	OTD -	6	OTD -

Power Adaptor Specifications (ZyWALL 10/10W/50)

Chart H-4 North American AC Power Adaptor Specifications

AC Power Adapter model AD48-1201200DUY

Input power: AC120Volts/60Hz/0.25A

Output power: DC12Volts/1.2A

Power consumption: 10 W

Plug: North American standards

Safety standards: UL, CUL (UL 1950, CSA C22.2 No.234-M90)

AC Power Adapter model AD48-1201200DUY

Input power: AC120Volts/60Hz

Output power: DC12Volts/1.2A

Power consumption: 9 W

Plug: North American standards

Safety standards: UL, CUL (UL1950, CSA C22.2 NO. 234-M90)

Chart H-5 European Union AC Power Adaptor Specifications

AC Power Adapter model AD-1201200DV

Input power: AC230Volts/50Hz/0.2A

Output power: DC12Volts/1.2A

Chart H-5 European Union AC Power Adaptor Specifications

Power consumption: 10 W

Plug: European Union standards

Safety standards: TUV, CE (EN 60950)

AC Power Adapter model JAD-121200E

Input power: AC230Volts/50Hz,

Output power: DC12Volts/1.2A

Power consumption: 9 W

Plug: European Union standards

Safety standards: TUV, CE (EN 60950)

Chart H-6 UK AC Power Adaptor Specifications

AC Power Adapter model AD-1201200DK

Input power: AC230Volts/50Hz/0.2A

Output power: DC12Volts/1.2A

Power consumption: 10 W

Plug: United Kingdom standards

Safety standards: TUV, CE (EN 60950, BS7002)

Chart H-7 Japan AC Power Adaptor Specifications

AC Power Adapter model JOD-48-1124

Input power: AC100Volts/ 50/60Hz/ 27VA

Output power: DC12Volts/1.2A

Power consumption: 10 W

Plug: Japan standards

Safety standards: T-Mark

Chart H-8 Australia and New Zealand AC Power Adaptor Specifications

AC Power Adapter model AD-1201200Ds or AD-121200DS

Input power: AC240Volts/50Hz/0.2A

Output power: DC12Volts/1.2A

Power consumption: 10 W

Plug: Australia and New Zealand standards

Safety standards: NATA (AS 3260)

Appendix I
Universal Plug and Play

What is Universal Plug and Play?

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

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

UPnP broadcasts are only allowed on the LAN.

Please see your Users Guide for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

NAT Traversal

UPnP NAT Traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT Traversal and UPnP.

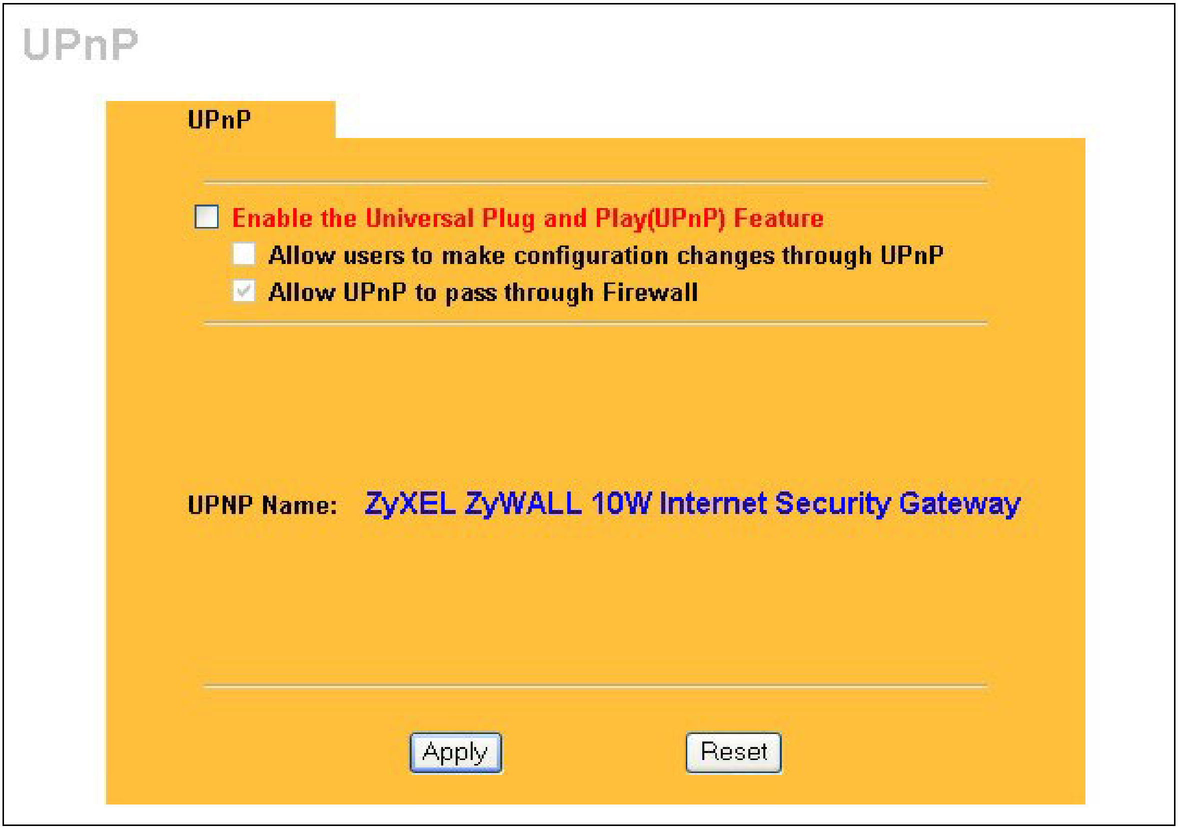
See the Network Address Translation (NAT) chapter in your User's Guide for further information about NAT.

Are there any cautions about UPnP?
The automated nature of NAT Traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

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

Opening UPnP

In the web configurator, click **Advanced** and then **UPnP**.



UPnP

UPnP

☐ Enable the Universal Plug and Play(UPnP) Feature
☐ Allow users to make configuration changes through UPnP
☑ Allow UPnP to pass through Firewall

UPNP Name: ZyXEL ZyWALL 10W Internet Security Gateway

Diagram I-1 UPnP

Chart I-1 UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) feature	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyWALL's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyWALL so that they can communicate through the ZyWALL, for example by using NAT Traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through firewall	Select this check box to create a static LAN to LAN/ZyWALL rule that allows forwarding of ports 1900 and 80. Selecting this check box also creates a dynamic firewall rule every time a NAT forwarding port is reserved for UPnP. This setting remains active until you disable UPnP or clear this check box. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets) instead of creating firewall rule that gives them access.
UPnP Name	This identifies the ZyWALL in UPnP applications.
Apply	Click Apply to save the setting to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

Installing UPnP in Windows Examples

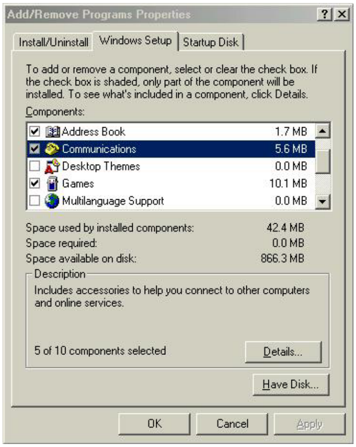
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

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

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



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

Components:

☑ Address Book	1.7 MB
☑ Communications	5.6 MB
☐ Desktop Themes	0.0 MB
☑ Games	10.1 MB
☐ Multilanguage Support	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description

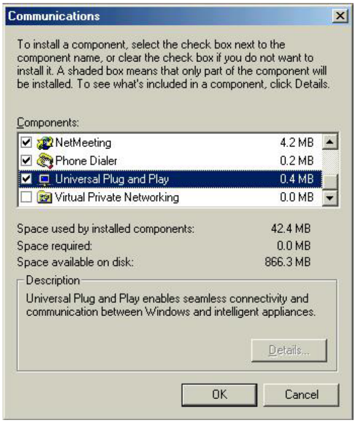
Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

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

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

Step 5. Restart the computer when prompted.



