P-335

Firewall Router with Print Server

P-335WT

802.11g Wireless Firewall Router with Print Server

User's Guide

Version 3.60
4/2005

ZyXEL
Unleash Networking Power

Copyright

Disclaimer

Trademarks

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

Go to www.zyxel.com

1 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

2 Select the certification you wish to view from this page

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用
　　　　　者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現
　　　　　有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
　　　　　前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍
　　　　　受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

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.

Safety Warnings

1 To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.

2 Do not use this product near water, for example, in a wet basement or near a swimming pool.

3 Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Customer Support

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

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

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[A] FAX	WEB SITE FTP SITE	REGULAR MAIL
CORPORATE HEADQUARTERS (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.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
CZECH REPUBLIC	info@cz.zyxel.com info@cz.zyxel.com	+420 241 091 350 +420 241 091 359	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden

METHOD	SUPPORT E-MAIL	TELEPHONE[A]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
UNITED KINGDOM	technical@zyxel.co.uk	+44 (0) 8702 909090	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11, The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44 (0) 8702 909091	ftp.zyxel.co.uk	

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

-

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the P-335, Firewall Router with Print Server or the P-335WT, 802.11g Wireless Firewall Router with Print Server. This manual is designed to guide you through the configuration of your Prestige for its various applications.

> **Note:** Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your Prestige. Not all features can be configured through all interfaces.

Some parts of this manual relate to the Wireless Broadband Router. This manual may refer to the P-335, P-335WT, Firewall Router with Print Server or 802.11g Wireless Firewall Router with Print Server as the Prestige.

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

About This User's Guide

This User's Guide is designed to guide you through the configuration of your Prestige using the web configurator or the SMT. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator

> **Note:** Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your Prestige. Not all features can be configured through all interfaces.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Compact Guide

  The Compact Guide is designed to help you get up and running right away. They contain connection information and instructions on getting started.

- Web Configurator Online Help

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

- ZyXEL Glossary and Web Site

Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.
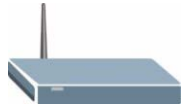
User Guide Feedback

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

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a 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.

Graphics Icons Key

Prestige	Computer	Notebook computer
Server	DSLAM	Firewall
Modem	Switch	Router
Wireless Signal	Printer	

CHAPTER 1
Getting to Know Your Prestige

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

1.1 Prestige Internet Security Gateway Overview

The Prestige is the ideal secure gateway for all data passing between the Internet and LAN's.

By integrating NAT, firewall, media bandwidth management and VPN capability, ZyXEL's Prestige is a complete security solution that protects your Intranet and efficiently manages data traffic on your network. The built-in print server allows computers on the LAN to share a USB printer eliminating the need to assign a dedicated computer as a print server or have a standalone print server device.

The embedded web configurator is easy to operate.

1.2 Prestige Features

The following sections describe Prestige features.

1.2.1 Physical Features

1.2.1.1 USB Port

The Prestige uses a USB 1.1 port to connect to a printer with a USB interface. Printers that use USB 1.0 are also compatible. Computers on the LAN use the printer by sending print requests to the print server in the Prestige.

1.2.1.2 OTIST Button (P-335WT only)

Use this button to activate OTIST (One-Touch Intelligent Security Technology). OTIST allows your Prestige to assign wireless clients the Prestige's SSID and static WEP or WPA-PSK encryption settings. The wireless client must also support OTIST and have OTIST enabled.

1.2.1.3 10/100M Auto-negotiating Ethernet/Fast Ethernet Interface(s)

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

1.2.1.4 Auto-crossover 10/100 Mbps Ethernet Interface(s)

These interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

1.2.1.5 4-Port Switch

A combination of switch and router makes your Prestige a cost-effective and viable network solution. You can add up to four computers to the Prestige without the cost of a hub. Add more than four computers to your LAN by using a hub.

1.2.1.6 Time and Date

The Prestige allows you to get the current time and date from an external server when you turn on your Prestige. You can also set the time manually.

1.2.1.7 Reset Button

The Prestige reset button is built into the rear panel. Use this button to restore the factory defaults.

1.2.2 Non-Physical Features

1.2.2.1 Print Server

The Prestige has a built-in print server that allows computers on the LAN to share a USB printer. This eliminates the need to assign a dedicated computer as a print server or have a standalone print server device.

1.2.2.2 OTIST (P-335WT only)

One-Touch Intelligent Security Technology (OTIST) allows your Prestige to give wireless clients the Prestige's security settings.The wireless client must also support OTIST. The Prestige's OTIST feature supports static WEP or WPA-PSK encryption security settings.

1.2.2.3 Media Bandwidth Management

ZyXEL's Media Bandwidth Management allows you to specify bandwidth classes based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth classes.

1.2.2.4 Trend Micro Security Services

TMSS (Trend Micro Security Services) identifies vulnerabilities and protects computers and networks that have Internet connections. **TMSS** is enabled by default on the Prestige but you must register at the **TMSS** web page. After you register, you can configure **TMSS** using the Prestige web configurator.

1.2.2.5 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 Prestige VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

1.2.2.6 Firewall

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

1.2.2.7 IEEE 802.1x Network Security (P-335WT only)

The Prestige supports the IEEE 802.1x standard to enhance user authentication. Use the built-in user profile database to authenticate up to 32 users using MD5 encryption. Use an EAP-compatible RADIUS (RFC2138, 2139 - Remote Authentication Dial In User Service) server to authenticate a limitless number of users using EAP (Extensible Authentication Protocol). EAP is an authentication protocol that supports multiple types of authentication.

1.2.2.8 Content Filtering

Content filtering allows you to block access to forbidden Internet web sites, schedule when the Prestige should perform the filtering and give trusted LAN IP addresses unfiltered Internet access.

1.2.2.9 Brute-Force Password Guessing Protection

The Prestige has a special protection mechanism to discourage brute-force password guessing attacks on the Prestige'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.

1.2.2.10 802.11b Wireless LAN Standard (P-335WT only)

The Prestige, complies with the 802.11b wireless standard.

The 802.11b data rate and corresponding modulation techniques are as follows. The modulation technique defines how bits are encoded onto radio waves.

Table 1   IEEE 802.11b

DATA RATE (KBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying**)**
5.5 / 11	CCK (Complementary Code Keying)

1.2.2.11 802.11g Wireless LAN Standard (P-335WT only)

The Prestige, complies with the 802.11g wireless standard and is also fully compatible with the 802.11b standard. This means an 802.11b radio card can interface directly with an 802.11g device (and vice versa) at 11 Mbps or lower depending on range. 802.11g has several intermediate rate steps between the maximum and minimum data rates. The 802.11g data rate and modulation are as follows:

Table 2 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

1.2.2.12 Packet Filtering

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

1.2.2.13 Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the Prestige and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

1.2.2.14 Call Scheduling

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

1.2.2.15 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.

1.2.2.16 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 Prestige supports one PPTP server connection at any given time.

1.2.2.17 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.

1.2.2.18 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 Prestige supports both versions 1 and 2.

1.2.2.19 IP Alias

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

1.2.2.20 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 Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two (SNMPv2).

1.2.2.21 Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

1.2.2.22 Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway on the LAN when the Prestige cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

1.2.2.23 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.

1.2.2.24 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 Prestige 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.

1.2.2.25 Any IP

The Any IP feature allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the Prestige are not in the same subnet.

1.2.2.26 Full Network Management

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

1.2.2.27 RoadRunner Support

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

1.2.2.28 Logging and Tracing

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

1.2.2.29 Upgrade Prestige Firmware via LAN

The firmware of the Prestige can be upgraded via the LAN (refer to Maintenance- F/W Upload Screen).

1.2.2.30 Embedded FTP and TFTP Servers

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

1.2.2.31 Wireless Association List (P-335WT only)

With the Wireless Association List, you can see the list of the wireless stations that are currently using the Prestige to access your wired network.

1.2.2.32 Wireless LAN Channel Usage (P-335WT only)

The Wireless Channel Usage displays whether the radio channels are used by other wireless devices within the transmission range of the Prestige. This allows you to select the channel with minimum interference for your Prestige.

1.3 Applications for the Prestige

Here are some examples of what you can do with your Prestige.

1.3.1 Print Server Application

The following figure shows how you can setup your printer to operate on a LAN using the Prestige as a router and print server.

Figure 1   Prestige Print Server Application
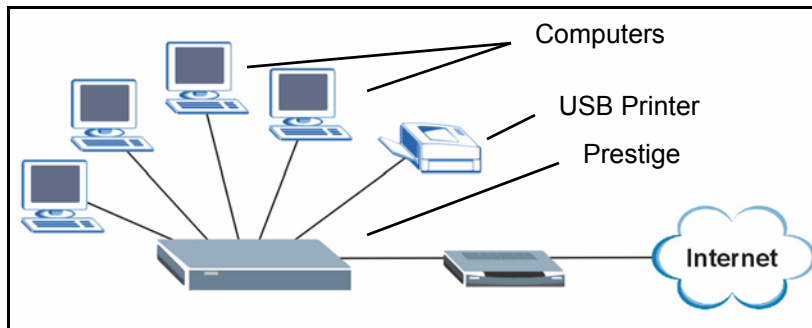
1.3.2 Secure Broadband Internet Access via Cable or DSL Modem

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

Figure 2 Secure Internet Access via Cable, DSL or Wireless Modem
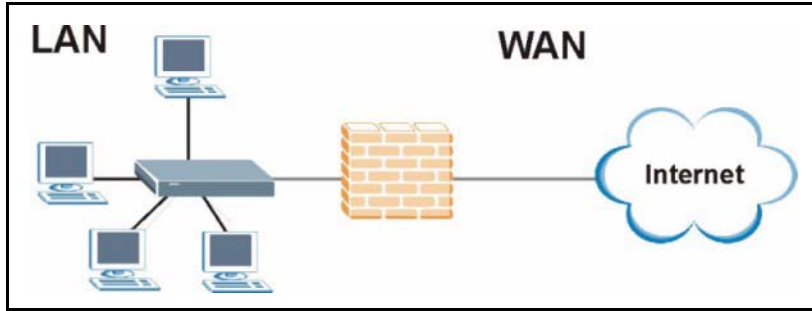
1.3.3 VPN Application

Prestige 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 3 VPN Application
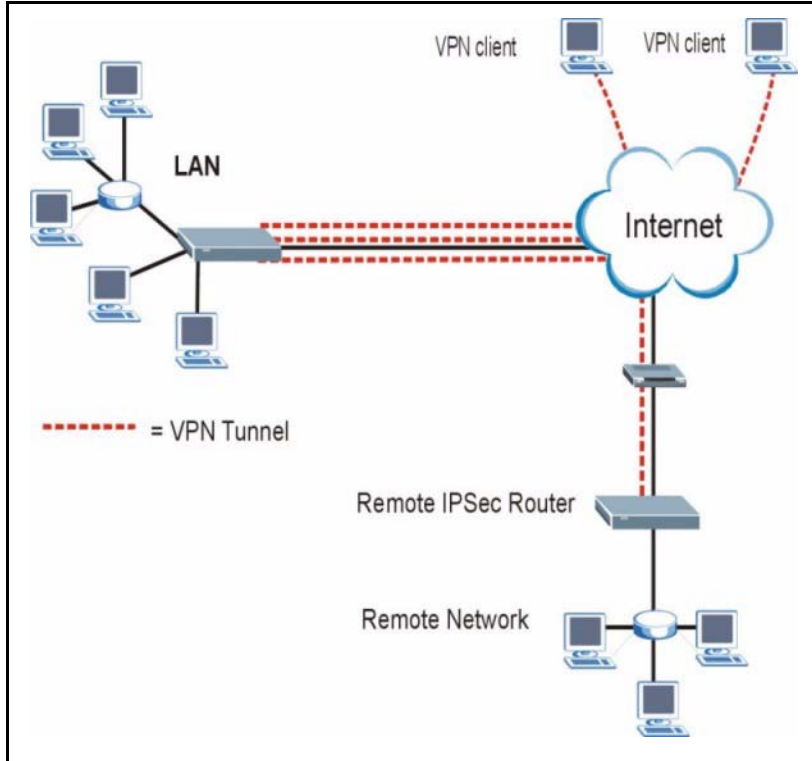
1.3.4 Wireless LAN Application (P-335WT only)

Add a wireless LAN to your existing network without expensive network cables. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network.

Figure 4 Internet Access Application Example
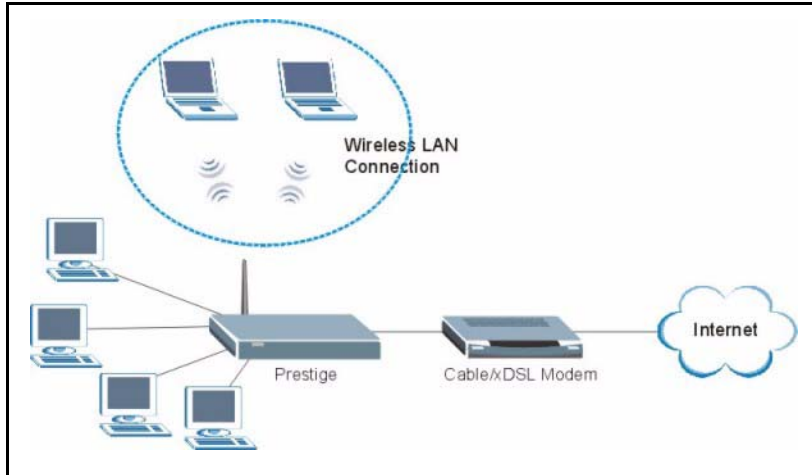
CHAPTER 2
Introducing the Web Configurator

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

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy Prestige setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.
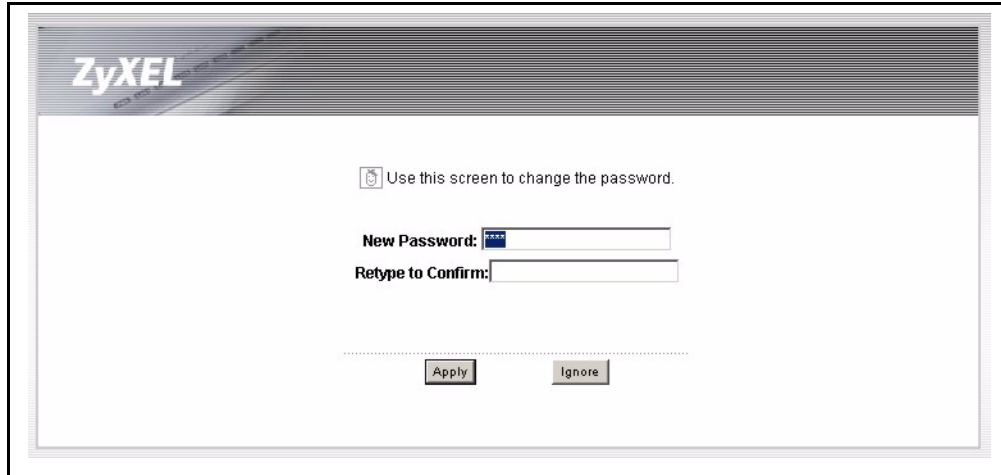
In order to use the web configurator you need to allow:

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

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

2.2 Accessing the Prestige Web Configurator

1 Make sure your Prestige hardware is properly connected and prepare your computer/computer network to connect to the Prestige (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "192.168.1.1" as the URL.

4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

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

Figure 5 Change Password Screen

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

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

2.3 Resetting the Prestige

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

2.3.1 Procedure To Use The Reset Button

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

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

2.3.2 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen.

- Click **WIZARD** for initial configuration including general setup, **Wireless LAN Setup**, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
- Click a link under **ADVANCED** to configure advanced Prestige features.
- Click **BW SETUP** for initial configuration of media bandwidth management.

- Click to view the web configurator in the language of your choice.
- Click **LOGOUT** at any time to exit the web configurator.
- Click **MAINTENANCE** to view information about your Prestige or upgrade configuration/firmware files. Maintenance includes **Status** (Statistics), **DHCP Table**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore, Defaults) and **Restart**.

Figure 6   The MAIN MENU Screen of the Web Configurator
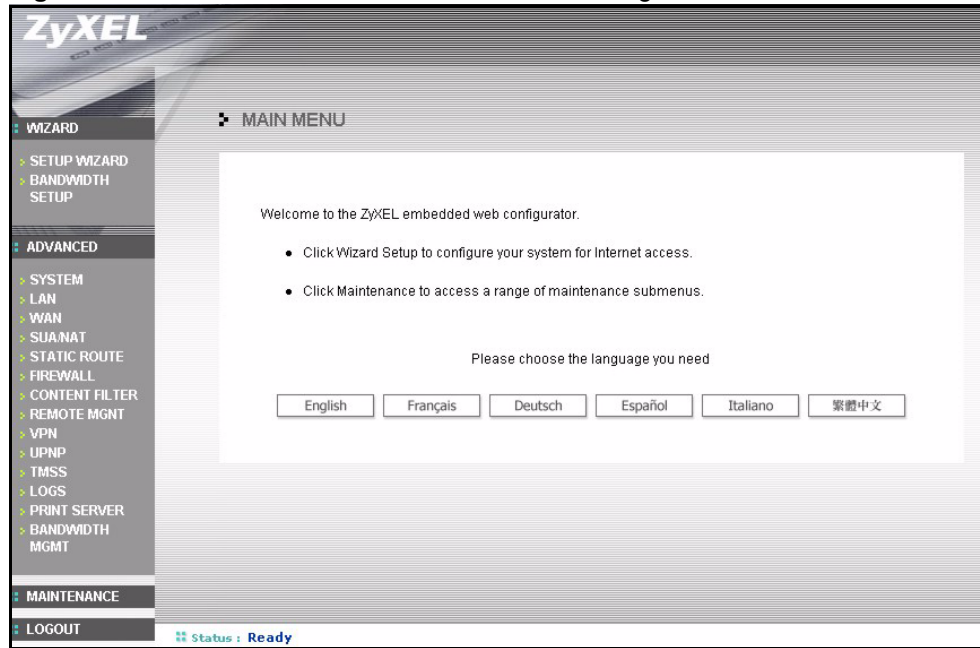
2.3.3 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure Prestige features.

The following table describes the sub-menus.

Table 3 Screens Summary

LINK	TAB	FUNCTION
WIZARD SETUP		Use these screens for initial configuration including general setup, Wireless LAN setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
BANDWIDTH SETUP		Use these screens for initial configuration of media bandwidth management.
SYSTEM	General	This screen contains administrative and system-related information.
	DDNS	Use this screen to set up dynamic DNS.
	Password	Use this screen to change your password.
	Time Zone	Use this screen to change your Prestige's time and date.
LAN	IP	Use this screen to configure LAN DHCP, TCP/IP settings and to enable Any IP.
	Static DHCP	Use this screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.
	IP Alias	Use this screen to partition your LAN interface into subnets.
WIRELESS (P-335WT only)	Wireless	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the Prestige to block access to devices or block the devices from accessing the Prestige.
	Roaming	This screen allows you to configure your Prestige roaming capabilities.
	OTIST	This screen allows you to assign wireless clients the Prestige's wireless security settings.
WAN	Route	This screen allows you to configure route priority.
	WAN ISP	Use this screen to change your Prestige's WAN ISP settings.
	WAN IP	Use this screen to change your Prestige's WAN IP settings.
	WAN MAC	Use this screen to change your Prestige's WAN MAC settings.
	Traffic Redirect	Use this screen to configure your traffic redirect properties and parameters.
SUA/NAT	SUA Server	Use this screen to configure servers behind the Prestige.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Trigger Port	Use this screen to change your Prestige's trigger port settings.
STATIC ROUTE	IP Static Route	Use this screen to configure IP static routes.
FIREWALL	Settings	Use this screen to activate/deactivate the firewall and log packets related to firewall rules.
	Services	Use this screen to enable service blocking (LAN to WAN firewall rules).
CONTENT FILTER	Filter	This screen allows you to block sites containing certain keywords in the URL and set the days and times for the Prestige to perform content filtering.

Table 3   Screens Summary

LINK	TAB	FUNCTION
REMOTE MGMT	TELNET	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the Prestige.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the Prestige.
	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the Prestige.
	SNMP	Use this screen to configure your Prestige's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the Prestige.
	Security	Use this screen to change your anti-probing settings.
VPN	Summary	Use this screen to view the rule summary.
	Rule Setup	Use this screen to configure VPN connections.
	SA Monitor	Use this screen to display and manage active VPN connections.
	Global Setting	Use this screen to allow NetBIOS packets through the VPN connections.
UPnP	UPnP	Use this screen to enable UPnP on the Prestige.
TMSS	Service Settings	Use this screen to decide which computers in the network you can apply TMSS.
	Antivirus Protection	This screen allows you to check the computers in the network for Trend Micro Internet Security.
	Parental Controls	This screen allows a parent (LAN administrator) to control a LAN user's Internet access privileges by blocking specified website categories.
LOGS	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your Prestige's log settings.
PRINT SERVER		Use this screen to view the printer and printer port name and to monitor the printer status.
BW MGMT	Configuration	Use this screen to configure your Prestige's settings for Media Bandwidth Management.
	Monitor	View the bandwidth usage of the LAN, WAN and WLAN configured bandwidth rules.

Table 3 Screens Summary

LINK	TAB	FUNCTION
MAINTENANCE	Status	This screen contains administrative and system-related information.
	DHCP Table	This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.
	Any IP	Use this screen to allow a computer to access the Internet without changing the network settings of the computer, when the IP addresses of the computer and the Prestige are not in the same subnet.
	F/W Upload	Use this screen to upload firmware to your Prestige.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your Prestige.
	Restart	This screen allows you to reboot the Prestige without turning the power off.
LOGOUT		Click this label to exit the web configurator.

Chapter 2 Introducing the Web Configurator

CHAPTER 3
Wizard Setup

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

3.1 Wizard Setup Overview

The web configurator's Wizard Setup helps you configure your device to access the Internet. The second screen has three variations depending on what encapsulation type you use. Refer to your ISP (Internet Service Provider) checklist in the Quick Start Guide to know what to enter in each field. Leave a field blank if you don't have that information.

3.2 Wizard Setup: General Setup and System Name

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

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

3.2.1 Domain Name

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

Click **Next** to configure the Prestige for Internet access.

Figure 7   Wizard Setup : General

3.3 Wizard Setup: Wireless LAN (P-335WT only)

Set up your wireless LAN using the following screen.

Figure 8   Wizard Setup : Wireless LAN

The following table describes the labels in this screen.

Table 4   Wizard Setup : Wireless LAN

LABEL	DESCRIPTION
Name(SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the Prestige, make sure all wireless stations use the same SSID in order to access the network.
Choose Channel ID	To manually set the Prestige to use a channel, select a channel from the drop-down list box.

Table 4 Wizard Setup : Wireless LAN

LABEL	DESCRIPTION
Security	The **Security** can be selected as auto, none, basic or extended.
	Choose **Auto** to use WPA-PSK security with a default **Pre-Shared Key** and proceed to another wireless LAN setup screen where you can enable OTIST. Choose this option only if your wireless clients support WPA-PSK.
	Choose **None** to have no wireless LAN security configured and proceed to another wireless LAN setup screen where you can enable OTIST.
	Choose **Basic(WEP)** security if you want to configure **WEP Encryption** parameters.
	Choose **Extend(WPA-PSK)** security to configure a **Pre-Shared Key**.
	The third screen varies depending on which security level you select.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

3.3.1 Wizard Setup : Wireless LAN : Basic Security

Choose **Basic(WEP)** to setup WEP Encryption parameters.

Figure 9   Wizard Setup : Wireless LAN : Basic Security

The following table describes the labels in this screen.

Table 5   Wizard Setup : Wireless LAN Setup : Basic Security

LABEL	DESCRIPTION
Passphrase	Enter a Passphrase (up to 32 printable characters) and clicking **Generate**. The Prestige automatically generates a WEP key.
WEP Encryption	Select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Prestige and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **256-bit WEP**, then enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

3.3.2 Wizard Setup : Wireless LAN : Extended Security

Choose **Extend(WPA-PSK)** security in the Wireless LAN Setup screen to set up a **Pre-Shared Key**.

Figure 10   Wizard Setup : Wireless LAN : Extended Security

The following table describes the labels in this screen.

Table 6   Wizard Setup : Wireless LAN : Extended Security

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the advanced wireless screen. You need to configure an authentication server to do this.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

3.4 Wizard Setup : Wireless LAN : OTIST (P-335WT only)

The following screen allows you to enable Prestige One-Touch Intelligent Security Technology (OTIST). One-Touch Intelligent Security Technology (OTIST) allows your Prestige to assign wireless clients the Prestige's SSID and static WEP or WPA-PSK encryption settings. The wireless client must also support OTIST and have OTIST enabled. See OTIST on page 124 for more information.

Figure 11   Wizard Setup : Wireless LAN : OTIST
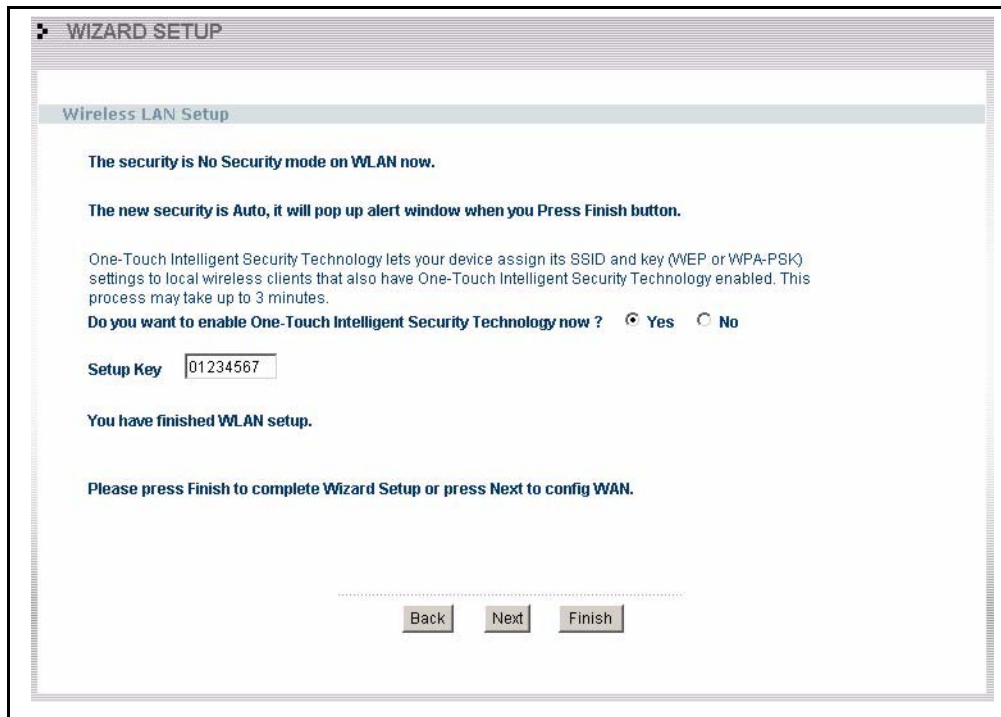
The following table describes the labels in this screen.

Table 7   Wizard Setup : Wireless LAN : OTIST

	DESCRIPTION
Do you want to enable One-Touch Intelligent Security Technology now?	Select the **Yes** radio button and click **Finish** to enable One-Touch Intelligent Security Technology (OTIST), complete the wizard setup and save your configuration.
	Select the **Yes** radio button and click **Next** to proceed with the setup wizard and enable OTIST only when you click **Finish** in the final wizard screen.
	Click **No** and then **Next** to proceed to the following screen.
	Click **No** and then **Finish** to complete the wizard setup and save your configuration.
Setup Key	The default OTIST **Setup Key** is "01234567". This key can be changed in the web configurator. Be sure to use the same OTIST **Setup Key** on the Prestige and wireless clients.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Finish	Click **Finish** to enable OTIST and complete the wizard setup.

Refer to the chapter on wireless LAN for more information.

3.5 Wizard Setup : Internet Access

The Prestige offers three choices of encapsulation. They are **Ethernet**, **PPP over Ethernet** or **PPTP**.

3.5.1 Ethernet

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Figure 12   Wizard Setup : Internet Access : Ethernet Encapsulation

The following table describes the labels in this screen.

Table 8   Wizard Setup : Internet Access : Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPP over Ethernet** or **PPTP** for a dial-up connection.
Service Type	Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**. The following fields are not applicable (**N/A**) for the **Standard** service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server	This field only applies when you select **Telia Login** in the **Service Type** field. Type the domain name of the Telia login server, for example "login1.telia.com".
Relogin Every (min)	This field only applies when you select **Telia Login** in the **Service Type** field. The Telia server logs the Prestige out if the Prestige does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the Prestige to wait between logins.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.5.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, 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 end users 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 specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

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

Refer to the appendix for more information on PPPoE.

Figure 13 Wizard Setup : Internet Access : PPPoE Encapsulation

The following table describes the labels in this screen.

Table 9 Wizard Setup : Internet Access : PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose **PPP over Ethernet** from the pull-down list box. PPPoE forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

3.5.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers 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.

Refer to the appendix for more information on PPTP.

> **Note:** The PRESTIGE supports one PPTP server connection at any given time.

Figure 14   Wizard Setup : Internet Access : PPTP Encapsulation

The following table describes the fields in this screen

Table 10   Wizard Setup : Internet Access : PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **PPTP** from the drop-down list box.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. The default is 100 seconds.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.

Table 10 Wizard Setup : Internet Access : PPTP Encapsulation

LABEL	DESCRIPTION
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP.
	This field is optional and depends on the requirements of your ISP.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.6 Wizard Setup : WAN

These wizard screens allow you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address.

3.6.1 WAN IP Address Assignment

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

Table 11 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.

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

3.6.2 IP Address and Subnet Mask

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

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

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

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Prestige, 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 Prestige 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 Prestige unless you are instructed to do otherwise.

3.6.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, 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 computer before you can access it.

The Prestige can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.

2 If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

3.6.4 WAN MAC Address

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

You can configure the WAN port's MAC address by either using 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 or upload a different "rom" file.

Table 12 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(Prestige LAN IP)

The following wizard screen allows you to assign a fixed IP address or give the Prestige an automatically assigned IP address depending on your ISP.

Figure 15 Wizard Setup : WAN
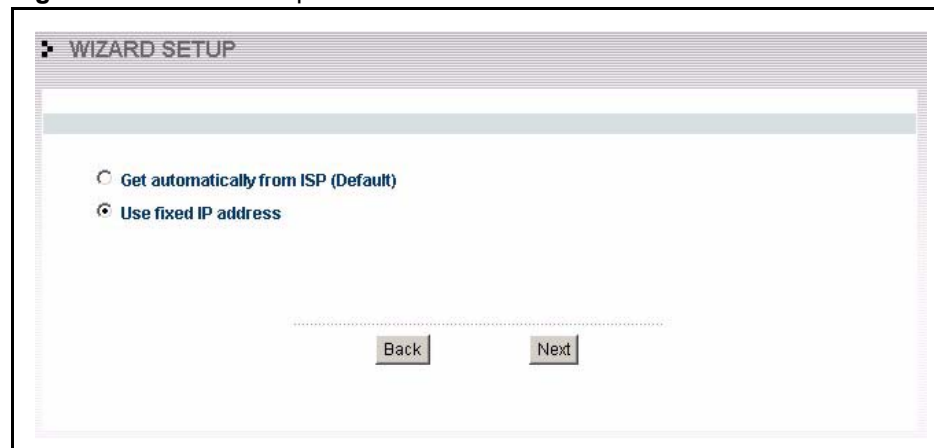
The following table describes the labels in this screen

Table 13 Wizard Setup : WAN

LABEL	DESCRIPTION
Get automatically from ISP(default)	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address. Select **Use fixed IP address** to give the Prestige a fixed, unique IP address. The fixed IP address should be in the same subnet as your broadband modem or router.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

Select **Use fixed IP address** in the previous wizard screen and click **Next** to view the following screen. Fill in the fields and click **Next** to continue.

Figure 16   Wizard Setup : WAN IP and DNS Server Address Assignment

The following table describes the labels in this screen

Table 14   Wizard Setup : WAN IP and DNS Server Address Assignment

LABEL	DESCRIPTION
WAN IP Address Assignment	
My WAN IP Address	Enter the IP address of your Prestige in dotted decimal notation.
	If you change the Prestige's IP address, you must use the new IP address if you want to access the web configurator again.
Remote IP Address	Enter a **Remote IP Address** appropriate to your network.
Remote IP Subnet Mask	Enter the **Remote IP Subnet Mask** of the neighboring device, if you know it. If you do not, leave the Remote IP Subnet Mask field as 0.0.0.0.
System DNS Server Address Assignment (if applicable)	
DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The Prestige uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.
	Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.

Table 14   Wizard Setup : WAN IP and DNS Server Address Assignment

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

Select **Get automatically from ISP (Default)** in the first WAN wizard setup screen and click **Next** to view the following WAN MAC Address screen. Click **Next** to go to the final wizard setup screen.

Figure 17   Wizard Setup : WAN MAC Address
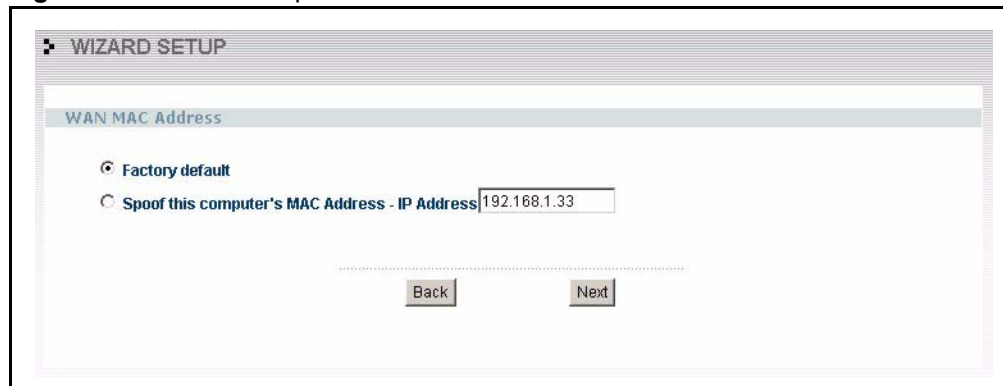
The following table describes the labels in this screen

Table 15   Wizard Setup : WAN MAC Address

LABEL	DESCRIPTION
WAN MAC Address	The MAC address field allows you to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. 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 or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.7 Wizard Setup : Complete

Follow the on-screen instructions and click **Finish** to complete the wizard setup and save your configuration.

Figure 18   Wizard Setup : Complete
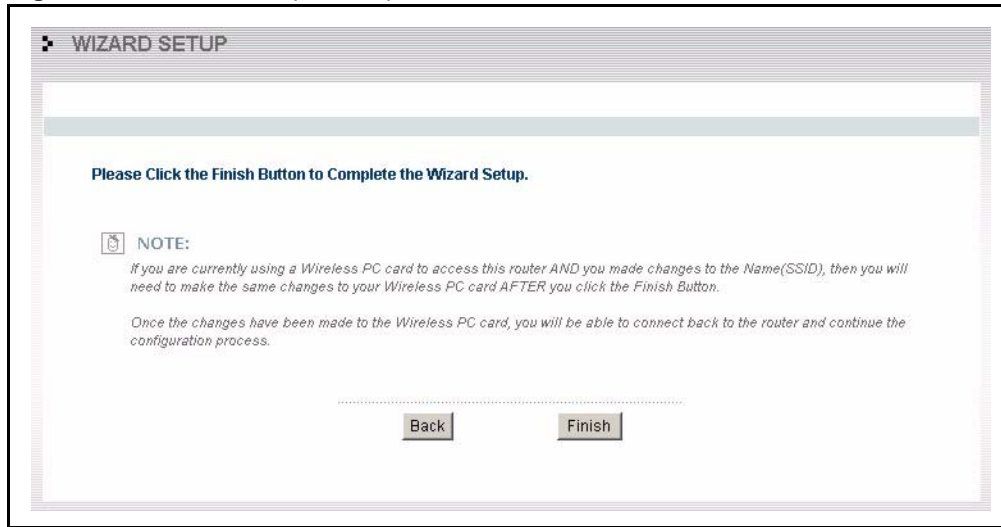
Well done! You have successfully set up your Prestige to operate on your network and access the Internet

CHAPTER 4
Media Bandwidth Management Setup

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

4.1 Media Bandwidth Management Setup Overview

The web configurator's **BW SETUP** allows you to specify bandwidth classes based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth classes.

The Prestige applies bandwidth management to traffic that it forwards out through the LAN, WAN and WLAN interfaces regardless of the traffic's source. For example, bandwidth management can be applied to the following situations:a LAN user surfing the Web or a LAN user downloading from a server behind the Prestige.

The Prestige does not control the bandwidth of traffic that comes into these interfaces.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the Prestige and be managed by bandwidth management.

4.2 Media Bandwidth Management Setup

Click **BM SETUP** in the main menu to display the first wizard screen.

Figure 19   Media Bandwidth Management Setup

The following fields describe the label in this screen.

Table 16   Media Bandwidth Management Setup

LABEL	DESCRIPTION
Active	Select the **Active** check box to have the Prestige apply bandwidth management to traffic going out through the Prestige's WAN, LAN or WLAN port.
Managed Bandwidth (Kbps)	Enter the amount of **Managed Bandwidth** in kbps (2 to 100,000) that you want to allocate for traffic. 20 kbps to 20,000 kbps is recommended. The recommendation is to set this speed to be equal to or less than the speed of the broadband device connected to the WAN port.
	For example, set the speed to 1000 Kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1000 Kbps.
Next	Click **Next** to continue.

4.3 Media Bandwidth Management Setup : Services

Use the second wizard screen to select the services that you want to apply bandwidth management.

Figure 20   Media Bandwidth Management Setup : Services
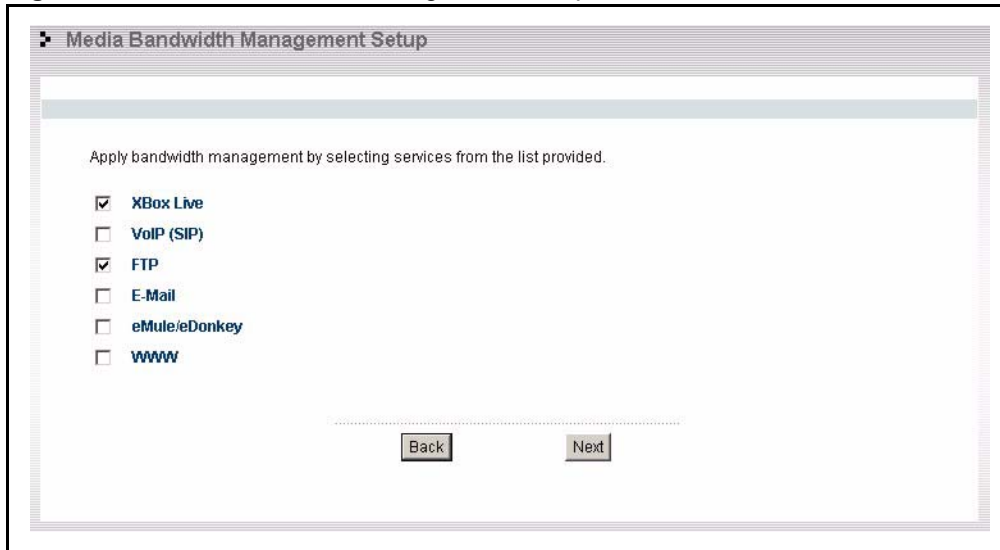
The following table describes the labels in this screen.

Table 17   Media Bandwidth Management Setup : Services

LABEL	DESCRIPTION
Choose Channel ID	Create bandwidth management classes by selecting services from the list provided. • XBox Live • VoIP (SIP) • FTP • E-Mail • eMule/eDonkey • WWW For a detailed description of these services, see the *Media Bandwidth Management chapter.*
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

4.4 Media Bandwidth Management Setup : Service Priority

Use the following wizard screen to select the priorities that you want to apply to the services listed.

Figure 21   Media Bandwidth Management Setup : Service Priority
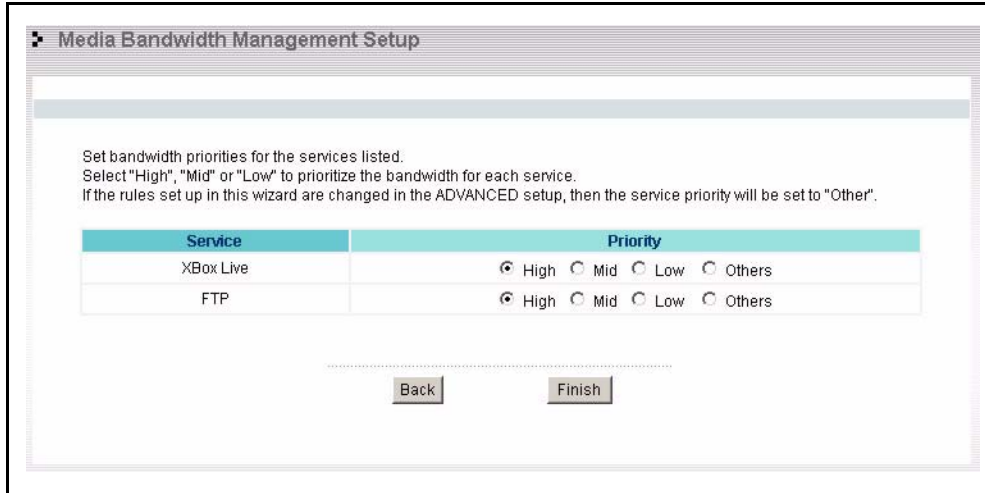
The following table describes the fields in this screen.

Table 18   Media Bandwidth Management Setup : Service Priority

LABELS	DESCRIPTION
Service	These fields display the services selected in the previous screen.
Priority	Select **High**, **Mid** or **Low** priority for each service to have your Prestige use a priority for traffic that matches that service.
	If the rules set up in this wizard are changed in **ADVANCED - BW MGMT - Configuration**, then the service priority radio button will be set to **Others**.
	The **ADVANCED - BW MGMT - Configuration - Edit** configuration screens allow you to edit these rule configurations.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to complete and save the bandwidth management setup.

4.5 Media Bandwidth Management Setup Complete

Well done! You have finished configuration of Media Bandwidth Management. You may now continue configuring your device.

Figure 22   Media Bandwidth Management Setup : Complete
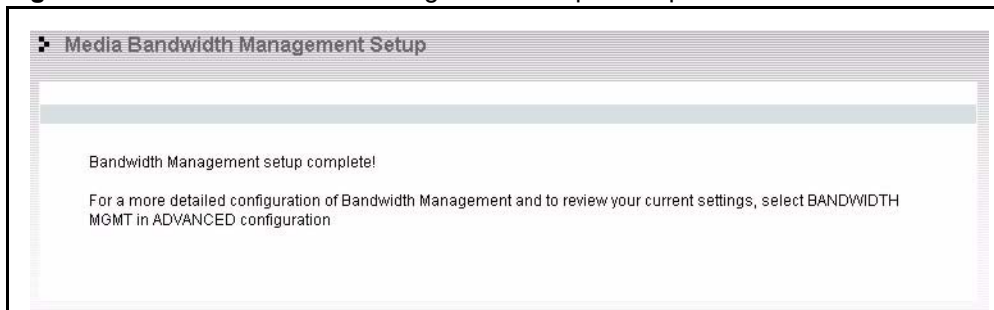
CHAPTER 5
System Screens

This chapter provides information on the System screens.

5.1 System Overview

See the Wizard Setup chapter for more information on the next few screens.

5.2 Configuring General Setup

Click **SYSTEM** to open the **General** screen.

Figure 23   System General Setup

The following table describes the labels in this screen.

Table 19   System General Setup

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the Prestige in an Ethernet network.. It is recommended you enter your computer's "Computer name" in this field (see the *Wizard Setup* chapter for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
System DNS Servers (if applicable)	
DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The Prestige uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	

Table 19 System General Setup

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The field below displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field below. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

5.3 Dynamic DNS

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

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

5.3.1 DynDNS Wildcard

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

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

5.4 Configuring Dynamic DNS

To change your Prestige's DDNS, click **SYSTEM**, then the **DDNS** tab. The screen appears as shown.

Figure 24 DDNS

The following table describes the labels in this screen.

Table 20 DDNS

LABEL	DESCRIPTION
Enable DDNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
DDNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.

Table 20 DDNS

LABEL	DESCRIPTION
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

5.5 Configuring Password

To change your Prestige's password (recommended), click **SYSTEM**, then the **Password** tab. The screen appears as shown. This screen allows you to change the Prestige's password.

Figure 25 Password

The following table describes the labels in this screen.

Table 21 Password

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

5.6 Configuring Time Setting

To change your Prestige's time and date, click **SYSTEM**, then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the Prestige's time based on your local time zone.

Figure 26 Time Setting

The following table describes the labels in this screen.

Table 22 Time Setting

LABEL	DESCRIPTION
Time Protocol	Select the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.
	The main difference between them is the format.
	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.
	The default, **NTP (RFC 1305),** is similar to Time (RFC 868).
	Select **None** to enter the time and date manually.
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays the time of your Prestige.
	Each time you reload this page, the Prestige synchronizes the time with the time server.
New Time	This field displays the last updated time from the time server.
	When you select **None** in the **Time Protocol** field, enter the new time in this field and then click **Apply**.

Table 22   Time Setting

LABEL	DESCRIPTION
Current Date	This field displays the date of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
New Date	This field displays the last updated date from the time server. When you select **None** in the **Time Protocol** field, enter the new date in this field and then click **Apply**.
Time Zone	Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 6
LAN Screens

This chapter describes how to configure LAN settings.

6.1 LAN Overview

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

6.2 DHCP Setup

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

6.2.1 IP Pool Setup

The Prestige is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the Prestige itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

6.2.2 System DNS Servers

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter.

6.3 LAN TCP/IP

The Prestige 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 Prestige are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- 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 explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

6.3.2 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter for this information.

6.3.3 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the Prestige 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.

RIP Version controls the format and the broadcasting method of the RIP packets that the Prestige 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** send 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 **RIP Version** to **RIP-1**.

6.3.4 Multicast

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

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address

224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

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

6.4 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the Prestige to be in the same subnet to allow the computer to access the Internet (through the Prestige). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the Prestige.

With the Any IP feature and NAT enabled, the Prestige allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the Prestige are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the Prestige and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a Prestige is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the Prestige are not in the same subnet.

Figure 27   Any IP Example Application
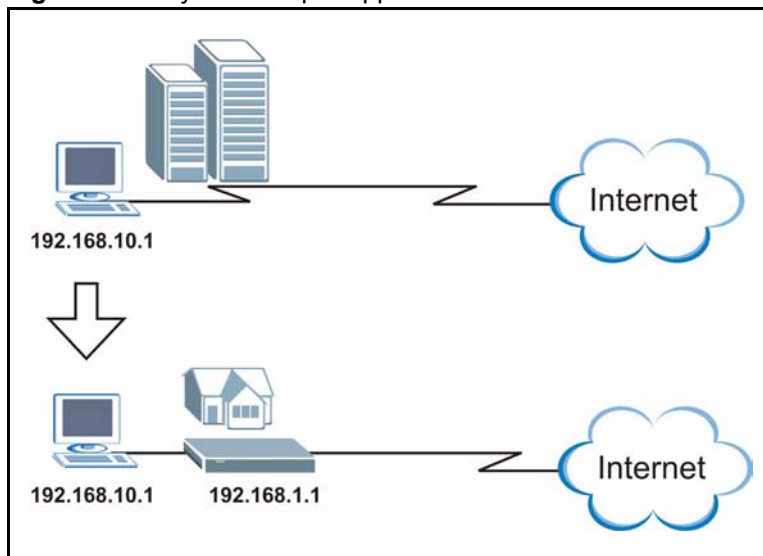
The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the Prestige's IP address.

> **Note:** You *must* enable NAT to use the Any IP feature on the Prestige

6.4.1 How Any IP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the Prestige) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the Prestige.

   1 When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the Prestige) by looking at the MAC address in its ARP table.

   2 When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.

   3 The Prestige receives the ARP request and replies to the computer with its own MAC address.

   4 The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the Prestige.

   5 When the Prestige receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the Prestige and the Internet as if it is in the same subnet as the Prestige.

6.5 Configuring IP

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

Figure 28 LAN IP

The following table describes the labels in this screen.

Table 23 LAN IP

LABEL	DESCRIPTION
DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the **DHCP Server** check box selected unless your ISP instructs you to do otherwise. Clear it to disable the Prestige acting as a DHCP server. When configured as a server, the Prestige provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.

Table 23 LAN IP

LABEL	DESCRIPTION
DNS Servers Assigned by DHCP Server	
The Prestige passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The Prestige only passes this information to the LAN DHCP clients when you select the **DHCP Server** check box. When you clear the **DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**.
	Select **DNS Relay** to have the Prestige act as a DNS proxy. The Prestige's LAN IP address displays in the field to the right (read-only). The Prestige tells the DHCP clients on the LAN that the Prestige itself is the DNS server. When a computer on the LAN sends a DNS query to the Prestige, the Prestige forwards the query to the Prestige's system DNS server (configured in the **SYSTEM General** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to **None** after you click **Apply**.
	Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
LAN TCP/IP	
IP Address	Type the IP address of your Prestige in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Prestige 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 Prestige 255.255.255.0.
RIP Direction	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. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the Prestige 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. **Both** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Prestige 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**.
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.

Table 23   LAN IP

LABEL	DESCRIPTION
Any IP Setup	
Active	Select this option to activate the Any-IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and sub-net mask) of the computer, even when the IP addresses of the computer and the Prestige are not in the same subnet.
	When you disable the Any-IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the Prestige's LAN IP address can connect to the Prestige or access the Internet through the Prestige.
Windows Networking (NetBIOS over TCP/IP): 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. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.
	Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

6.6 Configuring Static DHCP

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

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

To change your Prestige's Static DHCP settings, click **LAN**, then the **Static DHCP** tab. The screen appears as shown.