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

Components:

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

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description

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

Installing UPnP in Windows XP

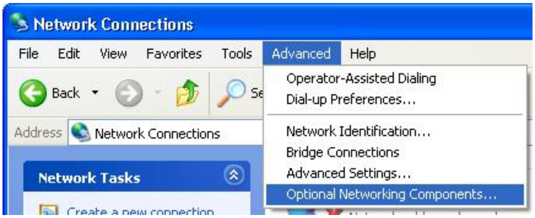
Follow the steps below to install the UPnP in Windows ME

Step 1. Click **start** and **Control Panel**.

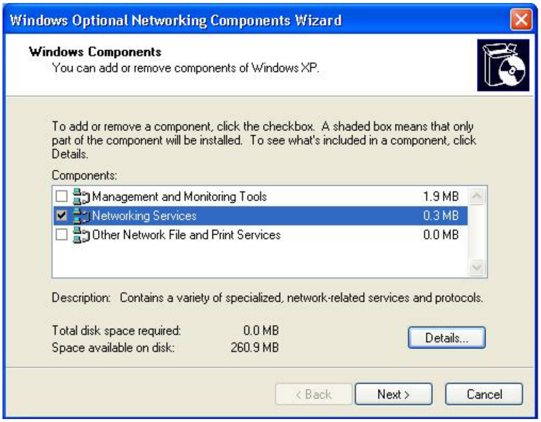
Step 2. Double-click **Network Connections**.

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

The **Windows Optional Networking Components Wizard** window displays.



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



Windows Optional Networking Components Wizard

Windows Components
You can add or remove components of Windows XP.

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

Components:

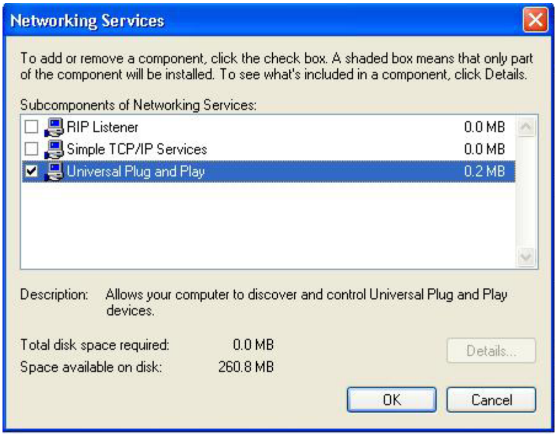
□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

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

Total disk space required: 0.0 MB
Space available on disk: 260.9 MB

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

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



Networking Services

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

Subcomponents of Networking Services:

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

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

Total disk space required: 0.0 MB
Space available on disk: 260.8 MB

Using UPnP in Windows XP Example

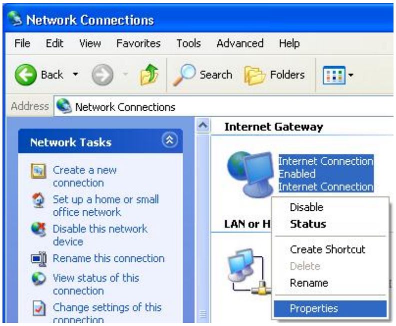
This appendix shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

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

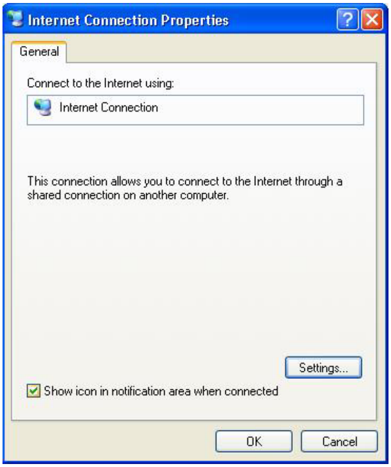
Auto-discover Your UPnP-enabled Network Device

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

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



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



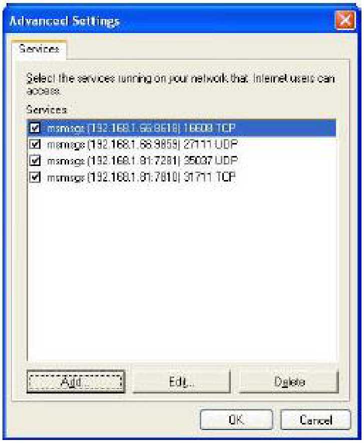
Connect to the Internet using:

Internet Connection

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

☑ Show icon in notification area when connected

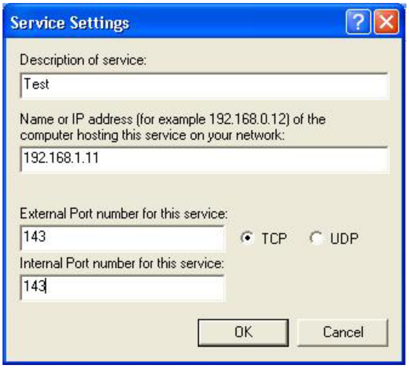
Step 4. You may edit or delete the port mappings or click **Add** to manually add port mappings.



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

Services

☑ msmsgs (192.168.1.66:9618) 16608 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.91:7281) 35037 UDP
☑ msmsgs (192.168.1.91:7810) 31711 TCP



Description of service:

Test

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

192.168.1.11

External Port number for this service:

143

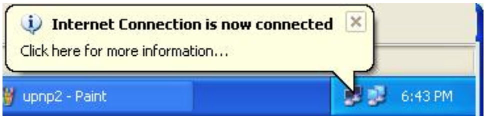
● TCP ○ UDP

Internal Port number for this service:

143

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

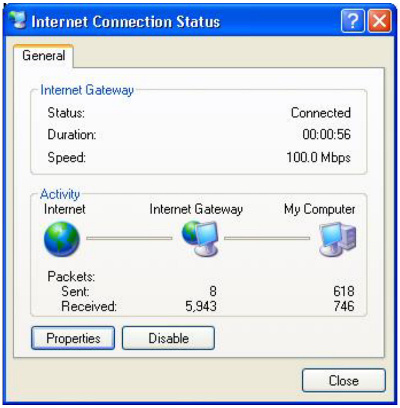
Step 5. Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.



Internet Connection is now connected

Click here for more information...

Step 6. Double-click the icon to display your current Internet connection status.



Internet Connection Status

General

Internet Gateway

Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

Activity

	Internet Gateway	My Computer
Packets:		
Sent:	8	618
Received:	5,943	746

Web Configurator Easy Access

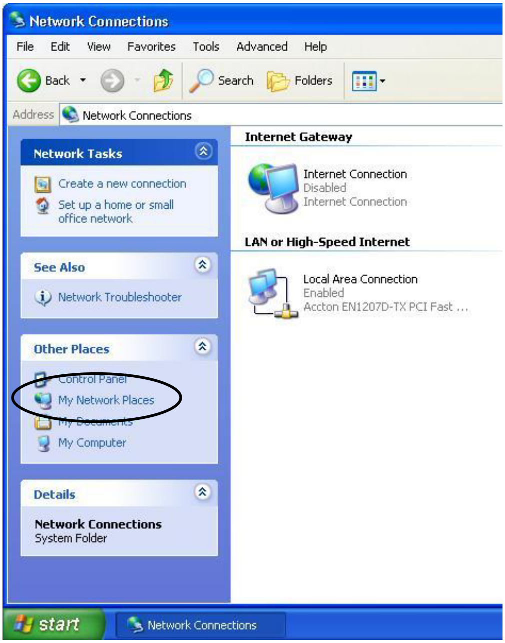
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This comes helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

Step 1. Click **start** and then **Control Panel**.

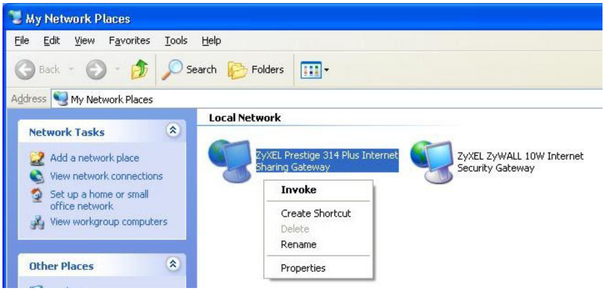
Step 2. Double-click **Network Connections**.

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

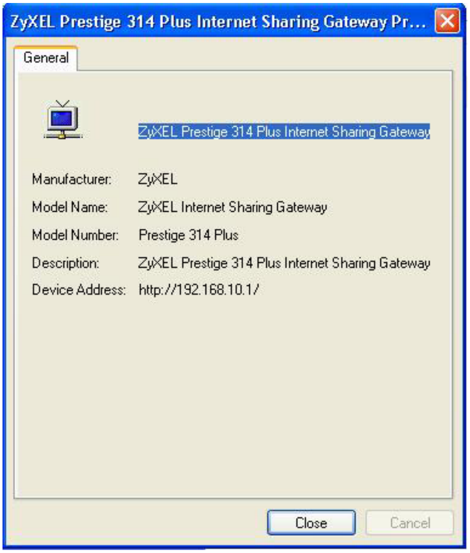


Step 4. An icon with the description for each UPnP-enabled device displays under **Local Network**.

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


My Network Places
File Edit View Favorites Tools Help
Back Search Folders
Address My Network Places
Network Tasks
Add a network place
View network connections
Set up a home or small office network
View workgroup computers
Other Places
Local Network
ZyXEL Prestige 314 Plus Internet Sharing Gateway
ZyXEL ZyWALL 10W Internet Security Gateway
Invoke
Create Shortcut
Delete
Rename
Properties

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



ZyXEL Prestige 314 Plus Internet Sharing Gateway Pr...

ZyXEL Prestige 314 Plus Internet Sharing Gateway

Manufacturer:	ZyXEL
Model Name:	ZyXEL Internet Sharing Gateway
Model Number:	Prestige 314 Plus
Description:	ZyXEL Prestige 314 Plus Internet Sharing Gateway
Device Address:	http://192.168.10.1/

Appendix J
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Chart J-1 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Host IDs of all zeros or all ones are not allowed.

Therefore:

- A class "C" network (8 host bits) can have 2^8 –2 or 254 hosts.

- A class “B” address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class “A” address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Chart J-2 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

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; each bit of the mask corresponds to a bit of the IP address. 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 as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

Chart J-3 “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 left most 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.

Chart J-4 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

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.

	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"). You want to have two separate 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.

In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form 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.

Chart J-5 Subnet 1

	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
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

Chart J-6 Subnet 2

	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

The remaining 7 bits determine the number of hosts each subnet can have. 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 of 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 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart J-7 Subnet 1

	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
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	

Chart J-8 Subnet 2

	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	

Chart J-9 Subnet 3

	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

Chart J-10 Subnet 4

	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 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Chart J-11 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	223	254	255

The following table is a summary for class “C” subnet planning.

Chart J-12 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 *Chart J-1*) available for subnetting.

The following table is a summary for class “B” subnet planning.

Chart J-13 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

Chart J-13 Class B Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 K
Safety Warnings and Instructions

1. Be sure to read and follow all warning notices and instructions.
2. The maximum recommended ambient temperature for the ZyWALL is 40º Celsius (104º Fahrenheit). Care must be taken to allow sufficient air circulation or space between units when the ZyWALL is installed inside a closed rack assembly. The operating ambient temperature of the rack environment might be greater than room temperature.
3. Installation in a rack without sufficient airflow can be unsafe.
4. Racks should safely support the combined weight of all equipment.
5. The connections and equipment that supply power to the ZyWALL should be capable of operating safely with the maximum power requirements of the ZyWALL. In case of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the ZyWALL is printed on the nameplate.
6. The power cord or power adaptor must plug in to the right supply voltage, i.e. 110VAC for North America and 230VAC for Europe. Make sure that the supplied AC voltage is correct and stable.
7. Installation in restricted access areas must comply with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
8. Do not allow anything to rest on the power cord and do not locate the product where anyone can walk on the power cord.
9. Do not service the product by yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
10. Generally, when installed after the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult the appropriate regulatory agencies and inspection authorities to ensure compliance.
11. A rare condition can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate building are interconnected, the voltage potential can cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action before interconnecting the products.

Appendix L
Removing and Installing a ZyWALL 100 Fuse

This appendix shows you how to remove and install fuses for the ZYWALL 100.

The ZYWALL 100 uses a 0.5 Amp, 250 VAC fuse. The ZYWALL-100 comes from the factory; with two fuses installed in the fuse housing. If you need to install a new fuse, follow the procedure below.

Removing a Fuse

Disconnect all power from the ZYWALL 100 before you begin this procedure.

Step 1. Place the rear panel of the ZYWALL 100 in front of you.

Step 2. Remove the power cord from the back of the unit.

Step 3. The fuse housing is located between the power switch and the power port. Use a small flat-head screwdriver to carefully pry out the fuse housing.

Step 4. A burnt-out fuse is blackened, darkened or cloudy inside its glass casing. A working fuse has a completely clear glass casing. Pull gently, but firmly, to remove the burnt out fuse from the fuse housing. Dispose of the burnt-out fuse.

Installing a Fuse

Step 1. The ZyWALL 100 is shipped from the factory with one spare fuse included in a box-like section of the fuse housing. Push the middle part of the box-like section to access the spare fuse. Put another spare fuse in its place in order to always have one on hand.

Step 2. Push the replacement fuse into the fuse housing until you hear a click.

Step 3. Firmly, but gently, push the fuse housing back into the ZYWALL 100 until you hear a click.

Step 4. Plug the power cord back into the unit.

Part XII:

Command and Log Appendices

This part provides information on the command line interface, firewall and NetBIOS commands and logs and password protection.

Appendix M
Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or zyxel.com for more detailed information on these commands.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

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.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Appendix N
Firewall Commands

The following describes the firewall commands. See the *Command Interpreter* appendix for information on the command structure.