Figure 29 Static DHCP

The following table describes the labels in this screen.

Table 24 Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address in this field.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

6.7 Configuring IP Alias

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

To change your Prestige's IP Alias settings, click **LAN**, then the **IP Alias** tab. The screen appears as shown.

Figure 30 IP Alias

The following table describes the labels in this screen.

Table 25 IP Alias

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the Prestige.
IP Address	Enter the IP address of your Prestige in dotted decimal notation.
IP Subnet Mask	Your Prestige 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 Prestige.
RIP Direction	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. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the Prestige 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.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Prestige 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**.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

C H A P T E R 7
Wireless LAN (P-335WT)

This chapter discusses how to configure Wireless LAN.

7.1 Introduction

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

Note: See the WLAN appendix for more detailed information on WLANs.

7.2 Wireless Security Overview

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

Wireless security methods available on the Prestige are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Prestige identity.

7.2.1 Encryption

- Use WPA security if you have WPA-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA-PSK if you have WPA-aware wireless clients but no RADIUS server.
- If you don't have WPA-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off. You can use Passphrase to automatically generate 64-bit or 128-bit WEP keys or manually enter 64-bit, 128-bit or 256-bit WEP keys.

7.2.2 Authentication

WPA has user authentication and you can also configure IEEE 802.1x to use a RADIUS server to authenticate wireless clients before joining your network.

- Use RADIUS authentication if you have a RADIUS server. See the appendices for information on protocols used when a client authenticates with a RADIUS server via the Prestige.

7.2.3 Restricted Access

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

7.2.4 Hide Prestige Identity

If you hide the ESSID, then the Prestige cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the Prestige may be inconvenient for some valid WLAN clients. If you don't hide the ESSID, at least you should change the default one.

7.2.5 G-plus

G-plus is an enhancement to the IEEE 802.11g wireless standard. G-plus combines multiple frames into a larger frame size. This increases wireless transmission speeds by allowing larger frames (up to 4 KB) to be sent.

G-plus speed applies only to unicast traffic (not broadcast or multicast). G-plus is automatically disabled if wireless transmission speeds fall below 11 Mbps.

7.2.6 Using OTIST

To automatically configure the wireless security settings and set the wireless client to use the same SSID and WEP or WPA-PSK settings, use the OTIST setup wizard or the advanced wireless OTIST screen.

To manually configure the security setting, enter the WEP or WPA-PSK keys and SSID in the wireless screen. After that, you can enter the same settings in the wireless client or run OTIST to have the wireless client acquire the SSID and key automatically.

If you change the SSID or the keys after OTIST, you need to run OTIST again or enter them manually in the wireless client.

Note: You must activate and start OTIST on both the Prestige and the wireless client at the same time.

See the wireless client Quick Start Guide for information on wireless client OTIST setup. For more information on OTIST see Activating OTIST on page 125.

7.3 Configuring Wireless LAN on the Prestige

1 Configure the **SSID** and **WEP** in the **Wireless** screen. If you configure **WEP**, you can't configure **WPA** or **WPA-PSK**.

2 Use the **MAC Filter** screen to restrict access to your wireless network by MAC address.

3 Configure the RADIUS authentication database settings in the **Wireless** screen.

4 If you have OTIST-enabled clients, configure **OTIST** in the **OTIST** screen. **OTIST** transfers device SSID and WEP or WPA-PSK key settings (if enabled) to wireless clients.

The following figure shows the relative effectiveness of these wireless security methods available on your Prestige.

Figure 31 Prestige Wireless Security Levels
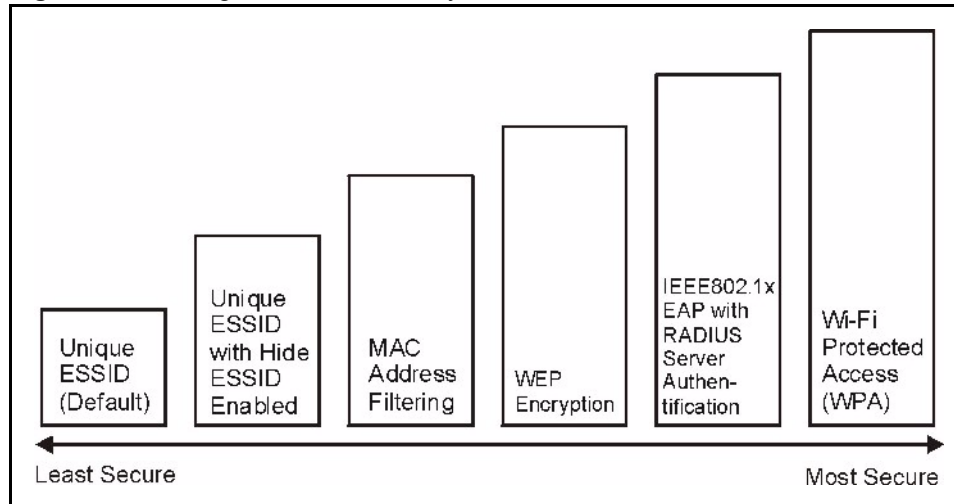
Note: You must enable the same wireless security settings on the Prestige and on all wireless clients that you want to associate with it.

7.4 Configuring the Wireless Screen

Note: If you are configuring the Prestige from a computer connected to the wireless LAN and you change the Prestige's SSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the Prestige's new settings.

Click the **WIRELESS** link under **ADVANCED** to open the **Wireless** screen.

Figure 32 Wireless

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

Table 26 Wireless

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. **Note:** If you are configuring the Prestige from a computer connected to the wireless LAN and you change the Prestige's SSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the Prestige's new settings.

Chapter 7 Wireless LAN (P-335WT)

Table 26   Wireless

LABEL	DESCRIPTION
Hide Name(SSID)	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through passive scanning using a site survey tool.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. Refer to the Wizard Setup chapter for more information on channels.
RTS/CTS Threshold	Enter a value between 0 and 2432. If you select the **G+ Enhanced** checkbox a value of **4096** is displayed.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. If you select the **G+ Enhanced** checkbox a value of **4096** is displayed.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

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

7.4.1 No Security

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

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

Figure 33   Wireless: No Security

The following table describes the labels in this screen.

Table 27   Wireless No Security

LABEL	DESCRIPTION
Security	Choose **No Security** from the drop-down list box.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long, Short** and **Dynamic**. The default setting is **Long**. See the section on preamble for more information.

Table 27   Wireless No Security

LABEL	DESCRIPTION
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Prestige.
	Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Prestige.
	Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the Prestige. The transmission rate of your Prestige might be reduced.
G+ Enhanced	Select **G+ Enhanced** checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the Prestige. This permits the Prestige to transmit at a higher speed than the **802.11g Only** mode.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.4.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your Prestige allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys but only one key can be enabled at any one time.

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

7.4.3 Configuring WEP Encryption

In order to configure and enable WEP encryption; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **Static WEP** from the **Security** list.

Figure 34 Wireless: Static WEP Encryption

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

Table 28 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Passphrase	Enter a Passphrase (up to 32 printable characters) and clicking **Generate**. The Prestige automatically generates a WEP key.
WEP Encryption	Select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** to enable data encryption.

Table 28   Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Authentication Method	This field is activated when you select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** in the **WEP Encryption** field. Select **Auto**, **Open System** or **Shared Key** from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Prestige and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **256-bit WEP**, then enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** and **Dynamic**. The default setting is **Dynamic**. See the section on preamble for more information.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Prestige. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Prestige. Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the Prestige. The transmission rate of your Prestige might be reduced.
G+ Enhanced	Select **G+ Enhanced** checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the Prestige. This permits the Prestige to transmit at a higher speed than the **802.11g Only** mode.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.4.4 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA is preferred to WEP as WPA has user authentication and improved data encryption. See the appendix for more information on WPA user authentication and WPA encryption.

If you don't have an external RADIUS server, you should use WPA-PSK (WPA -Pre-Shared Key). WPA-PSK only requires a single (identical) password entered into each WLAN member. As long as the passwords match, a client will be granted access to a WLAN.

Note: You can't use the Local User Database for authentication when you select WPA.

7.4.5 WPA-PSK Application Example

A WPA-PSK application looks as follows.

1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must be between 8 and 63 printable characters (including spaces; alphabetic characters are case-sensitive).

2 The AP checks each client's password and (only) allows it to join the network if the passwords match.

3 The AP derives and distributes keys to the wireless clients.

The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

Figure 35 WPA - PSK Authentication
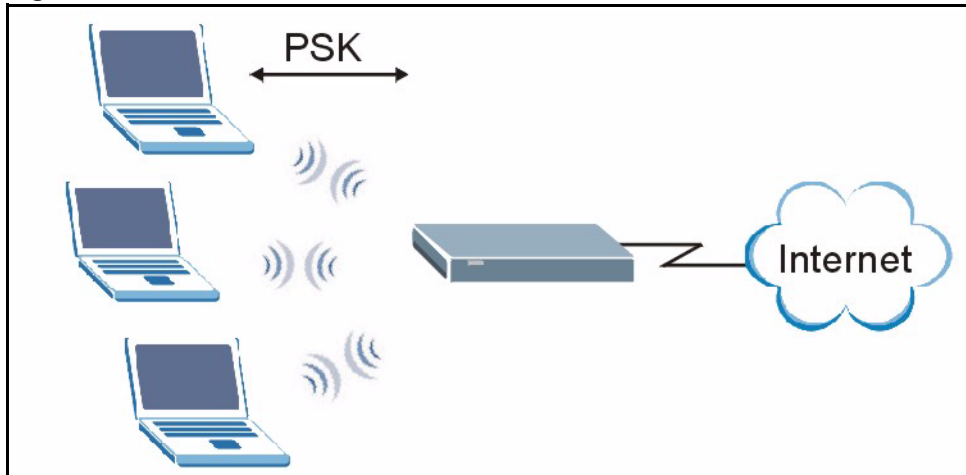
7.4.6 Configuring WPA-PSK Authentication

In order to configure and enable WPA-PSK Authentication; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **WPA-PSK** from the **Security** list.

Figure 36   Wireless: WPA-PSK

The following table describes the labels in this screen.

Table 29   Wireless: WPA-PSK

LABEL	DESCRIPTION
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials.
	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).
	Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

Table 29 Wireless: WPA-PSK

LABEL	DESCRIPTION
Idle Timeout	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
WPA Group Key Update Timer	The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or **RADIUS** server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in **WPA-PSK** mode. The Prestige default is **1800** seconds (30 minutes).
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** or **Dynamic**. The default setting is **Long**. See the section on preamble for more information.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Prestige.
	Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Prestige.
	Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the Prestige. The transmission rate of your Prestige might be reduced.
G+ Enhanced	Select **G+ Enhanced** checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the Prestige. This permits the Prestige to transmit at a higher speed than the **802.11g Only** mode.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.4.7 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Funk Software's Odyssey client is bundled free (at the time of writing) with the Prestige client adaptor(s). This adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client.

7.4.8 WPA with RADIUS Application Example

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

1 The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 37   WPA with RADIUS Application Example
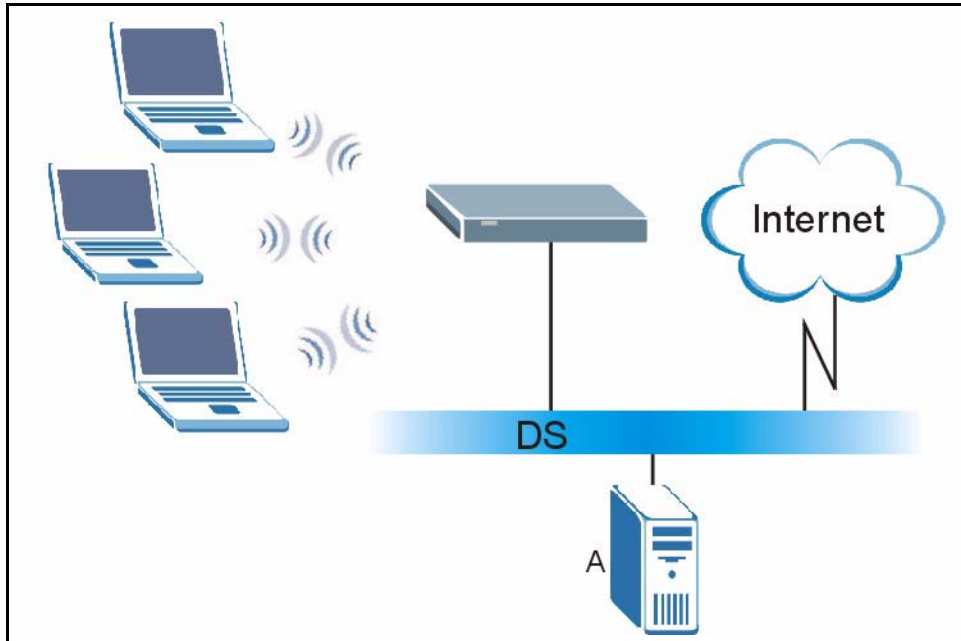
7.4.9 Configuring WPA Authentication

In order to configure and enable WPA Authentication; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **WPA** from the **Security** list.

Figure 38   Wireless: WPA

The following table describes the labels in this screen.

Table 30   Wireless: WPA

LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). **Note:** If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
WPA Group Key Update Timer	The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or **RADIUS** server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in **WPA-PSK** mode. The Prestige default is **1800** seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Prestige. The key must be the same on the external authentication server and your Prestige. The key is not sent over the network.
Accounting Server	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the Prestige. The key must be the same on the external accounting server and your Prestige. The key is not sent over the network.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** or **Dynamic**. The default setting is **Long**. See the section on preamble for more information.

Table 30 Wireless: WPA

LABEL	DESCRIPTION
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Prestige.
	Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Prestige.
	Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the Prestige. The transmission rate of your Prestige might be reduced.
G+ Enhanced	Select **G+ Enhanced** checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the Prestige. This permits the Prestige to transmit at a higher speed than the **802.11g Only** mode.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.4.10 802.1x Overview

You need the following for IEEE 802.1x authentication.

- A computer with an IEEE 802.11 a/b/g wireless LAN adapter and equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station computer must be running IEEE 802.1x-compliant software. Not all Windows operating systems support IEEE 802.1x (see the Microsoft web site for details). For other operating systems, see their documentation. If your operating system does not support IEEE 802.1x, then you may need to install IEEE 802.1x client software.
- An optional network RADIUS server for remote user authentication and accounting.

7.4.11 Configuring 802.1x and Dynamic WEP Key Exchange

In order to configure and enable 802.1x and Dynamic WEP Key Exchange; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **802.1x + Dynamic WEP** from the **Security** list.

Figure 39   Wireless: 802.1x and Dynamic WEP

The following table describes the labels in this screen.

Table 31   Wireless: 802.1x and Dynamic WEP

LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). **Note:** If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Dynamic WEP Key Exchange	Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the Prestige when you configure dynamic WEP key exchange. This field is not available when you set **Security** to **WPA** or **WPA-PSK**.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Prestige. The key must be the same on the external authentication server and your Prestige. The key is not sent over the network.
Accounting Server	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the Prestige. The key must be the same on the external accounting server and your Prestige. The key is not sent over the network.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** or **Dynamic**. The default setting is **Long**. See the section on preamble for more information.

Table 31   Wireless: 802.1x and Dynamic WEP

LABEL	DESCRIPTION
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Prestige.
	Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Prestige.
	Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the Prestige. The transmission rate of your Prestige might be reduced.
G+ Enhanced	Select **G+ Enhanced** checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the Prestige. This permits the Prestige to transmit at a higher speed than the **802.11g Only** mode.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.4.12 Configuring 802.1x and Static WEP Key Exchange

In order to configure and enable 802.1x and Static WEP Key Exchange; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **802.1x + Static WEP** from the **Security** list.

Figure 40 Wireless: 802.1x and Static WEP

The following table describes the labels in this screen.

Table 32   Wireless: 802.1x and Static WEP

LABEL	DESCRIPTION
Passphrase	Enter a Passphrase (up to 32 printable characters) and clicking **Generate**. The Prestige automatically generates a WEP key.
WEP Encryption	Select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** to enable data encryption.
Authentication Method	This field is activated when you select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** in the WEP Encryption field. Select Auto, Open System or Shared Key from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
Hex	Select this option in order to enter hexadecimal characters as the WEP keys. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Prestige and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **256-bit WEP**, then enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). **Note:** If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Prestige. The key must be the same on the external authentication server and your Prestige. The key is not sent over the network.
Accounting Server	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.

Table 32   Wireless: 802.1x and Static WEP

LABEL	DESCRIPTION
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**.
	You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the Prestige.
	The key must be the same on the external accounting server and your Prestige. The key is not sent over the network.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** or **Dynamic**. The default setting is **Long**. See the section on preamble for more information.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Prestige.
	Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Prestige.
	Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the Prestige. The transmission rate of your Prestige might be reduced.
G+ Enhanced	Select **G+ Enhanced** checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the Prestige. This permits the Prestige to transmit at a higher speed than the **802.11g Only** mode.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.4.13 Configuring 802.1x

In order to configure and enable 802.1x; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **802.1x + No WEP** from the **Security** list.

Figure 41   Wireless: 802.1x

The following table describes the labels in this screen.

Table 33 Wireless: 802.1x and No WEP

LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). **Note:** If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Prestige. The key must be the same on the external authentication server and your Prestige. The key is not sent over the network.
Accounting Server	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the Prestige. The key must be the same on the external accounting server and your Prestige. The key is not sent over the network.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** or **Dynamic**. The default setting is **Long**. See the section on preamble for more information.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Prestige. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Prestige. Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the Prestige. The transmission rate of your Prestige might be reduced.

Table 33   Wireless: 802.1x and No WEP

LABEL	DESCRIPTION
G+ Enhanced	Select **G+ Enhanced** checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the Prestige. This permits the Prestige to transmit at a higher speed than the **802.11g Only** mode.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5 MAC Filter

The MAC filter screen allows you to configure the Prestige to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the Prestige (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your Prestige's MAC filter settings, click the **WIRELESS** link under **ADVANCED** and then the **MAC Filter** tab. The screen appears as shown.

Figure 42 MAC Address Filter

The following table describes the labels in this menu.

Table 34 MAC Address Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table.
	Select **Deny Association** to block access to the Prestige, MAC addresses not listed will be allowed to access the Prestige
	Select **Allow Association** to permit access to the Prestige, MAC addresses not listed will be denied access to the Prestige.
Set	This is the index number of the MAC address.

Table 34 MAC Address Filter

LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the Prestige in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.6 Roaming

See the appendix for background information on roaming.

To enable roaming on your Prestige, click the **WIRELESS** link under **ADVANCED** and then the **Roaming** tab. The screen appears as shown.

Figure 43 Roaming

The following table describes the labels in this screen.

Table 35 Roaming

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

7.7 OTIST

OTIST (One-Touch Intelligent Security Technology) allows your Prestige to set the wireless client to use the same wireless settings as the Prestige.

Note: The wireless client must support OTIST and have OTIST enabled.

The following are the wireless settings that the Prestige assigns to the wireless client if OTIST is enabled on both devices and the OTIST setup keys are the same.

 • SSID
 • Security (WEP or WPA-PSK)

Note: This will replace the pre-configured wireless settings on the wireless clients.

Click the **WIRELESS** link under **ADVANCED** and then the **OTIST** tab to display the next screen.

Figure 44 OTIST
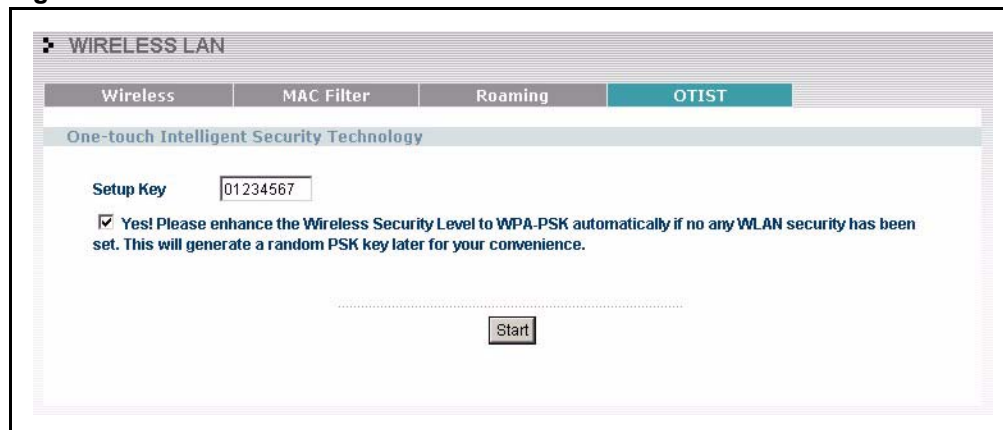
The following table describes the labels in this screen.

Table 36 OTIST

LABEL	DESCRIPTION
Setup Key	Type an OTIST **Setup Key** of exactly eight ASCII characters in length. The default OTIST setup key is "01234567". **Note:** If you change the OTIST setup key here, you must also make the same change on the wireless client(s).
Yes!	If the Prestige has no wireless security configured, select this checkbox to enable WPA-PSK security and automatically generate a WPA-PSK key on the Prestige. The WPA-PSK security settings can then be assigned to the wireless client when you start OTIST.
Start	Click **Start** to encrypt the wireless security data using the setup key and have the Prestige set the wireless station to use the same wireless settings as the Prestige. You must also activate and start OTIST on the wireless station at the same time. The process takes three minutes to complete.

7.7.1 Activating OTIST

After you click **Start**, a dialog box displays the security mode and the WEP key or pre-shared key depending on which mode is configured. Click **OK** to proceed with the OTIST setup.

Figure 45 OTIST Start
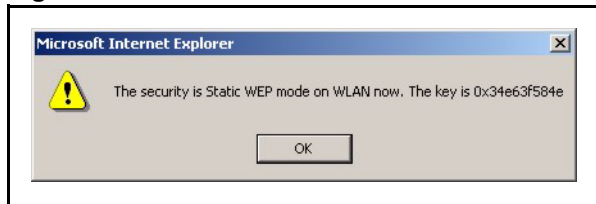
Note: The process takes three minutes. During this time the Prestige assigns its security settings to OTIST-enabled wireless clients within range that have selected to associate with this Prestige.

Figure 46 OTIST Process

When the previous screen closes, your current Prestige security configuration is automatically saved to the wireless clients.

Note: See your wireless client documentation for information on enabling OTIST on it. If there are multiple OTIST-enabled Prestiges within range and with the same OTIST setup key, then the wireless client must choose which Prestige should assign its settings to it.

7.7.2 OTIST button

Use the OTIST button to set up OTIST using the current OTIST **Setup Key** and the Prestige's current wireless security settings.

1 Log out of your current configuration management session.

2 Push the OTIST button once on the back panel of the Prestige device to enable OTIST.

CHAPTER 8
WAN Screens

This chapter describes how to configure WAN settings.

8.1 WAN Overview

See the *Wizard Setup* chapter for more information on the fields in the WAN screens.

8.2 TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the Prestige's routes to the Internet. If the routes have the same metric, the Prestige uses the following pre-defined priorities:

1 **WAN**: designated by the ISP or a static route (see the IP Static Route Setup chapter)

2 **Traffic Redirect** (see*see the Configuring Traffic Redirect section*)

For example, if **WAN** has a metric of "1" and **Traffic Redirect** has a metric of "2", the **WAN** connection acts as the primary default route. If the **WAN** route fails to connect to the Internet, the Prestige tries **Traffic Redirect** next.

8.3 Configuring Route

Click **WAN** to open the **Route** screen.

Figure 47 WAN: Route

The following table describes the labels in this screen.

Table 37 WAN: Route

LABEL	DESCRIPTION
WAN Traffic Redirect	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost". The metric sets the priority for the Prestige's routes to the Internet. If the routes have the same metric, the Prestige uses the following pre-defined priorities: 1. **WAN**: designated by the ISP or a static route 2. **Traffic Redirect**. For example, if **WAN** has a metric of "1" and **Traffic Redirect** has a metric of "2", the **WAN** connection acts as the primary default route. If the **WAN** route fails to connect to the Internet, the Prestige tries **Traffic Redirect** next.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4 Configuring WAN ISP

To change your Prestige's WAN ISP settings, click **WAN**, then the **WAN ISP** tab. The screen differs by the encapsulation.

8.4.1 Ethernet Encapsulation

The screen shown next is for **Ethernet** encapsulation.

Figure 48 Ethernet Encapsulation

The following table describes the labels in this screen.

Table 38 Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**. The following fields do not appear with the **Standard** service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type the password again to make sure that you have entered it correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server	This field only applies when you select **Telia Login** in the **Service Type** field. Type the domain name of the Telia login server, for example "login1.telia.com".
Relogin Every(min)	This field only applies when you select **Telia Login** in the **Service Ty**pe field. The Telia server logs the Prestige out if the Prestige does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the Prestige to wait between logins.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.2 PPPoE Encapsulation

The Prestige 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 **PPP over Ethernet** 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 Prestige (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Prestige does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

Figure 49   PPPoE Encapsulation

The following table describes the labels in this screen.

Table 39   PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The **PPP over Ethernet** choice is for a dial-up connection using PPPoE. The Prestige 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 (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the User Name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.3 PPTP Encapsulation

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

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

The screen shown next is for **PPTP** encapsulation.

Figure 50   PPTP Encapsulation

The following table describes the labels in this screen.

Table 40   PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
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 Prestige supports only one PPTP server connection at any given time.
	To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the Prestige automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.

Table 40   PPTP Encapsulation

LABEL	DESCRIPTION
My IP Subnet Mask	Your Prestige 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 Prestige.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

8.5 Configuring WAN IP

To change your Prestige's WAN IP settings, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP (Default**);otherwise click **Use fixed IP Address** and enter the IP address in the field provided.

Figure 51   WAN: IP

The following table describes the labels in this screen.

Table 41   WAN: IP

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
My WAN IP Subnet Mask (Ethernet only)	Type your network's IP subnet Mask.
Remote IP Address	Enter the Remote IP Address (if your ISP gave you one) in this field.
Gateway/Remote IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.

Table 41 WAN: IP

LABEL	DESCRIPTION
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
	Choose **None** to disable NAT**.**
	Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.
	Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set!
	For more information about NAT refer to the *NAT* chapter in this *User's Guide*.
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create.
Metric (PPPoE and PPTP only)	This field sets this route's priority among the routes the Prestige uses.
	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Private (PPPoE and PPTP only)	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.
	Choose **Both**, **None**, **In Only** or **Out Only**.
	When set to **Both** or **Out Only**, the Prestige will broadcast its routing table periodically.
	When set to **Both** or **In Only**, the Prestige will incorporate RIP information that it receives.
	When set to **None**, the Prestige will not send any RIP packets and will ignore any RIP packets received.
	By default, **RIP Direction** is set to **Both**.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving).
	Choose **RIP-1**, **RIP-2B** or **RIP-2M**.
	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, the **RIP Version** field is set to **RIP-1**.

Table 41   WAN: IP

LABEL	DESCRIPTION
Multicast	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): 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. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between WAN and LAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

8.6 Configuring WAN MAC

To change your Prestige's WAN MAC settings, click **WAN**, then the **WAN MAC** tab. The screen appears as shown.

Figure 52   MAC Setup

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Spoof this computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. 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 or upload a different ROM file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

8.7 Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the Prestige cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the Prestige still provides firewall protection.

Figure 53   Traffic Redirect WAN Setup
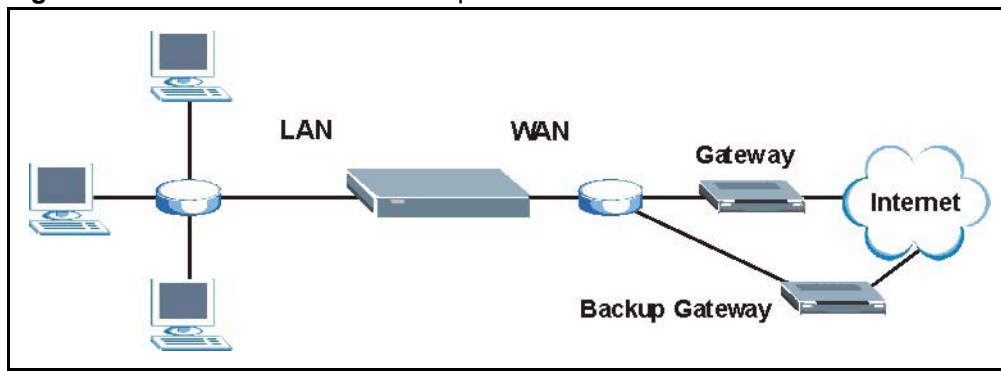
The following network topology allows you to avoid triangle route security issues (see the Appendices) when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the Prestige itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/Prestige firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

Figure 54   Traffic Redirect LAN Setup
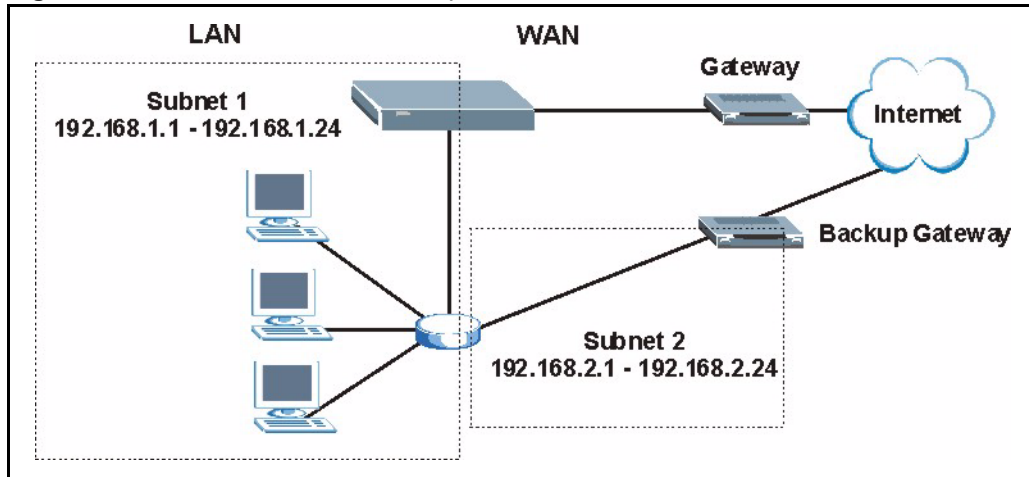
8.8 Configuring Traffic Redirect

To change your Prestige's Traffic Redirect settings, click **WAN**, then the **Traffic Redirect** tab. The screen appears as shown.

Figure 55 WAN: Traffic Redirect

The following table describes the labels in this screen.

Table 42 Traffic Redirect

LABEL	DESCRIPTION
Active	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Metric	This field sets this route's priority among the routes the Prestige uses.
	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the Prestige will use the default gateway IP address. Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you are using PPTP or PPPoE Encapsulation, type "**0.0.0.0**" to configure the Prestige to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Type the number of times your Prestige may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
Period (seconds)	Type the number of seconds for the Prestige to wait between checks to see if it can connect to the WAN IP address (**Check WAN IP Address** field) or default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout (seconds)	Type the number of seconds for your Prestige to wait for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The WAN connection is considered "down" after the Prestige times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.

Table 42   Traffic Redirect

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

CHAPTER 9
Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Prestige.

9.1 NAT Overview

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

9.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Prestige. 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 43   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.

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

9.1.2 What NAT Does

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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your Prestige 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)*.

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

Figure 56   How NAT Works
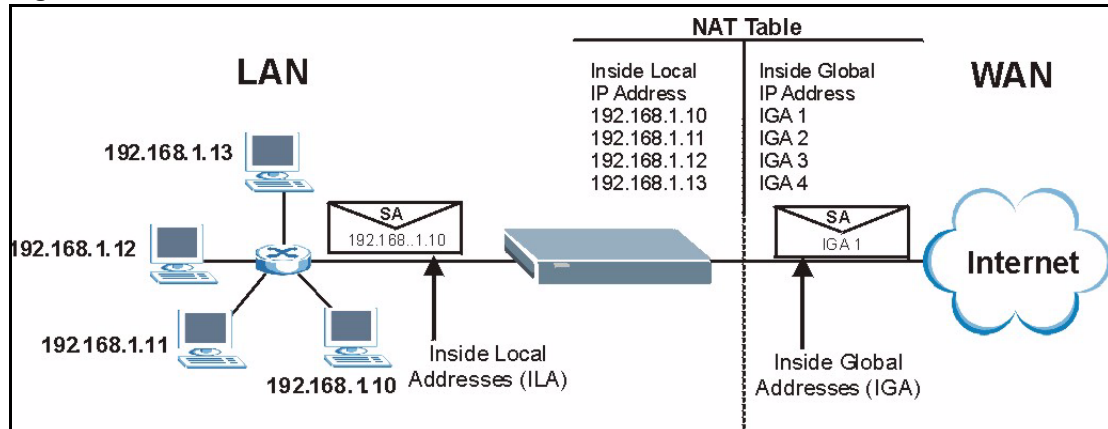
9.1.4 NAT Application

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

Figure 57   NAT Application With IP Alias
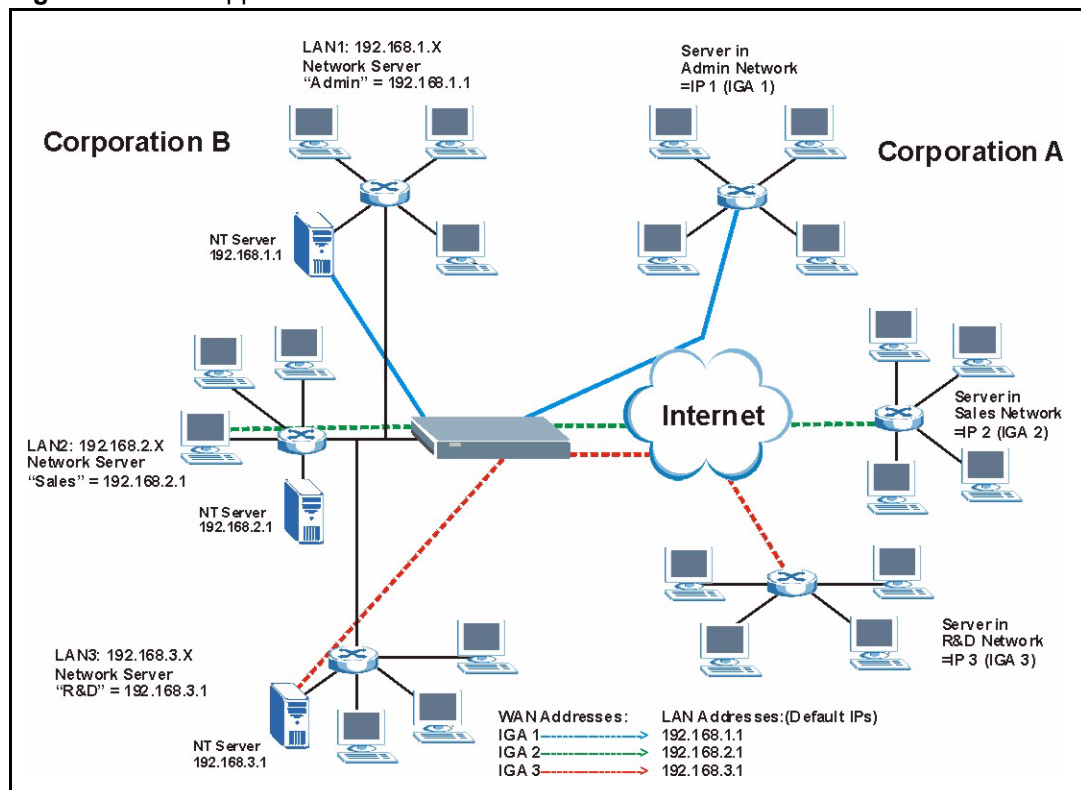
9.1.5 NAT Mapping Types

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

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

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

The following table summarizes these types.

Table 44   NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1-1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M-1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M-M Ov
Many 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

9.2 Using NAT

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

9.2.1 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**. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in the **WAN IP** screen.

9.3 SUA Server

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

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

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

9.3.1 Default Server IP Address

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

> **Note:** If you do not assign a Default Server IP Address, the Prestige discards all packets received for ports that are not specified in this screen or remote management.

9.3.2 Port Forwarding: Services and Port Numbers

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.

Use the **SUA Server** page 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.

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.

> **Note:** 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 Supporting CD for more examples and details on SUA/NAT.

Table 45 Services and Port Numbers

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

9.3.3 Configuring Servers Behind SUA (Example)

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

Figure 58   Multiple Servers Behind NAT Example
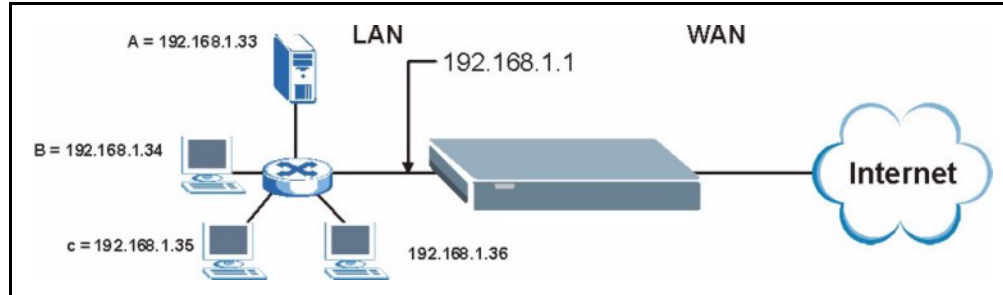
9.4 Configuring SUA Server

> **Note:** If you do not assign a Default Server IP Address, the Prestige discards all packets received for ports that are not specified in this screen or remote management.

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to Table 45 for port numbers commonly used for particular services.

Figure 59 SUA/NAT Setup

The following table describes the labels in this screen.

Table 46 SUA/NAT Setup

LABEL	DESCRIPTION
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen.
	If you do not assign a **Default Server** IP Address, the Prestige discards all packets received for ports that are not specified in this screen or remote management.
#	Number of an individual SUA server entry.
Active	Select this check box to enable the SUA server entry. Clear this checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number here. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.
End Port	
Server IP Address	Enter the inside IP address of the server here.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

9.5 Configuring Address Mapping

Ordering your rules is important because the Prestige applies the rules in the order that you specify. When a rule matches the current packet, the Prestige takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your Prestige's Address Mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown.

Figure 60 Address Mapping

The following table describes the labels in this screen.

Table 47 Address Mapping

LABEL	DESCRIPTION
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.
Global End IP	This is the end Inside Global Address (IGA).
	This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.

Table 47   Address Mapping

LABEL	DESCRIPTION
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.
	2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.
	3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses.
	4. **Many One-to-One** mode maps each local IP address to unique global IP addresses.
	5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Insert	Click **Insert** to insert a new mapping rule before an existing one.
Edit	Click **Edit** to go to the **Address Mapping Rule** screen.
Delete	Click **Delete** to delete an address mapping rule.

9.5.1 Configuring Address Mapping

To edit an address mapping rule, select the radio button of a rule and click the **Edit** button to display the screen shown next.

Figure 61   Address Mapping Rule

The following table describes the labels in this screen.

Table 48   Address Mapping Rule

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following.
	1. **One-to-One**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.
	2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature.
	3. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.
	4. **Many One-to-One**: Many One-to-one mode maps each local IP address to unique global IP addresses.
	5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address.
	This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

9.6 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 Prestige 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 Prestige's WAN port receives a response with a specific port number and protocol ("incoming" port), the Prestige 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.

9.6.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 62   Trigger Port Forwarding Process: Example
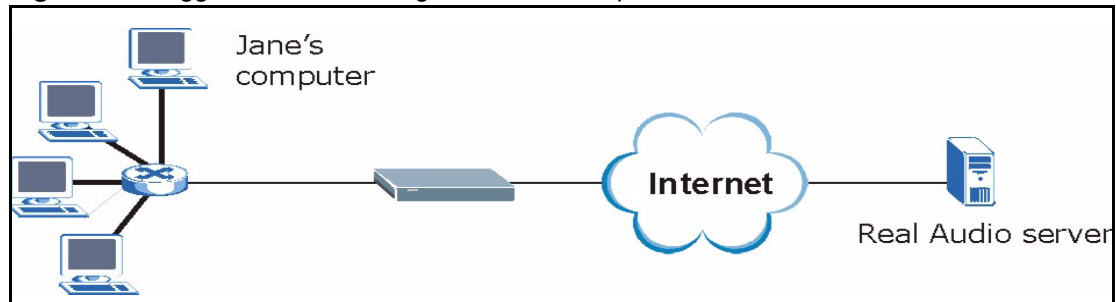
1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a "trigger" port and causes the Prestige to record Jane's computer IP address. The Prestige 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 Prestige 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 Prestige times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

9.6.2 Two Points To Remember About Trigger Ports

1 Trigger events only happen on data that is going coming from inside the Prestige 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.

9.7 Configuring Trigger Port Forwarding

To change your Prestige's trigger port settings, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown.

> **Note:** Only one LAN computer can use a trigger port (range) at a time

Figure 63 Trigger Port

The following table describes the labels in this screen.

Table 49 Trigger Port

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
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 Prestige forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the Prestige to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 10
Static Route Screens

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

10.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following figure through remote node router R1. However, the Prestige 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 R1 (via gateway router R2). The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

Figure 64   Example of Static Routing Topology
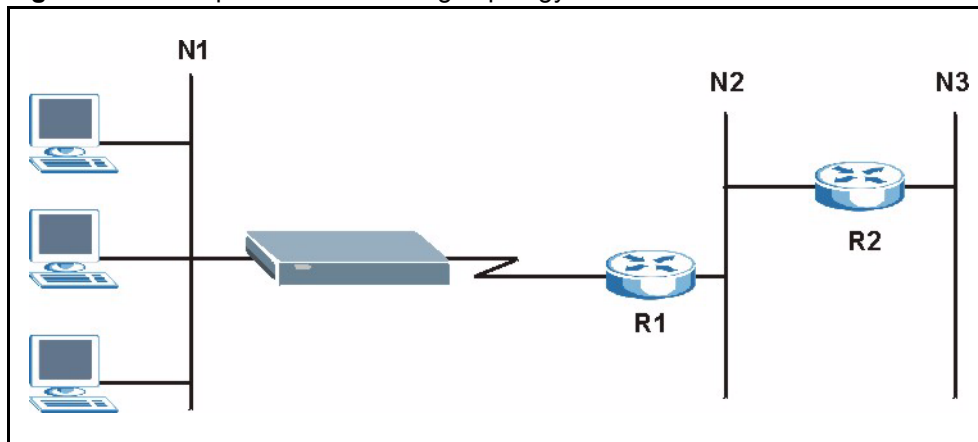
10.2 Configuring IP Static Route

Click **STATIC ROUTE** to open the screen as shown next.

Figure 65 Static Route

The following table describes the labels in this screen.

Table 50 Static Route

LABEL	DESCRIPTION
#	Number of an individual static route.
Name	Name that describes or identifies this route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over the WAN, the gateway must be the IP address of one of the remote nodes.
Edit	Select a static route index number and then click **Edit** to set up a static route on the Prestige.
Delete	To delete a static route on the Prestige, click a static route index number, then click **Delete**.

10.2.1 Configuring Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.

Figure 66 Static Route: Edit

The following table describes the labels in this screen.

Table 51 Static Route: Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

C HAPTER 11
UPNP

This chapter introduces the Universal Plug and Play feature.

11.1 Universal Plug and Play Overview

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

11.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

11.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

  1 Dynamic port mapping

  2 Learning public IP addresses

  3 Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the *SUA/NAT* chapter for further information about NAT.

11.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

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

11.2 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 later in this *User's Guide* for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

11.3 Configuring UPnP

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

Figure 67 Configuring UPnP
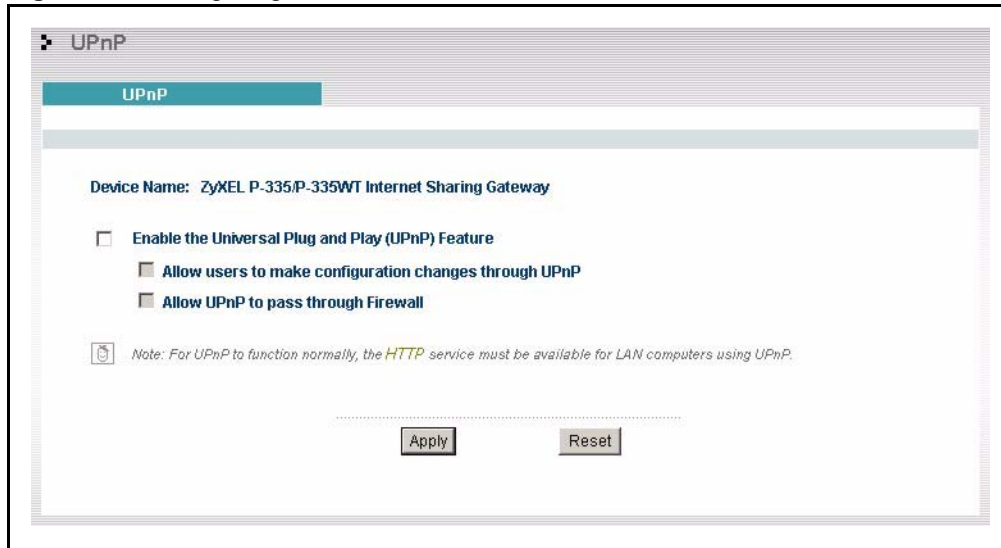
The following table describes the labels in this screen.

Table 52 Configuring 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 Prestige'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 Prestige so that they can communicate through the Prestige, 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	UPnP broadcasts are only allowed on the LAN. If you block LAN-to-LAN/Prestige traffic using the firewall, then you need to select this check box to allow UPnP-enabled traffic to pass through the firewall. This setting remains active until you disable UPnP.Clear this check box if you do not want to create a hole in the firewall for UPnP application packets (for example, MSN packets).
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

11.4 Installing UPnP in Windows Example

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

11.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.
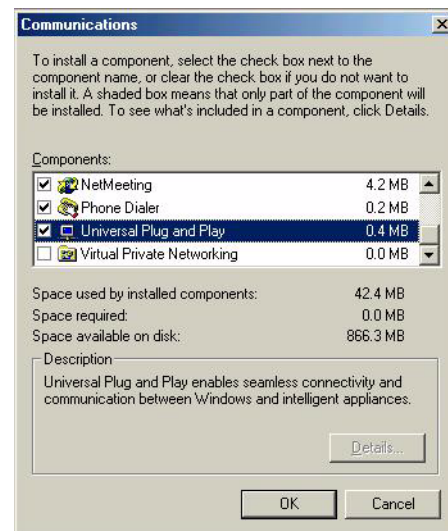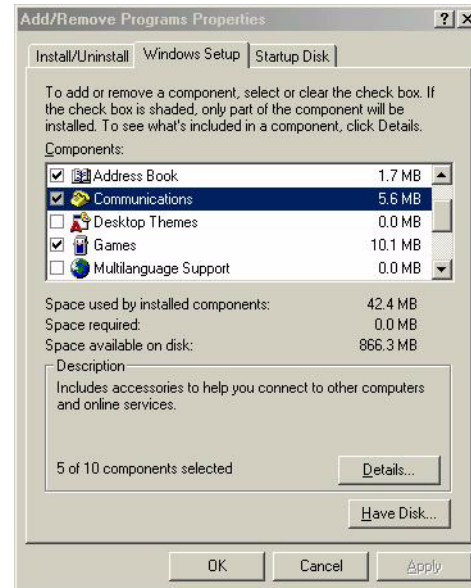
11.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.
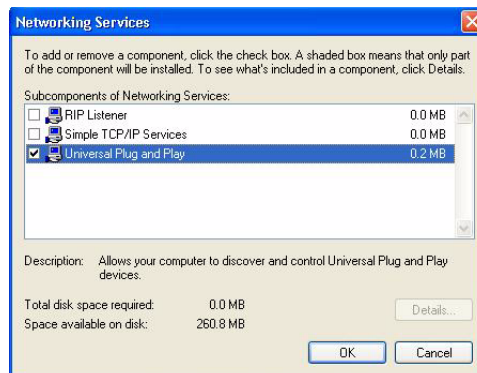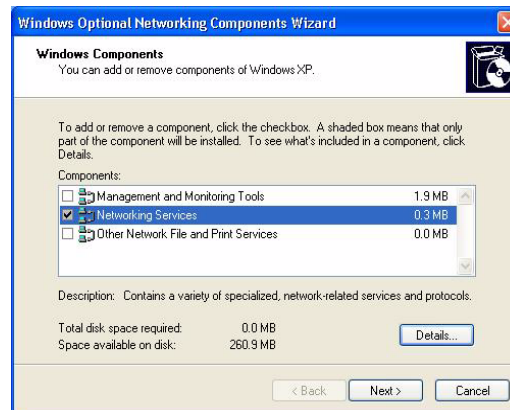
11.5 Using UPnP in Windows XP Example

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

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

11.5.1 Auto-discover Your UPnP-enabled Network Device

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

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

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

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

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

5 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray
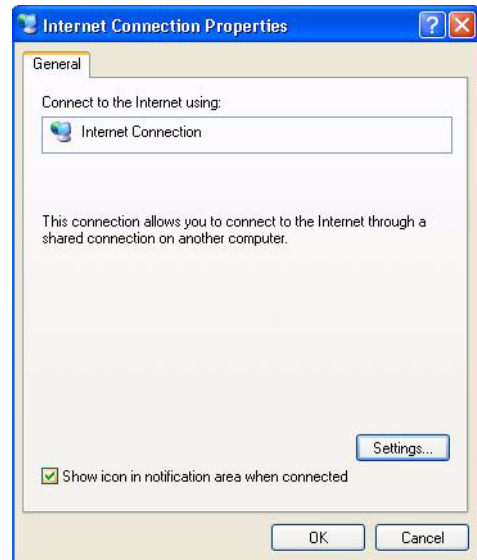
6 Double-click the icon to display your current Internet connection status.
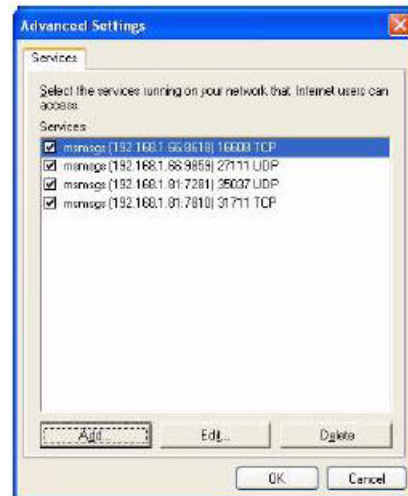
11.5.2 Web Configurator Easy Access

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

Follow the steps below to access the web configurator.
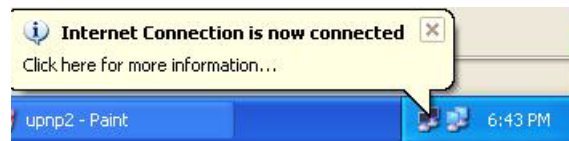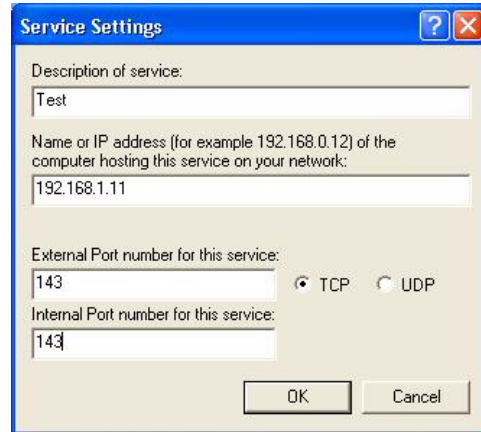
11.5.3 Web Configurator Easy Access

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

Follow the steps below to access the web configurator.
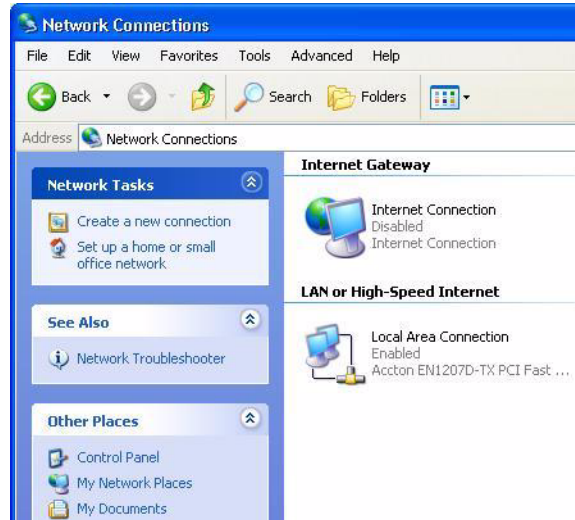
C HAPTER 12
Trend Micro Security Services

This chapter contains information about configuring Trend Micro Security Services (TMSS).