Chart N-1 Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
Firewall		
Set-Up		
	`config edit firewall active <yes | no>`	This command turns the firewall on or off.
	`config retrieve firewall`	This command returns the previously saved firewall settings.
	`config save firewall`	This command saves the current firewall settings.
Display		
	`config display firewall`	This command shows the of all the firewall settings including e-mail, attack, and the sets/ rules.
	`config display firewall set <set #>`	This command shows the current configuration of a set; including timeout values, name, default-permit, and etc. If you don't put use a number (#) after "set", information about all of the sets/rules appears.
	`config display firewall set <set #> rule <rule #>`	This command shows the current entries of a rule in a firewall rule set.
	`config display firewall attack`	This command shows all of the attack response settings.

Chart N-1 Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
	`config display firewall e-mail`	This command shows all of the e-mail settings.
	`config display firewall ?`	This command shows all of the available firewall sub commands.
Edit		
E-mail	`config edit firewall e-mail mail-server <ip address of mail server>`	This command sets the IP address to which the e-mail messages are sent.
	`config edit firewall e-mail return-addr <e-mail address>`	This command sets the source e-mail address of the firewall e-mails.
	`config edit firewall e-mail email-to <e-mail address>`	This command sets the e-mail address to which the firewall e-mails are sent.
	`config edit firewall e-mail policy <full | hourly | daily | weekly>`	This command sets how frequently the firewall log is sent via e-mail.
	`config edit firewall e-mail day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>`	This command sets the day on which the current firewall log is sent through e-mail if the ZyWALL is set to send it on a weekly basis.
	`config edit firewall e-mail hour <0-23>`	This command sets the hour when the firewall log is sent through e- mail if the ZyWALL is set to send it on an hourly, daily or weekly basis.
	`config edit firewall e-mail minute <0-59>`	This command sets the minute of the hour for the firewall log to be sent via e- mail if the ZyWALL is set to send it on a hourly, daily or weekly basis.

Chart N-1 Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
Attack	`config edit firewall attack send-alert <yes | no>`	This command enables or disables the immediate sending of DOS attack notification e-mail messages.
	`config edit firewall attack block <yes | no>`	Set this command to `yes` to block new traffic after the tcp-max-incomplete threshold is exceeded. Set it to `no` to delete the oldest half-open session when traffic exceeds the tcp-max-incomplete threshold.
	`config edit firewall attack block-minute <0-255>`	This command sets the number of minutes for new sessions to be blocked when the tcp-max-incomplete threshold is reached. This command is only valid when `block` is set to `yes`.
	`config edit firewall attack minute-high <0-255>`	This command sets the threshold rate of new half-open sessions per minute where the ZyWALL starts deleting old half-opened sessions until it gets them down to the minute-low threshold.
	`config edit firewall attack minute-low <0-255>`	This command sets the threshold of half-open sessions where the ZyWALL stops deleting half-opened sessions.
	`config edit firewall attack max-incomplete-high <0-255>`	This command sets the threshold of half-open sessions where the ZyWALL starts deleting old half-opened sessions until it gets them down to the max incomplete low.
	`config edit firewall attack max-incomplete-low <0-255>`	This command sets the threshold where the ZyWALL stops deleting half-opened sessions.
	`config edit firewall attack tcp-max-incomplete <0-255>`	This command sets the threshold of half-open TCP sessions with the same destination where the ZyWALL starts dropping half-open sessions to that destination.

Chart N-1 Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
Sets	`config edit firewall set <set #> name <desired name>`	This command sets a name to identify a specified set.
	`Config edit firewall set <set #> default-permit <forward | block>`	This command sets whether a packet is dropped or allowed through, when it does not meet a rule within the set.
	`Config edit firewall set <set #> icmp-timeout <seconds>`	This command sets the time period to allow an ICMP session to wait for the ICMP response.
	`Config edit firewall set <set #> udp-idle-timeout <seconds>`	This command sets how long a UDP connection is allowed to remain inactive before the ZyWALL considers the connection closed.
	`Config edit firewall set <set #> connection-timeout <seconds>`	This command sets how long ZyWALL waits for a TCP session to be established before dropping the session.
	`Config edit firewall set <set #> fin-wait-timeout <seconds>`	This command sets how long the ZyWALL leaves a TCP session open after the firewall detects a FIN-exchange (indicating the end of the TCP session).
	`Config edit firewall set <set #> tcp-idle-timeout <seconds>`	This command sets how long ZyWALL lets an inactive TCP connection remain open before considering it closed.
	`Config edit firewall set <set #> log <yes | no>`	This command sets whether or not the ZyWALL creates logs for packets that match the firewall's default rule set.
Rules	`Config edit firewall set <set #> rule <rule #> permit <forward | block>`	This command sets whether packets that match this rule are dropped or allowed through.

Chart N-1 Firewall Commands

<table>
<tr><th>FUNCTION</th><th>COMMAND</th><th>DESCRIPTION</th></tr>
<tr><td></td><td><code>Config edit firewall set <set #> rule <rule #> active <yes | no&gt;</code></td><td>This command sets whether a rule is enabled or not.</td></tr>
<tr><td></td><td><code>Config edit firewall set <set #> rule <rule #> protocol <integer protocol value &gt;</code></td><td>This command sets the protocol specification number made in this rule for ICMP.</td></tr>
<tr><td></td><td><code>Config edit firewall set <set #> rule <rule #> log <none | match | not-match | both&gt;</code></td><td>This command sets the ZyWALL to log traffic that matches the rule, doesn't match, both or neither.</td></tr>
<tr><td></td><td><code>Config edit firewall set <set #> rule <rule #> alert <yes | no&gt;</code></td><td>This command sets whether or not the ZyWALL sends an alert e-mail when a DOS attack or a violation of a particular rule occurs.</td></tr>
<tr><td></td><td><code>config edit firewall set <set #> rule <rule #> srcaddr-single <ip address&gt;</code></td><td>This command sets the rule to have the ZyWALL check for traffic with this individual source address.</td></tr>
<tr><td></td><td><code>config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask&gt;</code></td><td>This command sets a rule to have the ZyWALL check for traffic from a particular subnet (defined by IP address and subnet mask).</td></tr>
<tr><td></td><td><code>config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address&gt;</code></td><td>This command sets a rule to have the ZyWALL check for traffic from this range of addresses.</td></tr>
<tr><td></td><td><code>config edit firewall set <set #> rule <rule #> destaddr-single <ip address&gt;</code></td><td>This command sets the rule to have the ZyWALL check for traffic with this individual destination address.</td></tr>
<tr><td></td><td><code>config edit firewall set <set #> rule <rule #> destaddr-subnet <ip address> <subnet mask&gt;</code></td><td>This command sets a rule to have the ZyWALL check for traffic with a particular subnet destination (defined by IP address and subnet mask).</td></tr>
</table>

Chart N-1 Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
	`config edit firewall set <set #> rule <rule #> destaddr-range <start ip address> <end ip address>`	This command sets a rule to have the ZyWALL check for traffic going to this range of addresses.
	`config edit firewall set <set #> rule <rule #> TCP destport-single <port #>`	This command sets a rule to have the ZyWALL check for TCP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	`config edit firewall set <set #> rule <rule #> TCP destport-range <start port #> <end port #>`	This command sets a rule to have the ZyWALL check for TCP traffic with a destination port in this range.
	`config edit firewall set <set #> rule <rule #> UDP destport-single <port #>`	This command sets a rule to have the ZyWALL check for UDP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	`config edit firewall set <set #> rule <rule #> UDP destport-range <start port #> <end port #>`	This command sets a rule to have the ZyWALL check for UDP traffic with a destination port in this range.
Delete		
	`config delete firewall e-mail`	This command removes all of the settings for e-mail alert.
	`config delete firewall attack`	This command resets all of the attack response settings to their defaults.
	`config delete firewall set <set #>`	This command removes the specified set from the firewall configuration.