12.1 Trend Micro Security Services Overview

TMSS helps protect computers on a network that access the Internet through the Prestige.

TMSS scans computers behind the Prestige for potential vulnerabilities such as spyware, missing security patches, trojans etc. and then tells you how to update the computer so as to fix the vulnerability.

The Prestige includes TMSS "parental controls" that allows you to block web pages based on pre-defined web site categories such as pornography, gambling etc.

12.1.1 TMSS Web Page

TMSS is enabled by default on the Prestige, so you should see the following screen after you launch your web browser to connect to the Internet via the Prestige for the first time. You might not see this screen if you have a web pop-up blocker enabled, so disable it or manually enter http://tmss.trendmicro.com as the URL. Click **Continue** to go to the Active X control installation page.

Figure 68   TMSS First Time Access
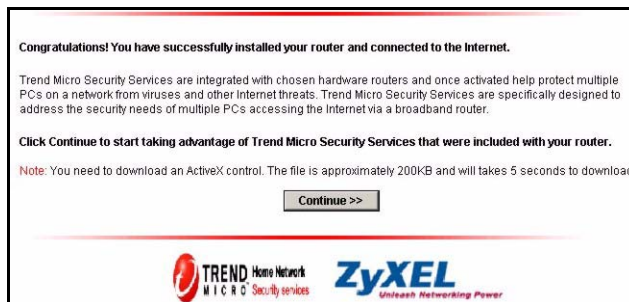
1 Download the **ActiveX** control to view the TMSS web page ("dashboard").

Note: Make sure that you have not restricted access to ActiveX, Cookies or Web Proxy features in the Prestige or web browser or you will not be able to access the TMSS web page.

Figure 69   Download ActiveX to View TMSS Web Page
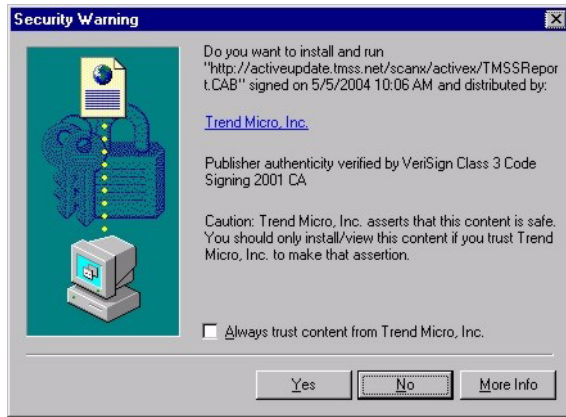
2 In the TMSS web page, click **Service Summary.**

Figure 70   TMSS Web Page(Dashboard)

3 Click **Activate My Services** to begin a 3-step process to activate TMSS.

Figure 71   TMSS Service Summary

4 Click **Next** to begin the process as outlined in the screen.

Figure 72   TMSS 3 Steps

5 Fill in the registration form and submit it.

Figure 73   TMSS Registration Form

6 After you submit the registration form, you will receive an e-mail with instructions for validating your e-mail address. Follow the instructions.

7 Download TMSS to each computer (behind the Prestige) that you want TMSS to monitor.

TMSS is now active and can now monitor Prestige LAN computers with TMSS installed (TMSS clients) for security updates. The following screen is an example of the **Service Summary** screen with TMSS activated.

Figure 74   Example TMSS Activated Service Summary Screen

You need a **Parental Control** license to activate configure **Parental Control** categories on the Prestige (see Figure 80 on page 179). The following screen is an example of the **Parental Control** screen with TMSS activated.

Figure 75   Example TMSS Activated Parental Controls Screen

After the free trial expires, you can buy the Trend micro Internet Security (TIS)[1] package. This package contains anti-virus software and a license for **Parental Control** (to forbid access to undesirable web site content based on pre-defined web site categories).

Note: See the TM User's Guide for details on all features.

12.2 Configuring TMSS on the Prestige

Click **TMSS** under **Advanced Setup**.

Figure 76   TMSS Main Screen

1 Use the **Service Settings** screen to enable or disable TMSS, configure how often the TMSS web page displays (Figure 70 on page 172) and exempt computers from TMSS monitoring.

---

1.   All TMSS processes and names used are correct at the time of writing.

2 Use the **Virus Protection** screen to configure if and how often updates are checked and to display the status of computers under TMSS monitoring.

3 Use the **Parental Controls** screen to schedule and block web pages based on pre-defined web site categories such as pornography, gambling etc.

12.2.1 TMSS Service Settings

Click **Service Settings** from the TMSS main screen (Figure 76 on page 174) to display the screen shown next.

Note: At the time of writing, TMSS may monitor up to 10 Prestige LAN computers with TMSS installed .

The Prestige must have an Internet connection for TMSS clients to display in this screen.

Figure 77 TMSS Service Settings

The following table describes the labels in this screen.

Table 53   Service Settings

	DESCRIPTION
Enable Trend Micro Security Services	Select the checkbox to enable **Trend Micro Security Services** on your Prestige.
Security Services Display Interval	
Automatically display TMSS Web page every:	Select from the drop-down list box how often the TMSS web page appears in your web browser .
Exception List	
Computer(s) that will display Trend Micro Home Network Security Services:	This box displays the Prestige LAN computers with TMSS installed (TMSS clients) that can be monitored by TMSS.
Computer(s) to exclude:	This box displays the Prestige LAN computers that are exempted from TMSS monitoring. Select a computer IP address from the previous list box and then click **Add>>** to omit it from TMSS monitoring. Select a computer IP address from this list box and then click **<<Remove** to have TMSS monitor it.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

12.3 Configuring Virus Protection

Select **Virus Protection** in the TMSS main screen (Figure 76 on page 174) to display the following screen. The anti-virus software is part of the TIS package (see the footnote on page 174). The virus pattern and the scan engine are both version numbers related to the anti-virus software.

Figure 78   Virus Protection

The following table describes the labels in this screen.

Table 54   Virus Protection

LABEL	DESCRIPTION
Check for Trend Micro Internet Security	
Automatically check for update components	Select the checkbox to have the Prestige download the latest scan engine and virus pattern version numbers (not the actual software) from the Trend Micro website. The Prestige can then compare version numbers currently on Prestige LAN computers with its latest downloaded version numbers and display the status in the table below.
Check for update components every	Select how often the Prestige should automatically check the Trend Micro Active Update server for updated components. Choose more frequent checking if there are many current virus threats or less frequent checking if there aren't and you have a lot of Internet traffic.
Scan engine	This field displays the latest TMSS anti-virus scan engine version number that the Prestige has downloaded.
Virus pattern	This field displays the latest TMSS anti-virus pattern version number that the Prestige has downloaded. **N/A** displays if there has been no reply for an update request.
Client Antivirus Protection Status	This table provides information on all TMSS client computers and the Prestige itself.
#	This field displays the index number of a TMSS client computer or the Prestige.
IP Address	This field displays the IP address of a TMSS client computer or Prestige.
Computer Name	This field displays the host name of a TMSS client computer or the Prestige system name.
Antivirus Software	This field displays **Internet Security** if TIS (see the footnote on page 174) is installed on the TMSS client computer. It displays **N/A** if you don't have TM anti-virus software installed.
Virus Pattern	This field displays the current TMSS anti-virus pattern version number on a TMSS client.
Scan Engine	This field displays the current TMSS anti-virus scan engine version number of a TMSS client.

Table 54 Virus Protection (continued)

LABEL	DESCRIPTION
Status	This field displays whether you have (the latest) Trend Micro anti-virus software installed on a TMSS client computer.
	Potential Threat displays if:
	• The Prestige had no response after an update request.
	• There is currently no Trend Micro anti-virus installed on the TMSS client.
	• The LAN computer is using a UNIX or Macintosh operating system. This message displayed for computers with these operating systems does not mean they may be a "potential threat" but rather that TMSS cannot monitor them.
	Needs Update displays if:
	• The Trend Micro anti-virus version numbers on the TMSS client is older than the version numbers downloaded to the Prestige.
	In both of these cases, you should either buy TM anti-virus software (TIS) if the free trial has expired and you have no other anti-virus software installed or update the TIS package.
	Up to date displays if:
	• The Trend Micro anti-virus version numbers on the TMSS client computer are the same as the numbers downloaded to the Prestige. You don't have to do anything in this case.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to begin configuring this screen afresh.

12.4 Parental Controls Configuration

Select **Parental Controls** from the **TMSS** main screen. You need a Trend Micro **Parental Control** license in order to configure this screen. If you don't have one or it has expired, you will see the following message when you access the **Parental Controls** screen.

Figure 79   No Parental Controls License

If you have completed the TMSS registration process and your license is valid, you can configure the **Parental Controls** configuration screen as shown in the following figure.

Figure 80   Parental Controls

The following table describes the labels in this screen.

Table 55   Parental Controls

LABEL	DESCRIPTION
Enable Parental Controls	Select the check box to enable this feature on your Prestige.
Blocking Schedule	The blocking schedule for TMSS is the same as that used for content filtering (web site blocking by keyword). If blocking schedule configuration changes are made here, then the same changes apply to the **CONTENT FILTER** screen and vice versa.
Day to Block	Select everyday or the day(s) of the week to activate web page blocking

Table 55 Parental Controls
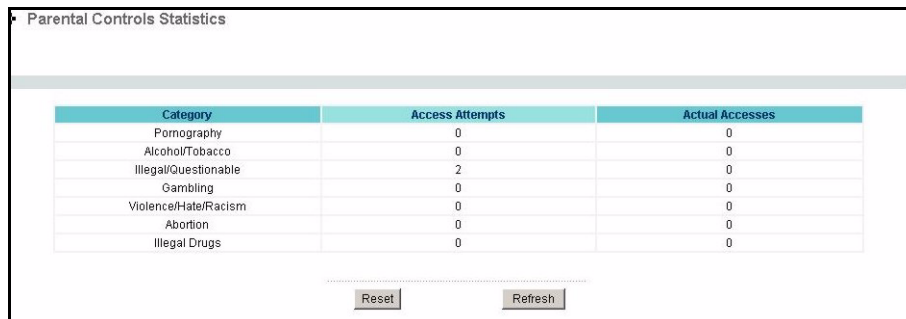
LABEL	DESCRIPTION
Time of Day to Block (24-Hour Format)	Select the time of day you want web page blocking to take effect. Configure blocking to take effect all day by selecting the **All Day** check box. You can also configure specific times by entering the start time in the Start (hr) and Start (min) fields and the end time in the End (hr) and End (min) fields. Enter times in 24-hour format; for example, "3:00pm" should be entered as "15:00".
Select Categories	
Pornography	Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Illegal/Questionable	Selecting this category excludes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers. This category includes sites identified as being malicious in any way such as web pages that may contain viruses, spyware etc.).
Violence/Hate/Racism	Selecting this category excludes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics.
Illegal Drugs	Selecting this category excludes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
Alcohol/Tobacco	Selecting this category excludes pages that promote or offer the sale alcohol/tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products.
Gambling	Selecting this category excludes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements).
Abortion	Selecting this category excludes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion.
Exception List	Use the **Exception List** to specify which computers are not to be restricted by **Parental Controls**. All TMSS clients are displayed in the **Available IP Addresses** list box. Use the **Add>>** or **<<Remove** buttons to move computer IP addresses to the **Selected IP Addresses** list box and then select one of the following radio buttons to apply an action.
Enforce Parental Control policies for all computers	Select the radio button to have **Parental Controls** enabled on computers with IP addresses listed in the **Available IP Addresses** list box. This is the default setting.
Include specified address ranges in the Parental Control enforcement.	Select the radio button to apply **Parental Controls** only to the computers with IP addresses listed in the **Selected IP Addresses** list box.

Table 55 Parental Controls

LABEL	DESCRIPTION
Exclude specified address ranges from the Parental Control enforcement.	Select the radio button to exempt computers with IP addresses displayed in the **Selected IP Addresses** list box from **Parental Controls**.
Available IP Addresses	This box displays the IP addresses of all TMSS clients.
Selected IP Addresses	This box displays the IP addresses of the computer(s) chosen from the **Available IP Addresses** box, to which you want to apply or exclude from **Parental Controls**. Select an IP address(es) in the **Available IP Addresses** list box and click **Add>>** to move it/them to the **Selected IP Addresses** box. Select an IP address(es) in the **Selected IP Addresses** list box and click **<<Remove** to move it/them to the **Available IP Addresses** list box.
Apply	Click **Apply** to save the settings.
Show Statistics	Click **Show Statistics** to view a record of access attempts and successes to web pages belonging to each category.
Reset	Click **Reset** to begin configuring this screen afresh.

12.4.1 Parental Controls Statistics

Click **Show Statistics** in the screen as shown in the previous figure to display a record of attempted entries to web pages or actual entries to web pages from a list of categories.

Figure 81   Parental Controls Statistics

The following table describes the labels in this screen.

Table 56   Parental Controls Statistics

LABEL	DESCRIPTION
Category	All Parental Control categories are displayed as shown.
Access Attempts	This field displays the number of attempts that have been made to access web page(s) from a category of web pages that you have selected in the **Parental Controls** screen (see Figure 80 on page 179).
Actual Accesses	This field displays the number of times access has been made to web page(s) from a category of web pages that you have *not* selected in the **Parental Controls** screen (see Figure 80 on page 179) or that have been accesses by exempted computers.

Table 56 Parental Controls Statistics

LABEL	DESCRIPTION
Reset	Click **Reset** to clear all of the fields in this screen.
Refresh	Click **Refresh** to renew the statistics screen.

C HAPTER 13
Firewall

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

13.1 Introduction

13.1.1 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.

13.1.2 Stateful Inspection Firewall.

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

13.1.3 About the Prestige Firewall

The Prestige firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click **FIREWALL** and then click the **Enable Firewall** check box). The Prestige's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Prestige 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 Prestige 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 Prestige has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem 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" is not allowed (by default) unless the remote host is authorized to use a specific service.

13.1.4 Guidelines For Enhancing Security With Your Firewall

1 Change the default password via web configurator.

2 Think about access control before you connect to the network in any way, including attaching a modem to the port.

3 Limit who can access 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.

13.2 Firewall Settings Screen

From the **MAIN MENU**, click **FIREWALL** to open the **Settings** screen.

Figure 82 Firewall: Settings

The following table describes the labels in this screen.

Table 57 Firewall: Settings

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The Prestige 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 Prestige firewall ignore the use of triangle route topology on the network. See the appendix for more on triangle route topology.
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create.
LAN to WAN	To log packets related to firewall rules, make sure that **Access Control** under **Log** is selected in the **Logs**, **Log Settings** screen.
Packets to Log	Choose what **LAN to WAN** packets to log. Choose from: **No Log** **Log Blocked** (blocked LAN to WAN services appear in the **Blocked Services** textbox in the **Services** screen (with **Enable Services Blocking** selected)) **Log All** (log all **LAN to WAN** packets)
WAN to LAN	To log packets related to firewall rules, make sure that **Access Control** under **Log** is selected in the **Logs**, **Log Settings** screen.

Table 57 Firewall: Settings

LABEL	DESCRIPTION
Packets to Log	Choose what **WAN to LAN** and WAN to WAN/Prestige packets to log. Choose from: **No Log** **Log Forwarded** (see how to forward WAN to LAN traffic in the next section) **Log All** (log all **WAN to LAN** packets).
Trusted Computer IP Address	You can allow a specific computer to access all Internet resources without restriction. Enter the IP address of the trusted computer in this field.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

13.3 The Firewall, NAT and Remote Management

Figure 83   Firewall Rule Directions
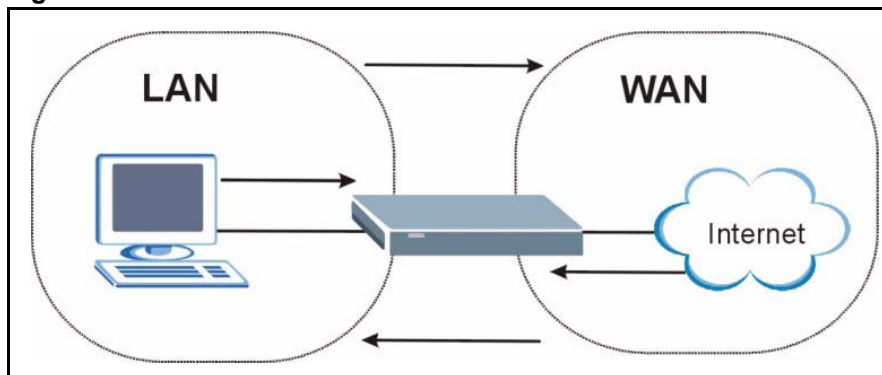
13.3.1 LAN-to-WAN rules

LAN-to-WAN rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet.

How can you block certain LAN to WAN traffic?

You may choose to block certain **LAN-to-WAN** traffic in the **Services** screen (click the **Services** tab). All services displayed in the **Blocked Services** list box are **LAN-to-WAN** firewall rules that block those services originating from the LAN.

Blocked **LAN-to-WAN** packets are considered alerts. Alerts are "higher priority logs" that include system errors, attacks and attempted access to blocked web sites. Alerts appear in red in the **View Log** screen. You may choose to have alerts e-mailed immediately in the **Log Settings** screen.

LAN-to-LAN/Prestige means the LAN to the Prestige LAN interface. This is always allowed, as this is how you manage the Prestige from your local computer.

13.3.2 WAN-to-LAN rules

WAN-to-LAN rules are Internet to your local network firewall rules. The default is to block all traffic from the Internet to your local network.

How can you forward certain WAN to LAN traffic? You may allow traffic originating from the WAN to be forwarded to the LAN by:

- Configuring NAT port forwarding rules in the web configurator **SUA Server** screen or SMT NAT menus.
- Configuring **One-to-One** and **Many-One-to-One** NAT mapping rules in the web configurator **Address Mapping** screen or SMT NAT menus.
- Configuring **WAN** or **LAN & WAN** access for services in the **Remote Management** screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/Prestige firewall rules. WAN-to-WAN/Prestige firewall rules are Internet to the Prestige WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what **WAN-to-LAN** and WAN-to-WAN/Prestige packets to log.
- Allow NetBIOS traffic from the WAN to the LAN using the **WAN IP** web screen or SMT menu 24.8 commands.

Forwarded **WAN-to-LAN** packets are not considered alerts.

13.4 Services

Click on the **Services** tab. The screen appears as shown next. Use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Figure 84   Firewall: Service
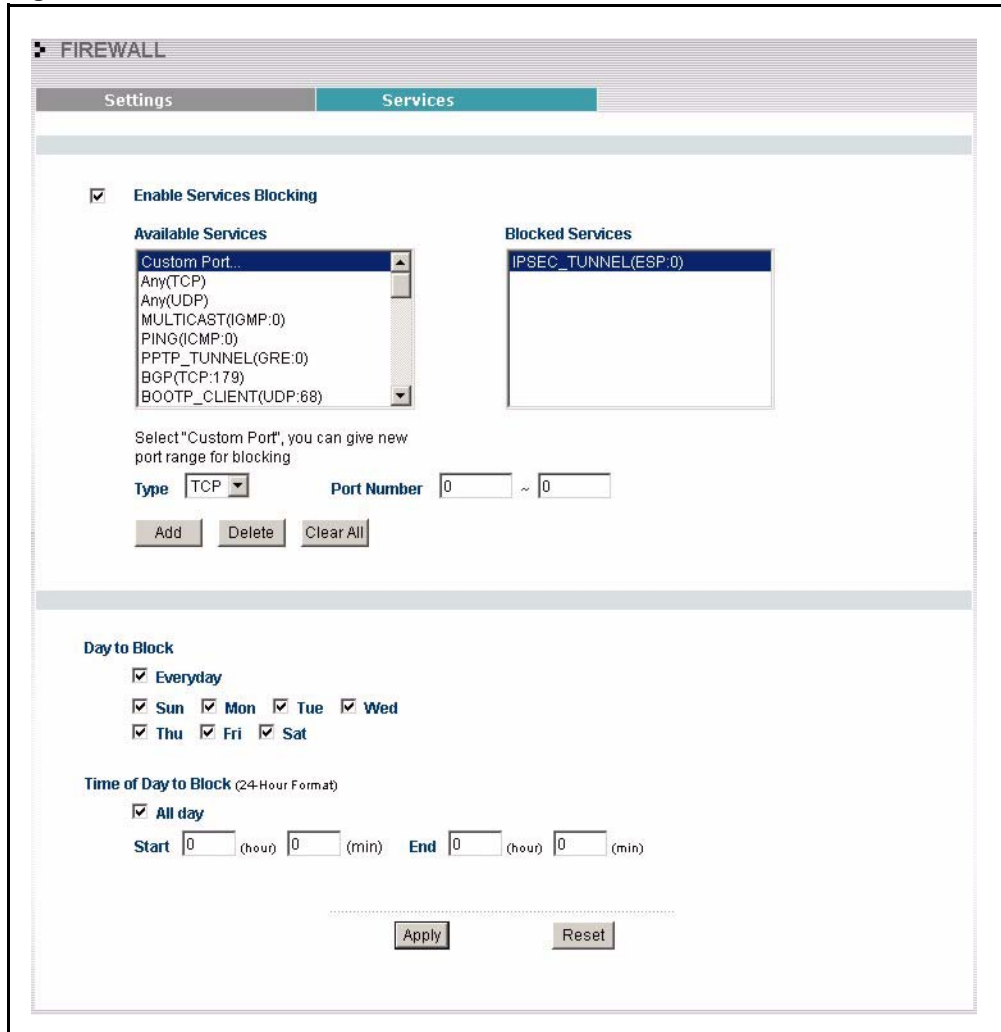
The following table describes the labels in this screen.

Table 58   Firewall: Service

LABEL	DESCRIPTION
Enable Services Blocking	Select this check box to enable this feature.
Available Service	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click **Add** to add the port to the **Blocked Service** field.
Blocked Service	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking. Choose the IP port (**TCP**, **UDP** or **TCP**/**UDP**) that defines your customized port from the drop down list box.
"Custom Port"	A custom port is a service that is not available in the pre-defined **Available Services** list and you must define using the next two fields.
Type	Services are either **TCP** and/or **UDP**. Select from either **TCP** or **UDP**.

Table 58 Firewall: Service

LABEL	DESCRIPTION
Port Number	Enter the port number range that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range from 6345-6349.
Add	Select a service from the **Available Services** drop-down list and then click **Add** to add a service to the Blocked Service.
Delete	Select a service from the **Blocked Services List** and then click **Delete** to remove this service from the list.
Clear All	Click **Clear All** to empty the **Blocked Service**.
Day to Block:	Select a check box to configure which days of the week (or everyday) you want the content filtering to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting the **All Day** check box. You can also configure specific times that by entering the start time in the **Start (hr)** and **Start (min)** fields and the end time in the **End (hr)** and **End (min)** fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

CHAPTER 14
Content Filtering

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

14.1 Introduction to Content Filtering

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

14.2 Restrict Web Features

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

14.3 Days and Times

The Prestige also allows you to define time periods and days during which the Prestige performs content filtering.

14.4 Configure Content Filtering

Click **Content Filter** on the navigation panel, to open the following screen.

Figure 85   Content Filter

The following table describes the labels in this screen.

Table 59 Content Filter

LABEL	DESCRIPTION
Trusted Computer IP Address	To enable this feature, type an IP address of any one of the computers in your network (displayed in **Parental Controls**) that you want to have as a trusted computer. This allows the selected computer(s) in parental controls to have full access to all features that are configured to be blocked by content filtering and parental controls. Leave this field blank to have no trusted computers. You must also exclude this IP address and any others in the **Parental Controls** screen, by performing one of the following actions • Select **Exclude specified address ranges from the Parental Control enforcement** and then **Add** the IP address(es) to the **Select IP Addresses** field. • Select **Include specified address ranges in the Parental Control enforcement.** All trusted computer IP address(es) are displayed in the Available IP Address field.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The Prestige can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click this button to remove all of the listed keywords.
Day to Block	Select check boxes for the days that you want the Prestige to perform content filtering. Select the **Everyday** check box to have content filtering turned on all days of the week.

Table 59   Content Filter

LABEL	DESCRIPTION
Time of Day to Block	Time of Day to Block allows the administrator to define during which time periods content filtering is enabled. Time of Day to Block restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected.
	Enter the time period, in 24-hour format, during which content filtering will be enforced. Select the **All Day** check box to have content filtering always active on the days selected in **Day to Block** with time of day limitations not enforced.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

14.5 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

14.5.1 Domain Name or IP Address URL Checking

By default, the Prestige checks the URL's domain name or IP address when performing keyword blocking.

This means that the Prestige checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

14.5.2 Full Path URL Checking

Full path URL checking has the Prestige check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

14.5.3 File Name URL Checking

Filename URL checking has the Prestige check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.Prestige

CHAPTER 15
Remote Management Screens

This chapter provides information on the Remote Management screens.

15.1 Remote Management Overview

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

> **Note:** 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

You may manage your Prestige from a remote location via:

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

> **Note:** When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

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

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

1 Telnet

2 HTTP

15.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1 A filter in SMT 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 one of the remote management screens.

3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.

4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

5 There is a firewall rule that blocks it.

15.1.2 Remote Management and NAT

When NAT is enabled:

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

15.1.3 System Timeout

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

15.2 Configuring WWW

To change your Prestige's World Wide Web settings, click **REMOTE MGMT** to display the **WWW** screen.

Figure 86 Remote Management: WWW

The following table describes the labels in this screen.

Table 60 Remote Management: WWW

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

15.3 Configuring Telnet

You can configure your Prestige for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the Prestige.

Figure 87 Telnet Configuration on a TCP/IP Network
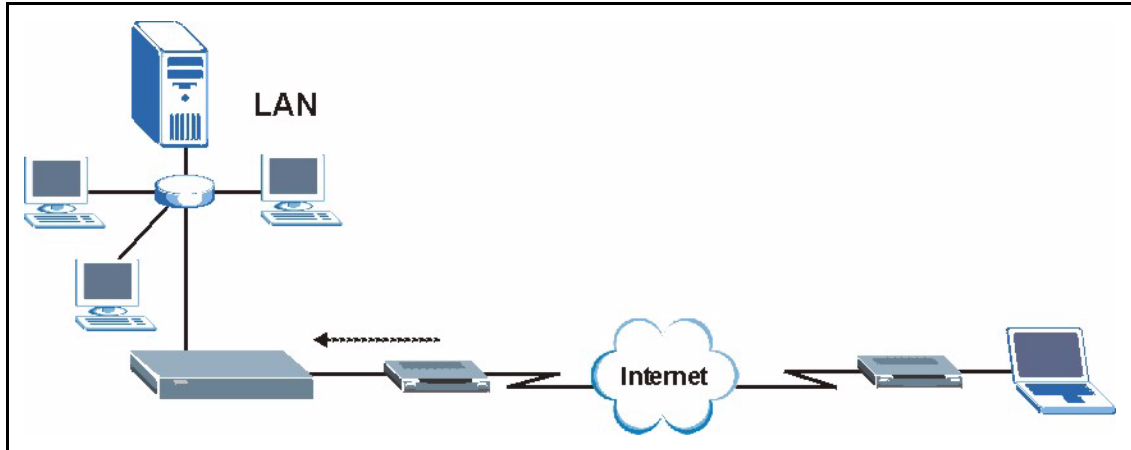
15.4 Configuring TELNET

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

Figure 88 Remote Management: Telnet

The following table describes the labels in this screen.

Table 61 Remote Management: Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Prestige using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the Prestige using this service. Select **All** to allow any computer to access the Prestige using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Prestige using this service.

Table 61   Remote Management: Telnet

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

15.5 Configuring FTP

You can upload and download the Prestige'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.

To change your Prestige's FTP settings, click **REMOTE MGMT**, then the **FTP** tab. The screen appears as shown.

Figure 89   Remote Management: FTP

The following table describes the labels in this screen.

Table 62   Remote Management: FTP

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

15.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

> **Note:** SNMP is only available if TCP/IP is configured.

Figure 90   SNMP Management Model
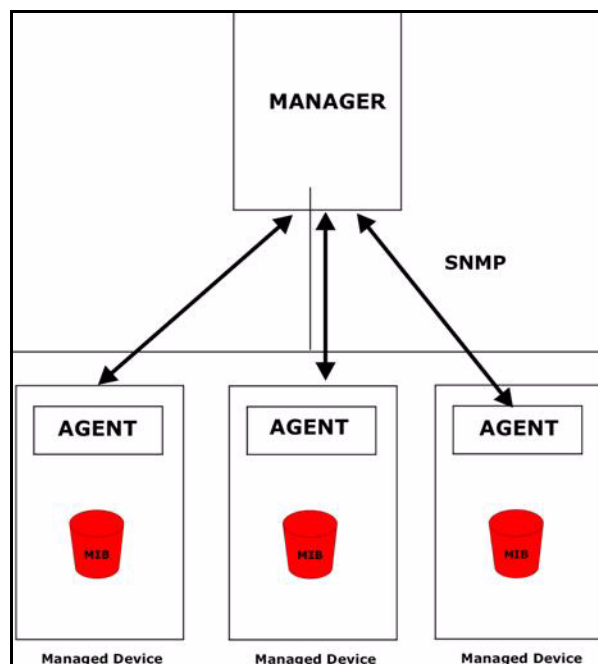
An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Prestige). 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.

15.6.1 Supported MIBs

The Prestige 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.

15.6.2 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

Table 63 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.

15.6.3 Configuring SNMP

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

Figure 91   Remote Management: SNMP

The following table describes the labels in this screen.

Table 64   Remote Management: SNMP

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

Table 64   Remote Management: SNMP

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

15.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on Wizard Setup for background information.

To change your Prestige's DNS settings, click **REMOTE MGMT**, then the **DNS** tab. The screen appears as shown.

Figure 92   Remote Management: DNS

The following table describes the labels in this screen.

Table 65   Remote Management: DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the Prestige.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to send DNS queries to the Prestige. Select **All** to allow any computer to send DNS queries to the Prestige. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the Prestige.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

15.8 Configuring Security

To change your Prestige's security settings, click **REMOTE MGMT**, then the **Security** tab. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your Prestige, an ICMP response packet is automatically returned. This allows the outside user to know the Prestige exists. Your Prestige supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your Prestige when unsupported ports are probed.

Figure 93   Security
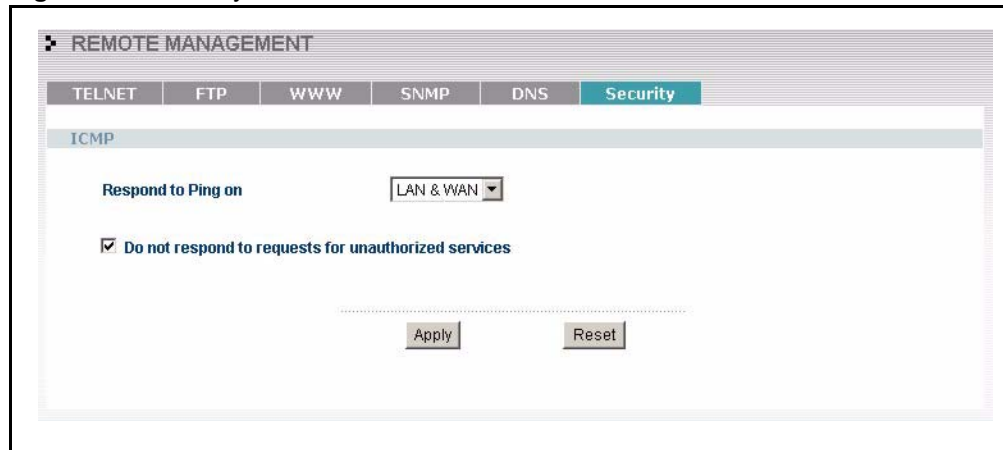
The following table describes the labels in this screen.

Table 66   Security

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The Prestige will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests**.** Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the Prestige by probing for unused ports. If you select this option, the Prestige will not respond to port request(s) for unused ports, thus leaving the unused ports and the Prestige unseen. By default this option is not selected and the Prestige will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports.
	Note that the probing packets must first traverse the Prestige's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the Prestige reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on|off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.

Table 66 Security

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

C H A P T E R 16
Introduction to IPSec

This chapter introduces the basics of IPSec VPNs

16.1 VPN Overview

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

16.1.1 IPSec

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

16.1.2 Security Association

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

16.1.3 Other Terminology

16.1.3.1 Encryption

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

Figure 94 Encryption and Decryption
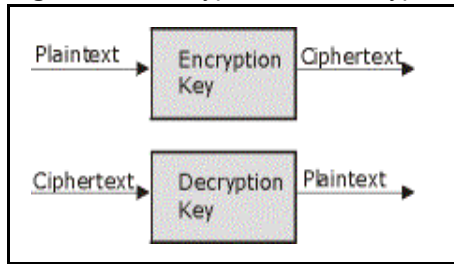
16.1.3.2 Data Confidentiality

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

16.1.3.3 Data Integrity

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

16.1.3.4 Data Origin Authentication

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

16.1.4 VPN Applications

The Prestige supports the following VPN applications.

- Linking Two or More Private Networks Together

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

- Accessing Network Resources When NAT Is Enabled

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

- Unsupported IP Applications

  A VPN tunnel may be created to add support for unsupported emerging IP applications. See the chapter on *Getting to Know Your Prestige* for an example of a VPN application.

16.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 95 IPSec Architecture
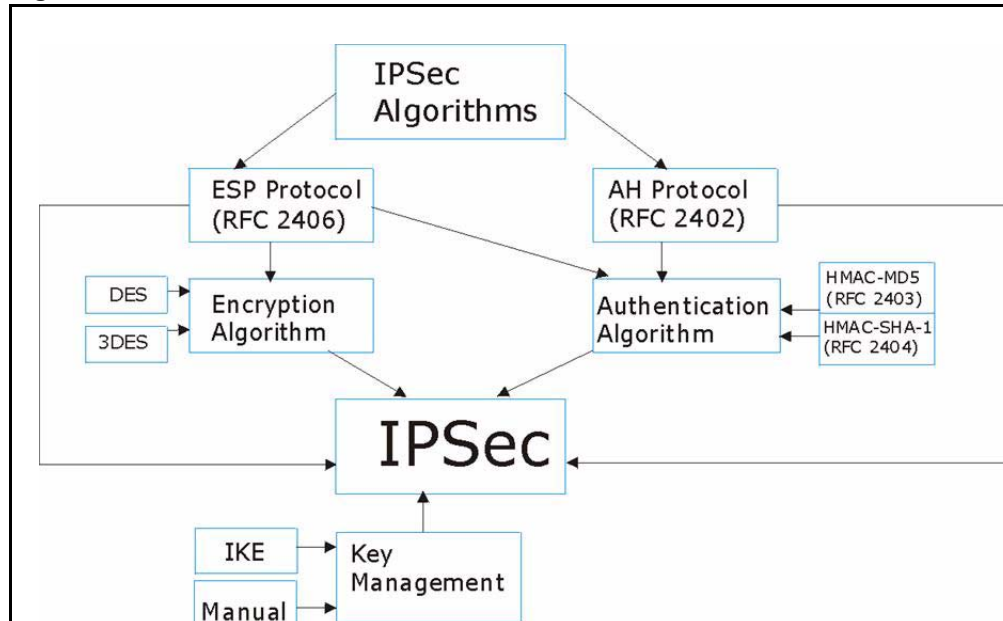
16.2.1 IPSec Algorithms

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 *the IPSec Algorithms section* for more information.

16.2.2 Key Management

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

16.3 Encapsulation

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

Figure 96 Transport and Tunnel Mode IPSec Encapsulation
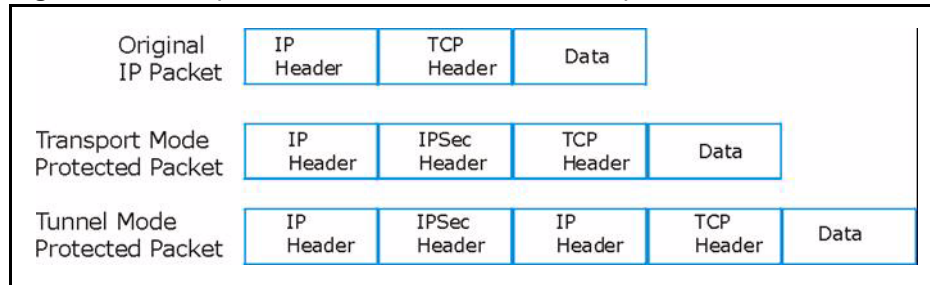
16.3.1 Transport Mode

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.

16.3.2 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.

16.4 IPSec and NAT

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

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

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

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

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

Table 67   VPN and NAT

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

CHAPTER 17
VPN Screens

This chapter introduces the VPN Web Configurator. See the *Logs* chapter for information on viewing logs and the Appendices for IPSec log descriptions.

17.1 VPN/IPSec Overview

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

17.2 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.

17.2.1 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.

17.2.2 ESP (Encapsulating Security Payload) Protocol

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

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

.

Table 68 AH and ESP

		AH
Encryption	**DES** (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	
	AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
	Select NULL to set up a phase 2 tunnel without encryption.	
Authentication	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

17.3 My IP Address

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

17.4 Secure Gateway Address

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

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

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The Prestige 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).

17.4.1 Dynamic Secure Gateway Address

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

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

17.5 Summary Screen

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

Figure 97   IPSec Summary Fields
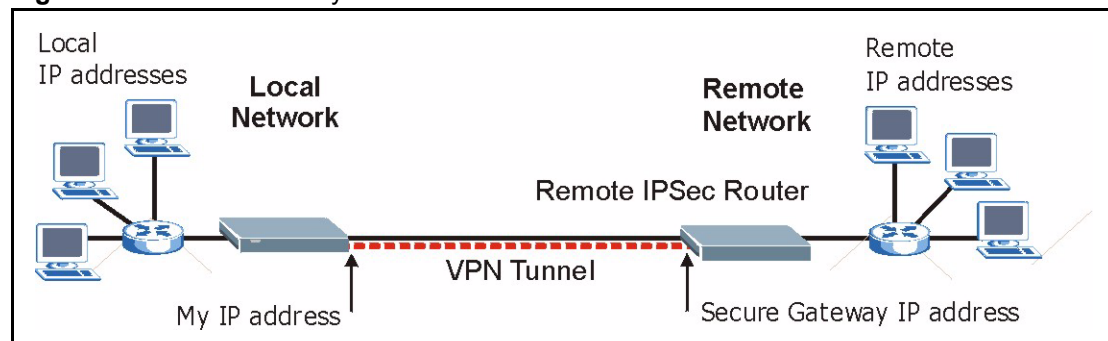
Local and remote IP addresses must be static.

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

Figure 98 VPN: Summary

The following table describes the labels in this screen.

Table 69 VPN: Summary

LABEL	DESCRIPTION
#	The VPN policy index number.
Active	This field displays whether the VPN policy is active or not. A **Y** signifies that this VPN policy is active. **N** signifies that this VPN policy is not active.
Local Addr.	This is the IP address of the computer on your local network behind your Prestige.
Remote Addr.	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router.
	A single (static) IP address is displayed when the **Remote Address Start** and **Remote Address End/Mask** fields in the **Rule Setup IKE** (or **Manual**) screen are both configured to the same IP address.
	The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Address Start** and **Remote Address End/Mask** fields in the **Rule Setup IKE** (or **Manual**) screen are configured for a range of IP addresses.
	A (static) IP address and a subnet mask are displayed when the **Remote Address Start** and **Remote Address End/Mask** fields in the **Rule Setup IKE** (or **Manual**) screen are configured for a subnet.
	This field displays **0.0.0.0** when the **Secure Gateway Address** field is set to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).
Algorithm	This field displays the security protocols used for an SA.
	Both **AH** and **ESP** increase Prestige processing requirements and communications latency (delay).
Gateway	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway Addr** field in the **Rule Setup IKE** screen to **0.0.0.0.**
Select the radio button next to a VPN index number and then click **Edit** to edit a specific VPN policy. Click the radio button next to an empty VPN policy index number and then **Edit** to add a new VPN policy.	
Select the radio button next to a VPN policy number you want to delete and then click **Delete**. When a VPN policy is deleted, subsequent policies do not move up in the list.	

17.6 Keep Alive

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

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

> **Note:** When there is outbound traffic with no inbound traffic, the Prestige automatically drops the tunnel after two minutes.
> **Note:**

17.7 NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between IPSec routers A and B.

Figure 99   NAT Router Between IPSec Routers
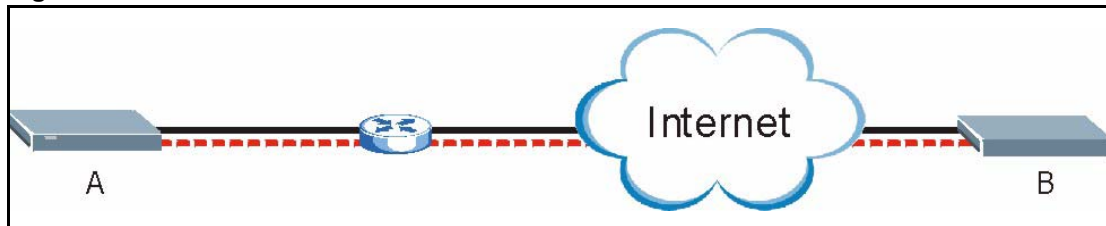
Normally you cannot set up a VPN connection with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. In the previous figure, IPSec router A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet's header so it does not match the header for which IPSec router B is checking. Therefore, IPSec router B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. IPSec router B checks the UDP port 500 header and responds. IPSec routers A and B build a VPN connection.

17.7.1 NAT Traversal Configuration

For NAT traversal to work you must:

- Use ESP security protocol (in either transport or tunnel mode).

        • Use IKE keying mode.

        • Enable NAT traversal on both IPSec endpoints.

In order for IPSec router A (see the figure) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

17.7.2 Remote DNS Server

In cases where you want to use domain names to access Intranet servers on a remote network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote network

The following figure depicts an example where three VPN tunnels are created from Prestige A; one to branch office 2, one to branch office 3 and another to headquarters. In order to access computers that use private domain names on the headquarters (HQ) network, the Prestige at branch office 1 uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP.

Figure 100   VPN Host using Intranet DNS Server Example
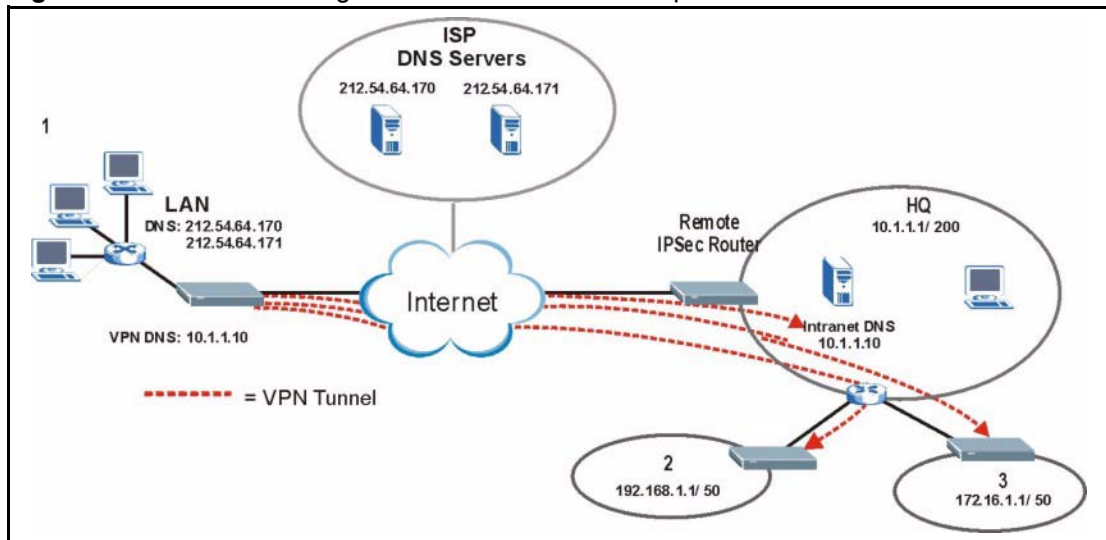
Note: If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote network.

17.8 ID Type and Content

With aggressive negotiation mode (see *Section* Negotiation Mode), the Prestige identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Prestige to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the Prestige from IPSec routers with dynamic IP addresses (see the Telecommuter VPN/IPSec Examples section for a telecommuter configuration example).

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

With main mode (see *Section* Negotiation Mode), the ID type and content are encrypted to provide identity protection. In this case the Prestige can only distinguish between up to eight different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The Prestige can distinguish up to eight incoming SAs because you can select between three encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (the Configuring Advanced IKE Settings section). 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 70 Local ID Type and Content Fields

LOCAL ID TYPE	CONTENT
IP	Type the IP address of your computer or leave the field blank to have the Prestige automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this Prestige.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this Prestige.
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 71 Peer ID Type and Content Fields

PEER ID TYPE	CONTENT
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Prestige automatically use the address in the **Secure Gateway Address** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.

Table 71   Peer ID Type and Content Fields

PEER ID TYPE	CONTENT
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 Address** field below.	

17.8.1 ID Type and Content Examples

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

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

Table 72   Matching ID Type and Content Configuration Example

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

The two Prestiges in this example cannot complete their negotiation because Prestige B's **Local ID type** is **IP**, but Prestige A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Figure 101   Mismatching ID Type and Content Configuration Example

PRESTIGE A	PRESTIGE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

17.9 Pre-Shared Key

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

17.10 Editing VPN Rules

Click **Edit** on the **Summary** screen or click the **Rule Setup** tab to edit VPN rules.

Figure 102   VPN: Rule Setup (Basic)

The following table describes the labels in this screen.

Table 73   VPN: Rule Setup (Basic)

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select this check box to have the Prestige 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.

Table 73 VPN: Rule Setup (Basic)

LABEL	DESCRIPTION
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.
	The remote IPSec router must also have NAT traversal enabled.
	You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.
IPSec Keying Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting.
Local Address	The local IP address must be static and correspond to the remote IPSec router's configured remote IP addresses.
	Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Start	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote address fields do not apply when the **Secure Gateway Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.
	Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
	Enter a (static) IP address on the network behind the remote IPSec router.
Remote Address End/Mask	When the remote IP address is a single address, type it a second time here.
	When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The Prestige assigns this additional DNS server to the Prestige's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
My IP Address	Enter the WAN IP address of your Prestige. The Prestige 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.
Local ID Type	Select **IP** to identify this Prestige by its IP address.
	Select **DNS** to identify this Prestige by a domain name.
	Select **E-mail** to identify this Prestige by an e-mail address.

Table 73 VPN: Rule Setup (Basic)

LABEL	DESCRIPTION
Local Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The Prestige automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank.
	It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations.
	When there is a NAT router between the two IPSec routers.
	When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.
	When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this Prestige in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **IPSec Keying Mode** field must be set to **IKE**). The remote address fields do not apply when the **Secure Gateway Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address.
	Select **DNS** to identify the remote IPSec router by a domain name.
	Select **E-mail** to identify the remote IPSec router by an e-mail address.
Peer Content	The configuration of the peer content depends on the peer ID type.
	For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the Prestige will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description).
	For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
	It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations:
	When there is a NAT router between the two IPSec routers.
	When you want the Prestige to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
IPSec Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).
	Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described later).

Table 73 VPN: Rule Setup (Basic)

LABEL	DESCRIPTION
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.
	Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself.
	Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends
Encryption Algorithm	Select **DES** or **3DES** from the drop-down list box. The Prestige's encryption algorithm should be identical to the secure remote gateway. When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message. The **DES** encryption algorithm uses a 56-bit key. Triple **DES** (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Advanced	Click **Advanced** to configure more detailed settings of your IKE key management.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

17.11 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 103 Two Phases to Set Up the IPSec SA
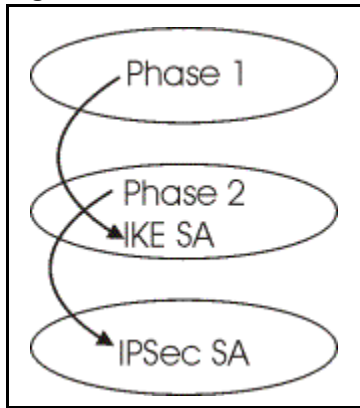
In phase 1 you must:

- 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 Perfect Forward Secrecy (PFS)*. 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 Prestige automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The Prestige 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.

17.11.1 Negotiation Mode

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

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

17.11.2 Diffie-Hellman (DH) Key Groups

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

17.11.3 Perfect Forward Secrecy (PFS)

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

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the Prestige. 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).

17.12 Configuring Advanced IKE Settings

Select **Advanced** at the bottom of the **Rule Setup IKE** screen. This is the **Rule Setup IKE-Advanced** screen as shown next.

Figure 104   VPN IKE: Advanced

The following table describes the labels in this screen.

Table 74 VPN IKE: Advanced

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN policy.
Keep Alive	Select this check box to turn on the Keep Alive feature for this SA.
	Turn on Keep Alive to have the Prestige automatically reinitiate 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.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.
	The remote IPSec router must also have NAT traversal enabled.
	You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.
IPSec Keying Mode	The advanced configuration page is only available with the **IKE** IPSec keying mode.
	Click the **Basic** button below in order to be able to choose the **Manual** IPSec keying mode.
	Make sure the remote gateway has the same configuration in this field.
Protocol Number	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **Yes**.
Local Address	The local IP address must be static and correspond to the remote IPSec router's configured remote IP addresses.
	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.
Local Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3
Local Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field (or equal to it for configuring an individual port).
Remote Address Start	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote address fields do not apply when the **Secure Gateway Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.
	Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
	Enter a (static) IP address on the network behind the remote IPSec router.

Table 74   VPN IKE: Advanced

LABEL	DESCRIPTION
Remote Address End/ Mask	When the remote IP address is a single address, type it a second time here.
	When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.
Remote Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3
Remote Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field (or equal to it for configuring an individual port).
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The Prestige assigns this additional DNS server to the Prestige's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
My IP Address	Enter the WAN IP address of your Prestige. The Prestige 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.
Local ID Type	Select **IP** to identify this Prestige by its IP address. Select **DNS** to identify this Prestige by a domain name. Select **E-mail** to identify this Prestige by an e-mail address.
Local Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The Prestige automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank.
	It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations.
	• When there is a NAT router between the two IPSec routers.
	• When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.
	When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this Prestige in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the remote secure gateway with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote secure gateway has a dynamic WAN IP address (the **IPSec Keying Mode** field must be set to **IKE**).
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address.
	Select **DNS** to identify the remote IPSec router by a domain name.
	Select **E-mail** to identify the remote IPSec router by an e-mail address.

Table 74   VPN IKE: Advanced

LABEL	DESCRIPTION
Peer Content	The configuration of the peer content depends on the peer ID type. • For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the Prestige will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). • For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. When you want the Prestige to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
IKE Phase 1	A phase 1 exchange establishes an IKE SA (Security Association).
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. The Prestige's negotiation mode should be identical to that on the remote secure gateway.
Encryption Algorithm	Select **DES** or **3DES** from the drop-down list box. The Prestige's encryption algorithm should be identical to the secure remote gateway. When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. The Prestige's authentication algorithm should be identical to the secure remote gateway. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate the source and integrity of packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select **SHA-1** for maximum security.
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.
IKE Phase 2	A phase 2 exchange uses the IKE SA established in phase 1 to negotiate the SA for IPSec.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop down list-box. The Prestige's encapsulation mode should be identical to the secure remote gateway.

Table 74   VPN IKE: Advanced

LABEL	DESCRIPTION
IPSec Protocol	Select **ESP** or **AH** from the drop-down list box. The Prestige's IPSec Protocol should be identical to the secure remote gateway. The ESP (Encapsulation Security Payload) protocol (RFC 2406) provides encryption as well as the authentication offered by AH. If you select **ESP** here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below). The AH protocol (Authentication Header Protocol) (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field.
Encryption Algorithm	The encryption algorithm for the Prestige and the secure remote gateway should be identical. When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select MD5 for minimal security and SHA-1 for maximum security.
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (None) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose from **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1, a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2, a 1024 bit (1Kb) random number (more secure, yet slower).
Basic	Select **Basic** to go to the previous VPN configuration screen.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

17.13 Manual Key Setup

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

17.13.1 Security Parameter Index (SPI)

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

> **Note:** Current ZyXEL implementation assumes identical outgoing and incoming SPIs

17.14 Configuring Manual Key

You only configure **VPN Manual Key** when you select **Manual** in the **IPSec Keying Mode** field on the **Rule Setup IKE** screen. This is the **Rule Setup Manual** screen as shown next.

Figure 105 Setup: Manual

The following table describes the labels in this screen.

Table 75 Rule Setup: Manual

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN policy.
IPSec Keying Mode	Select **IKE** or **Manual** from the drop-down list box. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
Protocol Number	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.

Table 75 Rule Setup: Manual

LABEL	DESCRIPTION
Local Address	The Local IP address must be static and correspond to the remote IPSec router's configured remote IP addresses.
	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.
Local Port Start	"0" is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Local Port End	Type a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If Local Port Start is left at 0, Local Port End will also remain at 0.
Remote Address Start	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote address fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.
	Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
	Enter a (static) IP address on the network behind the remote IPSec router.
Remote Address End/ Mask	When the remote IP address is a single address, type it a second time here.
	When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.
Remote Port Start	"0" is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Remote Port 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. If **Remote Port Start** is left at 0, **Remote Port End** will also remain at 0.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The Prestige assigns this additional DNS server to the Prestige's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
My IP Address	Enter the WAN IP address of your Prestige. The Prestige uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. The VPN tunnel has to be rebuilt if this IP address changes.
Secure Gateway IP Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **YES** from the drop-down menu to enable replay detection, or select **NO** to disable it.

Table 75 Rule Setup: Manual

LABEL	DESCRIPTION
IPSec Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next). Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described later).
Encryption Algorithm	Select **DES** or **3DES** from the drop-down list box. The Prestige's encryption algorithm should be identical to the secure remote gateway. When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Encryption Key (Only with ESP)	With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

17.15 Viewing SA Monitor

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

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

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

Figure 106 SA Monitor
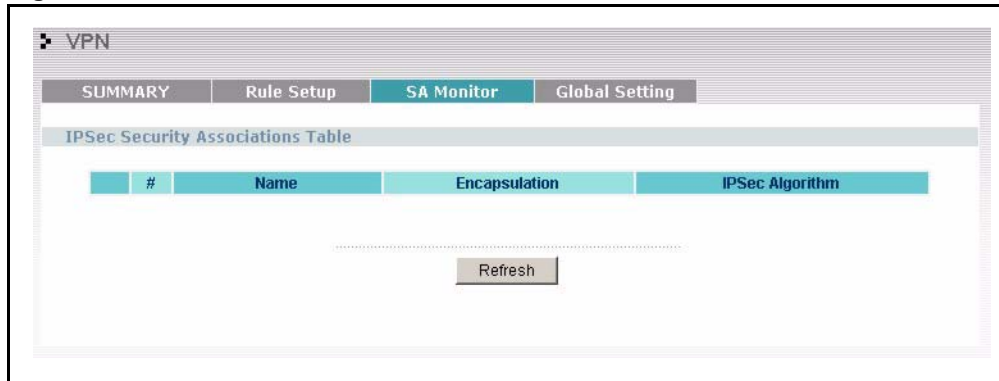
The following table describes the labels in this screen.

Table 76 SA Monitor

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays Tunnel or Transport mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase Prestige processing requirements and communications latency (delay).
Previous Page (If applicable)	Click **Previous Page** to view more items in the summary.
Refresh	Click **Refresh** to display the current active VPN connection(s).
Next Page (If applicable)	Click **Next Page** to view more items in the summary.

17.16 Configuring Global Setting

To change your Prestige's Global Settings, click **VPN**, then the **Global Setting** tab. The screen appears as shown.

Figure 107   VPN: Global Setting
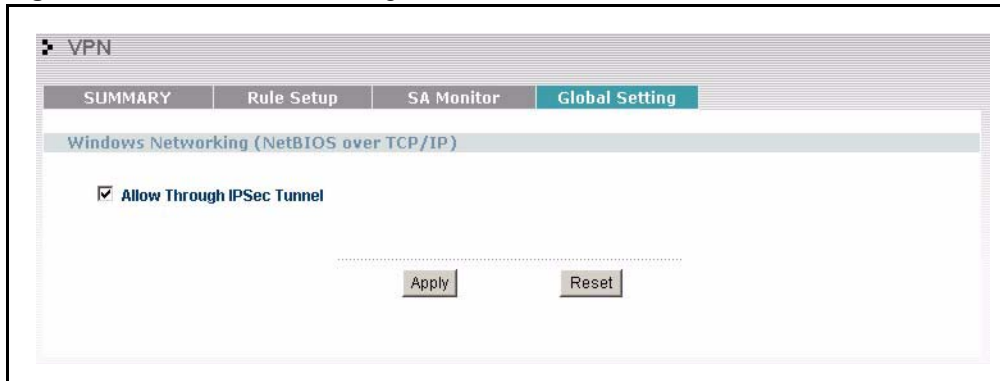
The following table describes the labels in this screen.

Table 77   VPN: Global Setting

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

17.17 Telecommuter VPN/IPSec Examples

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

17.17.1 Telecommuters Sharing One VPN Rule Example

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

Having everyone use the same pre-shared key may create a vulnerability. If the pre-shared key is compromised, all of the VPN connections using that VPN rule are at risk. A recommended alternative is to use a different VPN rule for each telecommuter and identify them by unique IDs (see *the Telecommuters Using Unique VPN Rules Example section*)..

Table 78   Telecommuter and Headquarters Configuration Example

		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 108   Telecommuters Sharing One VPN Rule Example
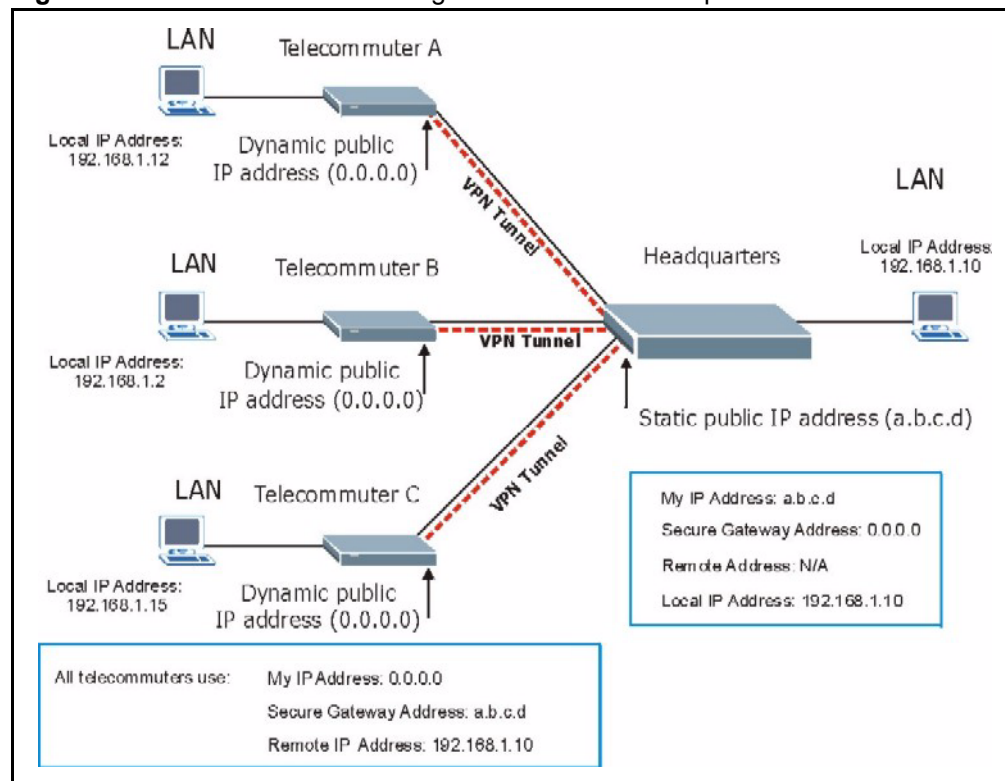
17.17.2 Telecommuters Using Unique VPN Rules Example

With aggressive negotiation mode (see *section* Negotiation Mode), the Prestige can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a Prestige at headquarters. They can use different IPSec parameters (including the pre-shared key) and the local IP addresses (or ranges of addresses) can overlap.

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

Figure 109 Telecommuters Using Unique VPN Rules Example
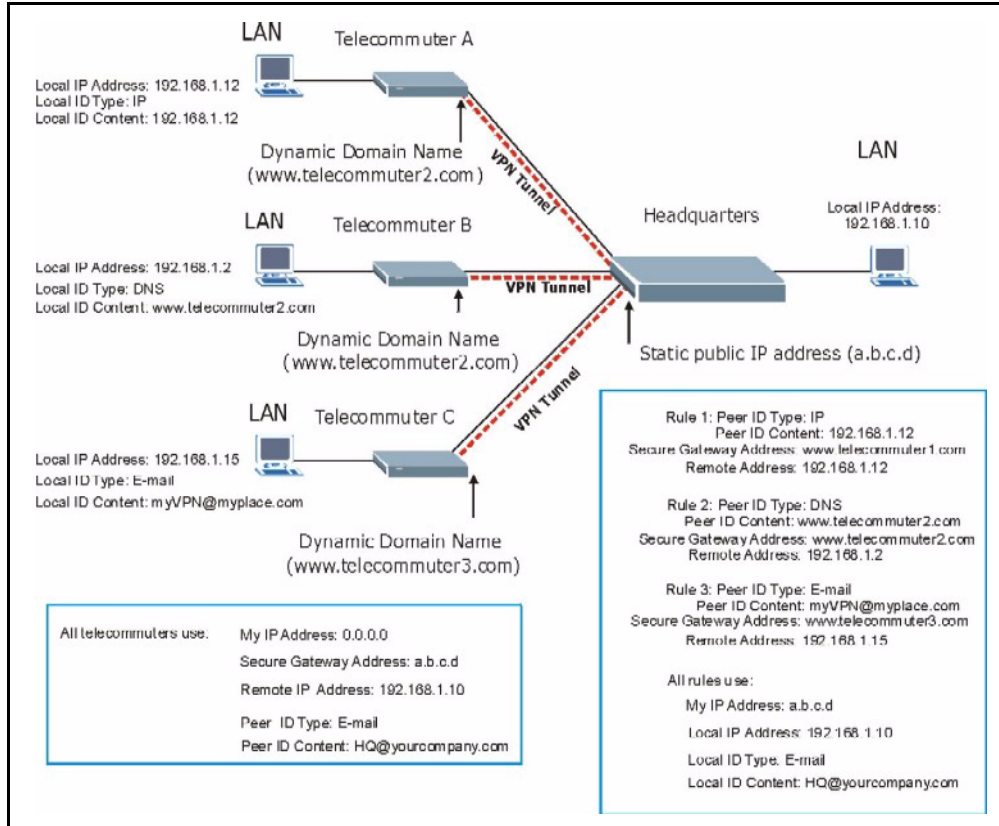
17.18 VPN and Remote Management

If a VPN tunnel uses a remote management service port (Telnet, FTP, WWW SNMP, DNS or ICMP) and terminates at the Prestige's LAN or WAN port, configure remote management (**REMOTE MGNT**) to allow access for that service.

If the VPN tunnel terminates at the Prestige's LAN IP address, configure remote management for **LAN**, **WAN** server access or **LAN & WAN**.

If the VPN tunnel terminates at the Prestige's WAN IP address, configure remote management for **WAN** server access or **LAN & WAN**.

CHAPTER 18
Centralized Logs

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

18.1 View Log

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

Click the **LOGS** 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 the Log Settings section). 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.

The following table describes the labels in this screen.

Table 79   View Logs

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see *section*) 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 Prestige'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.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**, see *section*).
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 Prestige's general log settings in one location.

Click the **LOGS** in 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 Prestige is to send logs; the schedule for when the Prestige is to send the logs and which logs and/or immediate alerts the Prestige to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

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

Figure 111 Log Settings

The following table describes the labels in this screen.

Table 80   Log Settings

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

CHAPTER 19
Print Server

This chapter discusses how to configure the print server on the Prestige.

19.1 Print Server Overview

A print server is a device or software that provides users on a network with shared access to one or more printers. The print server acts as a buffer, holding the information to be printed out in memory until the printer becomes free. Print servers can be programmed to print jobs in the order that they arrive or to give priority to particular users who, in effect, can jump the print queue. The advantages of a print server include efficient use of expensive resources, for example, laser printers. This avoids having to retry to print if the printer is initially busy.

19.2 Prestige Print Server

The Prestige has a built-in print server that allows the LAN to share a printer. There is no need to assign a dedicated computer as a print server or have a standalone print server device.

The print server supports Line Printer Remote (LPR) protocol. LPR is a cross-platform printing protocol that uses TCP/IP to establish connections between printers and computers on a network.

Each computer on the print server network must use the LPR protocol to communicate with the print server.

Print requests are sent by each computer to the Prestige. These request are placed in a queue and are then printed when the printer becomes available.

19.2.1 Installation Requirements

Use Appendix D, on page 435 in this User's Guide to set up your computer to use the Prestige print server.

To install the print server driver you will need the following requirements

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows ME, Windows NT 4.0, Windows 2000, Windows XP and Macintosh OS X
- A computer with an Ethernet port
- RJ-45 cables and a USB cable

The print server must be set up on each computer in your network that you want to use the print server. Before you set up the print server, make sure the USB printer is connected to the Prestige using the USB cable and that both the Prestige and the USB printer are turned on.

19.3 Prestige Print Server Configuration

From the **MAIN MENU** click **Print Server** to display the screen shown next.

Figure 112   Configuring Print Server Screen
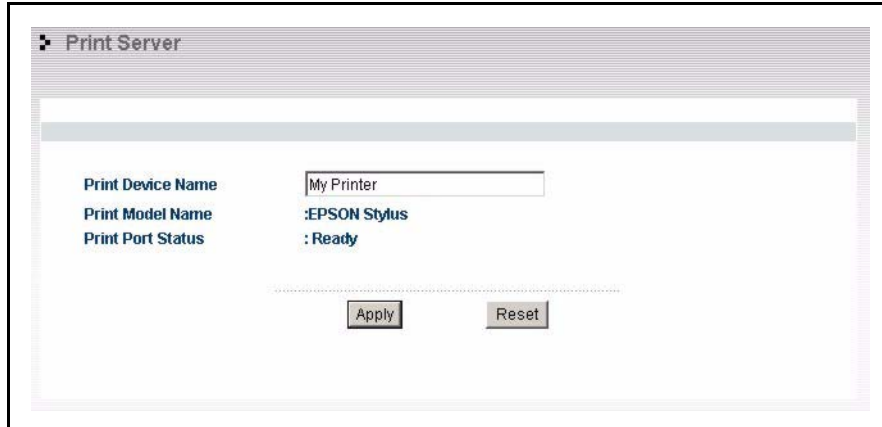
Table 81   Configuring Print Server

LABEL	DESCRIPTION
Print Device Name	Type a **Print Device Name** for recognition of the associated printer on the print server network. This name is displayed on a computer on the print server network when a print job is executed.
Print Model Name	This displays the model name of the printer currently associated to the Prestige print server.
Print Port Status	This field displays the print server status on the Prestige **Ready**: The print server has established a TCP/IP connection with a printer, is online and ready to print. **Printing**: A computer on the print server network is executed a print job. **PaperOut**: The printer loading tray has no paper to perform the printing job **Offline**: The computers in the print server network cannot use the print server. See the Appendix for troubleshooting the **Print Port Status**.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to configure the **Print Device Name** afresh.

C HAPTER 20
Media Bandwidth Management

This chapter contains information about configuring media bandwidth management, editing rules and viewing the Prestige's media bandwidth management logs.

20.1 Media Bandwidth Management Overview

ZyXEL's Media Bandwidth Management allows you to specify bandwidth management rules based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth rules.

The Prestige applies bandwidth management to traffic that it forwards out through an interface. The Prestige does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router, regardless of the traffic's source.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the Prestige and be managed by bandwidth management.

- The sum of the bandwidth allotments that apply to the WAN interface (WAN to LAN, LAN to WAN, WAN to WAN / Prestige) must be less than or equal to the **WAN BW Budget** that you configure in the **Media Bandwidth Management Configuration** screen.
- The sum of the bandwidth allotments that apply to the LAN port (LAN to WAN, WAN to LAN, LAN to LAN / Prestige) must be less than or equal to 100,000 kbps (you cannot configure the bandwidth budget for the LAN port).
- The sum of the bandwidth allotments that apply to the WLAN port (WLAN to WAN, WAN to WLAN, WLAN to WLAN / Prestige) must be less than or equal to 54,000 kbps (you cannot configure the bandwidth budget for the WLAN port).

20.1.1 Application-based Bandwidth Management Example

The bandwidth rules in the following example are based solely on application. Each bandwidth rule (VoIP, Web, FTP, E-mail and Video) is allotted 128 Kbps.

Figure 113   Application-based Bandwidth Management Example
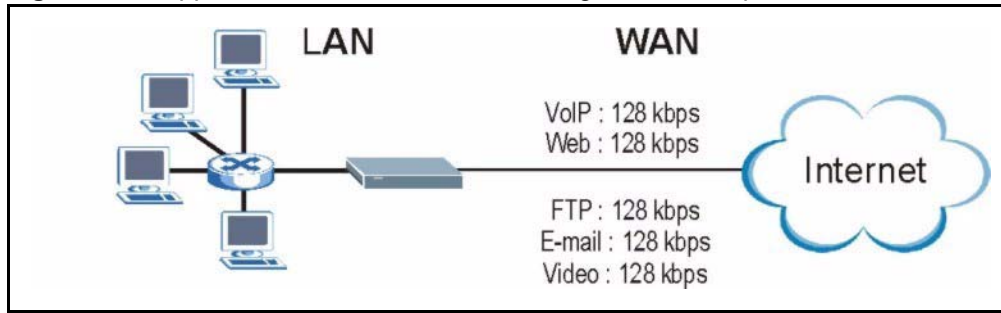
20.1.2 Subnet-based Bandwidth Management Example

The following example uses bandwidth rules based solely on LAN subnets. Each bandwidth rule (Subnet A and Subnet B) is allotted 320 Kbps.

Figure 114   Subnet-based Bandwidth Management Example
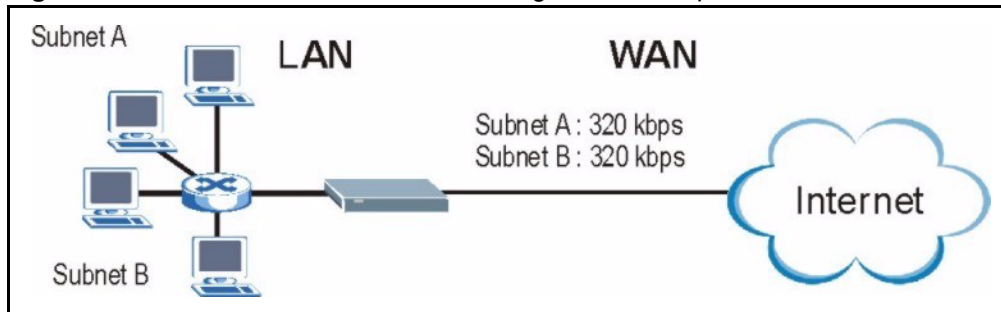
20.1.3 Application and Subnet-based Bandwidth Management Example

The following example uses bandwidth rules based on LAN subnets and applications (specific applications in each subnet are allotted bandwidth).

Figure 115   Application and Subnet-based Bandwidth Management Example
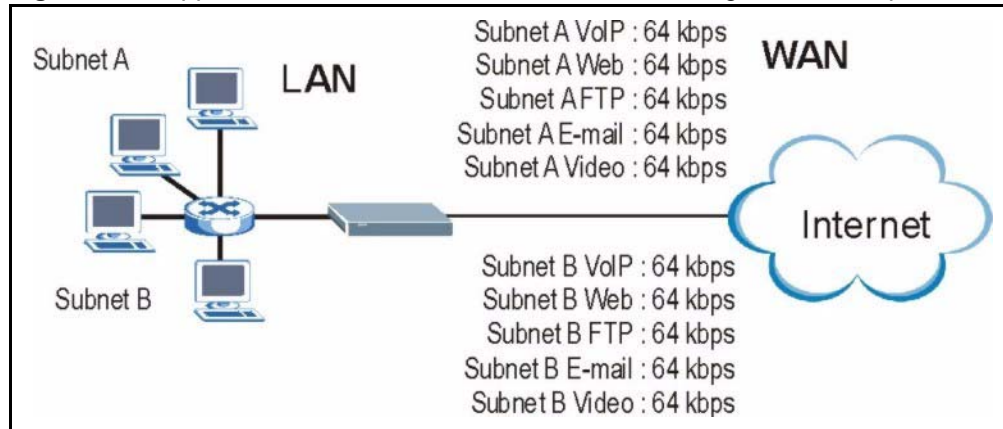
Table 82   Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

20.1.4 Bandwidth Usage Example

Here is an example of a Prestige that has bandwidth usage enabled on an interface. The first figure shows each bandwidth rule's bandwidth budget. The rules are set up based on subnets. The interface is set to 320 Kbps. Each subnet is allocated 64 Kbps. The unbudgeted 64 Kbps allows traffic that does not match a bandwidth management rule to go out when you do not select the **Use All Managed Bandwidth** option.

Figure 116 Bandwidth Usage Example
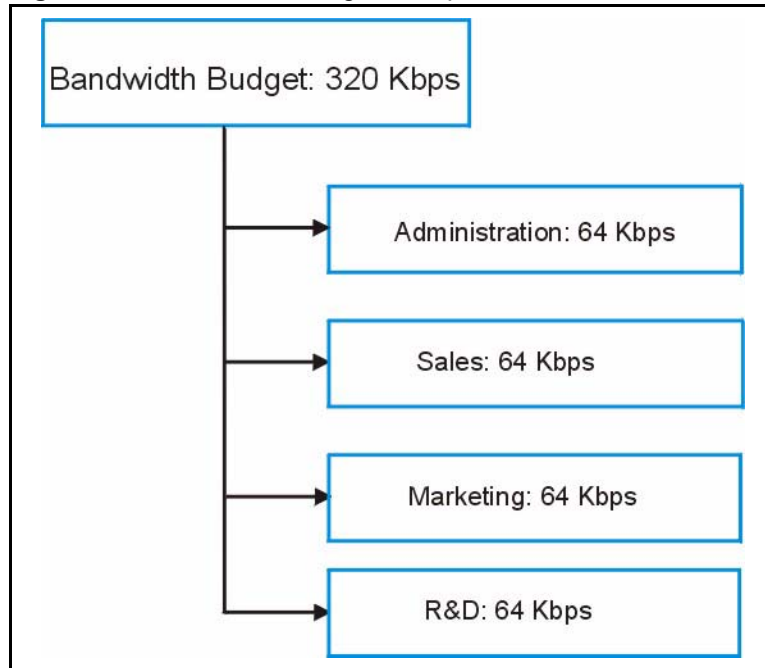
The following figure shows the bandwidth usage with the maximize bandwidth usage option enabled. The Prestige divides up the unbudgeted 64 Kbps among the rules that require more bandwidth. If the administration department only uses 32 Kbps of the budgeted 64 Kbps, the Prestige also divides the remaining 32 Kbps among the rules that require more bandwidth. Therefore, the Prestige divides a total of 96 Kbps total of unbudgeted and unused bandwidth among the rules that require more bandwidth.

In this case, suppose that all of the rules except for the administration rule need more bandwidth.

• Each rule gets up to its budgeted bandwidth. The administration rule only uses 32 Kbps of its budgeted 64 Kbps.
• Sales and Marketing are first to get extra bandwidth because they have the highest priority. If they each require 48 Kbps or more of extra bandwidth, the Prestige divides the total 96 Kbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (48 Kbps extra to each for a total of 112 Kbps for each) because they both have the highest priority level.
• R&D requires more bandwidth but only gets its budgeted 64 Kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing rules.
• The Prestige does not send any traffic that is not defined in the bandwidth filters because all of the unbudgeted bandwidth goes to the rules that need it.

Figure 117 Maximize Bandwidth Usage Example
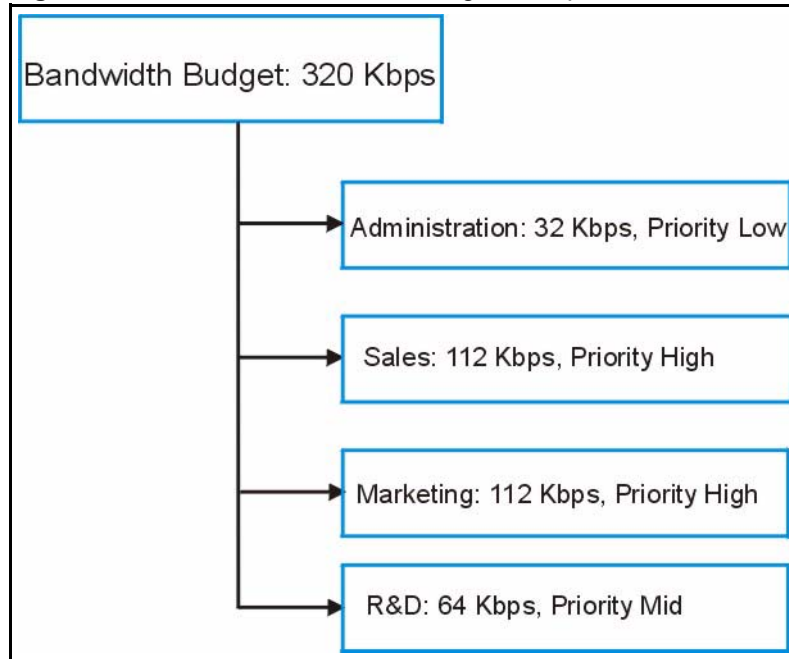
20.1.5 Bandwidth Management Priorities

The following table describes the priorities that you can apply to traffic that the Prestige forwards out through an interface.

Table 83 Media Mandwidth Management Priorities

PRIORITY LEVELS: TRAFFIC WITH A HIGHER PRIORITY GETS THROUGH FASTER WHILE TRAFFIC WITH A LOWER PRIORITY IS DROPPED IF THE NETWORK IS CONGESTED.	
High	Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).
Mid	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Low	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.

20.1.6 Bandwidth Management Services

The following is a description of the services that you can select and apply media bandwidth management to in **BW Setup**.

20.1.6.1 Xbox Live

This is Microsoft's gaming service that lets you play multiplayer Xbox games on the Internet via broadband technology. Xbox Live uses port 3074.

20.1.6.2 VoIP (SIP)

Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.

20.1.6.3 FTP

File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.

20.1.6.4 E-Mail

Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail:

POP3 - port 110

IMAP - port 143

SMTP - port 25

HTTP - port 80

20.1.6.5 eMule/eDonkey

These programs use advanced file sharing applications relying on central servers to search for files. They use default port 4662.

20.1.6.6 WWW

The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.

20.1.7 Services

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

Table 84 Commonly Used Services

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

Table 84 Commonly Used Services

SERVICE	DESCRIPTION
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.
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.

20.2 Media Bandwidth Management Configuration Screen

Click **ADVANCED** and then **BW MGMT** to open the media bandwidth management **Configuration** screen.

Figure 118   Bandwidth Management Configuration

The following table describes the labels in this screen.

Table 85 Bandwidth Management Configuration

LABEL	DESCRIPTION
Active	Select this check box to have the Prestige apply bandwidth management. Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. Enabling bandwidth management also allows you to control the maximum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.
WAN BW Budget (kbps)	Enter the amount of bandwidth in kbps (2 to 100,000) that you want to allocate for traffic. 20 kbps to 20,000 kbps is recommended. The recommendation is to set this speed to be equal to or less than the speed of the broadband device connected to the WAN port. For example, set the speed to 1000 Kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1000 Kbps.
#	This is the number of an individual bandwidth management rule.
Direction	Select **To LAN** to apply bandwidth management to traffic that the Prestige forwards to the LAN. Select **To WAN** to apply bandwidth management to traffic that the Prestige forwards to the WAN. Select **To WLAN** to apply bandwidth management to traffic that the Prestige forwards to the WLAN.
Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
Service	Select a service for your rule or you can define your own in the **Edit** screen.
Dest Port	Enter the port number of the destination. See Table 84 for a list of services and port numbers.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**.
Edit	Select a rule index number's radio button and then click **Edit** to set up this bandwidth management rule on the Prestige.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

20.3 Editing Bandwidth Management Rules

Use the **Bandwidth Management Configuration Edit** screen to configure a bandwidth management rule. Use bandwidth rules to allocate specific amounts of bandwidth capacity (bandwidth budgets) to specific applications and/or subnets.

20.3.1 Bandwidth Borrowing

Enable bandwidth borrowing by selecting **Use All Managed Bandwidth** on a rule to allow the rule to use any unused bandwidth. Unused bandwidth is given to the highest priority rule first.

20.4 Configuring Bandwidth Management Rules and Services

Select a radio button for a rule and then click **Edit** to open the **Bandwidth Management Configuration Edit** screen.

Figure 119   Bandwidth Management Edit

The following table describes the labels in this screen.

Table 86   Bandwidth Management Edit

LABEL	DESCRIPTION
Active	Select this check box to have the Prestige apply this bandwidth management rule. Enable a bandwidth management rule to give traffic that matches the rule priority over traffic that does not match the rule.
Rule Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
BW Budget	Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**. The higher the number, the higher the priority.

Table 86 Bandwidth Management Edit

LABEL	DESCRIPTION
Use All Managed Bandwidth	Select this option to allow a rule to borrow unused bandwidth on the interface.
	Bandwidth borrowing is governed by the priority of the rules. That is, a rule with the highest priority is the first to borrow bandwidth. Do not select this if you want to leave bandwidth available for other traffic types or if you want to restrict the amount of bandwidth that can be used for the traffic that matches this rule.
Service	Select a service for your rule or you can define your own.
Destination Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Netmask	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 Table 84 for a list of common services and port numbers.
Source Address	Enter the source IP address in dotted decimal notation.
Source Subnet Netmask	Enter the destination 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 for some common services and port numbers.
Protocol	Enter the protocol (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.
Delete	Click **Delete** to remove a rule configuration.

20.5 Monitor Screen

Select the **Monitor** tab in **BW MGMT** to view the bandwidth usage of the LAN, WAN and WLAN configured bandwidth rules. This is also shown as bandwidth usage over the bandwidth budget for each rule. The gray section of the bar represents the percentage of unused bandwidth and the orange color represents the percentage of bandwidth in use.

Figure 120 Bandwidth Management Monitor

C HAPTER 21
Maintenance

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

21.1 Maintenance Overview

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

21.2 Status Screen

Click **MAINTENANCE** to open the **Status** screen, which you can use to monitor your Prestige. Note that these fields are READ-ONLY and only for diagnostic purposes.

Figure 121 Maintenance Status

The following table describes the labels in this screen.

Table 87 Maintenance Status

LABEL	DESCRIPTION
System Name	This is the **System Name** you chose in the first Internet Access Wizard screen. It is for identification purposes
Model Name	The model name identifies your device type. The model name should also be on a sticker on your Prestige. If you are uploading firmware, be sure to upload firmware for this exact model name. This field is not available on all models.
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Routing Protocols	This shows the routing protocol - **IP** for which the Prestige is configured. This field is not configurable in all Prestige router models.
WAN Port	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - **Client** or **None**.
LAN Port	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role - **Server**, **Relay** or **None**.
Show Statistics	Click **Show Statistics** to display the real-time system statistics. Refer to *Section* for more information.

21.2.1 System Statistics

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

Figure 122   Maintenance System Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M/Full	2298	2689	0	0	0	2:12:47
WAN	Down	0	0	0	0	0	00:00:00
WLAN	G+	345	0	0	0	0	2:12:47

System Up Time : 2:12:54

Poll Interval(s) : 5   Set Interval   Stop

The following table describes the labels in this screen.

Table 88   Maintenance System Statistics

LABEL	DESCRIPTION
Port	This is the WAN, LAN or WLAN port.
Status	This displays 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	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the Prestige has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics, click **Stop**.

21.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

Figure 123   Maintenance DHCP Table

The following table describes the labels in this screen.

Table 89   Maintenance DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field.
	Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this check box to have the Prestige always assign this IP address to this MAC address (and host name).
Apply	Click **Apply** to have the MAC address and IP address also display in the **LAN Static DHCP** screen (where you can edit them).
Refresh	Click **Refresh** to renew the screen.

21.4 Any IP Table

Click **MAINTENANCE**, **Any IP Table**. The Any IP table shows current read-only information (including the IP address and the MAC address) of all network devices that use the Any IP feature to communicate with the Prestige.

Figure 124   Maintenance Any IP

The following table describes the labels in this screen.

Table 90   Maintenance Any IP

LABEL	DESCRIPTION
#	This field displays the index number.
IP Address	This field displays the IP address of the network device.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed IP address. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click **Refresh** to update this screen.

21.5 Association List

View the wireless stations that are currently associated to the Prestige in the **Association List** screen.

Figure 125 Maintenance Association List

The following table describes the labels in this screen.

Table 91 Maintenance Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the Prestige.
Refresh	Click **Refresh** to redisplay the current screen.

21.6 F/W Upload Screen

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

Click **MAINTENANCE**, and then the **F/W Upload** tab. Follow the instructions in this screen
to upload firmware to your Prestige.

Figure 126 Maintenance Firmware Upload

The following table describes the labels in this screen.

Table 92 Maintenance Firmware Upload

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

> **Note:** Do not turn off the Prestige while firmware upload is in progress!

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

Figure 127 Upload Warning
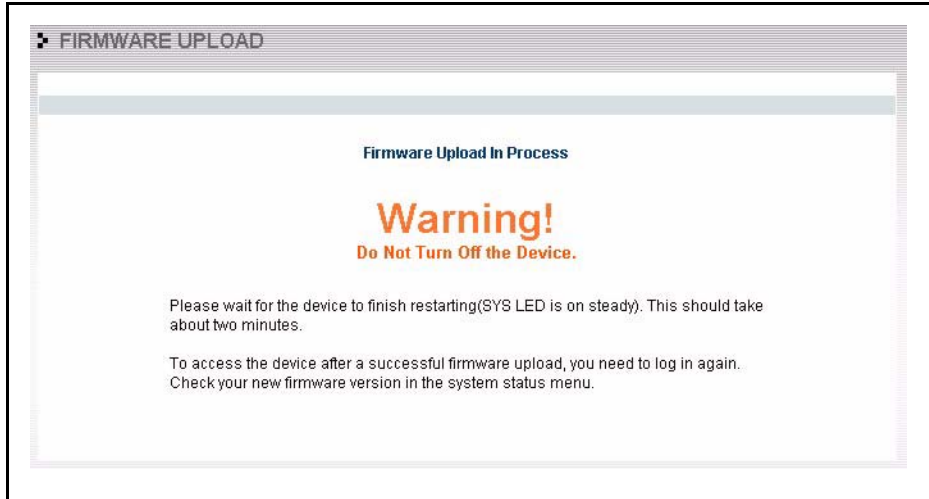
The Prestige automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 128 Network Temporarily Disconnected
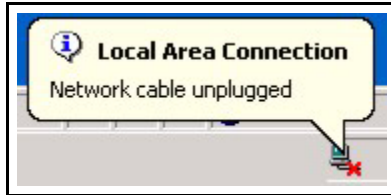
After two minutes, log in again and check your new firmware version in the **System Status** screen.

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

Figure 129   Upload Error Message
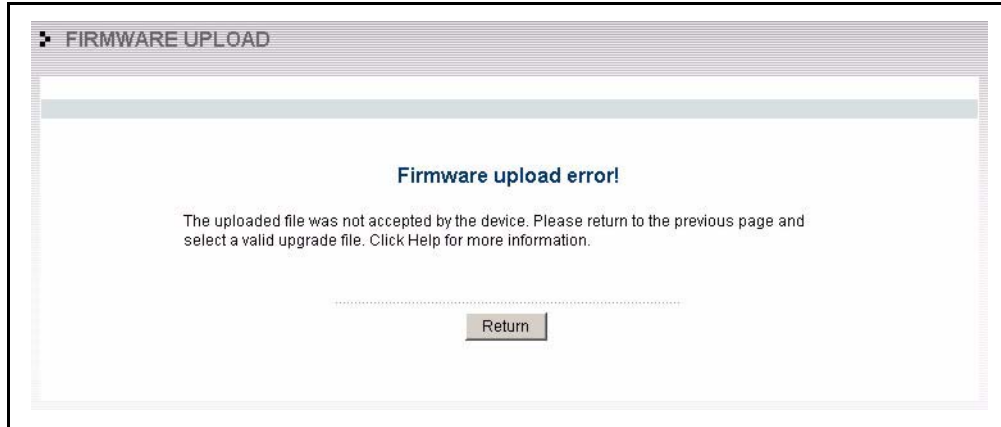
21.7 Configuration Screen

See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

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

Figure 130   Maintenance Configuration

21.7.1 Backup Configuration

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

Click **Backup** to save the Prestige's current configuration to your computer

21.7.2 Restore Configuration

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

Table 93   Maintenance Restore Configuration

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

> **Note:** Do not turn off the Prestige while configuration file upload is in progress

After you see a "configuration upload successful" screen, you must then wait one minute before logging into the Prestige again.

Figure 131   Configuration Restore Successful
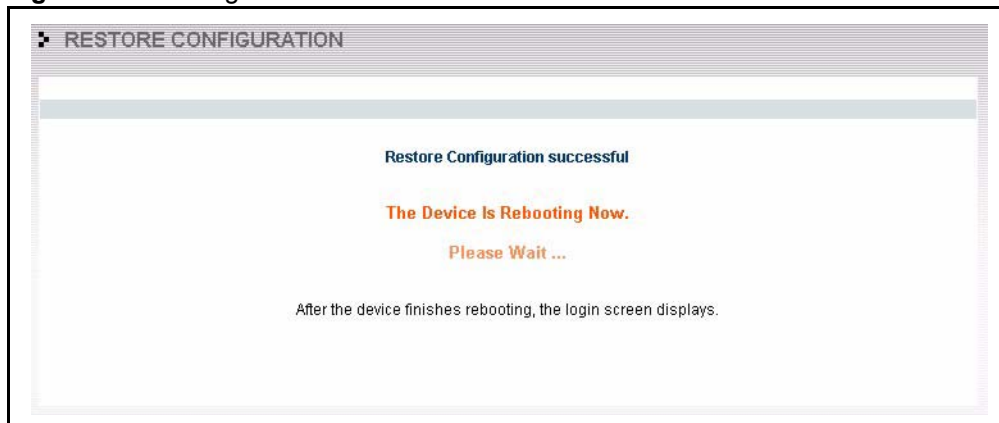
The Prestige automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 132   Temporarily Disconnected
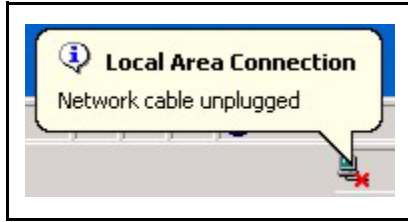
If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default Prestige IP address (192.168.1.1). See your *Quick Start Guide* for details on how to set up your computer's IP address.

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

Figure 133   Configuration Restore Error
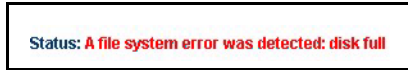
21.7.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the Prestige to its factory defaults.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your Prestige. Refer to the *Introducing the Web Configurator* chapter for more information on the **RESET** button.

21.8 Restart Screen

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

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the Prestige reboot. This does not affect the Prestige's configuration.

Figure 134 System Restart
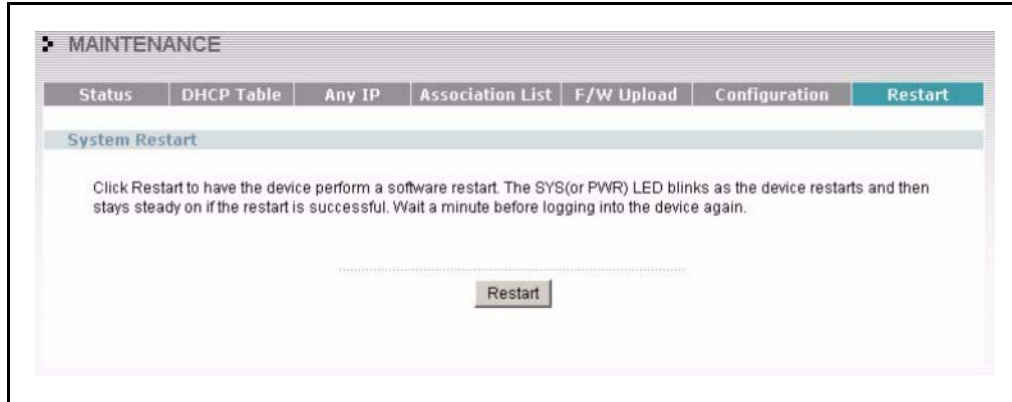
CHAPTER 22
Introducing the SMT

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

22.1 SMT Introduction

The Prestige's SMT (System Management Terminal) is a menu-driven interface that you can access over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus, how to navigate the SMT and how to configure SMT menus.

22.1.1 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your Prestige.

1 In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**.

2 Enter "1234" in the **Password** field.

3 After entering the password you will see the main menu.

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

22.1.2 Entering Password

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

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

Please note that if there is no activity for longer than five minutes after you log in, your Prestige will automatically log you out.

Figure 135 Login Screen

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

22.1.3 Prestige SMT Menu Overview

The following figure gives you an overview of the various SMT menu screens of your Prestige.

Figure 136 SMT Menu Overview

22.2 Navigating the SMT Interface

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

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

Table 94   Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, and then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?\> or **ChangeMe**	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with **ChangeMe** must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

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

Figure 137 SMT Main Menu

```
              Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

                        P-335/P-335WT 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
                                              26. Schedule Setup
                                              27. VPN/IPSec Setup
      Advanced Applications
        11. Remote Node Setup
        12. Static Routing Setup
        15. NAT Setup
                                                       99. Exit
               Enter Menu Selection Number:
```

22.2.1 System Management Terminal Interface Summary

The following table describes the fields in the previous screen.

Table 95 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN.
3	LAN Setup	Use this menu to set up your LAN and WLAN connection.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Use this menu to set up static routes.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	Use this menu to configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN/ IPSec Setup	Use this menu to configure VPN connections.
99	Exit	Use this to exit from SMT and return to a blank screen.

22.3 Changing the System Password

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

1 Enter 23 in the main menu to display **Menu 23 - System Security** as shown next.

Figure 138   Menu 23: System Security

```
        Menu 23 - System Security
        1.   Change Password
        2.   RADIUS Server

        4.   IEEE802.1x
```

2 Enter 23.1 in the main menu to display **Menu 23.1 - System Security - Change Password.**

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

Figure 139   Menu 23 System Password

```
        Menu 23.1 - System Security - Change Password

                  Old Password= ?
                  New Password= ?
                  Retype to confirm= ?
        Enter here to CONFIRM or ESC to CANCEL:
```

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

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

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

Chapter 22 Introducing the SMT

C HAPTER 23
Menu 1 General Setup

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

23.1 General Setup

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

In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the Prestige **System Name**.

In Windows 2000 click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the Prestige **System Name**.

In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

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

23.2 Procedure To Configure Menu 1

1 Enter 1 in the Main Menu to open **Menu 1 — General Setup** (shown next)

Figure 140 Menu 1 General Setup.

```
         Menu 1 - General Setup

                System Name= P-335/P-335WT
                Domain Name=

                First System DNS Server= From ISP
                  IP Address= N/A
                Second System DNS Server= From ISP
                  IP Address= N/A
                Third System DNS Server= From ISP
                  IP Address= N/A
                Edit Dynamic DNS= No


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

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

Table 96 Menu 1 General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
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.
	The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].
First System DNS Server Second System DNS Server Third System DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The Prestige uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
	Press [SPACE BAR] and then [ENTER] to select an option. Select **From ISP** if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The **IP Address** field below displays the (read-only) DNS server IP address that the ISP assigns.
	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the **IP Address** field. If you select **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you save your changes. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you save your changes.
	Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

23.2.1 Procedure to Configure Dynamic DNS

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

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

Figure 141   Menu 1.1 Configure Dynamic DNS

```
            Menu 1.1 - Configure Dynamic DNS

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


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

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

Table 97   Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.
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.
Host 1- 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.
User	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcards	Your Prestige 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.