	`config delete firewall set <set #> rule`
	`<rule #>`
		This command removes the specified rule in a firewall configuration set.

Appendix O
NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See the *Command Interpreter* appendix for information on the command structure.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

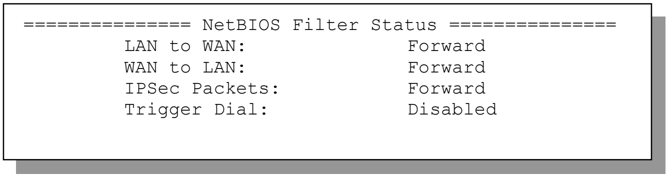
You can configure NetBIOS filters to do the following (filters for DMZ are not available on all models):

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN.
- Allow or disallow the sending of NetBIOS packets from the WAN to the LAN.
- Allow or disallow the sending of NetBIOS packets from the LAN to the DMZ.
- Allow or disallow the sending of NetBIOS packets from the WAN to the DMZ.
- Allow or disallow the sending of NetBIOS packets from the DMZ to the LAN.
- Allow or disallow the sending of NetBIOS packets from the DMZ to the WAN.
- Allow or disallow the sending of NetBIOS packets through VPN connections.
- Allow or disallow NetBIOS packets to initiate calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes for a ZyWALL that does not have DMZ.

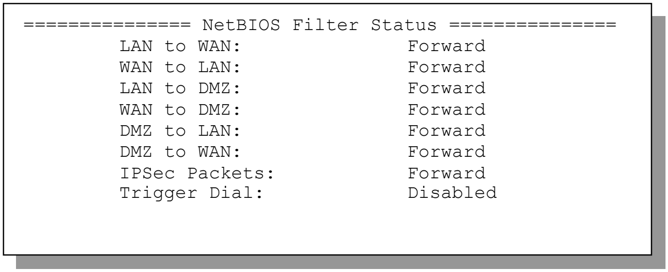


```
=============== NetBIOS Filter Status ===============
         LAN to WAN:                Forward
         WAN to LAN:                Forward
         IPSec Packets:             Forward
         Trigger Dial:              Disabled
```

Diagram O-1 NetBIOS Display Filter Settings Command Without DMZ Example

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes for a ZyWALL that has DMZ.



```
=============== NetBIOS Filter Status ===============
        LAN to WAN:                 Forward
        WAN to LAN:                 Forward
        LAN to DMZ:                 Forward
        WAN to DMZ:                 Forward
        DMZ to LAN:                 Forward
        DMZ to WAN:                 Forward
        IPSec Packets:              Forward
        Trigger Dial:               Disabled
```

Diagram O-2 NetBIOS Display Filter Settings Command With DMZ Example

The filter types and their default settings are as follows.

Chart O-1 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
LAN to WAN	This field displays whether NetBIOS packets are blocked or forwarded from the LAN to the WAN.	Forward
WAN to LAN	This field displays whether NetBIOS packets are blocked or forwarded from the WAN to the LAN.	Forward
LAN to DMZ	This field displays whether NetBIOS packets are blocked or forwarded from the LAN to the DMZ.	Forward

Chart O-1 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
WAN to DMZ	This field displays whether NetBIOS packets are blocked or forwarded from the WAN to the DMZ.	Forward
DMZ to LAN	This field displays whether NetBIOS packets are blocked or forwarded from the DMZ to the LAN.	Forward
DMZ to WAN	This field displays whether NetBIOS packets are blocked or forwarded from the DMZ to the WAN.	Forward
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

Syntax: `sys filter netbios config <type> <on|off>`

where

`<type> =` Identify which NetBIOS filter (numbered 0-3) to configure.

0 = LAN to WAN

1 = WAN to LAN

2 =LAN to DMZ

3 = WAN to DMZ

4 = DMZ to LAN

5 = DMZ to WAN

6 = IPSec packet pass through

7 = Trigger Dial

`<on|off>` = For types `0` and `1`, use `on` to enable the filter and block NetBIOS packets. Use `off` to disable the filter and forward NetBIOS packets.

For type `6`, use `on` to block NetBIOS packets from being sent through a VPN connection. Use `off` to allow NetBIOS packets to be sent through a VPN connection.

For type `7`, use `on` to allow NetBIOS packets to initiate dial backup calls. Use `off` to block NetBIOS packets from initiating dial backup calls.

Example commands

Command: `sys filter netbios config 0 on`

This command blocks LAN to WAN NetBIOS packets

Command: `sys filter netbios config 1 off`

This command forwards WAN to LAN NetBIOS packets

Command: `sys filter netbios config 6 on`

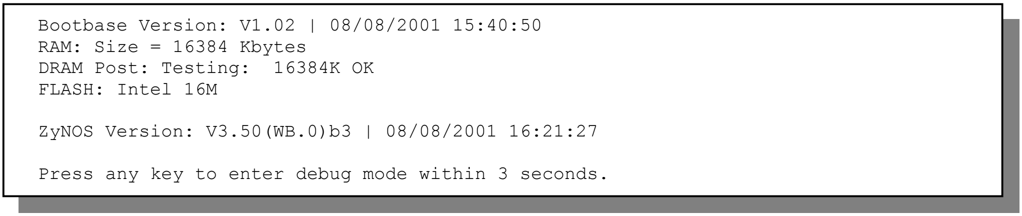
This command blocks IPSec NetBIOS packets

Command: `sys filter netbios config 7 off`

This command stops NetBIOS commands from initiating calls.

Appendix P
Boot Commands

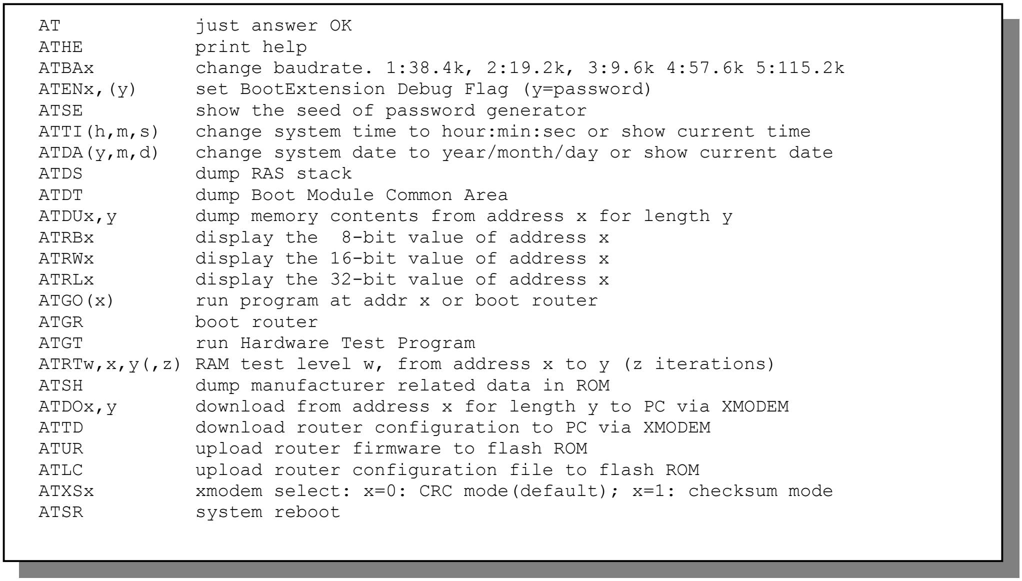
The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware (ZyNOS) is started. When you start up your ZyWALL, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example `ATUR` (for uploading firmware) and `ATLC` (for uploading the configuration file). These are already discussed in the *Firmware and Configuration File Maintenance* chapter.



```
Bootbase Version: V1.02 | 08/08/2001 15:40:50
RAM: Size = 16384 Kbytes
DRAM Post: Testing:  16384K OK
FLASH: Intel 16M

ZyNOS Version: V3.50(WB.0)b3 | 08/08/2001 16:21:27

Press any key to enter debug mode within 3 seconds.
```