Table 97 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION
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, http://www.dyndns.org/ traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).
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 Prestige's WAN IP address.	
DDNS does not work with a private IP address. When both fields are set to **No**, the Prestige 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 Prestige uses or is behind. You can set this field to **Yes** whether the IP address is public or private, static or dynamic.
User Specified IP Address	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 Prestige uses or is behind a static public IP address.
IP Address	Enter the static public IP address if you select **Yes** in the **User Specified IP Addr** field.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

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

CHAPTER 24
Menu 2 WAN Setup

This chapter describes how to configure the WAN using menu 2.

24.1 Introduction to WAN

This chapter explains how to configure settings for your WAN port.

24.2 WAN Setup

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

Figure 142   Menu 2 WAN Setup

```
            Menu 2 - WAN Setup

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

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

The following table describes the fields in this menu.

Table 98   Menu 2 WAN Setup

FIELD	DESCRIPTION
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 computer whose IP you give in the following field.
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.
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 25
Menu 3 LAN Setup

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

25.1 LAN Setup

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

Figure 143   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:
```

25.1.1 General Ethernet Setup

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

Figure 144   Menu 3.1 LAN Port Filter Setup.

```
              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:
```

If you need to define filters, please read Chapter 31, "Filter Configuration," on page 335 first, then return to this menu to define the filter sets.

25.2 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- For TCP/IP Ethernet setup refer to the *Internet Access Application* chapter.
- For bridging Ethernet setup refer to the *Bridging Setup* chapter.

25.3 TCP/IP Ethernet Setup and DHCP

Use menu 3.2 to configure your Prestige for TCP/IP.

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

Figure 145   Menu 3.2 TCP/IP and DHCP Ethernet Setup

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

   DHCP= Server                         TCP/IP Setup:
   Client IP Pool:
     Starting Address= 192.168.1.33     IP Address= 192.168.1.1
     Size of Client IP Pool= 32         IP Subnet Mask= 255.255.255.0
   First DNS Server= From ISP           RIP Direction= Both
     IP Address= N/A                      Version= RIP-1
   Second DNS Server= From ISP          Multicast= None
     IP Address= N/A                    Edit IP Alias= No
   Third DNS Server= DNS Relay
     IP Address= N/A
   DHCP Server Address= N/A

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

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

Table 99   DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
DHCP	This field enables/disables the DHCP server.
	If set to **Server**, your Prestige will act as a DHCP server.
	If set to **None**, the DHCP server will be disabled.
	If set to **Relay** the Prestige 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:
Client IP Pools	
Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.

Table 99 DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.
First DNS Server Second DNS Server Third DNS Server	The Prestige passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. Select **From ISP** if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The **IP Address** field below displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the **IP Address** field below. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you save your changes. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you save your changes. Select **DNS Relay** to have the Prestige act as a DNS proxy. The Prestige's LAN IP address displays in the **IP Address** field below (read-only). The Prestige tells the DHCP clients on the LAN that the Prestige itself is the DNS server. When a computer on the LAN sends a DNS query to the Prestige, the Prestige forwards the query to the Prestige's system DNS server (configured in menu 1) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to **None** after you save your changes. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
DHCP Server Address	If **Relay** is selected in the **DHCP** field above, then type the IP address of the actual, remote DHCP server here.

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

Table 100 Menu 3.2: LAN TCP/IP Setup Fields

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

25.3.1 IP Alias Setup

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

Figure 146 Physical Network & Partitioned Logical Networks
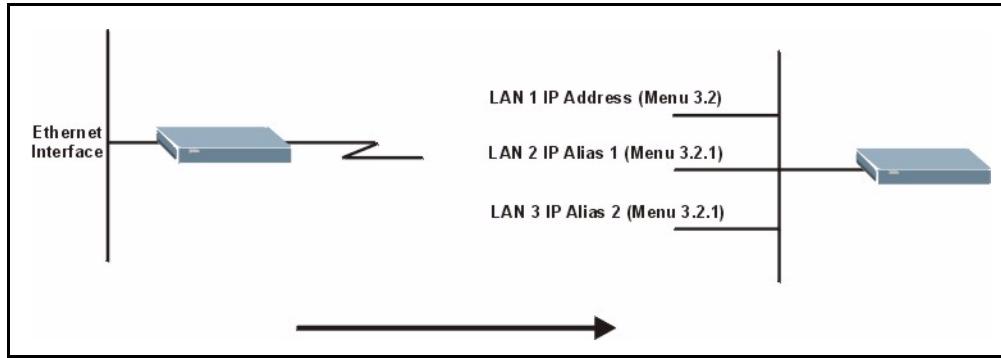
You must use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

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

Figure 147 Menu 3.2.1: IP Alias Setup

```
            Menu 3.2.1 - IP Alias Setup

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


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

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

Table 101 Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1, 2	Choose **Yes** to configure the LAN network for the Prestige.
IP Address	Enter the IP address of your Prestige in dotted decimal notation.

Table 101   Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION
IP Subnet Mask	Your Prestige 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 Prestige.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only, Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.
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.	

25.4 Wireless LAN Setup (P-335WT only)

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

Figure 148 Menu 3.5 Wireless LAN Setup

```
                 Menu 3.5 - Wireless LAN Setup

                 ESSID= Wireless
                 Hide ESSID= No
                 Channel ID= CH06 2437MHz
                 RTS Threshold= 2432
                 Frag. Threshold= 2432
                 WEP Encryption= Disable
                   Default Key= N/A
                   Key1= N/A
                   Key2= N/A
                   Key3= N/A
                   Key4= N/A
                   Authen. Method= N/A
                 Edit MAC Address Filter= No
                 Edit Roaming Configuration= No
                 Preamble= Long
                   802.11 Mode= Mixed

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

The following table describes the fields in this menu.

Table 102 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
ESSID	The ESSID (Extended Service Set IDentity) identifies the AP to which the wireless stations associate. Wireless stations associating to the AP must have the same ESSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters.
Hide ESSID	Press [SPACE BAR] and select **Yes** to hide the ESSID in the outgoing data frame so an intruder cannot obtain the ESSID through passive scanning.
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.
Fragment Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
WEP	Select **Disable** to allow wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Default Key	Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the Prestige and the wireless stations to communicate.

Table 102 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Prestige and the wireless stations must use the same WEP key for data transmission.
	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").
	If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
	Note: Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key
Authen. Method	Press [SPACE BAR] to select **Auto**, **Open System Only** or **Shared Key Only** and press [ENTER].
	This field is **N/A** if WEP is not activated.
	If WEP encryption is activated, the default setting is **Auto**.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** and **Auto**. The default setting is **Auto**.
	See the section on preamble for more information.
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.	

25.4.1 Configuring MAC Address Filter

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

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

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

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

Figure 149   Menu 3.5 Wireless LAN Setup

```
                    Menu 3.5 - Wireless LAN Setup

  ESSID= ZyXEL
  Hide ESSID= No
  Channel ID= CH06 2437MHz                 Edit MAC Address Filter= No
  RTS Threshold= 4096                      Edit Roaming Configuration= No
  Frag. Threshold= 4096
  WEP Encryption= 64-bit WEP               Preamble= Long
    Default Key= 1                         802.11 Mode= Mixed
    Key1= ********
    Key2= ********
    Key3= ********
    Key4= ********
    Authen. Method= Auto

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

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

Figure 150 Menu 3.5.1 WLAN MAC Address Filter

```
      Menu 3.5.1 - WLAN MAC Address Filter
                Active= No
                Filter Action= Allowed Association
 ------------------------------------------------------------------------------
   1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
   2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
   3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
   4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
   5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
   6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
   7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
   8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
   9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
  10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
  11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
  12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
 ------------------------------------------------------------------------------
               Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 103 Menu 3.5.1 WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table.
	To deny access to the Prestige, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router.
	The default action, **Allowed Association**, permits association with the Prestige. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
1..32	Type the MAC address of the of the client computers that are allowed or denied access to the Prestige in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
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.	

25.4.2 Configuring Roaming on the Prestige

Enable the roaming feature if you have two or more Prestige's on the same subnet. Follow the steps below to allow roaming on your Prestige.

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

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

Figure 151 Menu 3.5 Wireless LAN Setup

```
              Menu 3.5 - Wireless LAN Setup
               ESSID= Wireless
               Hide ESSID= No
               Channel ID= CH06 2437MHz
               RTS Threshold= 2432
               Frag. Threshold= 2432
               WEP Encryption= Disable
                 Default Key= N/A
                 Key1= N/A
                 Key2= N/A
                 Key3= N/A
                 Key4= N/A
                 Authen. Method= N/A
               Edit MAC Address Filter= No
               Edit Roaming Configuration = No
                 Preamble= Long
              Press ENTER to Confirm or ESC to Cancel:
```

3 Move the cursor to the **Edit Roaming Configuration** field. Press [SPACE BAR] to select **Yes** and then press [ENTER]. **Menu 3.5.2 – Roaming Configuration** displays as shown next.

Figure 152 Menu 3.5.2 Roaming Configuration

```
              Menu 3.5.2 - Roaming Configuration
                Active= Yes
                Port #= 3517
              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 104 Roaming Configuration

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable roaming on the Prestige if you have two or more Prestige's on the same subnet.
Port #	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is **3517**. Make sure this port is not used by other services.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

CHAPTER 26
Internet Access

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

26.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your Prestige to access the Internet. There are 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.

26.2 Ethernet Encapsulation

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

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

Figure 153 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
                    Retype to Confirm= N/A
                    Login Server= N/A
                    Relogin Every (min)=  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:
```

The following table describes the fields in this menu.

Table 105 Internet Access Setup (Ethernet

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

Table 105 Internet Access Setup (Ethernet (continued)

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), **RR-Telstra** or **Telia Login**. 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	Type your password again for confirmation.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Login Server	The Prestige 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.
Relogin Every (min)	This field is available when you select **Telia Login** in the **Service Type** field. The Telia server logs the Prestige out if the Prestige does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the Prestige to wait between logins.
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	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT. Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature.
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.	

26.3 Configuring the PPTP Client

> **Note:** The Prestige supports only one PPTP server connection at any given time

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.

Figure 154   Internet Access Setup (PPTP)

```
            Menu 4 - Internet Access Setup
                   ISP's Name= MyISP
                   Encapsulation= PPTP
                     Service Type= N/A
                     My Login=
                     My Password= ********
                     Retype to Confirm= ********
                     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:
```

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

Table 106   New Fields in Menu 4 (PPTP) Screen

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

26.4 Configuring the PPPoE Client

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

Figure 155   Internet Access Setup (PPPoE)

```
             Menu 4 - Internet Access Setup
                    ISP's Name= MyISP
                    Encapsulation= PPPoE
                      Service Type= N/A
                      My Login=
                      My Password= ********
                      Retype to Confirm= ********
                      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:
```

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

Table 107   New Fields in Menu 4 (PPPoE) screen

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

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.

26.5 Basic Setup Complete

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

> **Note:** 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 Prestige embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the chapters on firewall for more information on the firewall.

CHAPTER 27
Remote Node Configuration

This chapter covers remote node configuration.

27.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 Remote Node Profile**, **Menu 11.3 - Remote Node Network Layer Options**, **Menu 11.5 - Remote Node Filter** and **Menu 11.6 - Traffic Redirect Setup**.

27.2 Remote Node Profile Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Profile** (shown below).

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

27.2.1 Ethernet Encapsulation

There are two variations of menu 11 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.

Figure 156   Menu 11.1 Remote Node Profile for Ethernet Encapsulation

```
                     Menu 11.1 - Remote Node Profile
  Rem Node Name= MyISP                    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                     Edit Traffic Redirect= No
    Retype to Confirm= N/A
    Server= N/A
    Relogin Every (min)=  N/A
                  Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 108   Menu 11.1 Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node).
Encapsulation	**Ethernet** is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to **PPPoE** or **PPTP** encapsulation.
Service Type	Press [SPACE BAR] and then [ENTER] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Outgoing	
My Login	This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the Prestige calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server.
My Password	Enter the password assigned by your ISP when the Prestige calls this remote node. Valid for **PPPoE** encapsulation only.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
Server	This field is valid only when **RoadRunner** is selected in the **Service Type** field. The Prestige 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.
Relogin Every (min)	This field is available when you select **Telia Login** in the **Service Type** field. The Telia server logs the Prestige out if the Prestige does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the Prestige to wait between logins.
Route	This field refers to the protocol that will be routed by your Prestige – IP is the only option for the Prestige.
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.3 - Remote Node Network Layer Options**.

Table 108 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION
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.
Edit Traffic Redirect	Press [SPACE BAR] to select **Yes** or **No**. Select **Yes** and press [ENTER] to configure **Menu 11.6 Traffic Redirect Setup**. Select **No** (default) if you do not want to configure this feature.
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.	

27.2.2 PPPoE Encapsulation

The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the Prestige 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 appendix for more information on PPPoE.

Figure 157 Menu 11.1 Remote Node Profile for PPPoE Encapsulation

```
                    Menu 11.1 - Remote Node Profile
  Rem Node Name= MyISP                 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
    Retype to Confirm= ********
    Authen= CHAP/PAP

                                       Session Options:
                                         Edit Filter Sets= No
                                         Idle Timeout(sec)= 100
                                       Edit Traffic Redirect= No
              Press ENTER to Confirm or ESC to Cancel:
```

27.2.2.1 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.

27.2.2.2 Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The Prestige does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the Prestige 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 108 .

Table 109 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION
Service Name	If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: • **CHAP/PAP** - Your Prestige will accept either **CHAP** or **PAP** when requested by this remote node. • **CHAP**- accept CHAP only. • **PAP**- accept PAP only.
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.
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).
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.
Session Options	
Idle Timeout	Type the length of idle time (when there is no traffic from the Prestige to the remote node) in seconds that can elapse before the Prestige automatically disconnects the PPPoE connection. This option only applies when the Prestige initiates the call.

27.2.3 PPTP Encapsulation

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

Figure 158   Menu 11.1 Remote Node Profile for PPTP Encapsulation

```
                     Menu 11.1 - Remote Node Profile
    Rem Node Name= MyISP                    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 Connection= No
      Retype to Confirm= ********
      Authen= CHAP/PAP
    PPTP:                                   Session Options:
      My IP Addr=                             Edit Filter Sets= No
      My IP Mask=                             Idle Timeout(sec)= 100
      Server IP Addr=
      Connection ID/Name=                   Edit Traffic Redirect= No

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

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

Table 110   Menu 11.1 Remote Node Profile for PPTP Encapsulation

FIELD	DESCRIPTION
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.
My IP Addr	Enter the IP address of the WAN Ethernet port.
My IP Mask	Enter the subnet mask of the WAN Ethernet port.
Server IP Addr	Enter the IP address of the ANT modem.
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.

27.3 Edit IP

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 - Remote Node Network Layer Options**.

Figure 159   Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation

```
          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= 1
                  Private= N/A
                  RIP Direction= None
                    Version= N/A
                  Multicast= None
            Enter here to CONFIRM or ESC to CANCEL:
```

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and
Gateway IP Addr field for **Ethernet** encapsulation. The following table describes the fields
in this menu.

Table 111   Remote Node Network Layer Options

FIELD	DESCRIPTION
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.
(Rem) IP Address	If you have a static IP Assignment, enter the IP address assigned to you by your ISP.
(Rem) IP Subnet Mask	If you have a static IP Assignment, enter the subnet mask assigned to you.
Gateway IP Addr	This field is applicable to **Ethernet** encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.
My WAN Addr	This field is applicable to **PPPoE** and **PPTP** encapsulations only. 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 Prestige.
	Note that this is the address assigned to your local Prestige, not the remote router.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
	Choose **None** to disable NAT.
	Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.
	Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set!
	See the *NAT chapter* for a full discussion on this feature.
Metric	Enter a number from 1 to 15 to set this route's priority among the Prestige'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 111   Remote Node Network Layer Options

FIELD	DESCRIPTION
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select 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.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/ **RIP-2M** or **None**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Prestige 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.
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.	

27.4 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 Prestige to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to the Filters chapter. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 160   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=
                  Enter here to CONFIRM or ESC to CANCEL:
```

Figure 161   Menu 11.5: Remote Node Filter (PPPoE or PPTP 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:
```

27.4.1 Traffic Redirect Setup

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

Figure 162 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:
```

The following table describes the fields in this screen.

Table 112 Menu 11.6: Traffic Redirect Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup. The default is **No**.
Configuration:	
	Enter the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Metric	Enter a number from 1 to 15 to set this route's priority among the Prestige's routes (see the *Metric* section in the *WAN and Dial Backup Setup* chapter) The smaller the number, the higher priority the route has.
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your Prestige's WAN accessibility. The Prestige 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 Prestige to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Enter the number of times your Prestige 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.
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.
Timeout (sec)	Enter the number of seconds the Prestige 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 Prestige times out the number of times specified in the **Fail Tolerance** field.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen	

CHAPTER 28
Static Route Setup

This chapter shows how to setup IP static routes.

28.1 IP Static Route Setup

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

Figure 163   Menu 12 IP Static Route Setup

```
            Menu 12 - IP Static Route Setup
                  1. _____
                  2. _____
                  3. _____
                  4. _____
                  5. _____
                  6. _____
                  7. _____
                  8. _____
            Enter selection number:
```

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

Figure 164   Menu12.1 Edit IP Static Route

```
           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:
```

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

Table 113   Menu12.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.

Table 113   Menu12.1 Edit IP Static Route

FIELD	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on *IP Subnet Mask* in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

CHAPTER 29
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

29.1 Using NAT

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

29.1.1 SUA (Single User Account) Versus NAT

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

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

> **Note:** Choose Full Feature if you have multiple public WAN IP addresses for your Prestige.

29.2 Applying NAT

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

Figure 165 Menu 4 Applying NAT for Internet Access

```
                   Menu 4 - Internet Access Setup
                      ISP's Name= MyISP
                      Encapsulation= Ethernet
                        Service Type= Standard
                        My Login= N/A
                        My Password= N/A
                        Retype to Confirm= N/A
                        Login Server= N/A
                        Relogin Every (min)=  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:
```

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

1 Enter 11 from the main menu.

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

3 Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

Figure 166 Menu 11.3 Applying NAT to the Remote Node

```
        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= 1
                Private= N/A
                RIP Direction= None
                  Version= N/A
                Multicast= None
        Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the options for Network Address Translation.

Table 114 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the **Address Mapping Set** field (menu 15.1 - see section).
	Select **None** to disable NAT.
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (menu 15.1 - see section). Choose **SUA Only** if you have just one public WAN IP address for your Prestige.

29.3 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

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

Figure 167 Menu 15 NAT Setup

```
                Menu 15 - NAT Setup
                        1. Address Mapping Sets
                        2. Port Forwarding Setup
                        3. Trigger Port Setup
                Enter Menu Selection Number:
```

29.3.1 Address Mapping Sets

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

Figure 168 Menu 15.1 Address Mapping Sets

```
                Menu 15.1 - Address Mapping Sets
                        1. NAT_SET
                      255. SUA (read only)
                Enter Menu Selection Number:
```

Enter 255 to display the next screen (see *the SUA (Single User Account) Versus NAT section*). The fields in this menu cannot be changed.

Figure 169 Menu 15.1.255 SUA Address Mapping Rules

```
                Menu 15.1.255 - Address Mapping Rules
 Set Name= SUA
 Idx  Local Start IP Local End IP    Global Start IP Global End IP   Type
 ---  -------------- --------------  --------------- --------------- ------
 1.   0.0.0.0        255.255.255.255 0.0.0.0                         M-1
 2.                                  0.0.0.0                         Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.
                Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

Table 115 SUA Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	**Local Start IP** is the starting local IP address (ILA).

Table 115   SUA Address Mapping Rules

FIELD	DESCRIPTION
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.
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Note: Menu 15.1.255 is read-only.

29.3.1.1 User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

Figure 170 Menu 15.1.1 First Set

```
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:
```

> **Note:** If the Set Name field is left blank, the entire set will be deleted.

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

29.3.1.2 Ordering Your Rules

Ordering your rules is important because the Prestige applies the rules in the order that you specify. When a rule matches the current packet, the Prestige 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 116 Menu 15.1.1 First Set

FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.

> **Note:** You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

> **Note:** An End IP address must be numerically greater than its corresponding IP Start address

Figure 171 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

```
         Menu 15.1.1.1 Address Mapping Rule
               Type= One-to-One
               Local IP:
                 Start= 0.0.0.0
                 End  = N/A
               Global IP:
                 Start= 0.0.0.0
                 End  = N/A
         Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

Table 117 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section* for an example.
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.
Start	This is the starting local IP address (ILA).
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.
Global IP	
	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.
End	This is the ending inside global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.
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.	

29.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

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

2 Enter 2 to display **Menu 15.2 - NAT Server Setup** as shown next.

Figure 172   Menu 15.2.1 NAT Server Setup

```
            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.       0                0           0.0.0.0
         Press ENTER to Confirm or ESC to Cancel:
```

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.

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.

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.

You assign the private network IP addresses. The NAT network appears as a single host on the
Internet. A is the FTP/Telnet/SMTP server.

Figure 173 Multiple Servers Behind NAT Example
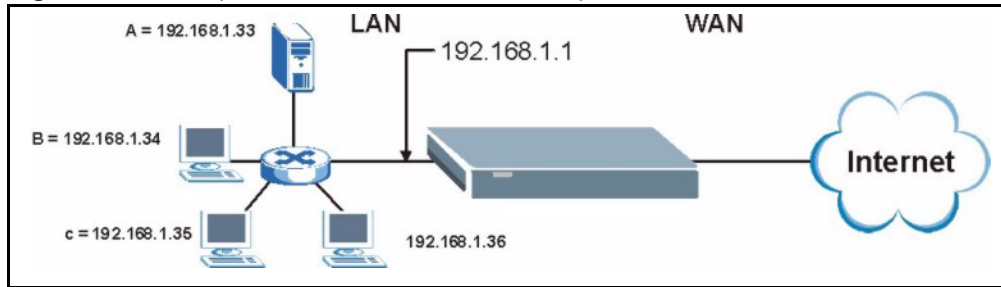
29.5 General NAT Examples

The following are some examples of NAT configuration.

29.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where the ILAs (Inside Local Addresses) of computers A through D map to one dynamic IGA (Inside Global Address) assigned by your ISP.

Figure 174 NAT Example 1
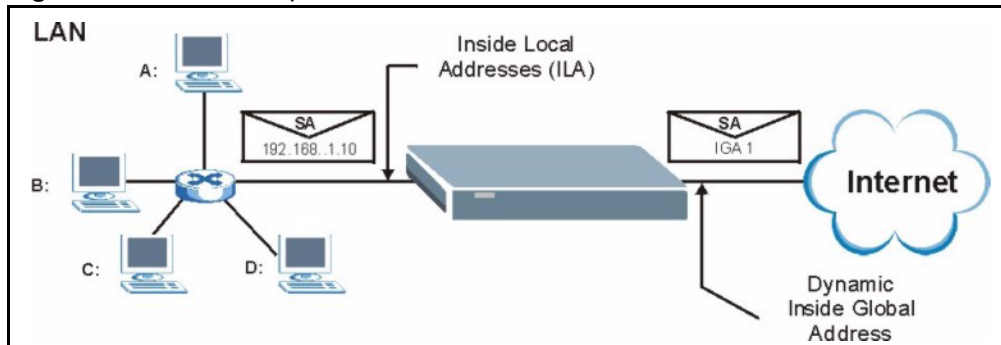
Figure 175   Menu 4 Internet Access & NAT Example

```
            Menu 4 - Internet Access Setup
                    ISP's Name= MyISP
                    Encapsulation= Ethernet
                      Service Type= Standard
                      My Login= N/A
                      My Password= N/A
                      Retype to Confirm= N/A
                      Login Server= N/A
                      Relogin Every (min)=  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:
```

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section General NAT Examples.* 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.

29.5.2 Example 2: Internet Access with an Inside Server

The dynamic Inside Global Address is assigned by the ISP.

Figure 176   NAT Example 2
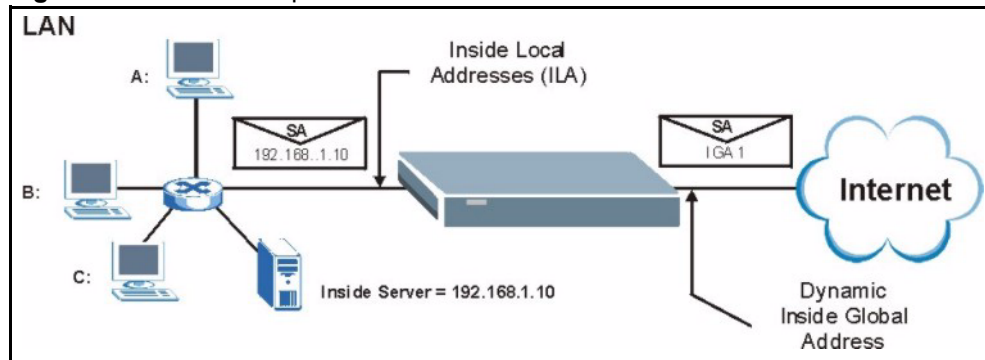
In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

Figure 177   Menu 15.2.1 Specifying an Inside Server

```
          Menu 15.2.1 - NAT Server Setup
      Rule   Start Port No.   End Port No.    IP Address
      ------------------------------------------------------
       1.      Default          Default      192.168.1.10
       2.        0                0                 0.0.0.0
       3.        0                0                 0.0.0.0
       4.        0                0                 0.0.0.0
       5.        0                0                 0.0.0.0
       6.        0                0                 0.0.0.0
       7.        0                0                 0.0.0.0
       8.        0                0                 0.0.0.0
       9.        0                0                 0.0.0.0
      10.        0                0                 0.0.0.0
      11.        0                0                 0.0.0.0
      12.        0                0                 0.0.0.0
          Press ENTER to Confirm or ESC to Cancel:
```

29.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

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

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

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

4 You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

Figure 178 NAT Example 3
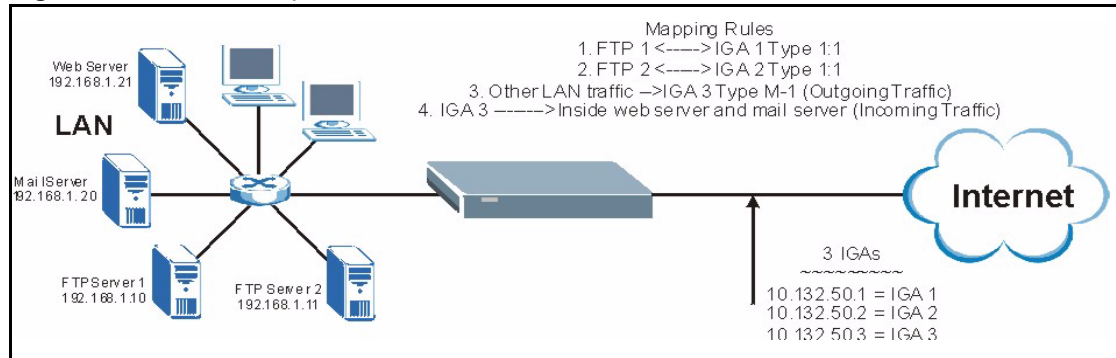
1 In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) see Figure 159.

2 Then enter 15 from the main menu.

3 Enter 1 to configure the Address Mapping Sets.

4 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA) *see Figure 180.*

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

7 When finished, menu 15.1.1.1 should look like as shown in *Example 3: Final Menu 15.1.1.*

Figure 179 NAT Example 3: Menu 11.3

```
        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= 1
                Private= N/A
                RIP Direction= None
                  Version= N/A
                Multicast= None
        Enter here to CONFIRM or ESC to CANCEL:
```

The following figures show how to configure the first rule.

Figure 180   Example 3: Menu 15.1.1.1

```
              Menu 15.1.1.1 Address Mapping Rule
                     Type= One-to-One
                     Local IP:
                        Start= 192.168.1.10
                        End  = N/A
                     Global IP:
                        Start= 10.132.50.1
                        End  = N/A
              Press ENTER to Confirm or ESC to Cancel:
              Press Space Bar to Toggle.
```

Figure 181   Example 3: Final Menu 15.1.1

```
         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.  192.168.1.10                     10.132.50.1                     1-1
    2.  192.168.1.11                     10.132.50.2                     1-1
    3.  0.0.0.0          255.255.255.255 10.132.50.3                     M-1
    4.                                   10.132.50.3                     Server
    5.
    6.
    7.
    8.
    9.
   10.
                    Action= None        Select Rule= N/A
                    Press ENTER to Confirm or ESC to Cancel:
```

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

1 Enter 15 from the main menu.

2 Enter 2 in **Menu 15 - NAT Setup**.

3 Enter 1 in **Menu 15.2 - NAT Server Setup** to see the following menu. Configure it as shown.

Figure 182 Example 3: Menu 15.2

```
         Menu 15.2 - NAT Server Setup
               Rule    Start Port No.   End Port No.   IP Address
               ----------------------------------------------------
                 1.    Default          Default        0.0.0.0
                 2.      80               80           192.168.1.21
                 3.      25               25           192.168.1.20
                 4.       0                0           0.0.0.0
                 5.       0                0           0.0.0.0
                 6.       0                0           0.0.0.0
                 7.       0                0           0.0.0.0
                 8.       0                0           0.0.0.0
                 9.       0                0           0.0.0.0
                10.       0                0           0.0.0.0
                11.       0                0           0.0.0.0
                12.       0                0           0.0.0.0
         Press ENTER to Confirm or ESC to Cancel:
         HTTP:80 FTP:21 Telnet:23 SMTP:25 POP3:110 PPTP:1723
```

29.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

Figure 183 NAT Example 4
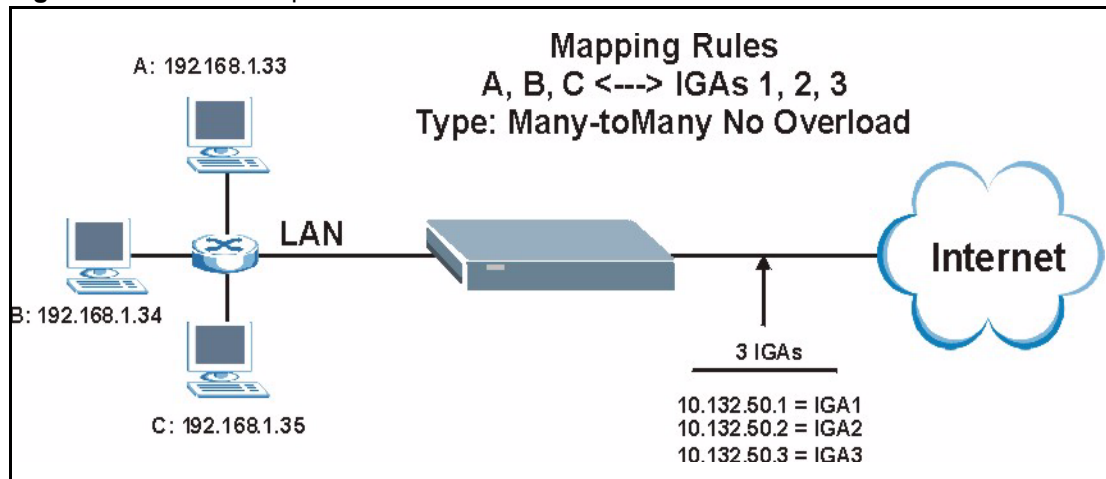
> **Note:** Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One and Many-to-Many No Overload mapping types.

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

Figure 184   Example 4: Menu 15.1.1.1 Address Mapping Rule.

```
            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:
```

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

Figure 185   Example 4: Menu 15.1.1 Address Mapping Rules

```
Menu 15.1.1 - Address Mapping Rules
  Set Name= Example4
 Idx  Local Start IP Local End IP   Global Start IP Global End IP   Type
 ---  -------------- -------------- --------------- --------------- ------
  1.  192.168.1.10   192.168.1.12    10.132.50.1     10.132.50.3   M:M NO OV
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.
                  Action= Edit        Select Rule=
                  Press ENTER to Confirm or ESC to Cancel:
```

29.6 Configuring Trigger Port Forwarding

> **Note:** 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.

Figure 186 Menu 15.3 Trigger Port Setup

```
    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:
```

The following table describes the fields in this screen.

Table 118 Menu 15.3 Trigger Port Setup

FIELD	DESCRIPTION
Rule	This is the rule index number.
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.
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 Prestige 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.
End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the Prestige 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.
End Port	Enter a port number or the ending port number in a range of port numbers.
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 30
Enabling the Firewall

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

30.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management (see the *Remote Management* chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

30.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your Prestige has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

30.3 Enabling the Firewall

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

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

Figure 187   Menu 21.2 Firewall Setup

```
                 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: No
         You can use the Web Configurator to configure the firewall.
                   Press ENTER to Confirm or ESC to Cancel:
```

> **Note:** Use the web configurator or the command interpreter to configure the firewall rules.

CHAPTER 31
Filter Configuration

This chapter shows you how to create and apply filters.

31.1 Introduction to Filters

Your Prestige 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.

Figure 188   Outgoing Packet Filtering Process
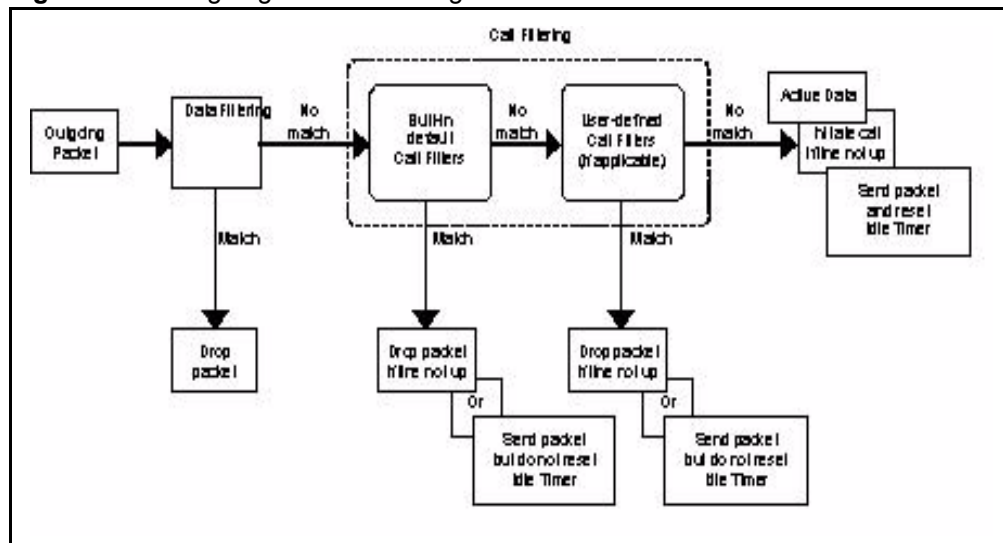
For incoming packets, your Prestige applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

31.1.1 The Filter Structure of the Prestige

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 Prestige 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 <u>cannot</u> 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 193 for the logic flow when executing an IP filter.

Figure 189   Filter Rule Process
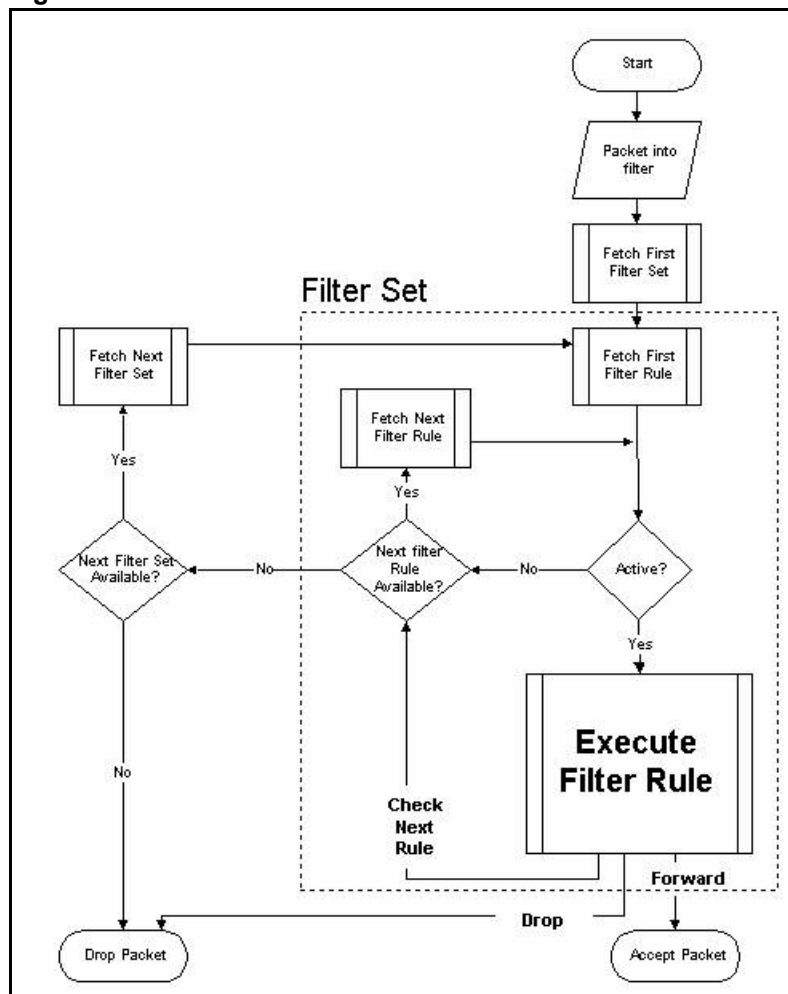
You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

31.2 Configuring a Filter Set

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

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

Figure 190   Menu 21: Filter and Firewall Setup

```
              Menu 21 - Filter and Firewall Setup
                       1. Filter Setup
                       2. Firewall Setup


              Enter Menu Selection Number:
```

2 Enter 1 to bring up the following menu.

Figure 191   Menu 21.1: Filter Set Configuration

```
                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:
```

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

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

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 119   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.

Table 119 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
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 120 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	 Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	 Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

31.2.1 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 Prestige will warn you and will not allow you to save.

31.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next

Figure 192 Menu 21.1.1.1 TCP/IP Filter Rule.

```
              Menu 21.1.1.1 - TCP/IP Filter Rule
                    Filter #: 1,1
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                    IP Protocol= 0      IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 137
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= N/A
                    More= No           Log= None
                    Action Matched= Check Next Rule
                    Action Not Matched= Check Next Rule
            Press ENTER to Confirm or ESC to Cancel:
```

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

Table 121 TCP/IP Filter Rule

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
IP Mask	Enter the IP mask to apply to the **Destination: IP Addr**.	0.0.0.0
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535

Table 121 TCP/IP Filter Rule

FIELD	DESCRIPTION	OPTIONS
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given **in Destination: Port #**.	None Less Greater Equal Not Equal
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Source: IP Addr**.	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**.	None Less Greater Equal Not Equal
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored.	Yes No
More	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	Yes No
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	None Action Matched Action Not Matched **Both**
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.	Check Next Rule Forward Drop
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.	Check Next Rule Forward Drop
When you have **Menu 21.1.1.1 - 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 193 Executing an IP Filter
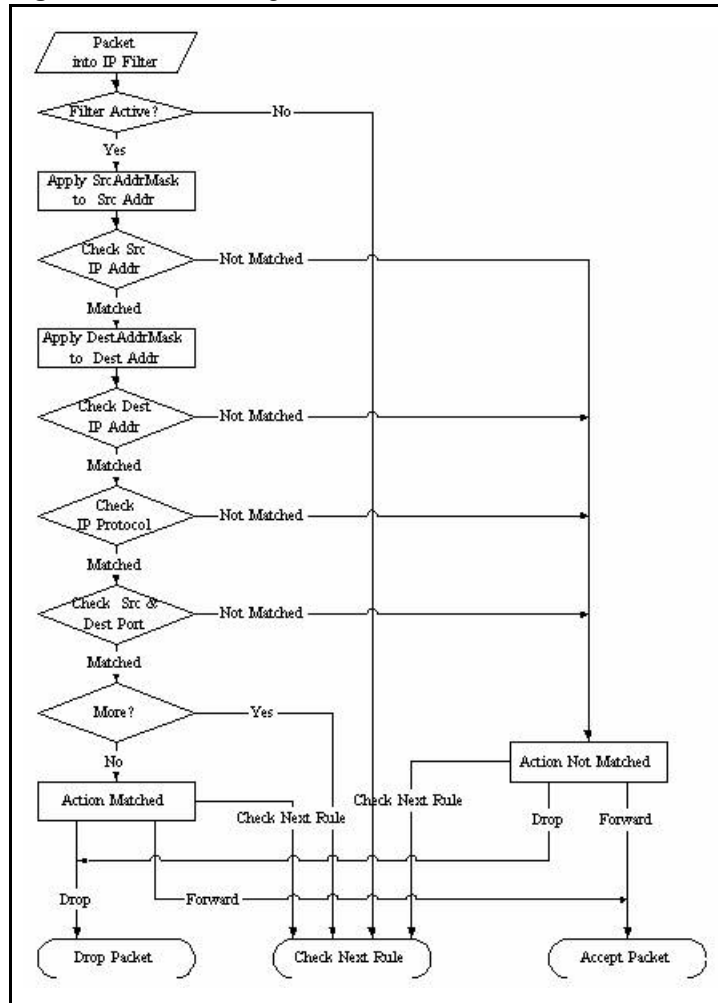
31.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige 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 Prestige 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.

Figure 194 Menu 21.1.4.1 Generic Filter Rule

```
        Menu 21.1.4.1 - Generic Filter Rule
              Filter #: 4,1
              Filter Type= Generic Filter Rule
              Active= No
              Offset= 0
              Length= 0
              Mask= N/A
              Value= N/A
              More= No            Log= None
              Action Matched= Check Next Rule
              Action Not Matched= Check Next Rule
        Press ENTER to Confirm or ESC to Cancel:
```

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

Table 122 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

Table 122 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
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**.		

31.3 Example Filter

Let's look at an example to block outside users from accessing the Prestige via telnet.

Figure 195   Telnet Filter Example
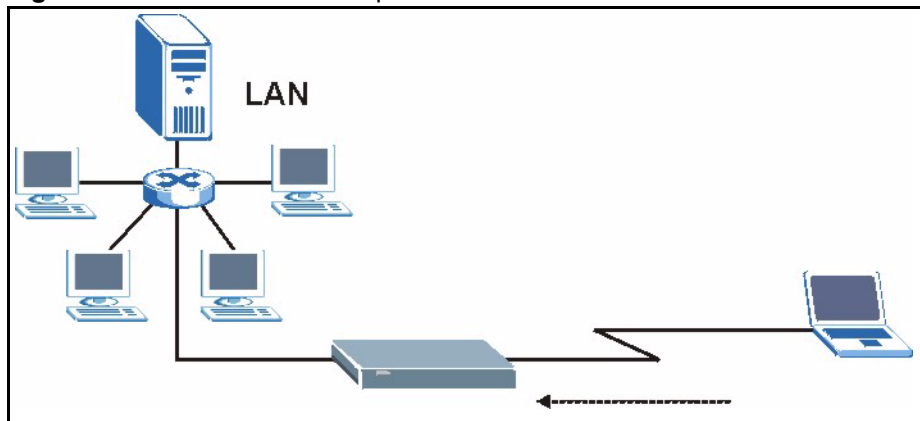
1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.

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

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

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

5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**

6 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Figure 196   Example Filter: Menu 21.1.3.1

```
           Menu 21.1.3.1 - TCP/IP Filter Rule
                   Filter #: 3,1
                   Filter Type= TCP/IP Filter Rule
                   Active= Yes
                   IP Protocol= 6        IP Source Route= No
                   Destination: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 23
                                Port # Comp= Equal
                        Source: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 0
                                Port # Comp= None
                   TCP Estab= No
                   More= No              Log= None
                   Action Matched= Drop
                   Action Not Matched= Forward
         Press ENTER to Confirm or ESC to Cancel:
         Press Space Bar to Toggle.
```

- Select **Yes** from the **Active** field to activate this rule.
- **6** is the TCP **IP Protocol**.
- The **Port #** for the telnet service (TCP protocol) is 23. See RFC 1060 for port numbers of well-known services.
- Select **Equal** from the **Port # Comp** field as you are looking for packets going to port 23 only.
- Select **Drop** in the **Action Matched** field so that the packet will be dropped if its destination is the telnet port.
- Select **Forward** from the **Action Not Matched** field so that the packet will be forwarded if its destination is not the telnet port.
- Press [SPACE BAR] and then [ENTER] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

Figure 197 Example Filter Rules Summary: Menu 21.1.3

```
                     Menu 21.1.3 - Filter Rules Summary
 # A Type                      Filter Rules                       M m n
 - - ---- -------------------------------------------------------- - - -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                      N D F
 2 N
 3 N
 4 N
 5 N
 6 N
                 Enter Filter Rule Number (1-6) to Configure:
```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

After you've created the filter set, you must apply it.

1 Enter 11 from the main menu to go to menu 11.

2 Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].

3 This brings you to menu 11.5. Apply a filter set (our example filter set 3).

4 Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

31.4 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 Prestige 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 Prestige 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 198   Protocol and Device Filter Sets
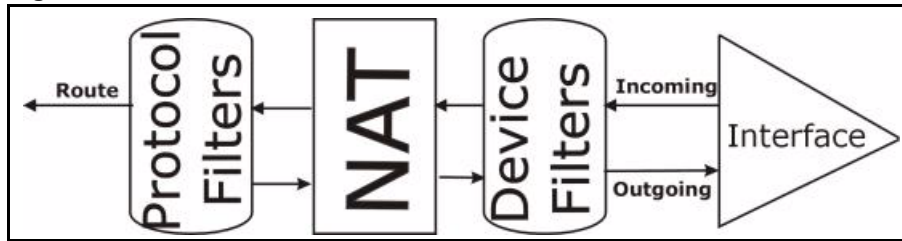
31.5 Firewall Versus Filters

Firewall configuration is discussed in the *firewall* chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

31.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The Prestige already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

> **Note:** If you do not activate the firewall, it is advisable to apply filters

31.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the Prestige and output filter sets filter outgoing traffic from the Prestige. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 199   Filtering LAN Traffic

```
                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:
```

31.6.2 Applying 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 Prestige already has filters to prevent NetBIOS traffic from triggering calls.

Figure 200   Filtering Remote Node Traffic

```
                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:
```

Chapter 31 Filter Configuration

CHAPTER 32
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

32.1 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 Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 201   SNMP Management Model
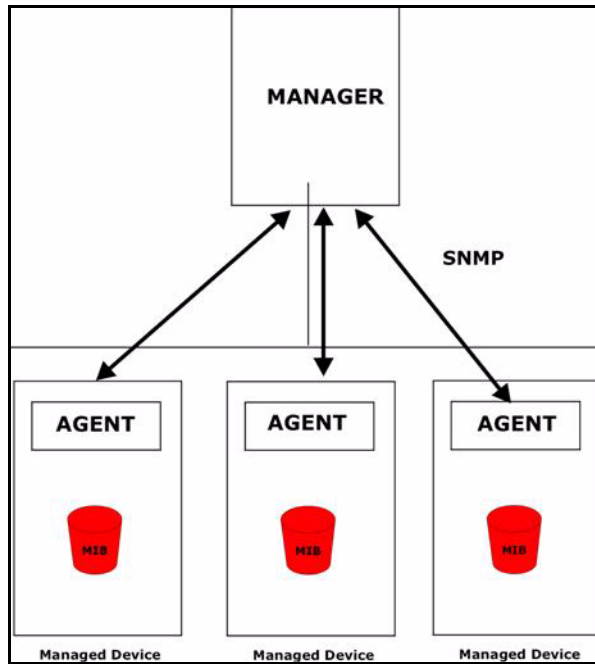
An SNMP managed network consists of two main components: agents and a manager.

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

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

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

1 Get - Allows the manager to retrieve an object variable from the agent.

2 GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.

3 Set - Allows the manager to set values for object variables within an agent.

4 Trap - Used by the agent to inform the manager of some events.

32.2 Supported MIBs

The Prestige supports RFC-1215 and MIB II as defined in RFC-1213 as well as ZyXEL private MIBs. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

32.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 — SNMP Configuration** as shown next. The "community" for Get, Set and Trap fields is SNMP terminology for password.

Figure 202   Menu 22 SNMP Configuration

```
                  Menu 22 - SNMP Configuration
                     SNMP:
                        Get Community= public
                        Set Community= public
                        Trusted Host= 0.0.0.0
                        Trap:
                           Community= public
                           Destination= 0.0.0.0
              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the SNMP configuration parameters.

Table 123   Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the **Set** community, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.
Trap:	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

32.4 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

Table 124   SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkDown (*defined in RFC-1215*)	A trap is sent with the port number when any of the links are down. See the following table.
4	linkUp (*defined in RFC-1215*)	A trap is sent with the port number.

Table 124 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
5	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP gets or sets requirements with 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.).

The port number is its interface index under the interface group.

Table 125 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
…	…
13	12
14	xDSL

CHAPTER 33
System Security

This chapter describes how to configure the system security on the Prestige.

33.1 System Security

You can configure the system password, an external RADIUS server and 802.1x in this menu.

33.1.1 System Password

Figure 203 Menu 23 System Security

```
                Menu 23 - System Security
                     1. Change Password
                     2. RADIUS Server
                     4. IEEE802.1x
```

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to the section on changing the system password in the *Introducing the SMT* chapter and the section on resetting the Prestige in the *Introducing the Web Configurator* chapter.

33.1.2 Configuring External RADIUS Server

Enter 23 in the main menu to display **Menu 23 – System Security**.

Figure 204 Menu 23 System Security

```
                Menu 23 - System Security
                     1. Change Password
                     2. RADIUS Server
                     4. IEEE802.1x
```

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 - System Security-RADIUS Server** as shown next.

Figure 205 Menu 23.2 System Security : RADIUS Server

```
            Menu 23.2 - System Security - RADIUS Server
              Authentication Server:
                Active= No
                Server Address= 10.11.12.13
                Port #= 1812
                Shared Secret= ********
              Accounting Server:
                Active= No
                Server Address= 10.11.12.13
                Port #= 1813
                Shared Secret= ********
              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 126 Menu 23.2 System Security : RADIUS Server

FIELD	DESCRIPTION
Authentication Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server.
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and Prestige.
Accounting Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external accounting server.
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port	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.
Shared Secret	Specify 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 Prestige.
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.	

33.1.3 802.1x

The IEEE802.1x standards outline enhanced security methods for both the authentication of wireless stations and encryption key management.

Follow the steps below to enable EAP authentication on your Prestige.

1 From the main menu, enter 23 to display **Menu23 – System Security**.

Figure 206   Menu 23 System Security

```
        Menu 23 - System Security
           1. Change Password
           2. RADIUS Server
           4. IEEE802.1x
```
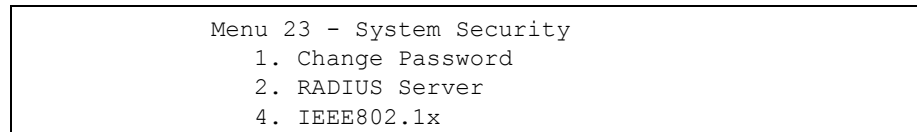
2 Enter 4 to display **Menu 23.4 – System Security – IEEE802.1x**.

Figure 207 Menu 23.4 System Security : IEEE802.1x

```
          Menu 23.4 - System Security - IEEE802.1x

             Wireless Port Control= No Authentication Required
             ReAuthentication Timer (in second)= 1800
             Idle Timeout (in second)= 3600

             Key Management Protocol= WPA-PSK
             Dynamic WEP Key Exchange= 64-bit WEP
             PSK = N/A
             WPA Mixed Mode= N/A
             Data Privacy for Broadcast/Multicast packets= N/A
             WPA Broadcast/Multicast Key Update Timer= N/A
             Authentication Databases= N/A

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

The following table describes the fields in this menu.

Table 127 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	Press [SPACE BAR] and select a security mode for the wireless LAN access.
	Select **No Authentication Required** to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting.
	Selecting **Authentication Required** means wireless stations have to enter usernames and passwords before access to the wired network is allowed.
	Select **No Access Allowed** to block all wireless stations access to the wired network.
	The following fields are not available when you select **No Authentication Required** or **No Access Allowed**.
ReAuthentication Timer (in second)	Specify how often a client has to re-enter username and password to stay connected to the wired network.
	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is **1800** seconds (or 30 minutes).
Idle Timeout (in second)	The Prestige automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed.
	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).
Key Management Protocol	Press [SPACE BAR] to select **802.1x**, **WPA** or **WPA-PSK** and press [ENTER].

Table 127 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**.
	Select **Disable** to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange.
	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
	Up to 32 stations can access the Prestige when you configure Dynamic WEP Key Exchange.
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select **WPA-PSK** in the **Key Management Protocol** field.
WPA Mixed Mode	Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable** and configure **Group Data Privacy** field.
Data Privacy for Broadcast/ Multicast packets	**Group Data Privacy** allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**.
	All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected.
WPA Broadcast/ Multicast Key Update Timer	The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The Prestige default is 1800 seconds (30 minutes).
Authentication Databases	The RADIUS is an external server.
	Select **RADIUS Only** to have the Prestige just check the user database on the specified RADIUS server for a wireless station's username and password.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the Prestige for authentication.

C HAPTER 34
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

Figure 208   Menu 24 System Maintenance

```
          Menu 24 - System Maintenance
          1.   System Status
          2.   System Information and Console Port Speed
          3.   Log and Trace
```

34.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next Figure 209 . System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your ADSL telephone line status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 — System Maintenance.** From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

Figure 209 Menu 24.1 System Maintenance : Status

```
            Menu 24.1 - System Maintenance - Status        07:33:32
                                              Wed. Dec.  24, 2003
Port   Status       TxPkts      RxPkts    Cols   Tx B/s   Rx B/s    Up Time
 WAN   100M/Full     15982      938667       0       78     2520     2:07:57
 LAN   100M/Full     22381       21235       0     2399      128     6:55:05
WLAN   54M             261           0       0        0        0     6:55:05
Port   Ethernet Address       IP Address        IP Mask       DHCP
 WAN   00:A0:C5:01:23:46      172.1.2.3       255.255.0.0    Client
 LAN   00:A0:C5:01:23:45      192.168.1.1   255.255.255.0    Server
    System up Time:     6:55:10
    Name:
    Routing: IP
    ZyNOS F/W Version: V3.60(JK.4)b1 | 07/14/2004
                            Press Command:
            COMMANDS: 1-Drop WAN 9-Reset Counters    ESC-Exit
```

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

Table 128 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	Identifies a port (WAN, LAN or WLAN) on the Prestige.
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.
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 Prestige has been on.
Name	This is the Prestige'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	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.	

34.2 System Information

To get to the System Information:

1 Enter 24 to display **Menu 24 — System Information and Console Port Speed**.

2 Enter 2 to display **Menu 24.2 — System Information**.

3 From this menu you have two choices as shown in the next figure:

Figure 210   Menu 24.2 System Information and Console Port Speed

```
         Menu 24.2 - System Information and Console Port
         Speed
         System Information
         Console Port Speed
         Please enter selection:
```

34.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next

Figure 211   Menu 24.2.1 System Maintenance : Information

```
         Menu 24.2.1 - System Maintenance - Information
            Name:  P334W
            Routing: IP
            ZyNOS F/W Version: V3.60(JK.0)b1 | 01/28/2004
            LAN
         Ethernet Address: 00:A0:C5:01:23:45
```

The following table describes the fields in this menu.

Table 129   Menu 24.2.1 System Maintenance : Information

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

34.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600 and 115200 bps. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

Figure 212 Menu 24.2.2 System Maintenance : Change Console Port Speed

```
            Menu 24.2.2 – System Maintenance – Change Console Port Speed
              Console Port Speed: 9600
          Press ENTER to Confirm or ESC to Cancel:
```

34.3 Log and Trace

There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the syslog facility for message logging.

34.3.1 Syslog Logging

The Prestige uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 — System Maintenance - Syslog Logging**, as shown next.

Figure 213 Menu 24.3.2 System Maintenance : Syslog Logging

```
              Menu 24.3.2 - System Maintenance - Syslog Logging
                    Syslog:
                    Active= No
                    Syslog Server IP Address= 0.0.0.0
                    Log Facility= Local 1
                    Press ENTER to Confirm or ESC to Cancel:
```

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 130 Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog Server 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.

Table 130   Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
Log Facility	Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to the documentation of your syslog program for more details.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your Prestige sends five types of syslog messages. Some examples (not all Prestige specific) of these syslog messages with their message formats are shown next:

34.3.1.1 CDR

Figure 214 Syslog Example

```
1 - CDR

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.)

C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)

C01 Incoming Call xxxx (= connected speed) xxxxx (= Remote Call ID)

L02 Tunnel Connected (L2TP)

C02 OutCall Connected xxxx (= connected speed) xxxxx (= Remote Call ID)

C02 CLID call refused

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

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=4500003c100100001f010004c0a86614ca849a7b08004a5c0200010061626364656566768696a6b6c
6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e000000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3 - Filter Log

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

Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP
spo=0208 dpo=0208]} S03>R01mF
Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF
Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF

4 - PPP Log

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
```

34.3.1.2 Packet triggered

```
Packet triggered Message Format
SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
Sring = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c
6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

34.3.1.3 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[fffffffffff0080] }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
```

34.3.1.4 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
```

34.3.1.5 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)
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 172.21.1.80     :137  -
>172.21.1.80     :137  |UDP|default permit:<2,0>|B
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 192.168.77.88   :520  -
>192.168.77.88   :520  |UDP|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.50     ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.25     ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
```

34.3.2 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

Figure 215 Call-Triggering Packet Example

```
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...
```

34.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Follow the procedure next to get to Diagnostic:

1 From the main menu, type 24 to open **Menu 24 – System Maintenance**.

2 From this menu, type 4 to open **Menu 24.4 – System Maintenance – Diagnostic**.

Figure 216   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
```

34.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in LAN & WAN DHCP. LAN DHCP has already been discussed. The Prestige 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 217   LAN & WAN DHCP
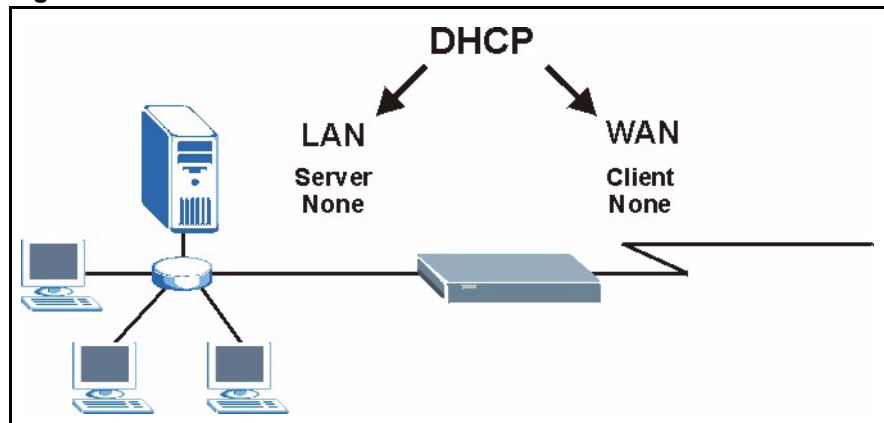
The following table describes the diagnostic tests available in menu 24.4 for your Prestige and associated connections.

Table 131   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.

Table 131 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Reboot System	Enter 11 to reboot the Prestige.
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 35
Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.

35.1 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 Prestige's settings, they can be saved back to your computer under a filename of your choosing.

 ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

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

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the Prestige.

```
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 Prestige 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 Prestige and the external filename refers to the filename <u>not</u> on the Prestige, 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 132   Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige 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 Prestige.	*.bin

35.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

35.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

Figure 218 Telnet in Menu 24.5

```
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 Prestige. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current Prestige 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 Prestige manual.
Press ENTER to Exit:
```

35.2.2 Using the FTP Command from the Command Line

1 Launch the FTP client on your computer.

2 Enter "open", followed by a space and the IP address of your Prestige.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is "1234").

5 Enter "bin" to set transfer mode to binary.

6 Use "get" to transfer files from the Prestige to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the Prestige to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.

7 Enter "quit" to exit the ftp prompt.

35.2.3 Example of FTP Commands from the Command Line

Figure 219 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

35.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 133 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous.
	This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.
	Normal.
	The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

35.2.5 TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

- You have disabled Telnet service in menu 24.11.
- You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the Prestige will disconnect the Telnet session immediately.
- You have an SMT console session running.

35.2.6 Backup Configuration Using TFTP

The Prestige supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

3 Enter command "sys stdio 0" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the Prestige 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 Prestige to the computer and "binary" to set binary transfer mode.

35.2.7 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 Prestige IP address, "get" transfers the file source on the Prestige (rom-0, name of the configuration file on the Prestige) to the file destination on the computer and renames it config.rom.

35.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 134 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the Prestige 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 Prestige. 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.

35.3 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 Prestige since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

> **Note:** WARNING! Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

35.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter

Figure 220 Telnet into Menu 24.6.

```
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 Prestige. 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 Prestige. This restores the configuration to
   your Prestige.
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 Prestige manual.
Press ENTER to Exit:
```

1 Launch the FTP client on your computer.

2 Enter "open", followed by a space and the IP address of your Prestige.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is "1234").

5 Enter "bin" to set transfer mode to binary.

6 Find the "rom" file (on your computer) that you want to restore to your Prestige.

7 Use "put" to transfer files from the Prestige to the computer, for example, "put config.rom rom-0" transfers the configuration file "config.rom" on your computer to the Prestige. See earlier in this chapter for more information on filename conventions.

8 Enter "quit" to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

35.3.2 Restore Using FTP Session Example

Figure 221   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
```

35.4 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**.

> **Note:** WARNING! Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

35.4.1 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 Prestige, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 222 Telnet Into Menu 24.7.1 Upload System Firmware

```
Menu 24.7.1 - System Maintenance - Upload System Firmware
To upload the system firmware, follow the procedure below:
  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put firmware filename 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:
```

35.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2

Figure 223 Telnet Into Menu 24.7.2 System Maintenance .

```
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 configuration filename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.
Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

35.4.3 FTP File Upload Command from the DOS Prompt Example

1 Launch the FTP client on your computer.

2 Enter "open", followed by a space and the IP address of your Prestige.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is "1234").

5 Enter "bin" to set transfer mode to binary.

6 Use "put" to transfer files from the computer to the Prestige, for example, "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the Prestige and renames it "ras". Similarly, "put config.rom rom-0" transfers the configuration file on your computer (config.rom) to the Prestige and renames it "rom-0". Likewise "get rom-0 config.rom" transfers the configuration file on the Prestige to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.

7 Enter "quit" to exit the ftp prompt.

> **Note:** The Prestige automatically restarts after a successful file upload.

35.4.4 FTP Session Example of Firmware File Upload

Figure 224   FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

35.4.5 TFTP File Upload

The Prestige also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

3 Enter the command "sys stdio 0" to disable the console timeout, so the TFTP transfer will not be interrupted. Enter "command sys stdio 5" to restore the five-minute console timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is "ras".

Note that the telnet connection must be active and the Prestige 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 Prestige to the computer, "put" the other way around, and "binary" to set binary transfer mode.

35.4.6 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 Prestige's IP address and "put" transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the Prestige).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

C HAPTER 36
System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

36.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type "exit" to return to the SMT main menu when finished.

Figure 225   Command Mode in Menu 24

```
                  Menu 24 - System Maintenance
            1.   System Status
            2.   System Information and Console Port Speed
            3.   Log and Trace
            4.   Diagnostic
            5.   Backup Configuration
            6.   Restore Configuration
            7.   Firmware Update
            8.   Command Interpreter Mode
            9.   Call Control
            10.  Time and Date Setting
            11.  Remote Management Setup
          Enter Menu Selection Number:
```

36.1.1 Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets [].
- The | symbol means "or".
- For example,
- sys filter netbios config <type> <on|off>
- means that you must specify the type of netbios filter and whether to turn it on or off.

36.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Figure 226 Valid Commands

```
                Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys    exit    device  ether
poe    pptp    config  wlan
ip     ipsec   ppp     bridge
hdap   radius  8021x
ras>
```

36.2 Call Control Support

The Prestige provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** 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 Prestige 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.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

Figure 227 Menu 24.9 System Maintenance : Call Control

```
                Menu 24.9 - System Maintenance - Call Control
                    1. Budget Management
                    2. Call History
                   Enter Menu Selection Number:
```

36.2.1 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.

Figure 228 Budget Management

```
Menu 24.9.1 - Budget Management
Remote Node    Connection Time/Total Budget      Elapsed Time/Total Period
1. MyISP       No Budget                         No Budget
Reset Node (0 to update screen):
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 135 Menu 24.9.1 - Budget Management

FIELD	DESCRIPTION
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.
Enter "0" to update the screen or press [ESC] to return to the previous screen.	

36.2.2 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.

Figure 229 Menu 24.9.2 - Call History

```
          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):
```

The following table describes the fields in this menu.

Table 136 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.	

36.3 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 Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

Figure 230 Menu 24: System Maintenance

```
        Menu 24 - System Maintenance
       1.  System Status
       2.  System Information and Console Port Speed
       3.  Log and Trace
       4.  Diagnostic
       5.  Backup Configuration
       6.  Restore Configuration
       7.  Upload Firmware
       8.  Command Interpreter Mode
       9.  Call Control
       10. Time and Date Setting
       11. Remote Management Setup
       Enter Menu Selection Number:
```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

Figure 231   Menu 24.10 System Maintenance: Time and Date Setting

```
     Menu 24.10 - System Maintenance - Time and Date Setting
Time Protocol= NTP (RFC-1305)
Time Server Address= time-b.nist.gov
Current Time:                           08 : 07 : 14
New Time (hh:mm:ss):                    08 : 06 : 48
Current Date:                           2003 - 12 - 24
New Date (yyyy-mm-dd):                  2003 - 12 - 24
Time Zone= GMT
Daylight Saving= No
Start Date (mm-dd):                            01 - 01
End Date (mm-dd):                              01 - 01
          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 137   Time and Date Setting Fields

FIELD	DESCRIPTION
Time Protocol	Enter the time service protocol that your timeserver sends when you turn on the Prestige. 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 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.
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 DateEnter 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.	

36.3.1 Resetting the Time

The Prestige resets the time in three instances:

1 On leaving menu 24.10 after making changes.

2 When the Prestige starts up, if there is a timeserver configured in menu 24.10.

3 24-hour intervals after starting.

C HAPTER 37
Remote Management

This chapter covers remote management (SMT menu 24.11).

37.1 Remote Management

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

You may manage your Prestige from a remote location via:

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

> **Note:** When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

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

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

Figure 232   Menu 24.11 – Remote Management Control

```
      Menu 24.11 - Remote Management Control
 TELNET Server:     Port = 23          Access = ALL
                    Secure Client IP = 0.0.0.0
 FTP Server:        Port = 21          Access = ALL
                    Secure Client IP = 0.0.0.0
 Web Server:        Port = 80          Access = ALL
                    Secure Client IP = 0.0.0.0
 SNMP Service:      Port = 161         Access = LAN only
                    Secure Client IP = 0.0.0.0
 DNS Service:       Port = 53          Access = LAN only
                    Secure Client IP = 0.0.0.0
              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 138   Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a service or protocol.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the Prestige.
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.
Secure Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the Prestige. Enter an IP address to restrict access to a client with a matching IP address.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

37.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.

You have disabled that service in menu 24.11.

The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.

1 There is an SMT console session running.

2 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

3 There is a firewall rule that blocks it.

CHAPTER 38
Call Scheduling

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

38.1 Introduction to Call Scheduling

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

Figure 233 Menu 26 Schedule Setup

```
        Menu 26 - Schedule Setup

        Schedule                      Schedule
          Set #        Name             Set #        Name
        ------   -------------------   ------   ----------------


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

        Enter Schedule Set Number to Configure= 0

        Edit Name= N/A

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

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2 ,3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

> **Note:** To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] (or delete) in the Edit Name field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

Figure 234 Menu 26.1 Schedule Set Setup

```
                        Menu 26.1 - Schedule Set Setup
            Active= Yes
            Start Date(yyyy/mm/dd) = 2000 - 01 - 01
            How Often= Once
            Once:
              Date(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:
```

If a connection has been already established, your Prestige 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 139 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.
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].

Table 139   Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION
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.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

Figure 235   Applying Schedule Set(s) to a Remote Node (PPPoE)

```
    Menu 11.1 - Remote Node Profile
 Rem Node Name= MyISP                    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
   Retype to Confirm= ********
   Authen= CHAP/PAP
                                         Session Options:
                                           Edit Filter Sets= No
                                           Idle Timeout(sec)= 100
                                         Edit Traffic Redirect= No
                 Press ENTER to Confirm or ESC to Cancel:
```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

C H A P T E R 39
VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

39.1 VPN/IPSec Overview

The VPN/IPSec main SMT menu has these main submenus:

1 Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.

2 **Menu 27.2 - SA Monitor** allows you to manage (refresh or disconnect) your SA connections.

This is an overview of the VPN menu tree.

Figure 236 VPN SMT Menu Tree
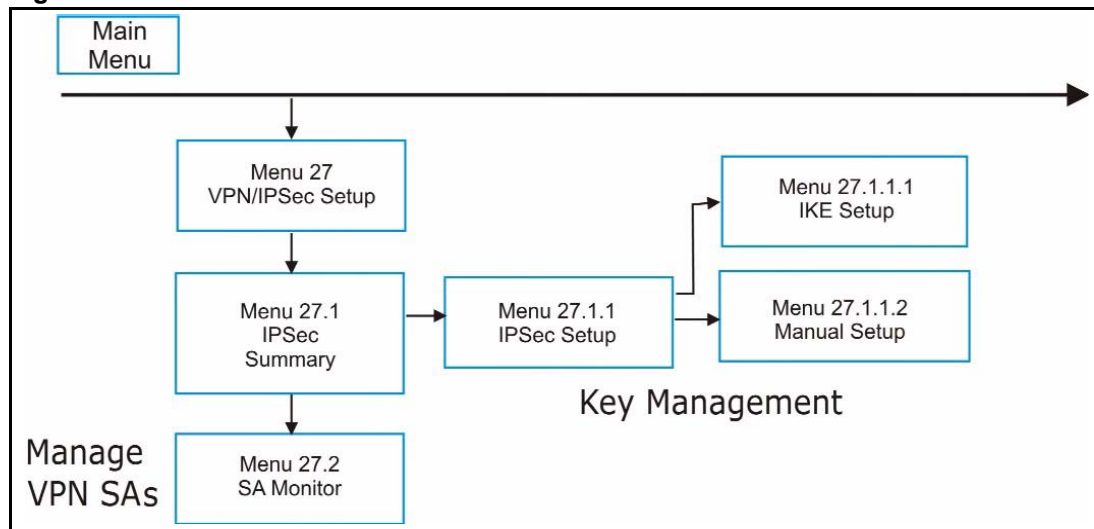
From the main menu, enter 27 to display the first VPN menu (shown next).

Figure 237 Menu 27 VPN/IPSec Setup

```
          Menu 27 - VPN/IPSec Setup
           1. IPSec Summary
           2. SA Monitor
          Enter Menu Selection Number:
```

39.2 IPSec Summary Screen

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 IPSec Summary**. This is a
summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by
selecting an index number and then configuring the associated submenus.

Figure 238 Menu 27

```
#      Name     A  Local Addr Start  - Local Addr End     Encap    IPSec Algorithm
-      Key Mgt  -  Remote Addr Start - Remote Addr End    ------   Secure GW Addr
       ---------    -----------------  ------------------            ------------------
                    -                  -
                    192.168.1.35
       Taiwan       172.16.2.40                                    ESP DES MD5
001    IKE      Y  1.1.1.1            192.168.1.38         Tunnel   193.81.13.2
002    zw50     N  4.4.4.4           172.16.2.46          Tunnel   AH SHA1
003    IKE      N  192.168.1.40      1.1.1.1              Tunnel   zw50test.zyxel.
       China        N/A               255.255.0.0                   ESP DES MD5
       IKE                            192.168.1.42                  0.0.0.0
                                      N/A


                                      NoneSelect Rule= N/A
```

Table 140 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION
#	This is the VPN policy index number.
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.
A	**Y** signifies that this VPN rule is active.

Table 140   Menu 27.1 IPSec Summary

FIELD	DESCRIPTION
Local Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the LAN behind your Prestige.
	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 Prestige.
	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 Prestige.
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 Prestige. 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 Prestige.
Encap	This field displays **Tunnel** mode or **Transport** mode. See earlier for a discussion of these. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption.
	AH (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits)**.**
	Both **AH** and **ESP** increase the Prestige's processing requirements and communications latency (delay).
	You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.
Key Mgt	This field displays the SA's type of key management, (**IKE** or **Manual**).
Remote Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the network behind the remote IPSec router.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the network behind the remote IPSec router.
	This field displays **N/A** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.

Table 140   Menu 27.1 IPSec Summary

FIELD	DESCRIPTION
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.
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.
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 <u>not</u> 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).
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

Figure 239   Menu 27.1.1 IPSec Setup

```
                      Menu 27.1.1 – IPSec Setup
Index= 1          Name= Taiwan
Active= Yes      Keep Alive= No      Nat Traversal= No
Local ID type           Content=
My IP Addr= 0.0.0.0
Peer ID type= IP        Content=
Secure Gateway Address= zw50test.zyxel.com.tw
Protocol= 0             DNS Server= 0.0.0.0

Local:            Addr Type= SINGLE             End= N/A
             Local IP Addr= 1.1.1.1            End/Subnet Mask= 255.255.0.0
                Port Start= 0                  End= N/A
                 Addr Type= SUBNET
Remote:        IP Addr Start= 4.4.4.4
                Port Start= 0

Enable Replay Detection = No
Key Management= IKE
Edit Key Management Setup= No

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

The following table describes the fields in this menu.

Table 141   Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION
Index	This is the VPN rule index number you selected in the previous menu.
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in **Menu 27.1 - IPSec Summary**.
Active	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to have the Prestige 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.
Nat Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.
	The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with **Manual** key management.
	In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.
Local ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER].
	Select **IP** to identify this Prestige by its IP address.
	Select **DNS** to identify this Prestige by a domain name.
	Select **E-mail** to identify this Prestige by an e-mail address.

Table 141 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer or leave the field blank to have the Prestige automatically use its own IP address.
	When you select **DNS** in the **Local ID Type** field, type a domain name (up to 31 characters) by which to identify this Prestige.
	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 Prestige.
	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 Prestige. The Prestige uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0.
	The VPN tunnel has to be rebuilt if this IP address changes.
Peer ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER].
	Select **IP** to identify the remote IPSec router by its IP address.
	Select **DNS** to identify the remote IPSec router by a domain name.
	Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	When you select **IP** in the **Peer ID Type** field, type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Prestige automatically use the address in the **Secure Gateway Address** field.
	When you select **DNS** in the **Peer ID Type** field, type a domain name (up to 31 characters) by which to identify the remote IPSec router.
	When you select **E-mail** in the **Peer ID Type** field, type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field below.
Secure Gateway Address	Type the IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection.
	Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**, see later).
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.
	Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Addr Type	This field displays **SINGLE** for a single IP address.
Local IP Addr	Enter a static IP address on the LAN behind your Prestige.

Table 141   Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. You cannot create a VPN tunnel if you try to connect using a port number that does not match this port number or range of port numbers.
	Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields are **N/A** when the **Secure Gateway Address** field is configured to 0.0.0.0.
	Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Use **RANGE** for a specific range of IP addresses. Use **SUBNET** to specify IP addresses on a network by their subnet mask.
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the network behind the remote IPSec router.
	When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the **Addr Type** field is configured to **SUBNET**, enter a static IP address on the network behind the remote IPSec router.
	This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.
End/Subnet Mask	When the **Addr Type** field is configured to **Single**, this field is **N/A**.
	When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the **Addr Type** field is configured to **SUBNET**, enter a subnet mask on the network behind the remote IPSec router.
	This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Someone behind the remote IPSec router cannot create a VPN tunnel when attempting to connect using a port number that does not match this port number or range of port numbers.
	Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.

Table 141   Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **Yes**. Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to enable replay detection.
Key Management	Press [SPACE BAR] to choose either **IKE** or **Manual** and then press [ENTER]. **Manual** is useful for troubleshooting if you have problems using **IKE** key management.
Edit Key Management Setup	Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the **Key Management** field to **IKE**, this will take you to **Menu 27.1.1.1 – IKE Setup**. If you set the **Key Management** field to **Manual**, this will take you to **Menu 27.1.1.2 – Manual Setup**.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

39.3 IKE Setup

To edit this menu, the **Key Management** field in **Menu 27.1.1 – IPSec Setup** must be set to **IKE**. Move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 – IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 – IKE Setup**.

Figure 240   Menu 27.1.1.1 IKE Setup

```
            Menu 27.1.1.1 - IKE Setup
          Phase 1
            Negotiation Mode= Main
            PSK= qwer1234
            Encryption Algorithm= DES
            Authentication Algorithm= MD5
            SA Life Time (Seconds)= 28800
            Key Group= DH1
          Phase 2
            Active Protocol= ESP
            Encryption Algorithm= DES
            Authentication Algorithm= SHA1
            SA Life Time (Seconds)= 28800
            Encapsulation= Tunnel
            Perfect Forward Secrecy (PFS)= None
        Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 142   Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION
Phase 1	
Negotiation Mode	Press [SPACE BAR] to choose from **Main** or **Aggressive** and then press [ENTER]. See earlier for a discussion of these modes. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
PSK	Prestige gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated.
	Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Prestige **DES** encryption algorithm uses a 56-bit key.
	Triple DES (**3DES**), is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in slightly increased latency and decreased throughput.
	Press [SPACE BAR] to choose from **3DES** or **DES** and then press [ENTER].
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slightly slower.
	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].

Table 142   Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION
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.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Press [SPACE BAR] to choose from **ESP** or **AH** and then press [ENTER]. See earlier for a discussion of these protocols.
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Select **NULL** to set up a tunnel without encryption.
Authentication Algorithm	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].
SA Life Time (Seconds)	Define the length of time before an IPSec Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).
Encapsulation	Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

39.4 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.

39.4.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. See the Web Configurator part on VPN for more information on these parameters.

Table 143   Active Protocol: Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

39.4.2 Security Parameter Index (SPI)

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**.

Figure 241   Menu 27.1.1.2 Manual Setup

```
           Menu 27.1.1.2 – Manual Setup
     Active Protocol= ESP Tunnel
     ESP Setup
       SPI (Decimal)=
       Encryption Algorithm= DES
         Key1=
         Key2= N/A
         Key3= N/A
       Authentication Algorithm= MD5
         Key= N/A

     AH Setup
       SPI (Decimal)= N/A
       Authentication Algorithm= N/A
         Key=
            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 144   Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION
Active Protocol	Press [SPACE BAR] to choose from **ESP Tunnel**, **ESP Transport**, **AH Tunnel** or **AH Transport** and then press [ENTER]. Choosing an **ESP** combination causes the **AH Setup** fields to be non-applicable (**N/A**)
ESP Setup	The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**.
SPI (Decimal)	The **SPI** must be unique and from one to four integers ("0" to "9").

Table 144 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Fill in the **Key1** field below when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter any encryption keys.
Key1	Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated.
	Fill in the **Key1** field when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**.
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.
AH Setup	The **AH Setup** fields are **N/A** if you chose an **ESP Active Protocol**.
SPI (Decimal)	The **SPI** must be from one to four unique decimal characters ("0" to "9") long.
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 40
SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

40.1 SA Monitor Overview

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

> **Note:** When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the Web configurator part on keep alive to have the Prestige renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

40.2 Using SA Monitor

1. Use the **Refresh** function to display active VPN connections.
2. Use the **Disconnect** function to cut off active connections.
3. Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