Diagram P-1 Option to Enter Debug Mode

Enter `ATHE` to view all available ZyWALL boot module commands as shown in the next screen. `ATBAx` allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example `ATBA3` will give a console port speed of 9.6 Kbps. `ATSE` displays the seed that is used to generate a password to turn on the debug flag in the firmware. The `ATSH` command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. `ATGO` allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.



```
AT             just answer OK
ATHE           print help
ATBAx          change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)      set BootExtension Debug Flag (y=password)
ATSE           show the seed of password generator
ATTI(h,m,s)    change system time to hour:min:sec or show current time
ATDA(y,m,d)    change system date to year/month/day or show current date
ATDS           dump RAS stack
ATDT           dump Boot Module Common Area
ATDUx,y        dump memory contents from address x for length y
ATRBx          display the  8-bit value of address x
ATRWx          display the 16-bit value of address x
ATRLx          display the 32-bit value of address x
ATGO(x)        run program at addr x or boot router
ATGR           boot router
ATGT           run Hardware Test Program
ATRTw,x,y(,z)  RAM test level w, from address x to y (z iterations)
ATSH           dump manufacturer related data in ROM
ATDOx,y        download from address x for length y to PC via XMODEM
ATTD           download router configuration to PC via XMODEM
ATUR           upload router firmware to flash ROM
ATLC           upload router configuration file to flash ROM
ATXSx          xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATSR           system reboot
```

Diagram P-2 Boot Module Commands

Appendix Q
Log Descriptions

Chart Q-1 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.

Chart Q-2 System Maintenance Logs

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

Chart Q-2 System Maintenance Logs

`TELNET Login Fail`	Someone has failed to log on to the router via telnet.
`FTP Login Successfully`	Someone has logged on to the router via ftp.
`FTP Login Fail`	Someone has failed to log on to the router via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.

Chart Q-3 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Chart Q-4 Content Filtering Logs

CATEGORY	LOG MESSAGE	DESCRIPTION
URLFOR	`IP/Domain Name`	The ZyWALL allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name.
URLBLK	`IP/Domain Name`	The ZyWALL blocked access to this IP address or domain name due to a forbidden keyword. All web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list.
JAVBLK	`IP/Domain Name`	The ZyWALL blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy.

Chart Q-5 Attack Logs

LOG MESSAGE	DESCRIPTION
`attack TCP`	The firewall detected a TCP attack.
`attack UDP`	The firewall detected an UDP attack.

Chart Q-5 Attack Logs

LOG MESSAGE	DESCRIPTION
`attack IGMP`	The firewall detected an IGMP attack.
`attack ESP`	The firewall detected an ESP attack.
`attack GRE`	The firewall detected a GRE attack.
`attack OSPF`	The firewall detected an OSPF attack.
`attack ICMP (type:%d, code:%d)`	The firewall detected an ICMP attack; see the section on ICMP messages for type and code details.
`land TCP`	The firewall detected a TCP land attack.
`land UDP`	The firewall detected an UDP land attack.
`land IGMP`	The firewall detected an IGMP land attack.
`land ESP`	The firewall detected an ESP land attack.
`land GRE`	The firewall detected a GRE land attack.
`land OSPF`	The firewall detected an OSPF land attack.
`land ICMP (type:%d, code:%d)`	The firewall detected an ICMP land attack; see the section on ICMP messages for type and code details.
`ip spoofing - WAN TCP`	The firewall detected a TCP IP spoofing attack on the WAN port.
`ip spoofing - WAN UDP`	The firewall detected an UDP IP spoofing attack on the WAN port.
`ip spoofing - WAN IGMP`	The firewall detected an IGMP IP spoofing attack on the WAN port.
`ip spoofing - WAN ESP`	The firewall detected an ESP IP spoofing attack on the WAN port.
`ip spoofing - WAN GRE`	The firewall detected a GRE IP spoofing attack on the WAN port.
`ip spoofing - WAN OSPF`	The firewall detected an OSPF 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. See the section on ICMP messages for type and code details.
`icmp echo ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack. See the section on ICMP messages for type and code details.

Chart Q-5 Attack Logs

LOG MESSAGE	DESCRIPTION
`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.
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack; see the section on ICMP messages for type and code details.
`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`	The firewall detected a TCP IP spoofing attack while the ZyWALL did not have a default route.
`ip spoofing - no routing entry UDP`	The firewall detected an UDP IP spoofing attack while the ZyWALL did not have a default route.
`ip spoofing - no routing entry IGMP`	The firewall detected an IGMP IP spoofing attack while the ZyWALL did not have a default route.
`ip spoofing - no routing entry ESP`	The firewall detected an ESP IP spoofing attack while the ZyWALL did not have a default route.
`ip spoofing - no routing entry GRE`	The firewall detected a GRE IP spoofing attack while the ZyWALL did not have a default route.
`ip spoofing - no routing entry OSPF`	The firewall detected an OSPF IP spoofing attack while the ZyWALL did not have a default route.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack while the ZyWALL did not have a default route; see the section on ICMP messages for type and code details.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack; see the section on ICMP messages for type and code details.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack; see the section on ICMP messages for type and code details.

Chart Q-6 Access Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: TCP (set:%d)`	TCP access matched the default policy of the listed ACL set and the ZyWALL blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: UDP (set:%d)`	UDP access matched the default policy of the listed ACL set and the ZyWALL blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: ICMP (set:%d, type:%d, code:%d)`	ICMP access matched the default policy of the listed ACL set and the ZyWALL blocked or forwarded it according to the ACL set's configuration. See the section on ICMP messages for type and code details.
`Firewall default policy: IGMP (set:%d)`	IGMP access matched the default policy of the listed ACL set and the ZyWALL blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: ESP (set:%d)`	ESP access matched the default policy of the listed ACL set and the ZyWALL blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: GRE (set:%d)`	GRE access matched the default policy of the listed ACL set and the ZyWALL blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: OSPF (set:%d)`	OSPF access matched the default policy of the listed ACL set and the ZyWALL blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: (set:%d)`	Access matched the default policy of the listed ACL set and the ZyWALL blocked or forwarded it according to the ACL set's configuration.
`Firewall rule match: TCP (set:%d, rule:%d)`	TCP access matched the listed firewall rule and the ZyWALL blocked or forwarded it according to the rule's configuration.
`Firewall rule match: UDP (set:%d, rule:%d)`	UDP access matched the listed firewall rule and the ZyWALL blocked or forwarded it according to the rule's configuration.
`Firewall rule match: ICMP (set:%d, rule:%d, type:%d, code:%d)`	ICMP access matched the listed firewall rule and the ZyWALL blocked or forwarded it according to the rule's configuration. See the section on ICMP messages for type and code details.