Figure 242 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:
```

The following table describes the fields in this menu.

Table 145 Menu 27.2 SA Monitor

FIELD	DESCRIPTION
#	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.
Encap.	This field displays **Tunnel** mode or **Transport** mode. See previous for discussion.
IPSec ALgorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption.
	An incoming SA may have an **AH** in addition to **ESP**. The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits).
	Both **AH** and **ESP** increase Prestige processing requirements and communications latency (delay).

Table 145   Menu 27.2 SA Monitor

FIELD	DESCRIPTION
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).
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 41
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

41.1 Problems Starting Up the Prestige

Table 146 Troubleshooting Starting Up Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adaptor is connected to the Prestige and plugged in to an appropriate power source. Make sure that the Prestige and the power source are both turned on.
	Turn the Prestige off and on.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

41.2 Problems with the LAN

Table 147 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	Check your Ethernet cable connections (refer to the Quick Start Guide for details). Check for faulty Ethernet cables.
	Make sure your computer's Ethernet Card is working properly.
I cannot access the Prestige from the LAN.	If **Any IP** is disabled, make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.

41.3 Problems with the WAN

Table 148 Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
The WAN LED is off.	Check the connections between the Prestige WAN port and the cable/DSL modem or ethernet jack.
	Check whether your cable/DSL device requires a crossover or straight-through cable.
I cannot get a WAN IP address from the ISP.	Click WAN to verify your settings.
	The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Refer to the WAN Setup chapter (web configurator or SMT).
I cannot access the Internet.	Make sure the Prestige is turned on and connected to the network.
	Verify your WAN settings. Refer to the chapter on WAN setup (web configurator) or the section on Internet Access (SMT).
	Make sure you entered the correct user name and password.
	If you use PPPoE pass through, make sure that bridge mode is turned on.
The Internet connection disconnects.	Check the schedule rules. Refer to Chapter 38 on page 393 (SMT).
	If you use PPPoE encapsulation, check the idle time-out setting. Refer to the Chapter 8 on page 129 (web configurator) or Chapter 27 on page 311 (SMT).
	Contact your ISP.

41.4 Problems Accessing the Prestige

Table 149   Troubleshooting Accessing the Prestige

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	The username is "admin". The default password is "1234". The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.
I cannot access the web configurator.	Make sure that there is not an SMT console session running. Use the Prestige's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection. Use the Prestige's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details. Your computer's and the Prestige's IP addresses must be on the same subnet for LAN access. If you changed the Prestige's LAN IP address, then enter the new one as the URL. Remove any filters in SMT menu 3.1 (LAN) or menu 11.5 (WAN) that block web service. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.

41.5 Problems with Restricted Web Pages and Keyword Blocking

Table 150   Troubleshooting Restricted Web Pages and Keyword Blocking

PROBLEM	CORRECTIVE ACTION
Access to a restricted web page is not blocked.	Make sure that the Enable Parental Control check box is selected in the Parental Control screen.
	Make sure that you select a category in the Parental Control screen to restrict access to web pages relevant to that category. For example, select the Gambling check box to prevent access to www.onlinegambling.com.
Access to a web page with a URL containing a forbidden keyword is not blocked.	Make sure that you select the Keyword Blocking check box in the Content Filtering screen. Make sure that the keywords that you type are listed in the Keyword List.
	If a keyword that is listed in the Keyword List is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the Content Filter chapter.

Table 150 Troubleshooting Restricted Web Pages and Keyword Blocking

PROBLEM	CORRECTIVE ACTION
Parental Control is configured correctly, but I can still access restricted web pages.	Restart the device to clear the cache.
	The content filter server may be unavailable. The **View Logs** screen can display content filtering log messages. See the Log Descriptions appendix for a list of possible log messages. In the **View Logs** screen copy and paste the log messages and e-mail them to customer support with an explanation of the problem.
	If you still have problems, contact your vendor or customer support for further advice.

Problems with the Password

Table 151 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige.	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, Chapter 2 on page 54 for details.

Problems with Remote Management

Table 152 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige from the LAN or WAN.	Refer to Section 15.1.1 on page 197 in Chapter 15 Remote Management Screens for scenarios when remote management may not be possible.
	When NAT is enabled: • Use the Prestige's WAN IP address when configuring from the WAN. • Use the Prestige's LAN IP address when configuring from the LAN.

41.5.1 Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).

• Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

41.5.1.1 Internet Explorer Pop-up Blockers

You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

41.5.1.1.1 Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 243   Pop-up Blocker
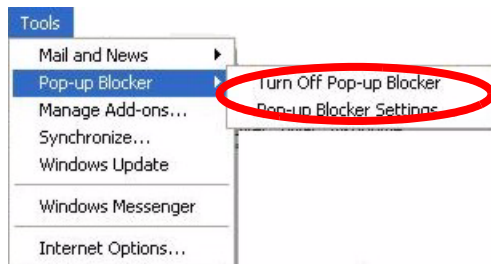
You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 244   Internet Options
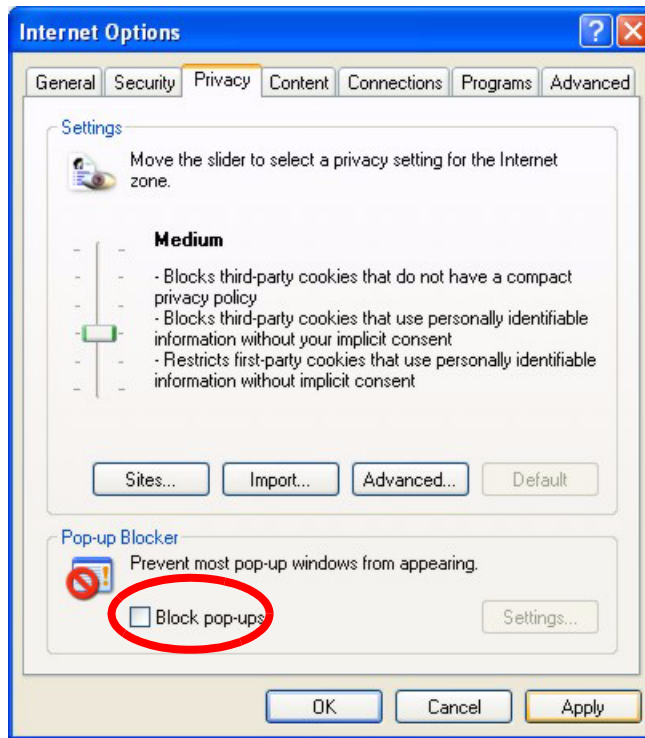
3 Click **Apply** to save this setting.

41.5.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 245 Internet Options
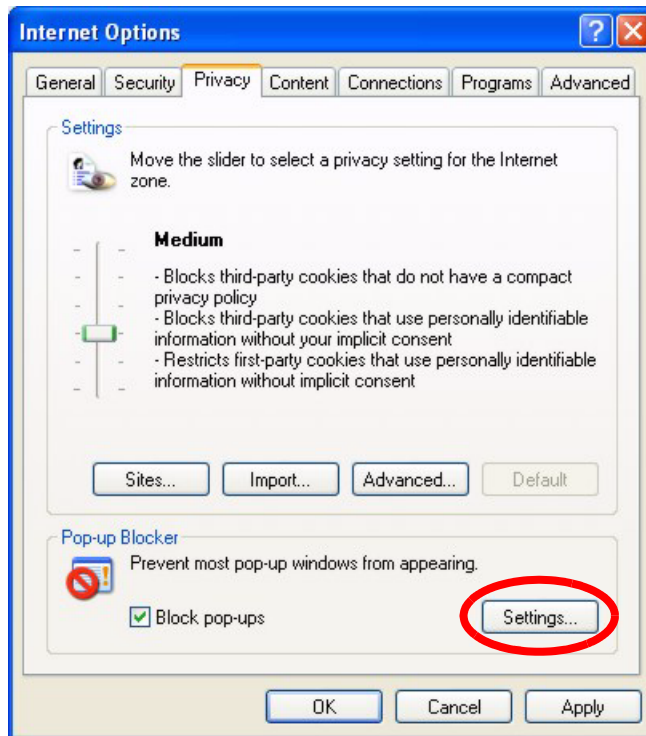
3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Note: If you change the IP address of your device, make sure that the new address matches the address you type in the **Pop-up Blocker Settings** screen.

Figure 246 Pop-up Blocker Settings
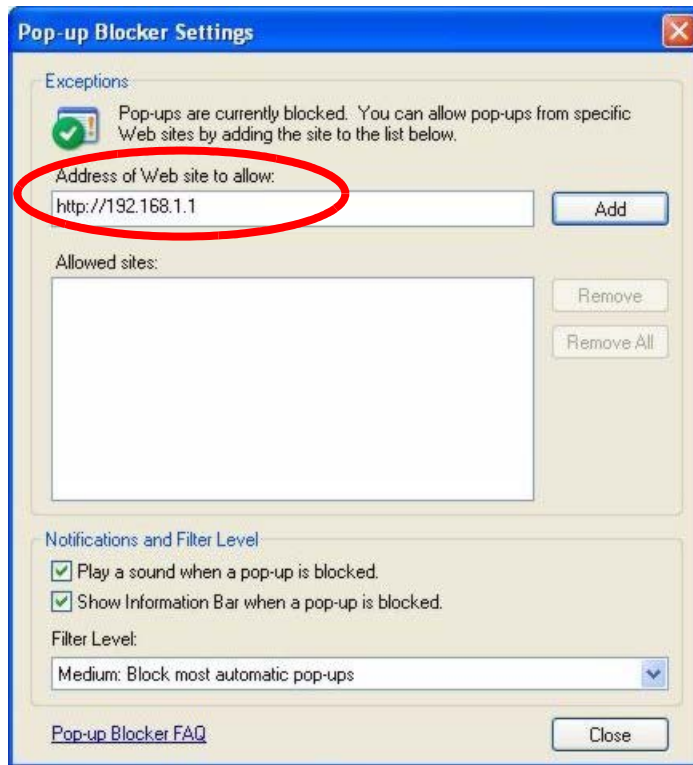
5 Click **Close** to return to the **Privacy** screen.

6 Click **Apply** to save this setting.

41.5.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 247 Internet Options
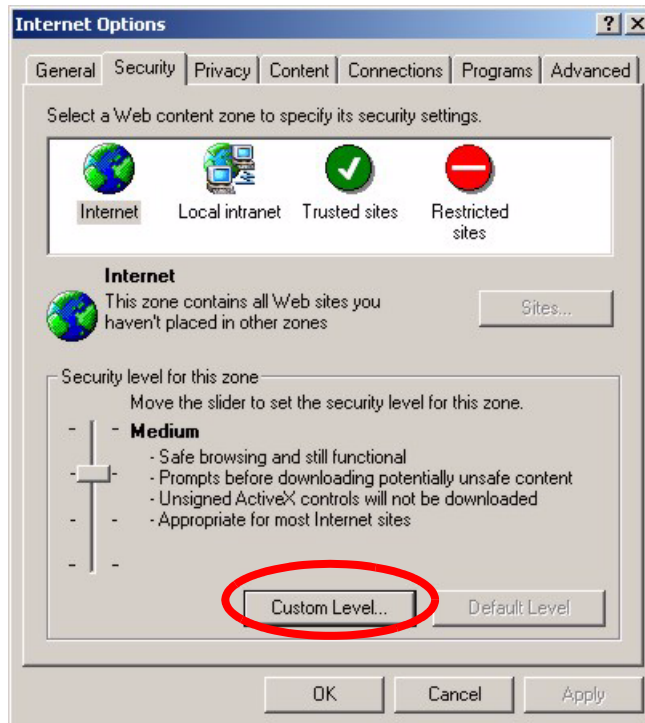
2 Click the **Custom Level...** button.

3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 248 Security Settings - Java Scripting
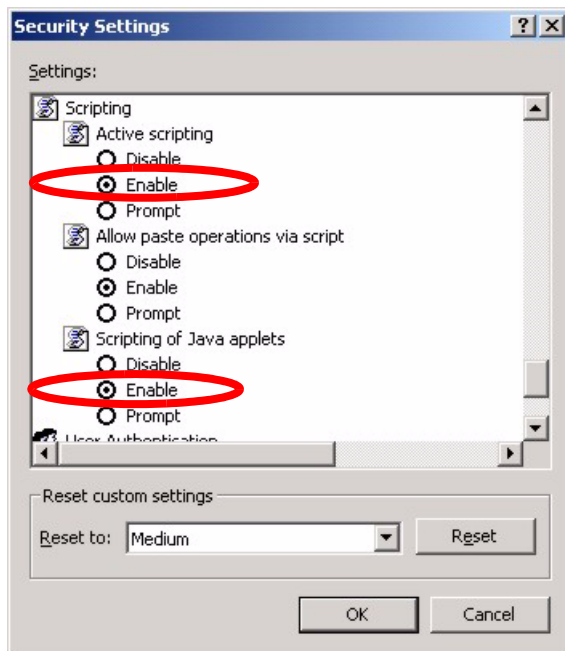
41.5.1.3 Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 249 Security Settings - Java
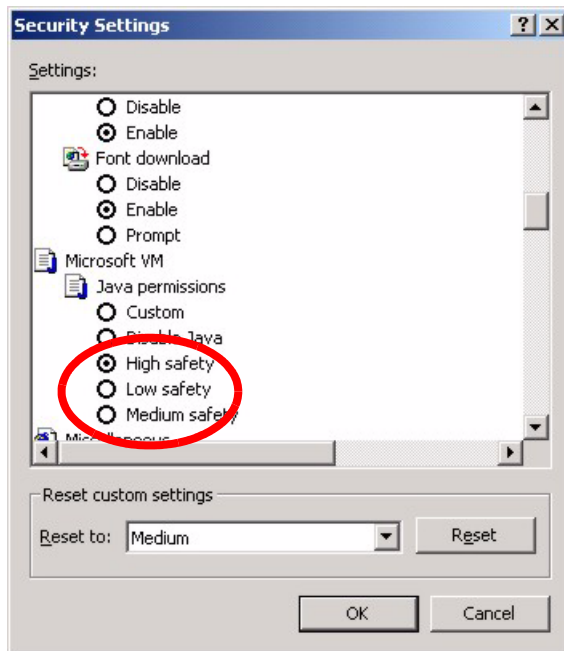
41.5.1.3.1 JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 250 Java (Sun)
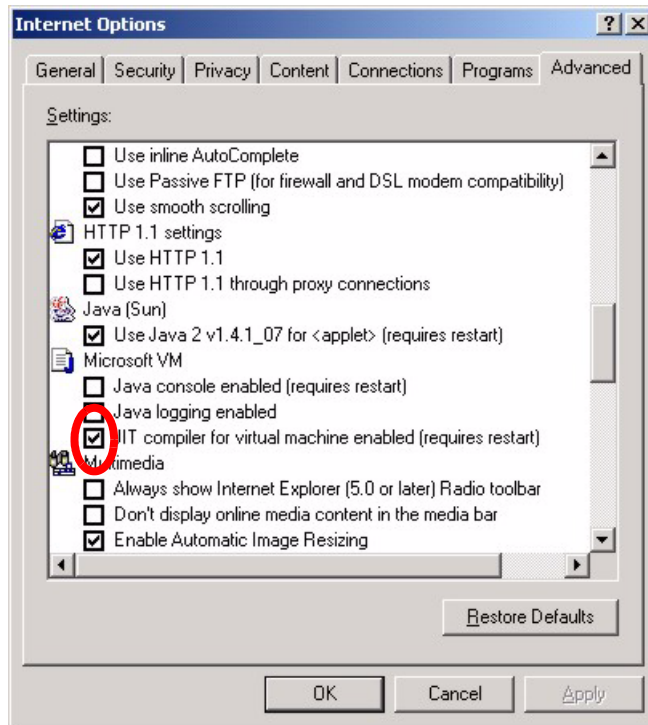
41.5.2 ActiveX Controls in Internet Explorer

If ActiveX is disabled, you will not be able to download ActiveX controls or to use Trend Micro Security Serivces. Make sure that ActiveX controls are allowed in Internet Explorer.

Screen shots for Internet Explorer 6 are shown. Steps may vary depending on your version of Internet Explorer.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

2 In the **Internet Options** window, click **Custom Level**.

Figure 251   Internet Options Security
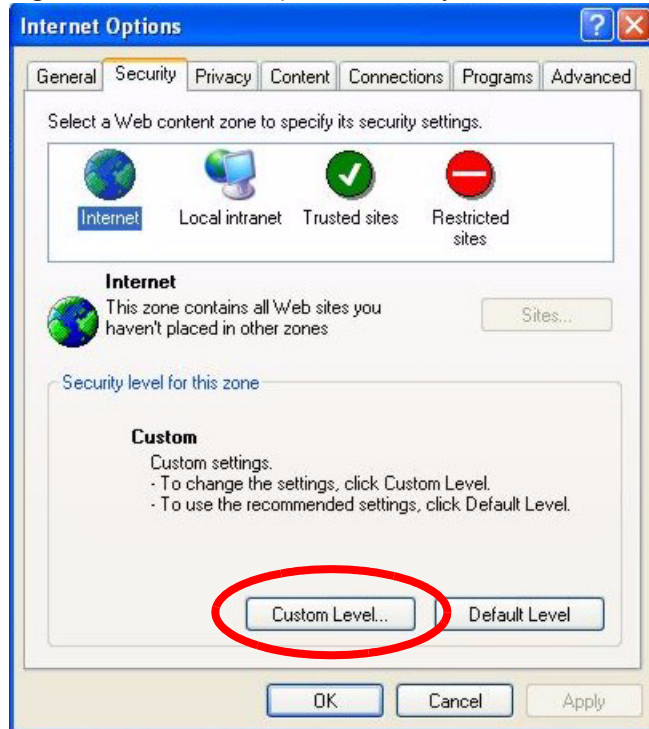
3 Scroll down to **ActiveX controls and plug-ins**.

4 Under **Download signed ActiveX controls** select the **Prompt** radio button.

5 Under **Run ActiveX controls and plug-ins** make sure the **Enable** radio button is selected.

6 Then click the **OK** button.

Figure 252 Security Setting ActiveX Controls
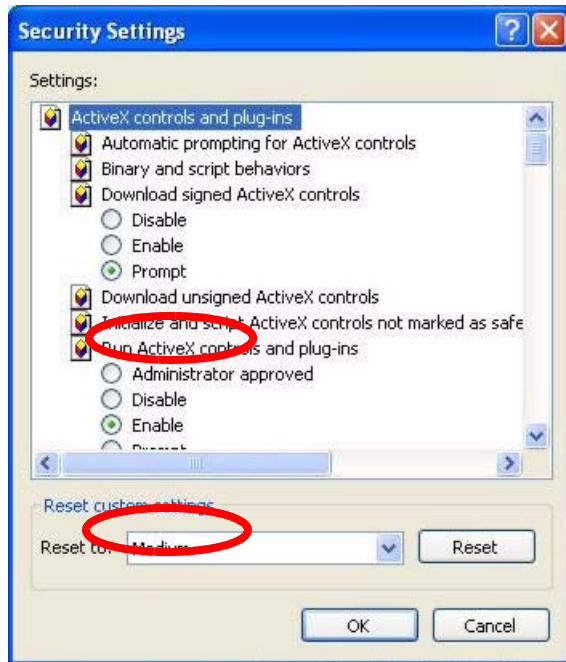
Appendix A
Product Specifications

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

Specification Tables

Table 153   Device

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.32 to 192.168.1.64
Dimensions	P-335: (150 W) x (190 D) x (22 H) mm P-335WT: (190 W) x (133 D) x (32 H) mm
Weight	P-335: 381g P-335WT: 424g
Power Specification	12VDC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
Operation Temperature	0º C ~ 50º C
Storage Temperature	-30º ~ 60º C
Operation Humidity	20% ~ 95%
Storage Humidity	20% ~ 95%

Table 154   Firmware

Standards	IEEE 802.3 Ethernet IEEE 802.3u Fast Ethernet TCP, UDP, ICMP, ARP, RIP - 1/RIP - 2 IP Routing (RFC 791) PPP over Ethernet (RFC 2516) MAC encapsulated routing (ENET encapsulation)
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol. Transparent bridging for unsupported network layer protocols. DHCP Server/Client/Relay RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy UPnP

Table 154 Firmware (continued)

Management	Embedded Web Configurator
	Menu-driven SMT (System Management Terminal) management
	CLI (Command Line Interpreter)
	Remote Management via Telnet or Web
	SNMP manageable
	FTP for firmware downloading, configuration backup and restoration.
	Syslog.
	Built-in Diagnostic Tools for FLASH memory, ADSL circuitry, RAM and LAN port
	Syslog
Wireless (P-335WT only)	IEEE 802.11g Compliance
	Frequency Range: 2.4 GHz
	Advanced Orthogonal Frequency Division Multiplexing (OFDM)
	Data Rates: 54Mbps and Auto Fallback
	Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit.
	WLAN bridge to LAN
	Up to 32 MAC Address filters
	WPA, WPA-PSK
	OTIST (One Touch Intelligent Security Technology)
	IEEE 802.1x
	External Radius server using EAP-MD5, TLS, TTLS
Firewall	Stateful Packet Inspection.
	Prevent Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc.
	Real time E-mail alerts.
	Reports and logs.
NAT/SUA	Port Forwarding
	2048 NAT sessions
	Multimedia application.
	PPTP under NAT/SUA.
	IPSec passthrough
	SIP ALG passthrough.
VPN	2 IPSec tunnels.
Trend Micro Security Service	Anti-virus scan engine, virus pattern version check.
	Web page blocking by category.
Content Filtering	Web page blocking by URL keyword.
Static Routes	8 IP
Other Features	Any IP
	Traffic Redirect
	Dynamic DNS
	IP Alias
	IP Policy Routing
	MBM (Multimedia Bandwidth Management) QoS (Quality of Service)

Appendix B
PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer 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:

- It provides you with a familiar dial-up networking (DUN) user interface.
- 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 and ISDN), the switching fabric is already in place.
- 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 computers use traditional dial-up networking.

Figure 253   Single-Computer per Router Hardware Configuration
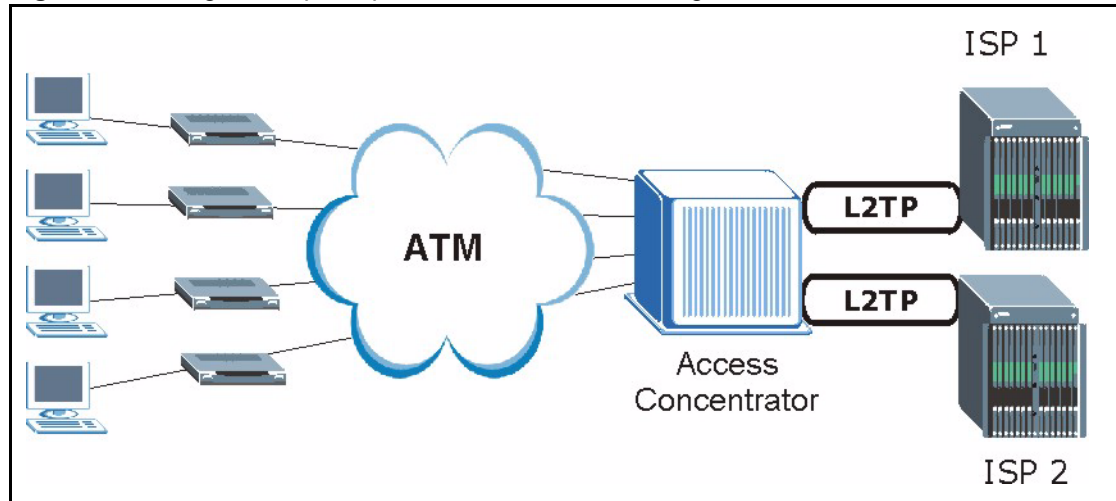
How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer 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 computer and the ISP.

Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the computers 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 computers.

Figure 254   Prestige as a PPPoE Client
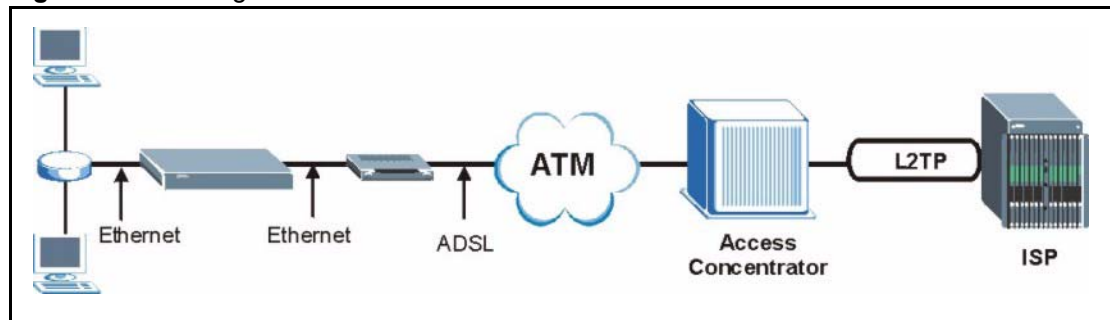
Appendix C
PPTP

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 computer 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 computer 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 computer 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.

Figure 255   Transport PPP frames over Ethernet
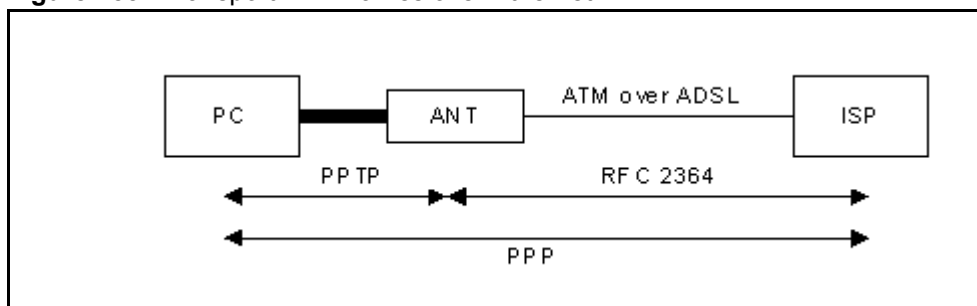
PPTP and the Prestige

When the Prestige is deployed in such a setup, it appears as a computer 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 Prestige's Internet connection. In SUA/NAT mode, the Prestige is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. You need to configure port forwarding for port 1723 to have the Prestige forward PPTP packets to the server. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The Prestige 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.

Figure 256   PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the computer, and hence the Prestige, 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 computer and an ANT.

Figure 257   Example Message Exchange between Computer and an ANT
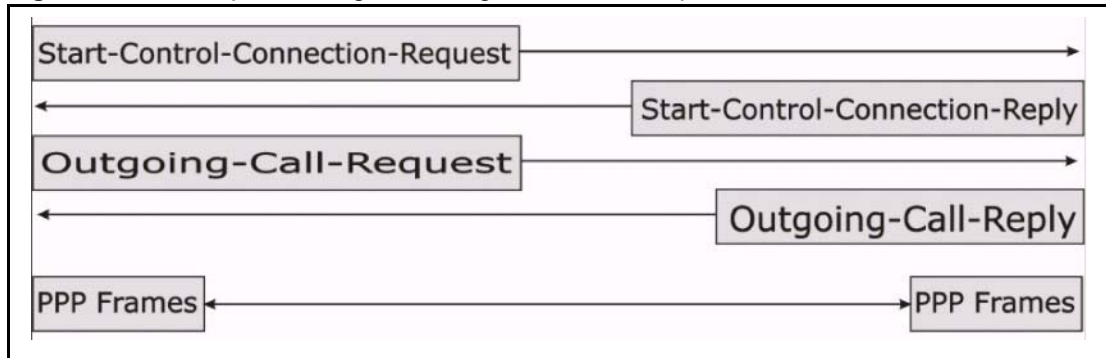
PPP Data Connection

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 D
Print Server

This appendix shows you how to set up a print server for the following operating systems:

- Windows 95
- Windows 98
- Windows 98 SE (Second Edition)
- Windows ME
- Windows 2000
- Windows XP
- Windows NT 4.0
- MAC OS X

- Use the **Setup Wizard for Windows NT/2000/XP** if you want to set up a print server on any of the operating systems listed above except Windows 95, Windows 98, Windows 98 SE (Second Edition), Windows ME and Macintosh OS X

  or

  If you want to use TCP/IP port protocol on any of the operating systems listed above except Macintosh OS X.

- Use the **Setup Wizard for Windows 98/ME/NT/2000/XP** if you want to set up a print server on Windows 95, Windows 98, Windows 98 SE (Second Edition), Windows ME

  or

  If you want to use UDP port protocol on any of the operating systems listed above except Macintosh OS X.

- Use the **Windows 2000/NT/XP : Computer Wizard** if you do not want to use the provided **Setup Wizard for Windows NT/2000/XP** or the **Setup Wizard for Windows 98/ME/NT/2000/XP**.

- Use the **Macintosh OS X** section to set up a print server on a Macintosh with operating system X or higher.

You must have a printer with a driver and you need to know the IP address of the Prestige.

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

TCP/IP should already be installed on computers using Microsoft Windows NT 4.0, Windows 2000, Windows XP and Macintosh OS X.

Installation Requirements

To install the print server driver you will need the following requirements

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows ME, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X
- A computer with an Ethernet port
- RJ-45 cables and a USB cable

The print server must be set up on each computer in your network that you want to use the print server. Before you set up the print server, make sure the USB printer is connected to the Prestige using the USB cable and that both the Prestige and the USB printer are turned on.

Windows NT/2000/XP : Print Server Setup Wizard

Use this wizard if you want to set up your network print server on Windows NT 4.0, Windows 2000 or Windows XP. The **Setup Wizard for Windows NT/2000/XP** allows you to set up your print server using Line Printer Remote (LPR) protocol. LPR is a cross-platform printing protocol that uses TCP/IP to establish connections between printers and computers on a network.

1 Load the CD-ROM that is supplied with the Prestige. Select **Network Print Server Setup**.

2 Click the **Setup Wizard for Windows NT/2000/XP** link.

Figure 258 Network Print Server Setup Wizard
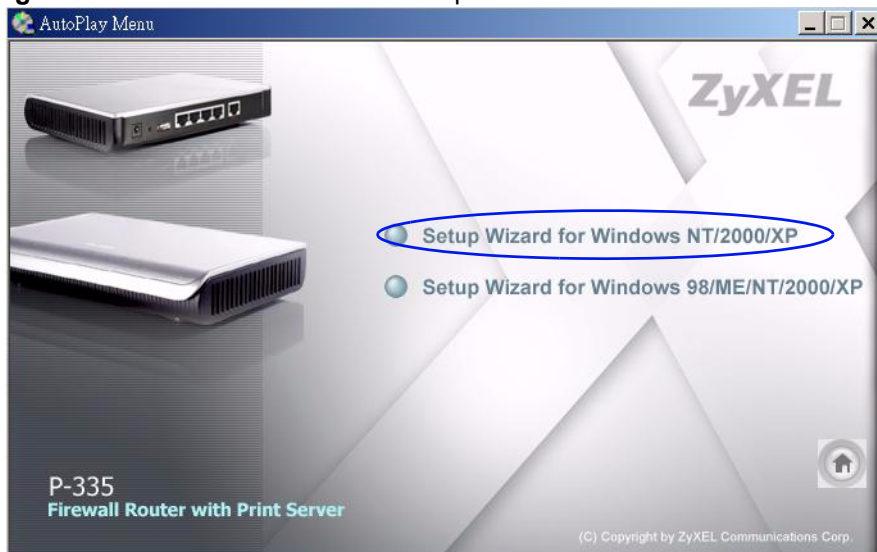
3 The **Welcome** screen displays. Click **Next** to continue.

Figure 259 Network Print Server Setup Wizard : Welcome

4 The **Select A Print Server** screen displays. The wizard automatically detects whether or not a print server is connected to your computer. Make sure that your Prestige is correctly connected and a compatible USB printer is connected to the Prestige. Highlight the print server and click **Next** to continue.

Figure 260 Network Print Server Setup Wizard : Select A Print Server
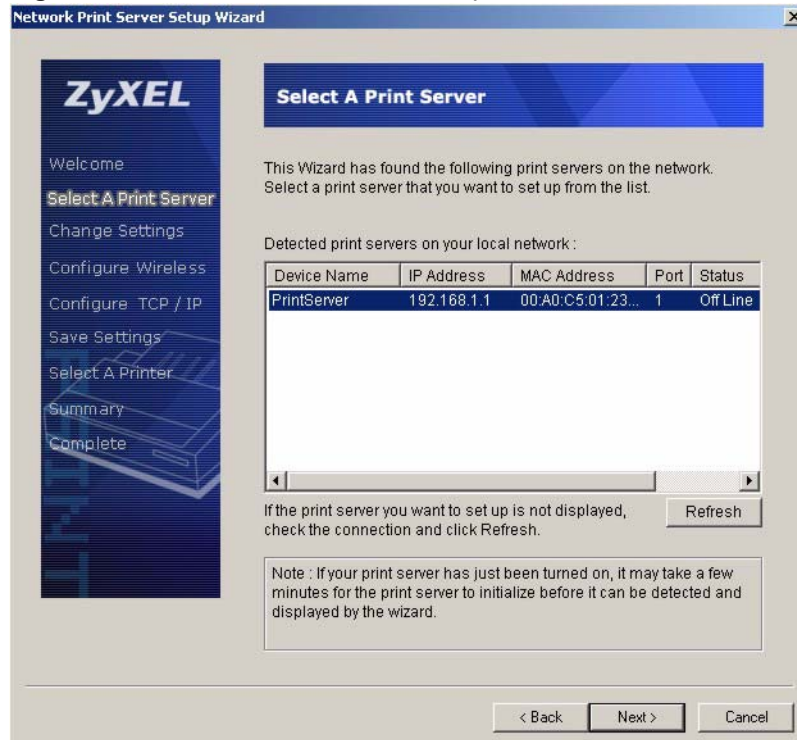
5 The **Change Settings** screen displays. Select the **Yes, I want to change settings** radio button, type a password and click **Next** to change your print server settings. Alternatively select **No, I don't want to change settings** and click **Next** to use the current print server settings and continue with the wizard.

Figure 261 Network Print Server Setup Wizard : Change Settings
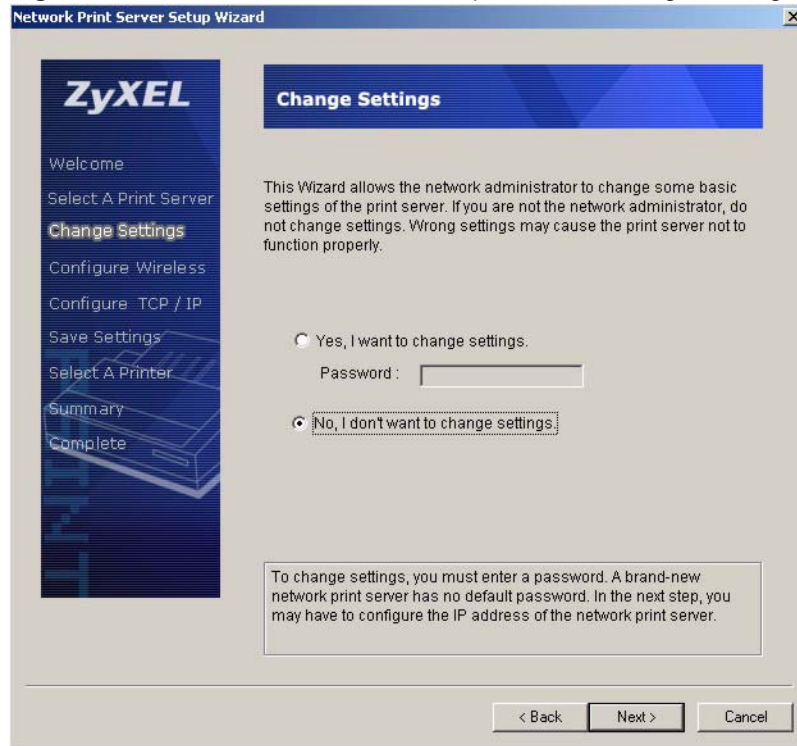
6 Select the printer which is connected to the Prestige USB port.

7 Click **Next** to continue.

Figure 262 Network Print Server Setup Wizard : Select A Printer
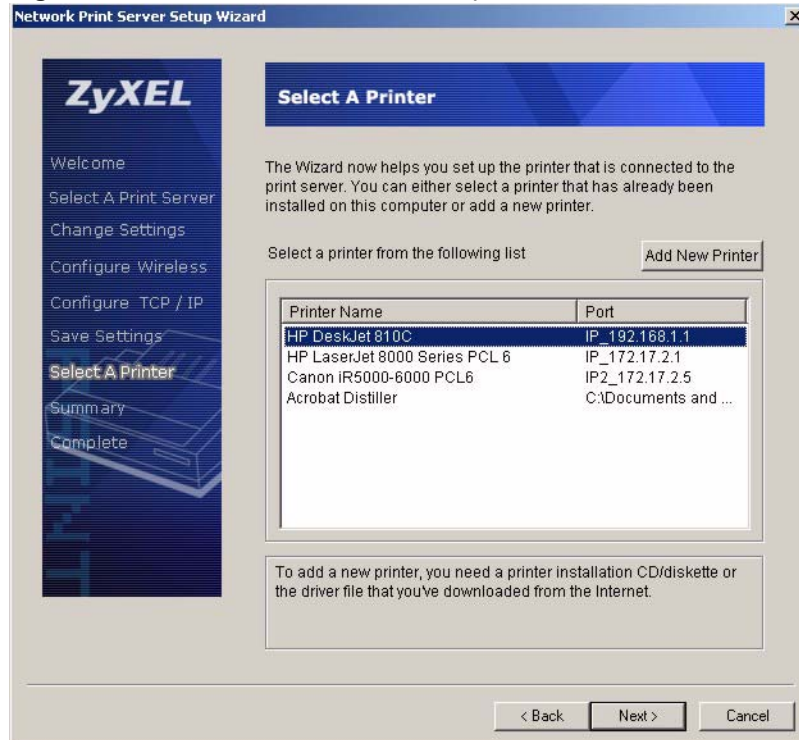
8 If your printer is not listed, you can use the pop-up help dialog box to guide you through the add printer process. After you have added a printer, the **Select A Printer** screen displays again. Select the printer you have added and click **Next** to continue.

Figure 263 Add Printer Help
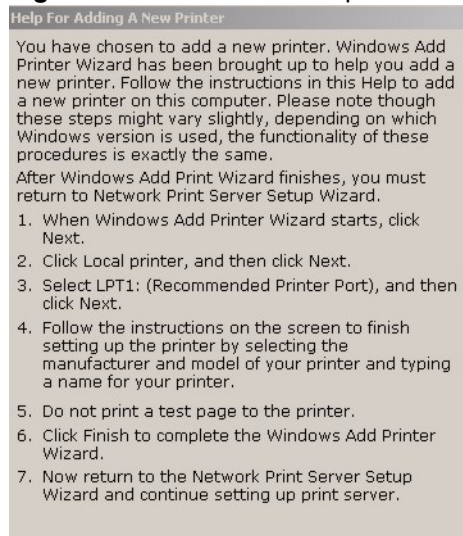
9 A **Summary** screen displays. Check your settings and click **Next** to continue.

Figure 264 Network Print Server Setup Wizard : Summary
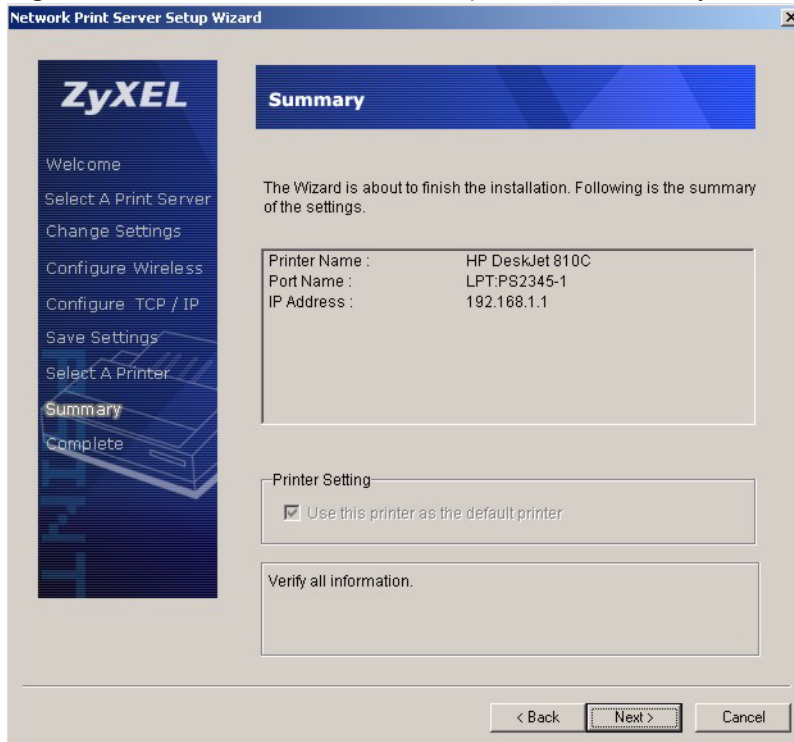
10Click **Finish** to save and close your **Network Print Server Setup Wizard**. Your print server setup is complete.

Figure 265 Network Print Server Setup Wizard : Installation Complete
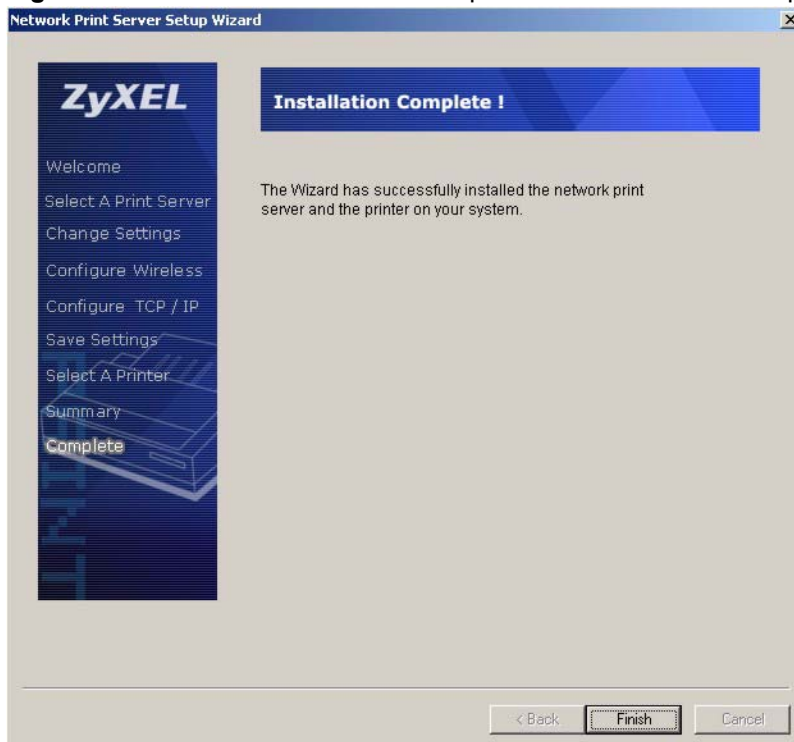
Windows 95/98/ME/NT/2000/XP : Print Server Setup Wizard

The following **Setup Wizard for Windows 98/ME/NT/2000/XP** uses a print server protocol called Line Printer Daemon (LPD). You must use this wizard if you want to set up your network print server on the following operating systems:

- Windows 95
- Windows 98
- Windows 98 SE (Second Edition)
- Windows ME.

LPD is a printing protocol that uses UDP to establish connections between printers and computers on a network.

1 Load the CD-ROM that is supplied with the Prestige. Select **Network Print Server Setup**.

2 Select the **Setup Wizard for Windows 98/ME/NT/2000/XP** link to begin the installation.

Figure 266

3 The **Welcome** screen displays. Read the on-screen information and click **Next** to continue.

Figure 267   Network Print Monitor Setup : Welcome
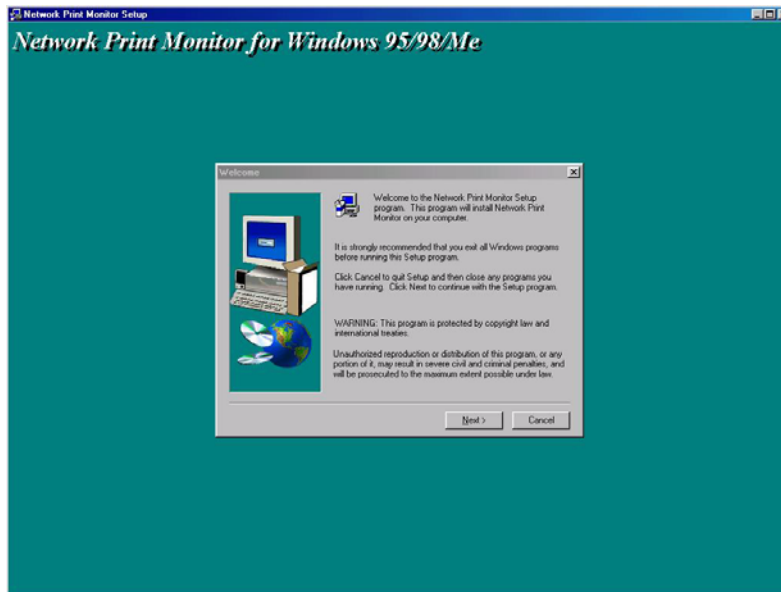
4 The **Choose Destination Location** screen displays. Choose a file location to install your print monitor and click **Next** to continue.

Figure 268   Network Print Monitor Setup : Location
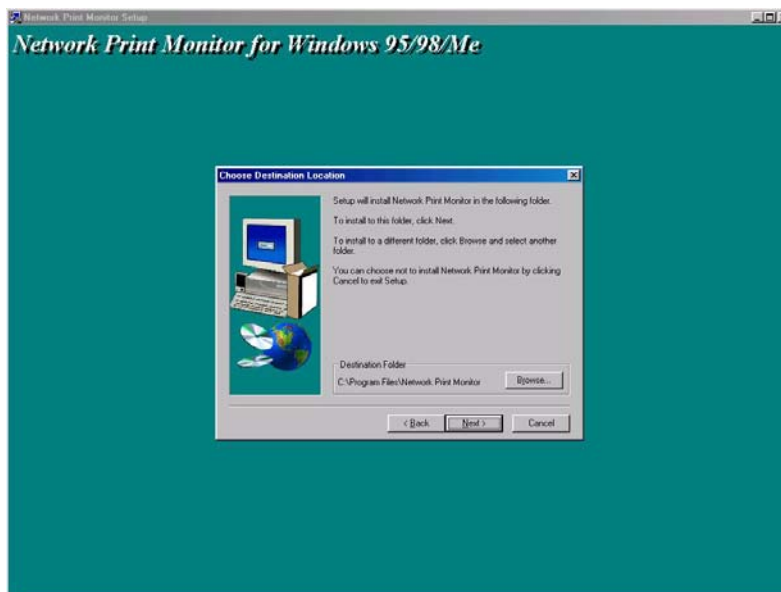
5 The **Setup Complete** screen displays. Click **Finish** to save your settings and close the wizard.

Figure 269 Network Print Monitor Setup : Complete
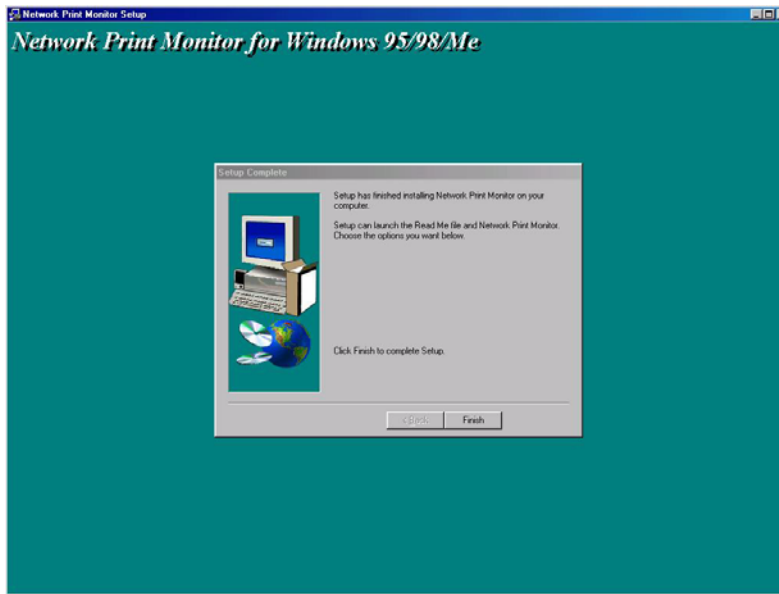
Windows 2000/NT/XP : Computer Wizard

Use the following wizard if you do not want to use the provided setup wizards.Windows 95, Windows 98, Windows 98 SE (Second Edition) and Windows ME have similar print server setups.

1 Click **Start**, **Settings**, **Control Panel** and double-click the **Printers** icon to open the **Printers** window.

2 Double-click the **Add Printer** icon.

Figure 270 Printers Screen
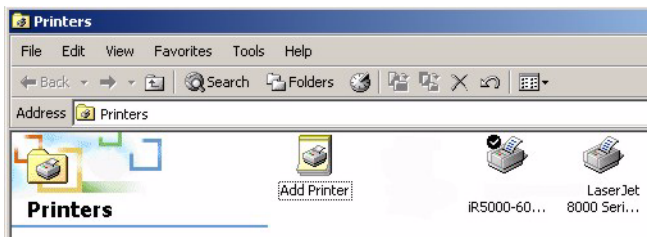
3 The **Add Printer Wizard** screen displays. Click **Next** to continue.

Figure 271 Add Printer Wizard Welcome Screen

4 Select the **Local printer** radio button.

5 Click **Next** to continue.

Figure 272 Local Printer Screen
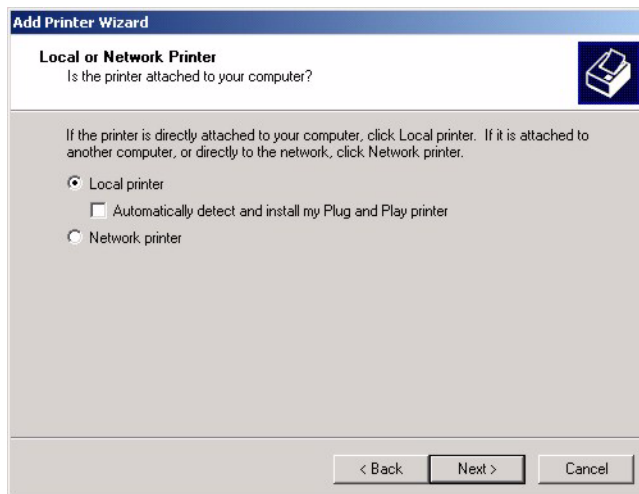
6 Select the **Create a new port** radio button.

7 Choose **Standard TCP/IP Port** from the **Type** drop-down list box.

8 Click **Next** to continue.

Figure 273 Select Printer Port Screen
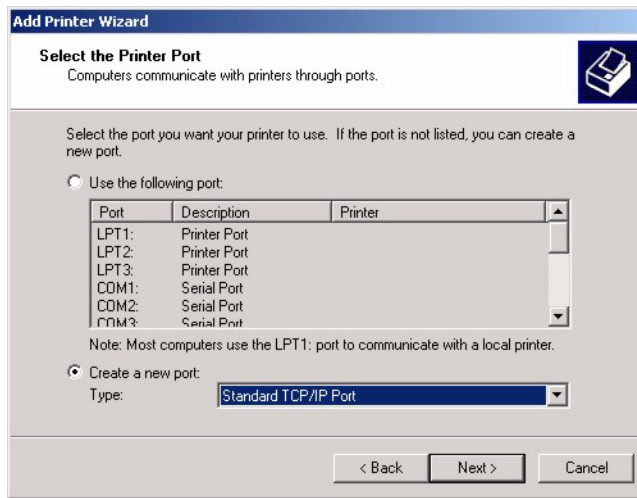
9 Follow the on-screen instructions and click **Next** to continue.

Figure 274 Add Standard TCP/IP Printer Port Screen
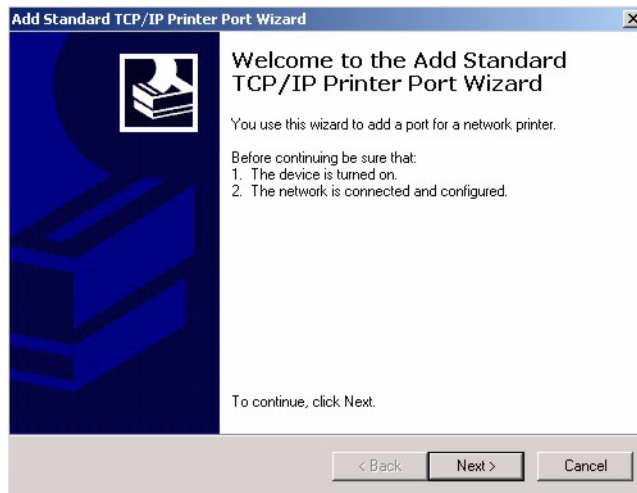
10 Type the **IP Address** of your Prestige. A default **Port Name** displays as you type the **IP Address**. Alternatively type a different name to change the **Port Name**.

11 Click **Next** to continue.

Figure 275   Add Port Screen

12 Select the **Custom** radio button and click the **Settings…** button. Fill in additional print server port information in the following screen.

Figure 276   Additional Port Information Screen

13 Select the **LPR** radio button as the printing **Protocol**.

14 Type **LP1** in the **LPR Settings Queue Name** field.

15 Click the **OK** button to return to the previous screen and then click **Next**.

Figure 277   Port Settings Screen

16 Make sure that your printer port settings are correct. Click the **Finish** button to complete
printer TCP/IP and port set up and then return to the **Add Pinter Wizard**.

Figure 278   Add Standard TCP/IP Printer Port Complete

17 Select the make of the printer that you want to connect to the print server in the
Manufacturers list of printers.

18 Select the printer model from the list of **Printers**.

19 If your printer is not displayed in the list of **Printers**, you can insert the printer driver
disk, click **Have Disk…** and install the new printer driver.

20 Click **Next** to continue.

Figure 279 Add Printer Screen
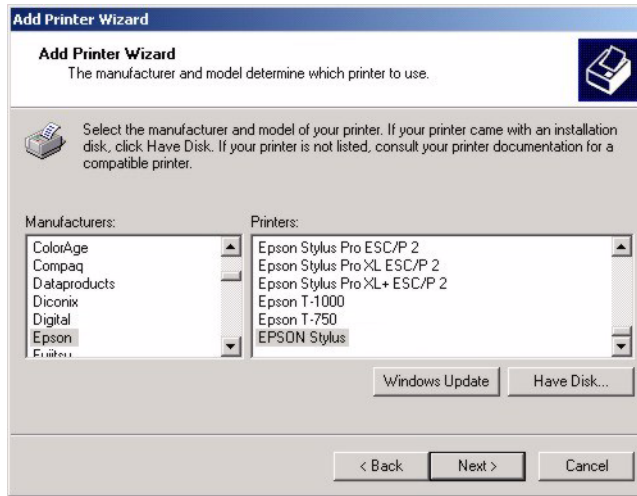
21 If the following screen displays, select **Keep** existing driver radio button if you already have a printer driver installed on your computer and you do not want to change it.

22 Click **Next** to continue.

Figure 280 Use Existing Driver Screen
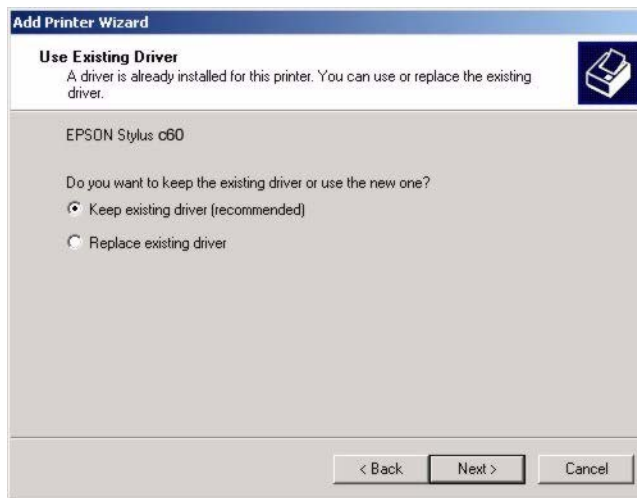
23 Type a name to identify the printer and then click **Next** to continue.

Figure 281 Name Your Printer Screen
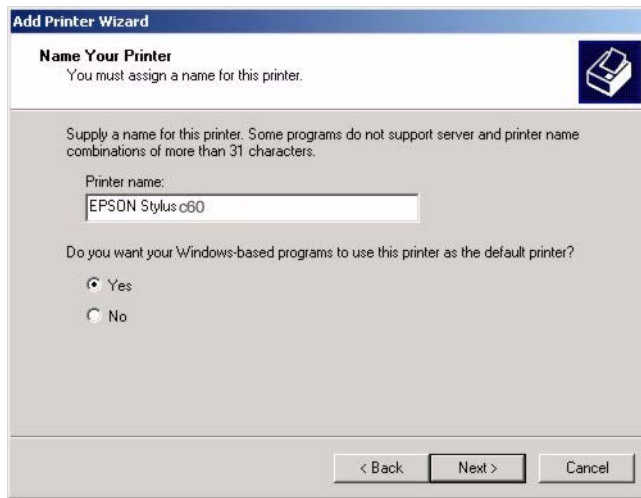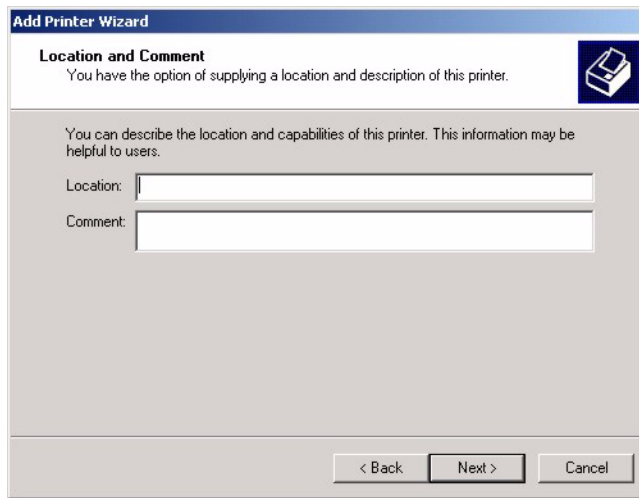
24 Select the **Do not share this printer** radio button.

25 Click **Next** to proceed to the following screen.

Figure 282 Printer Sharing Screen
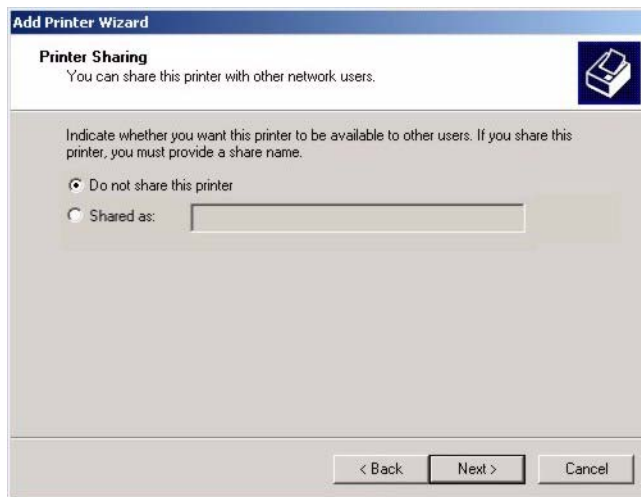
26 These fields are optional. Type where your printer is located in the **Location** field. Type additional information about the printer in the **Comment** field.
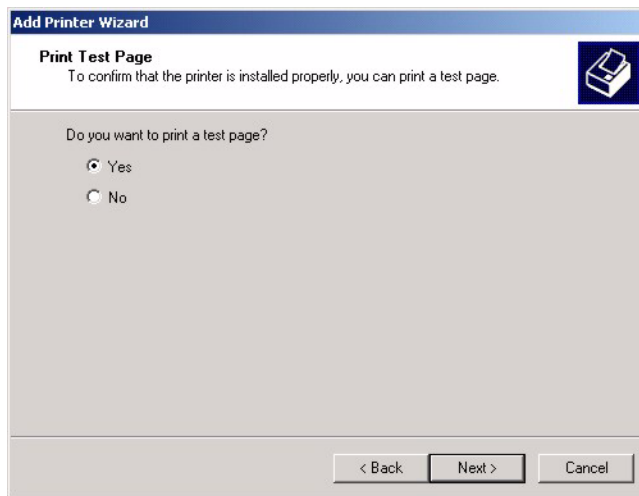
27 Click **Next** to continue.

Figure 283   Location and Comment Screen

28 Select the **Yes** radio button and then click the **Next** button if you want to print a test page.

A pop-up screen displays to ask if the test page printed correctly. Otherwise select the **No** radio button and then click **Next** to continue.

Figure 284   Print Test Page Screen

29 The following screen shows your current printer settings. Select the **Finish** button to complete the print server setup.

Figure 285   Add Printer Wizard Complete

Macintosh OS X

Use the following steps to set up a print server on your Macintosh computer.

1 Click the **Print Center** icon located in the Macintosh Dock. Proceed to step 6 to continue. If the Print Center icon is not in the Macintosh Dock proceed to the next step.

2 On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.

Figure 286   Macintosh HD
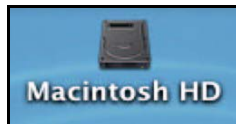
3 Double-click the **Applications** folder.

Figure 287   Macintosh HD folder
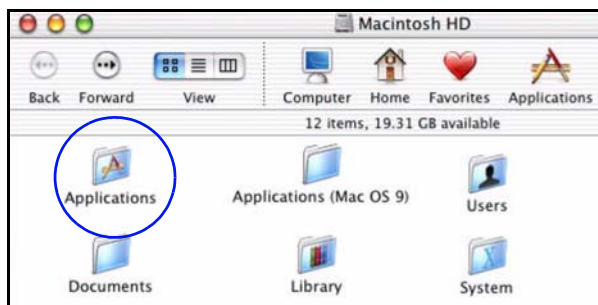
4 Double-click the **Utilities** folder.

Figure 288 Applications Folder
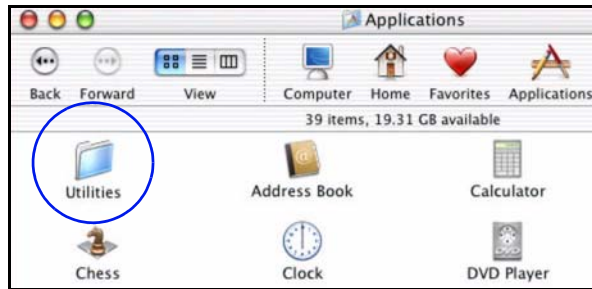
5 Double-click the **Print Center** icon.

Figure 289 Utilities Folder
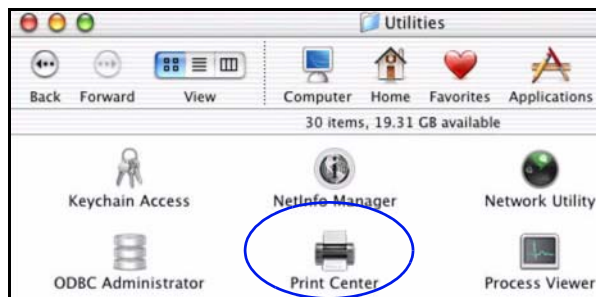
6 Click the **Add** icon at the top of the screen.

Figure 290 Printer List Folder
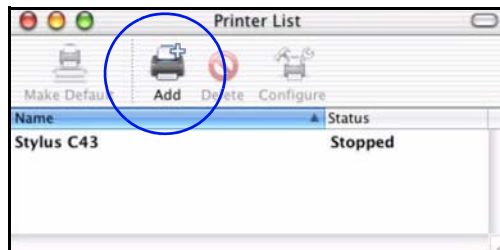
7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.

8 In the **Printer's Address** field, type the IP address of your Prestige.

9 Deselect the **Use default queue on server** check box.

10 Type **LP1** in the **Queue Name** field.

11 Select your **Printer Model** from the drop-down list box. If the printer's model is not listed, select **Generic**.

Figure 291   Printer Configuration
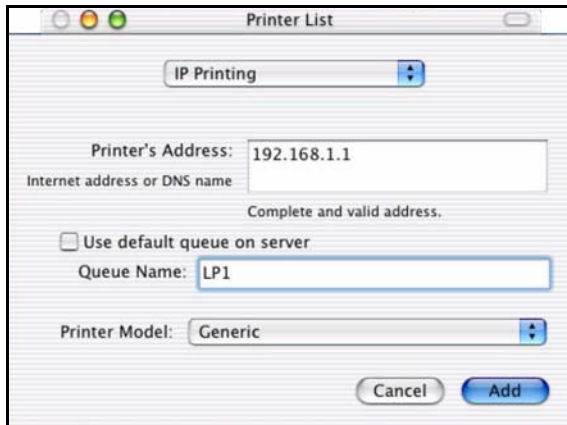
12Click **Add** to select a printer model, save and close the **Printer List** configuration screen.

Figure 292   Printer Model
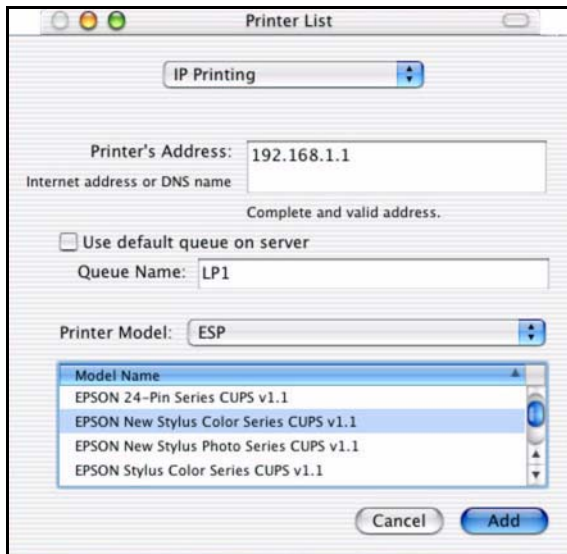
13The **Name** "**LP1 on 192.168.1.1**" displays in the **Printer List** field. The default printer **Name** displays in bold type.

Figure 293 Print Server
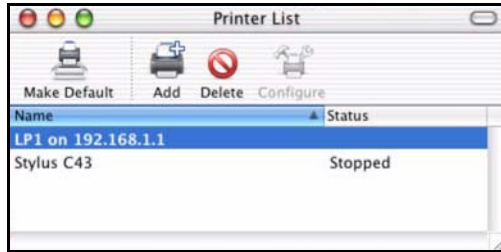
14Your Macintosh print server set up is complete. You can now use the Prestige's print server to print from a Macintosh computer. Refer to the "Print Server" on page 249 for information on your Prestige print server configuration screen.

Appendix E
Print Server Specifications

This appendix provides details on the print server interface and system requirements.

Table 155 Print Server Interface

PRINT SERVER INTERFACE	
USB	USB 1.1 (full speed) - compliant port, 1.5Mbps (low speed) and 12Mbps (full speed) data transmission rates. This port automatically detects the make and model of the USB printer connected to this port.

Table 156 Print Server Requirements and Specifications

PRINT SERVER REQUIREMENTS AND SPECIFICATIONS	
Network Operating System Support	Windows 95/98/98SE/Me Windows NT 4.0/2000/XP/2003 Mac OS X or higher
Network Protocol Support[a]	Print Monitor: UDP • Windows 95/98/98SE/Me • Windows NT 4.0/2000/XP/2003 LPD/LPR (RFC 1179): TCP/IP • Windows NT 4.0/2000/XP/2003 • Mac OS X or higher
DHCP (client) Support	Yes
Management	Web interface Windows-based wizard program

a. Only a printer with a USB connection can be used with the Prestige.

Prestige Print Server Compatible USB Printers

The following is a list of USB printer models compatible with the Prestige print server.

Table 157   Compatible USB Printers

PRINTER MODEL	TYPE
HP DeskJet 810C	Inkjet
HP DeskJet 845C	Inkjet
HP DeskJet 5550	Inkjet
HP DeskJet 1125C	Inkjet
HP DeskJet 1180	Inkjet
HP DeskJet 1220C	Inkjet
HP DeskJet 3535	Inkjet
HP DeskJet 5652	Inkjet
HP Photosmart 7150	Inkjet (Photo)
HP LaserJet 1500L	Laser
HP LaserJet 2200D	Laser
HP LaserJet 2300	Laser
HP LaserJet 3330	Laser (MFP)
HP LaserJet 1200 Series	Laser
Lexmark Z43	
Lexmark Z55	
Lexmark Z705	
Lexmark E210	
Lexmark E322	
Lexmark T420	
Lexmark T620	
Lexmark C750	
Lexmark W812	
Lexmark Z45	
Lexmark Z55	
Canon S200SPX	Inkjet
Canon Pixus Mp730	Inkjet
Canon Pixus 990i	Inkjet
Canon BJF9000	Inkjet
Canon S520	Inkjet
Canon I450	Inkjet
Canon I550	Inkjet
Canon I850	Inkjet
Canon I950	Inkjet
Canon I255	Inkjet
Canon I355	Inkjet
Canon I455	Inkjet
Canon I475D	Inkjet
Canon I560	Inkjet
Canon I865	Inkjet
Canon I905D	Inkjet
Canon I6100	Inkjet
Canon I6500	Inkjet
Canon BJ-330	Inkjet

Table 157   Compatible USB Printers (continued)

PRINTER MODEL	TYPE
Canon BJ F9000	Inkjet
Canon PIXUS 990i	Inkjet
Canon MP730	Inkjet
Epson Stylus C60	Inkjet
Epson Stylus Color 670	Inkjet
Epson Stylus Photo 830U	Inkjet (Photo)
Epson RX510	Inkjet(MFP)
Epson Laser lp-8900	Laser
Epson Stylus Photo 810	Inkjet (Photo)
Epson Stylus Photo 830	Inkjet (Photo)
Epson Stylus Photo 1270	Inkjet (Photo)
Epson Stylus Photo 2100	Inkjet (Photo)
Epson Aculaser C900	Laser
Epson Aculaser C1900	Laser
Epson Aculaser C4100	Laser
Epson EPL5800	
Epson EPL5900	
Epson EPL6100	
Epson CX3100	
Samsung ML-1710	
Samsung ML-1750	Laser
Samsung SRP 270	
IBM Infoprint 1412	Laser
IBM Infoprint 1332	Laser
Xerox Phaser 3310	Laser
Xerox 3310	
Kyocera PS-1010	Laser
Kyocera 1020D	Laser
Kyocera 1920	Laser
Kyocera FS-1010	Laser
Panasonic KX-P1121	Laser
Panasonic KX-P1624	

Appendix F
NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands.

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 :

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or disallow the sending of NetBIOS packets through VPN connections.
- Allow or disallow NetBIOS packets to initiate calls.

Display NetBIOS Filter Settings