Chart Q-6 Access Logs

LOG MESSAGE	DESCRIPTION
`Firewall rule match: IGMP (set:%d, rule:%d)`	IGMP access matched the listed firewall rule and the ZyWALL blocked or forwarded it according to the rule's configuration.
`Firewall rule match: ESP (set:%d, rule:%d)`	ESP access matched the listed firewall rule and the ZyWALL blocked or forwarded it according to the rule's configuration.
`Firewall rule match: GRE (set:%d, rule:%d)`	GRE access matched the listed firewall rule and the ZyWALL blocked or forwarded it according to the rule's configuration.
`Firewall rule match: OSPF (set:%d, rule:%d)`	OSPF access matched the listed a firewall rule and the ZyWALL blocked or forwarded it according to the rule's configuration.
`Firewall rule match: (set:%d, rule:%d)`	Access matched the listed firewall rule and the ZyWALL blocked or forwarded it according to the rule's configuration.
`Firewall rule NOT match: TCP  (set:%d, rule:%d)`	TCP access did not match the listed firewall rule and the ZyWALL logged it.
`Firewall rule NOT match: UDP (set:%d, rule:%d)`	UDP access did not match the listed firewall rule and the ZyWALL logged it.
`Firewall rule NOT match: ICMP (set:%d, rule:%d, type:%d, code:%d)`	ICMP access did not match the listed firewall rule and the ZyWALL logged it.
`Firewall rule NOT match: IGMP (set:%d, rule:%d)`	IGMP access did not match the listed firewall rule and the ZyWALL logged it.
`Firewall rule NOT match: ESP (set:%d, rule:%d)`	ESP access did not match the listed firewall rule and the ZyWALL logged it.
`Firewall rule NOT match: GRE (set:%d, rule:%d)`	GRE ac access did not match the listed firewall rule and the ZyWALL logged it.

Chart Q-6 Access Logs

LOG MESSAGE	DESCRIPTION
`Firewall rule NOT match: OSPF (set:%d, rule:%d)`	OSPF access did not match the listed firewall rule and the ZyWALL logged it.
`Firewall rule NOT match: (set:%d, rule:%d)`	Access did not match the listed firewall rule and the ZyWALL logged it.
`Filter default policy DROP!`	TCP access matched a default filter policy and the ZyWALL dropped the packet to block access.
`Filter default policy DROP!`	UDP access matched a default filter policy and the ZyWALL dropped the packet to block access.
`Filter default policy DROP!`	ICMP access matched a default filter policy and the ZyWALL dropped the packet to block access.
`Filter default policy DROP!`	Access matched a default filter policy and the ZyWALL dropped the packet to block access.
`Filter default policy DROP!`	Access matched a default filter policy (denied LAN IP) and the ZyWALL dropped the packet to block access.
`Filter default policy FORWARD!`	TCP access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	UDP access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	ICMP access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	Access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	Access matched a default filter policy (denied LAN IP). Access was allowed and the router forwarded the packet.
`Filter match DROP <set %d/rule %d>`	TCP access matched the listed filter rule and the ZyWALL dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	UDP access matched the listed filter rule and the ZyWALL dropped the packet to block access.

Chart Q-6 Access Logs

LOG MESSAGE	DESCRIPTION
`Filter match DROP <set %d/rule %d>`	ICMP access matched the listed filter rule and the ZyWALL dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	Access matched the listed filter rule and the ZyWALL dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	Access matched the listed filter rule (denied LAN IP) and the ZyWALL dropped the packet to block access.
`Filter match FORWARD <set %d/rule %d>`	TCP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	UDP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	ICMP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	Access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	Access matched the listed filter rule (denied LAN IP). Access was allowed and the router forwarded the packet.
`(set:%d)`	With firewall messages, this is the number of the ACL policy set and denotes the packet's direction (see *Chart Q-7*). With filter messages, this is the number of the filter set.
`(rule:%d)`	With firewall messages, the firewall rule number denotes the number of a firewall rule within an ACL policy set. With filter messages, this is the number of an individual filter rule.
`Router sent blocked web site message`	A message was sent to notify a user that the router blocked access to a requested web site
`Triangle route packet forwarded`	The firewall allowed a triangle route session to pass through.
`Firewall sent TCP packet in response to DoS attack`	The firewall detected a DoS attack and sent a TCP packet(s) in response.

Chart Q-6 Access Logs

LOG MESSAGE	DESCRIPTION
`Firewall sent TCP reset packets`	The firewall sent out TCP reset packets.
`Packet without a NAT table entry blocked`	The router blocked a packet that did not have a corresponding NAT table entry.
`Out of order TCP handshake packet blocked`	The router blocked a TCP handshake packet that came out of the proper order
`Drop unsupported/out-of-order ICMP`	The ZyWALL generates this log after it drops an ICMP packet due to one of the following two reasons: 1. The ZyWALL does not support the ICMP packet's protocol. 2. The ICMP packet is an echo reply for which there was no corresponding echo request.
`Router sent ICMP response packet (type:%d, code:%d)`	The router sent an ICMP response packet. This packet automatically bypasses the firewall. See the section on ICMP messages for type and code details.

Chart Q-7 ACL Setting Notes

ACL SET NUMBER	DIRECTION	DESCRIPTION
1	LAN to WAN	ACL set 1 for packets traveling from the LAN to the WAN.
2	WAN to LAN	ACL set 2 for packets traveling from the WAN to the LAN.
3	DMZ to LAN	ACL set 3 for packets traveling from the DMZ to the LAN.
4	DMZ to WAN	ACL set 4 for packets traveling from the DMZ to the WAN.
5	WAN to DMZ	ACL set 5 for packets traveling from the WAN to the DMZ.
6	LAN to DMZ	ACL set 6 for packets traveling from the LAN to the DMZ.
7	LAN to LAN/ZyWALL	ACL set 7 for packets traveling from the LAN to the LAN or the ZyWALL.
8	WAN to WAN/ZyWALL	ACL set 8 for packets traveling from the WAN to the WAN or the ZyWALL.

Chart Q-7 ACL Setting Notes

ACL SET NUMBER	DIRECTION	DESCRIPTION
9	DMZ to DMZ/ZyWALL	ACL set 9 for packets traveling from the DMZ to the DM or the ZyWALL.

Chart Q-8 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

Chart Q-8 ICMP Notes

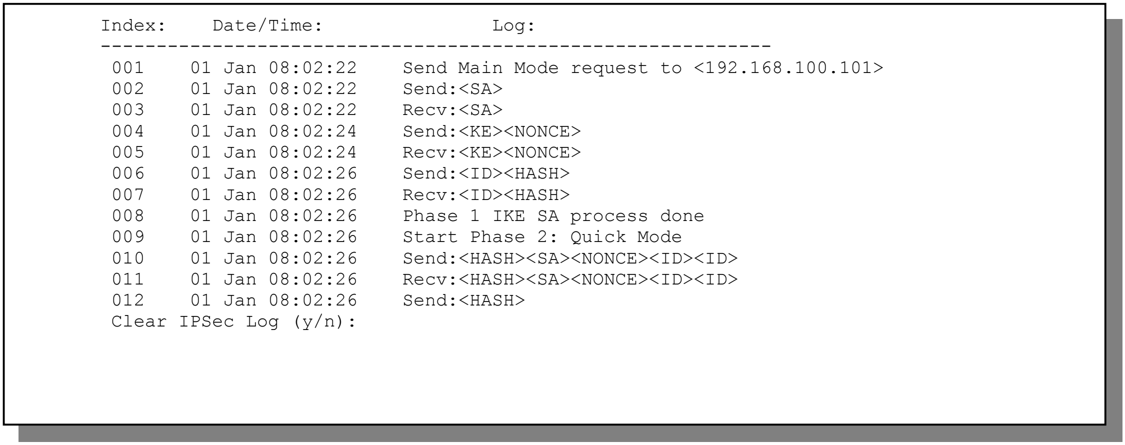
TYPE	CODE	DESCRIPTION
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information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

Chart Q-9 Sys log

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

VPN/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.

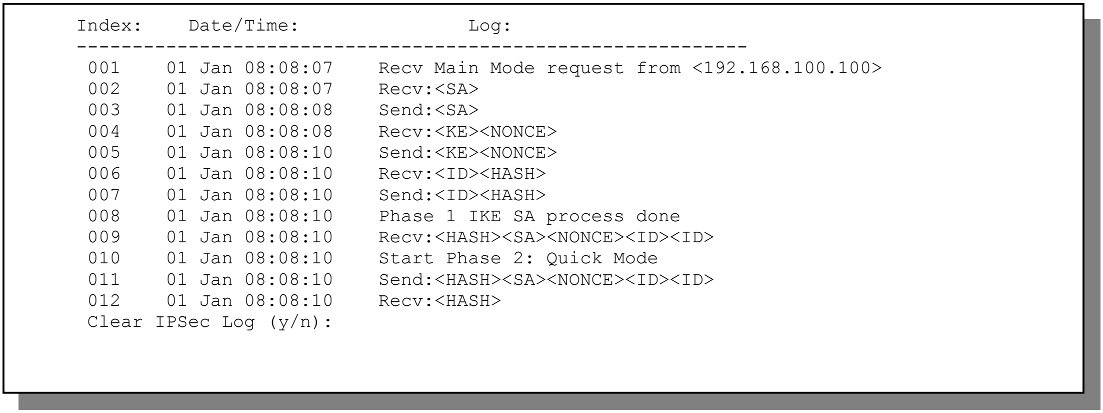


```
Index:    Date/Time:               Log:
------------------------------------------------------------
 001    01 Jan 08:02:22    Send Main Mode request to <192.168.100.101>
 002    01 Jan 08:02:22    Send:<SA>
 003    01 Jan 08:02:22    Recv:<SA>
 004    01 Jan 08:02:24    Send:<KE><NONCE>
 005    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):
```

Diagram Q-1 Example VPN Initiator IPSec Log

VPN Responder IPSec Log

The following figure shows a typical log from the VPN connection peer.



```
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):
```

Diagram Q-2 Example VPN Responder IPSec Log

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.

Double exclamation marks (!!) denote an error or warning message.

The following table shows sample log messages during IKE key exchange.

Chart Q-10 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
`Send <Symbol> Mode request to <IP>` `Send <Symbol> Mode request to <IP>`	The ZyWALL has started negotiation with the peer.
`Recv <Symbol> Mode request from <IP>` `Recv <Symbol> Mode request from <IP>`	The ZyWALL has received an IKE negotiation request from the peer.
`Recv:<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 Chart Q-12.
`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 ZyWALL 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 ZyWALL has received multiple requests from the same peer but it is still processing the first IKE packet from that peer.
`!! 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 ZyWALL 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.

Chart Q-10 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
`!! Remote IP <IP start> / <IP end> conflicts`	If the security gateway is "0.0.0.0", the ZyWALL will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the ZyWALL will not accept VPN connection requests from this peer.
`!! Active connection allowed exceeded`	The ZyWALL limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
`!! IKE Packet Retransmit`	The ZyWALL did not receive a response from the peer and so retransmits the last packet sent.
`!! Failed to send IKE Packet`	The ZyWALL cannot send IKE packets due to a network error.
`!! Too many errors! Deleting SA`	The ZyWALL deletes an SA when too many errors occur.
`!! Phase 1 ID type mismatch`	The ID type of an incoming packet does not match the local's peer ID type.
`!! Phase 1 ID content mismatch`	The ID content of an incoming packet does not match the local's peer ID content.
`!! No known phase 1 ID type found`	The ID type of an incoming packet does not match any known ID type.
`Peer ID: IP address type <IP address>`	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays the IP address type and IP address of the incoming packet.
`vs. My Remote <IP address>`	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured remote IP address type or IP address that the incoming packet did not match.

Chart Q-10 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
`vs. My Local <IP address>`	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured local IP address type or IP address that the incoming packet did not match.
`    -> <symbol>`	The router sent a payload type of IKE packet.
`Error ID Info`	The parameters configured for Phase 1 ID content do not match or the parameters configured for the Phase 2 ID (IP address of single, range or subnet) do not match. Please check all protocols and settings for these phases.

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.

The following table shows sample log messages during packet transmission.

Chart Q-11 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
`!! WAN IP changed to <IP>`	If the ZyWALL'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 ZyWALL will use the current ZyWALL WAN IP address (static or dynamic) to set up the VPN tunnel.
`!! Cannot find IPSec SA`	The ZyWALL cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
`!! 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.
`!! Discard REPLAY packet`	If the ZyWALL 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.

Chart Q-11 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
`Rule <#d> idle time out, disconnect`	If an SA has no packets transmitted for a period of time (configurable via CI command), the ZyWALL 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.

Chart Q-12 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

Log Commands

Go to the command line interface (the *Command Interpreter Appendix* explains how to access and use the commands).

Configuring What You Want the ZyWALL to Log

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

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

Chart Q-13 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
`access`	`0, 1, 2, 3`
`attack`	`0, 1, 2, 3`
`error`	`0, 1, 2, 3`
`ike`	`0, 1, 2, 3`
`ipsec`	`0, 1, 2, 3`
`javablocked`	`0, 1, 2, 3`
`mten`	`0, 1`
`upnp`	`0, 1`
`urlblocked`	`0, 1, 2, 3`
`urlforward`	`0, 1`
Use `0` to not record logs for that category, `1` to record only logs for that category, `2` to record only alerts for that category, and `3` to record both logs and alerts for that category.	

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

Displaying Logs

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

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

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

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

Log Command Example

This example shows how to set the ZyWALL to record the access logs and alerts and then view the results.

```
ras> sys logs load

ras> sys logs category access 3

ras> sys logs save

ras> sys logs display access


#  .time                 source                 destination
notes

    message

  0|11/11/2002 15:10:12 |172.22.3.80:137       |172.22.255.255:137
|ACCESS BLOCK

    Firewall default policy: UDP(set:8)

  1|11/11/2002 15:10:12 |172.21.4.17:138       |172.21.255.255:138
|ACCESS BLOCK

    Firewall default policy: UDP(set:8)

  2|11/11/2002 15:10:11 |172.17.2.1            |224.0.1.60
|ACCESS BLOCK

    Firewall default policy: IGMP(set:8)

  3|11/11/2002 15:10:11 |172.22.3.80:137       |172.22.255.255:137
|ACCESS BLOCK

    Firewall default policy: UDP(set:8)

  4|11/11/2002 15:10:10 |192.168.10.1:520      |192.168.10.255:520
|ACCESS BLOCK

    Firewall default policy: UDP(set:8)

  5|11/11/2002 15:10:10 |172.21.4.67:137       |172.21.255.255:137
|ACCESS BLOCK
```

Appendix R
Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See the *Command Interpreter* appendix for information on the command structure.

Chart R-1 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
`sys pwderrtm`	This command displays the brute-force guessing password protection settings.
`sys pwderrtm 0`	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
`sys pwderrtm N`	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.
Example	
`sys pwderrtm 5`	This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

Part XIII:

Index

This part provides an Index of key terms.

Index