```
sys filter netbios disp
```

This command gives a read-only list of the current NetBIOS filter modes for The Prestige.

NetBIOS Display Filter Settings Command Example

```
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Block
        Between LAN and DMZ: Block
        Between WAN and DMZ: Block
        IPSec Packets: Forward
        Trigger Dial: Disabled
```

The filter types and their default settings are as follows.

Table 158 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
Between LAN and WAN	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the WAN.	Block
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 = Between LAN and WAN
	3 = IPSec packet pass through
	4 = Trigger Dial
`<on|off>` =	For type 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 3, 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 4, use on to allow NetBIOS packets to initiate dial backup calls. Use off to block NetBIOS packets from initiating dial backup calls.

Example commands

`sys filter netbios config 0 on`	This command blocks LAN to WAN and WAN to LAN NetBIOS packets.
`sys filter netbios config 3 on`	This command blocks IPSec NetBIOS packets.
`sys filter netbios config 4 off`	This command stops NetBIOS commands from initiating calls.

Appendix G
Log Descriptions

Configure centralized logs using the embedded web configurator; see online help for details. This appendix provides descriptions of example log messages.

Table 159   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.

Table 160   System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`DHCP client gets %s`	A DHCP client got a new IP address from the DHCP server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`SMT Login Successfully`	Someone has logged on to the router's SMT interface.
`SMT Login Fail`	Someone has failed to log on to the router's SMT interface.
`WEB Login Successfully`	Someone has logged on to the router's web configurator interface.
`WEB Login Fail`	Someone has failed to log on to the router's web configurator interface.
`TELNET Login Successfully`	Someone has logged on to the router via telnet.
`TELNET Login Fail`	Someone has failed to log on to the router via telnet.
`FTP Login Successfully`	Someone has logged on to the router via ftp.
`FTP Login Fail`	Someone has failed to log on to the router via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`!! 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.

Table 161 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 162 ICMP Type and Code Explanations

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Appendix H
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 Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 294 WIndows 95/98/Me: Network: Configuration
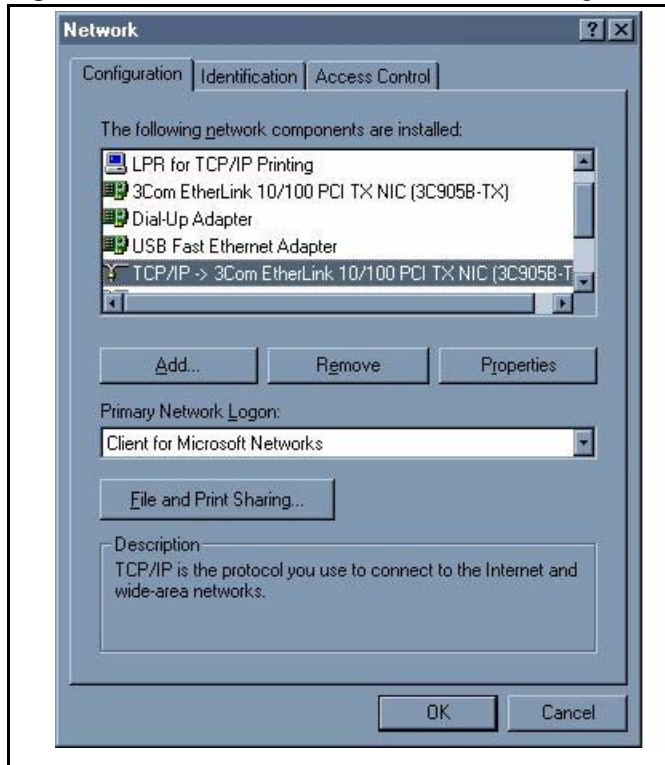
Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 295 Windows 95/98/Me: TCP/IP Properties: IP Address
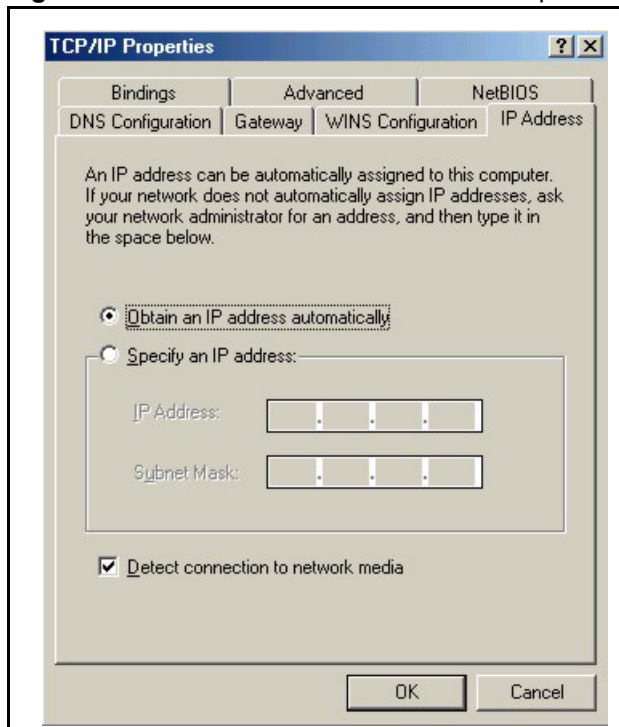
3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 296   Windows 95/98/Me: TCP/IP Properties: DNS Configuration
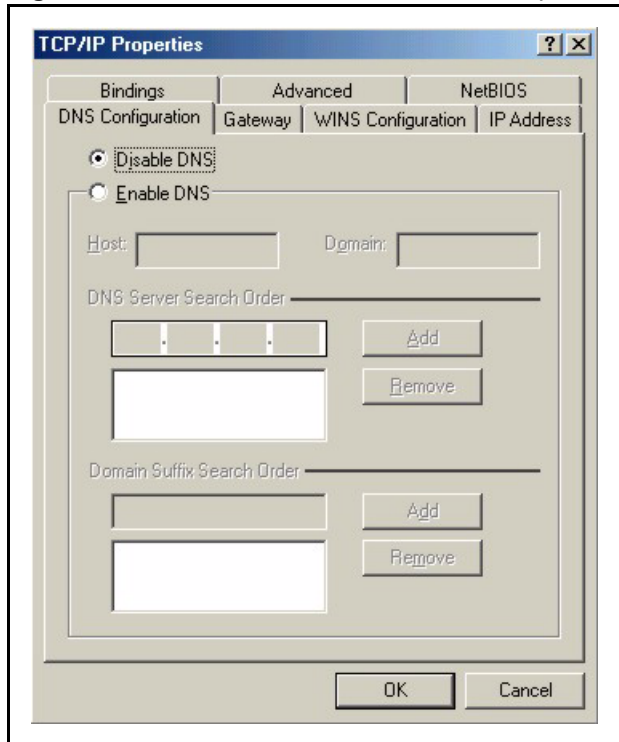
4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

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

Windows 2000/NT/XP

1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 297 Windows XP: Start Menu
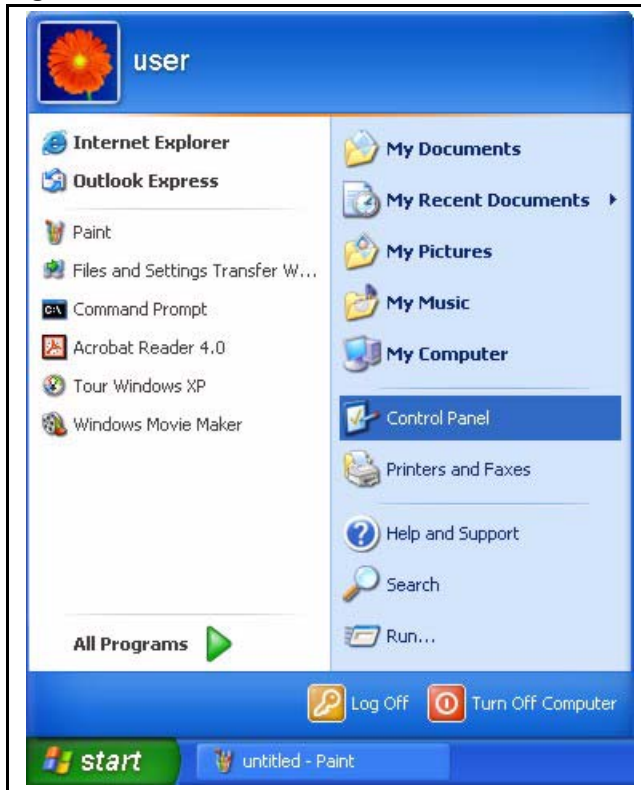
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 298 Windows XP: Control Panel

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

Figure 299   Windows XP: Control Panel: Network Connections: Properties
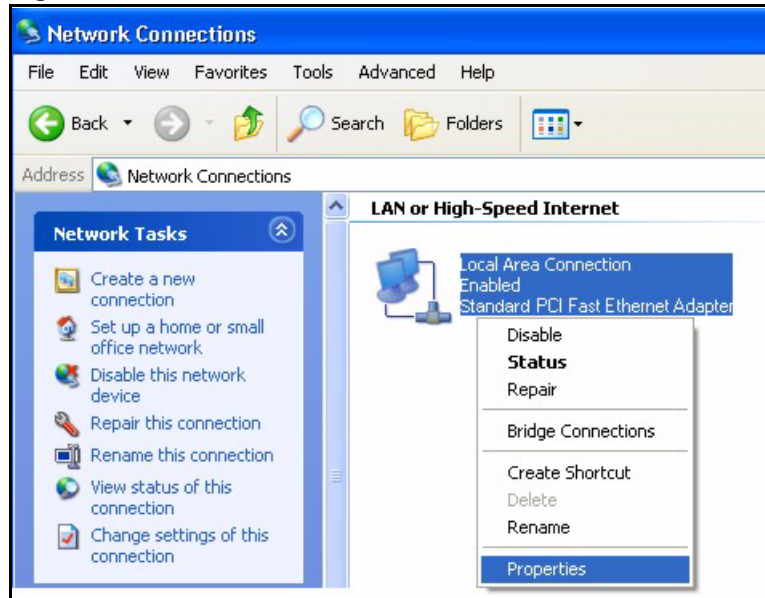
4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 300   Windows XP: Local Area Connection Properties
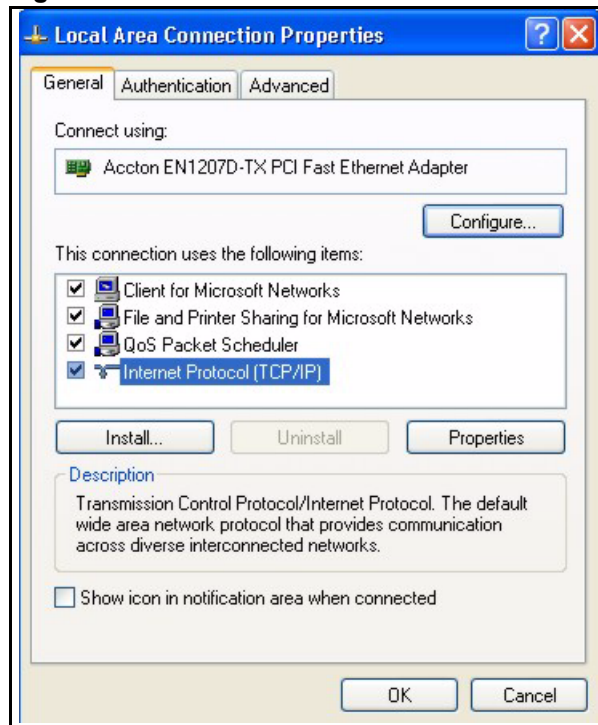
5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 301   Windows XP: Advanced TCP/IP Settings
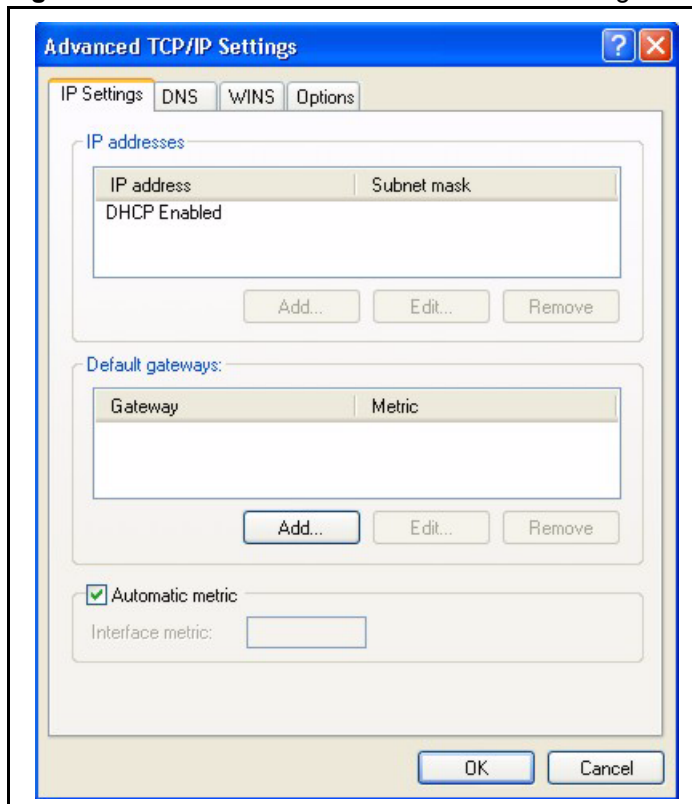
6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settin**gs tab and click **OK**.

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.

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

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 302 Windows XP: Internet Protocol (TCP/IP) Properties
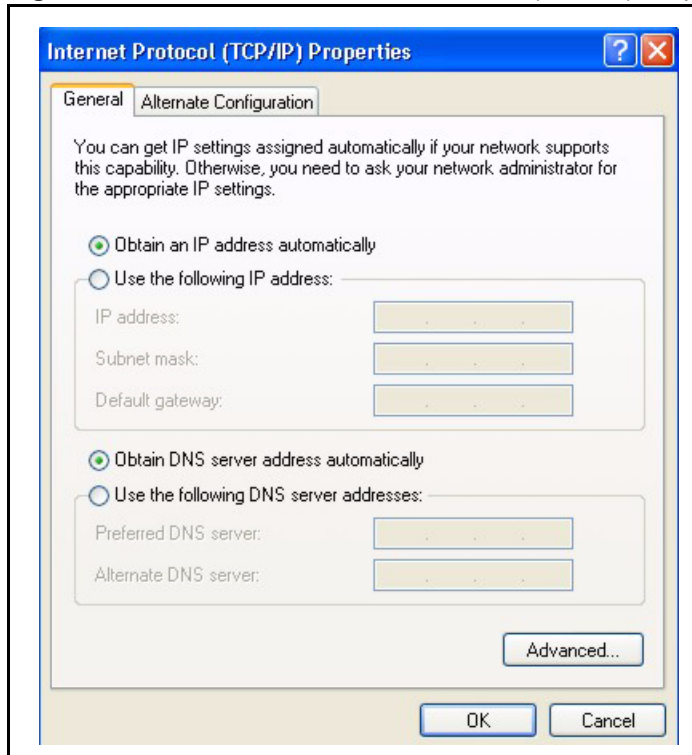
8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

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

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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

Figure 303 Macintosh OS 8/9: Apple Menu
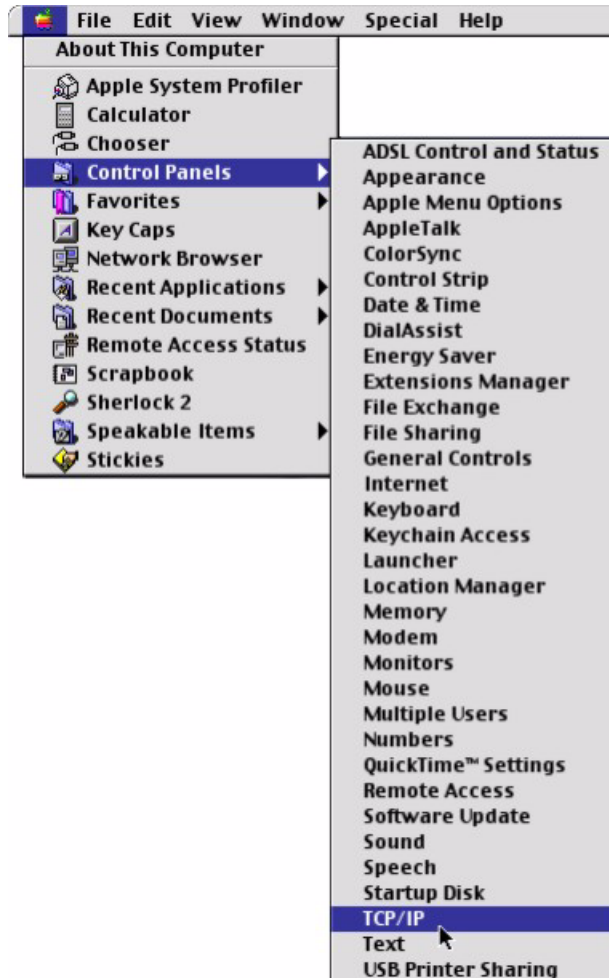
2 Select **Ethernet built-in** from the **Connect via** list.

Figure 304 Macintosh OS 8/9: TCP/IP
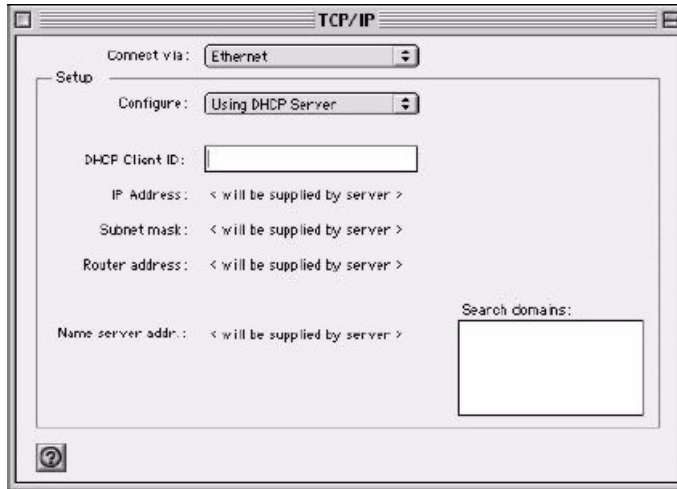
3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige 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 Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 305 Macintosh OS X: Apple Menu
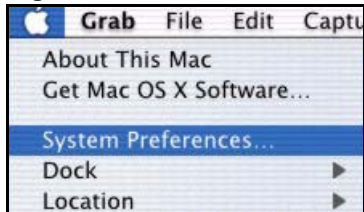
2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.

> - Select **Built-in Ethernet** from the **Show** list.
> - Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 306 Macintosh OS X: Network
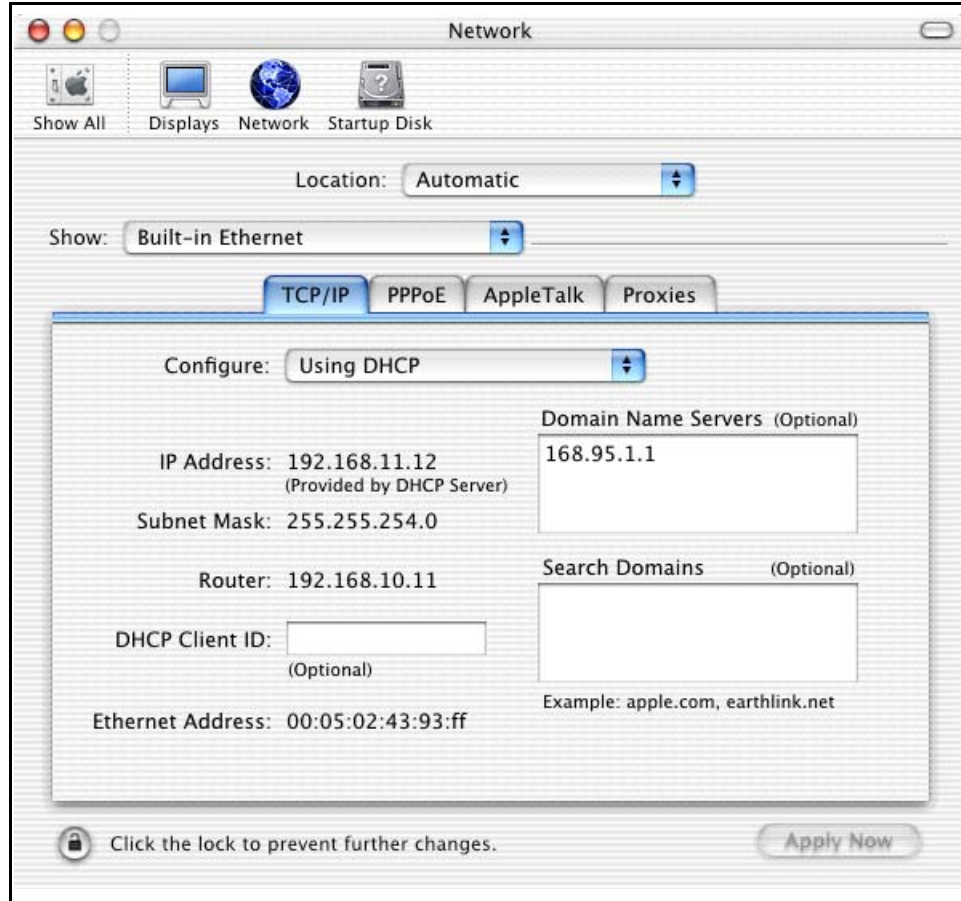
4 For statically assigned settings, do the following:

> - From the **Configure** box, select **Manually**.
> - Type your IP address in the **IP Address** box.
> - Type your subnet mask in the **Subnet mask** box.
> - Type the IP address of your Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix I
Wireless LANs

Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 307   Peer-to-Peer Communication in an Ad-hoc Network
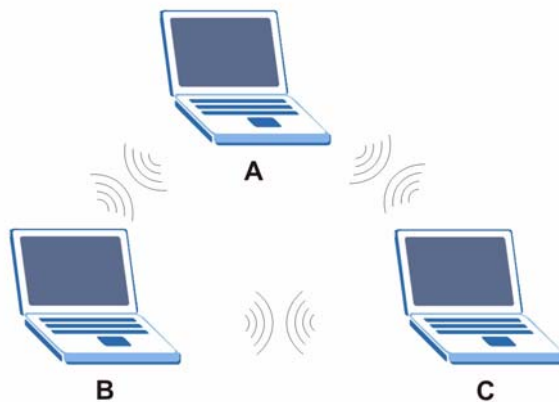
BSS

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

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

Figure 308 Basic Service Set
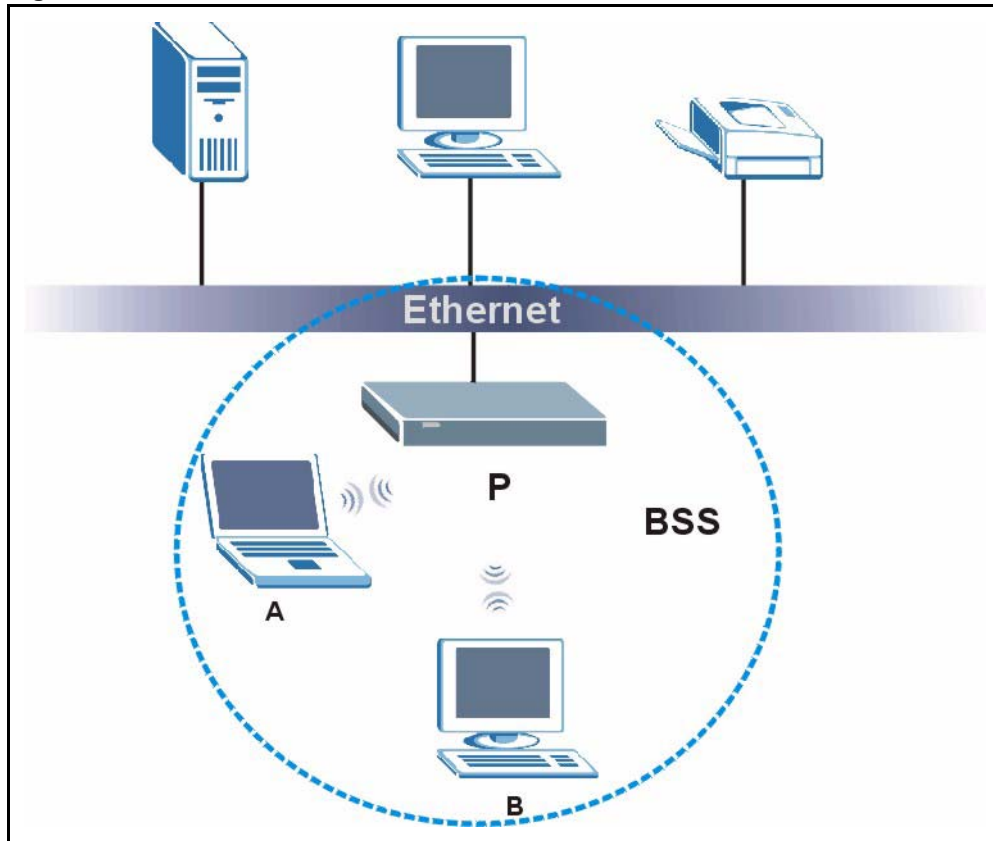
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

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

Figure 309 Infrastructure WLAN
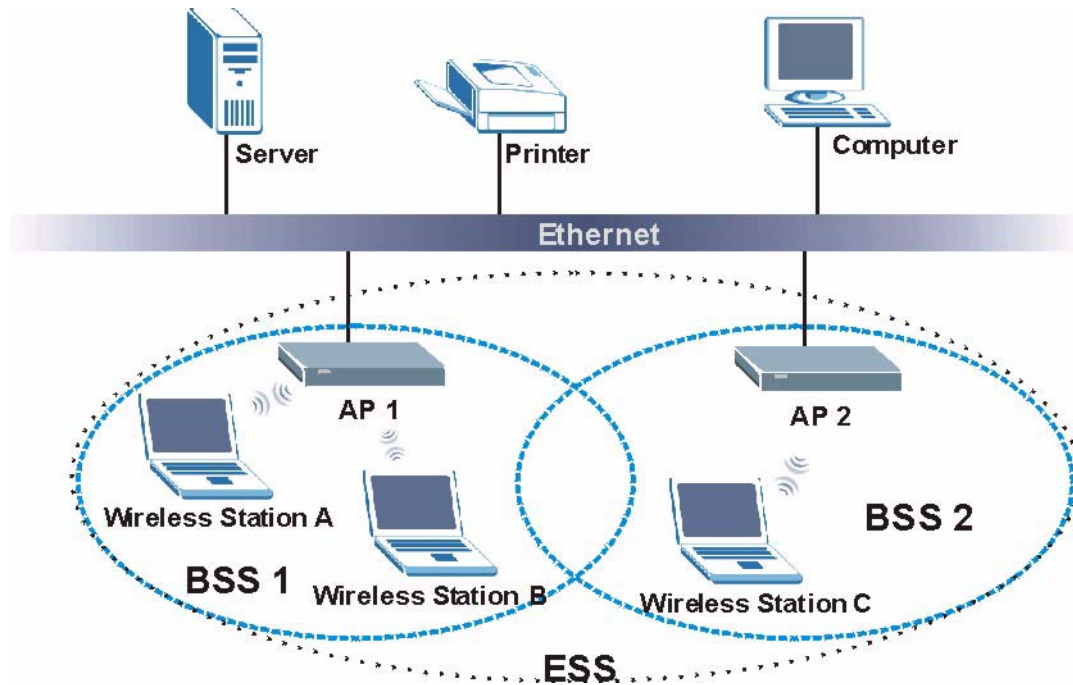
Channel

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

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

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 310 RTS/CTS
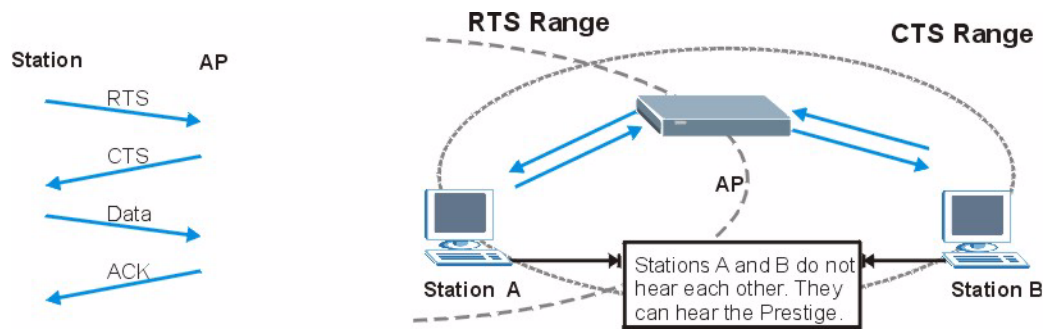
When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

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

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

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

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

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

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

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

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

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 163   IEEE802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS

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

- Authentication

  Determines the identity of the users.

- Authorization

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

- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station 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.

EAP Authentication

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

The type of authentication you use depends on the RADIUS server or the AP.

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

Figure 311 EAP Authentication
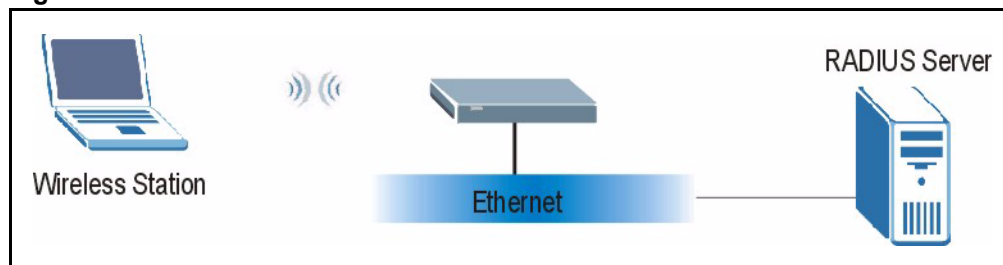
The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

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

2 The device sends a "request identity" message to the wireless station for identity information.

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

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

Types of Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

WEP Authentication Steps

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared Key**, and **Auto**. The following figure illustrates the steps involved.

Open system authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network.

Shared key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

When your device authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the device will accept either type of authentication request and the device will fall back to use open authentication if the shared key does not match.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 164   Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA

User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

Encryption

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

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

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

AES (Advanced Encryption Standard) also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data.

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

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

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

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 165 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	ENABLE IEEE 802.1X
Open	None	No	No
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Yes
WPA	TKIP	No	Yes
WPA-PSK	WEP	Yes	Yes
WPA-PSK	TKIP	Yes	Yes

Roaming

A wireless station is a device with an IEEE 802.11 mode compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

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

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in see Figure 313.

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless station may not be able to communicate with other wireless stations on the network and vice versa.

Figure 313 Roaming Example
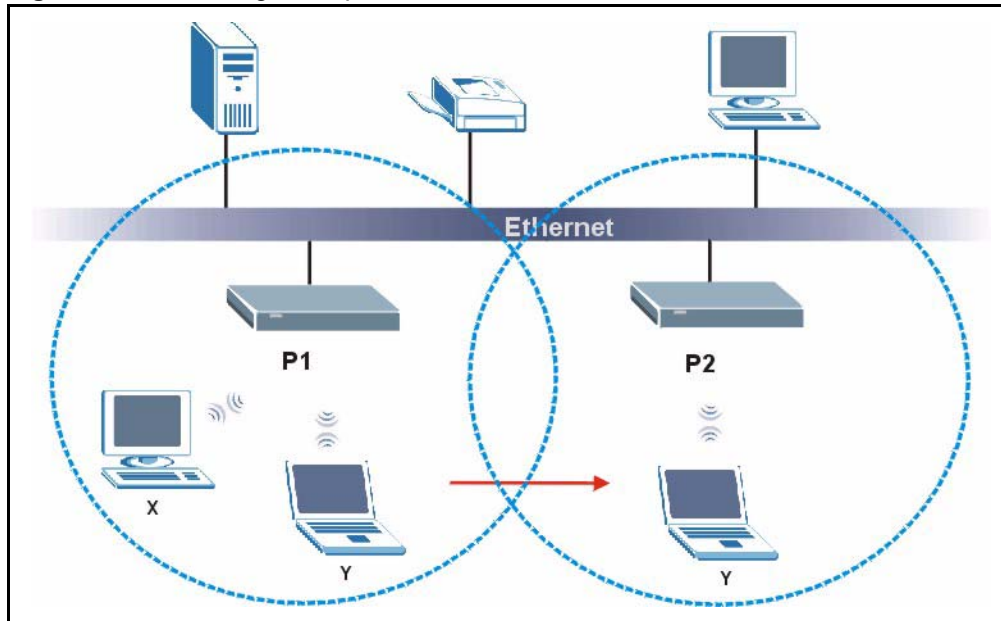
The steps below describe the roaming process.

1 As wireless station **Y** moves from the coverage area of access point **P1** to that of access point

2 **P2**, it scans and uses the signal of access point **P2**.

3 Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.

4 Access point **P1** updates the new position of wireless station.

5 Wireless station **Y** sends a request to access point **P2** for re-authentication.

Requirements for Roaming

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

1 All the access points must be on the same subnet and configured with the same ESSID.

2 If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.

3 The adjacent access points should use different radio channels when their coverage areas overlap.

4 All access points must use the same port number to relay roaming information.

The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

Appendix J
Antenna Selection and Positioning Recommendation

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Choosing the right antennas and positioning them properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less directional) to 90 degrees (very directional). The directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to –point application, position both transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Appendix K
Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password.

Table 166 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.

Appendix L
Triangle Route

The Ideal Setup

When the firewall is on, your Prestige 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 Prestige to protect your LAN against attacks.

Figure 314 Ideal Setup
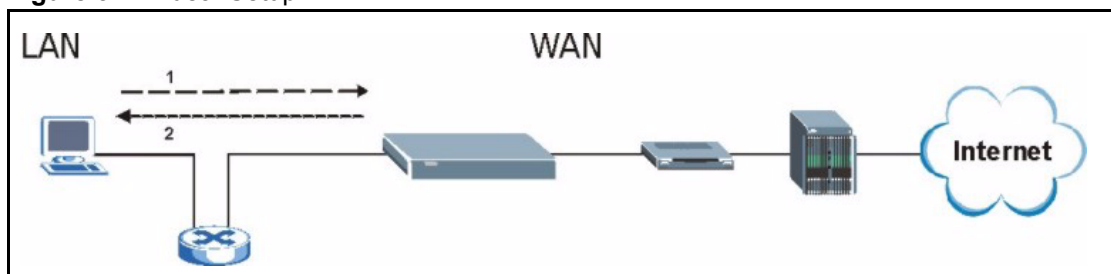
The "Triangle Route" Problem

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.

1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

2 The Prestige reroutes the SYN packet through Gateway **B** on the LAN to the WAN.

3 The reply from the WAN goes directly to the computer on the LAN without going through the Prestige.

As a result, the Prestige resets the connection, as the connection has not been acknowledged.

Figure 315 "Triangle Route" Problem
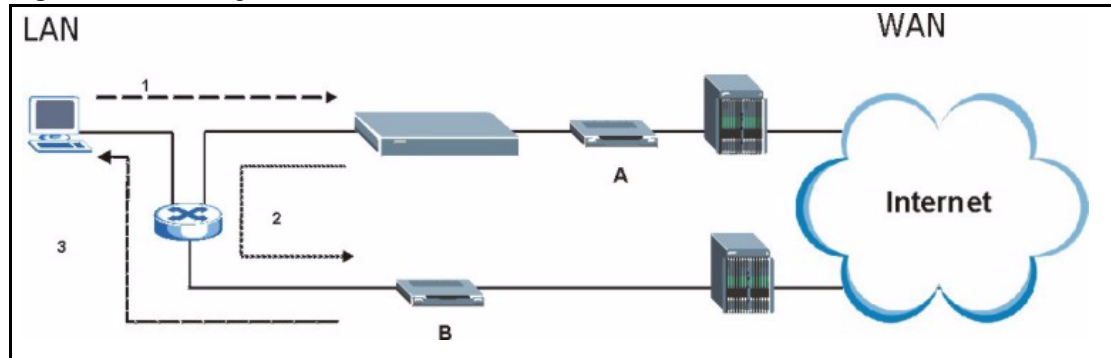
The "Triangle Route" Solutions

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 Prestige supports up to three logical LAN interfaces with the Prestige 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 Prestige to your LAN. The following steps describe such a scenario.

1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

2 The Prestige reroutes the packet to Gateway B, which is in the 192.168.2.1 to 192.168.2.24 subnet.

3 The reply from WAN goes through the Prestige to the computer on the LAN in the 192.168.1.1 to 192.168.1.24 subnet.

Figure 316   IP Alias
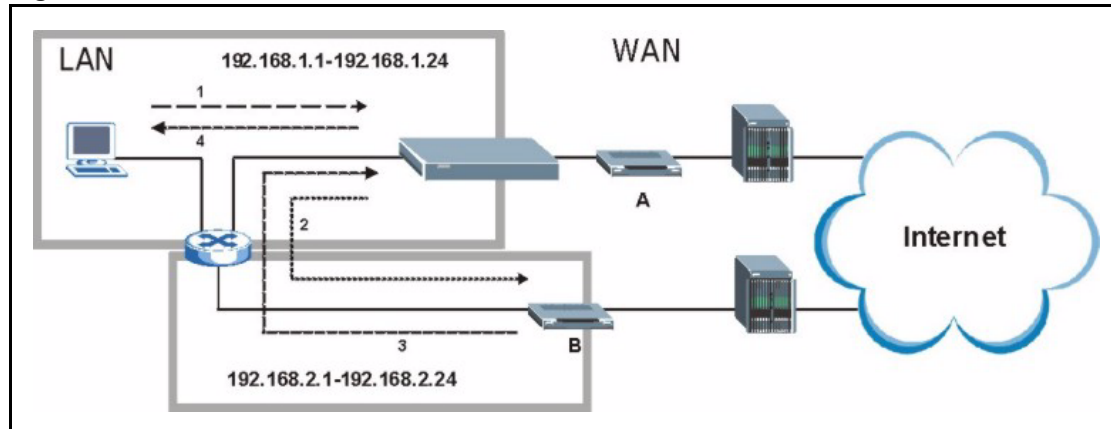
Gateways on the WAN Side

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 Prestige to your LAN. Therefore your LAN is protected.

Figure 317   Gateways on the WAN Side
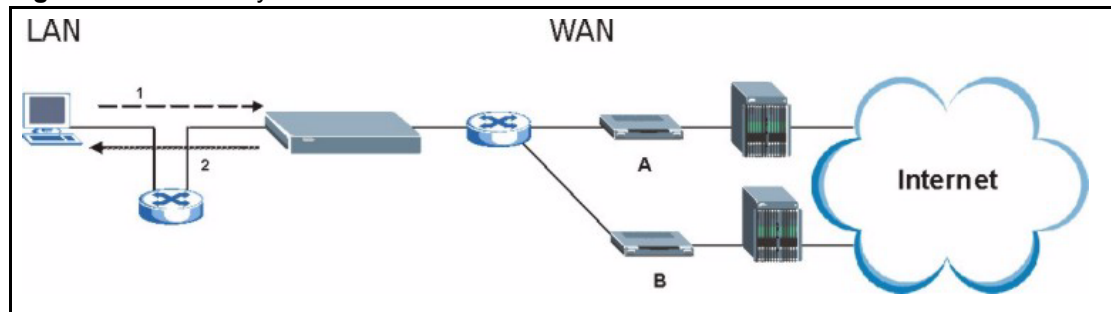
How To Configure Triangle Route

1 From the SMT main menu, enter 24.

2 Enter "8" in menu 24 to enter CI command mode.

3 Use the following command to allow triangle route:

```
sys firewall ignore triangle all on
```

or this command to disallow triangle route:

```
sys firewall ignore triangle all off
```

Appendix M
myZyXEL.com

Introduction

myZyXEL.com is ZyXEL's online services center where you can register your ZyXEL device. You can also generate an activation key and service set key that may be needed to use device-specific feature(s).

A Note on myZyXEL.com Numbers

You need the following (unique) numbers to install and activate device-specific feature(s).

Table 167   myZyXEL.com Numbers

TYPES	DESCRIPTION
Serial Number	You need the serial number to register your ZyXEL device. Locate the serial number on your ZyXEL device.
Authentication Code	This is the MAC address of your ZyXEL device. You need this number to register your ZyXEL device at myZyXEL.com. Locate the MAC address on your ZyXEL device.

myZyXEL.com Account Login

1 Go to myZeXEL.com using your web browser.

2 Create a new account (if you don't have one already) with a user name and password by filling in an account registration form at myZyXEL.com.

Figure 318 myZyXEL.com Login Screen

Note: You are automatically logged out of your myZyXEL.com account after five minutes of inactivity. Simply log back into your myZyXEL.com account if this happens to you.

Registering Your ZyXEL Device

1 After you have created a myZyXEL.com account, log in and register your ZyXEL device by clicking the hyperlink as shown in the next screen.

Figure 319 Logged Into myZyXEL.com

2 Click **Add** in the next screen.

Figure 320 Product Registration
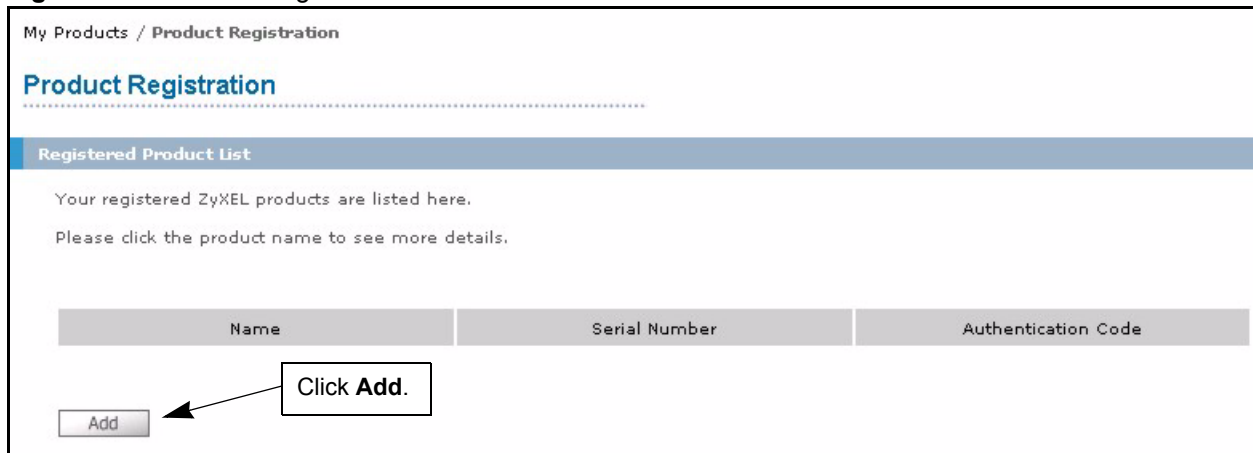
3 The **Add New Product** screen displays. Enter the produce serial number in the **Serial Number** field.

4 Your device category and model number automatically display in the **Category** and **Model** fields respectively. Otherwise, select the correct ones from the drop-down list boxes.

5 Enter the device MAC address in the **Authentication Code** field.

6 Enter a descriptive name in the **Friendly Name** field for identification purposes.

7 Click **Register**.

Figure 321   Add New Product

8 Specify the purchase information and click **Continue**.

Figure 322   Product Survey
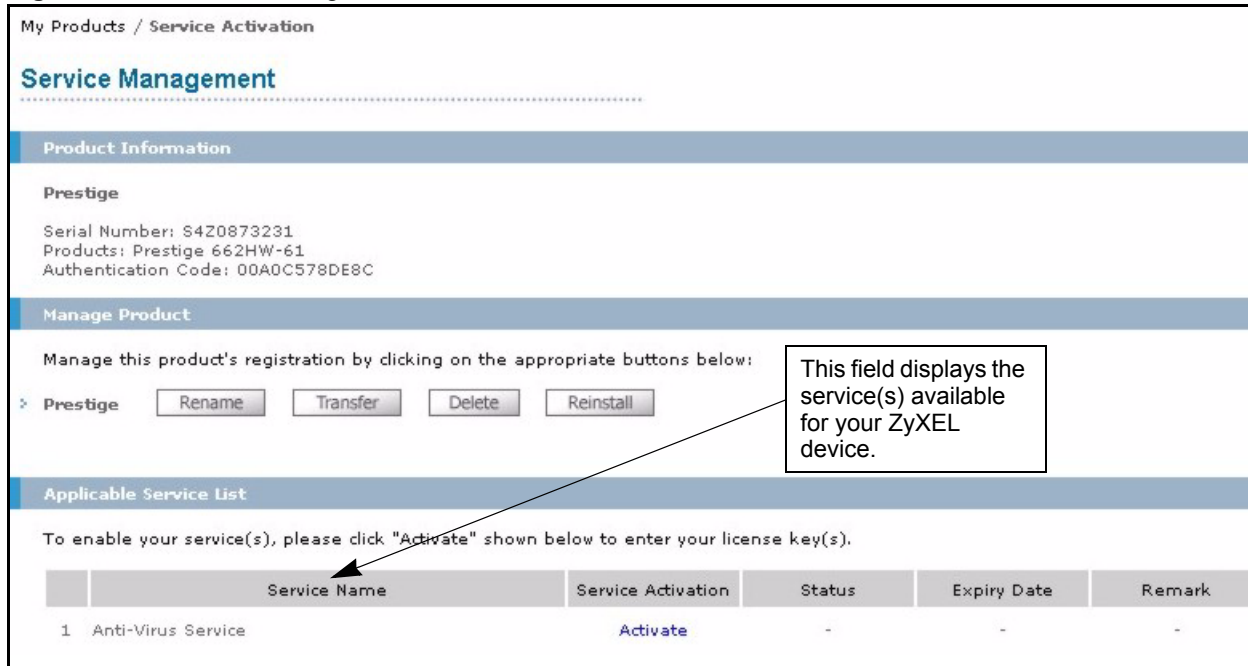
9 Click **Continue** again.

10 After you have registered your ZyXEL device, you can view its registration details in the screen shown next.

Figure 323 Service Management
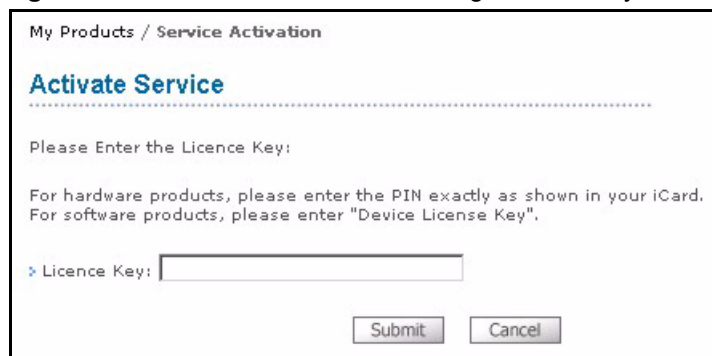
Activating a Service

The product is now registered but the related service(s) is *not* activated. You need to activate the service(s) before you can use it on your ZyXEL device.

1 Display the **Service Management** screen (see Figure 323) for your registered ZyXEL device (click **My Product** and the link for your ZyXEL device).

2 Click **Activate** for the corresponding service to display the next screen.

Figure 324 Service Activation: Entering Licence Key

3 Enter the license key exactly as displayed on the iCard that you have purchased or that comes with your ZyXEL device. Click **Submit**.

4 A screen displays indicating that you have successfully activated a service.

Congratulations! You have successfully registered your ZyXEL device and activated a service at myZyXEL.com.

Note: You must then activate the service(s) on your ZyXEL device via its web configurator to start using the service(s).

Index

Numerics

E

EAP **97**
EAP Authentication **483**, **484**
ECHO **148**
Edit IP **306**
eDonkey **256**
E-Mail **256**
eMule **256**
Encapsulation **306**, **309**
Encryption **487**
ESS **478**
Ethernet **427**
Ethernet Encapsulation **148**, **305**, **306**
Extended Service Set **478**
Extended Service Set IDentification **100**

F

Factory LAN Defaults **87**
Fail Tolerance **313**
Filename Conventions **371**
Filter **291**, **311**
   Applying **346**
   Example **343**
   Generic Filter Rule **341**
   Generic Rule **342**
   NAT **345**
   Remote Node **347**
   Structure **336**
Filter Log **364**
Finger **148**
Finland, Contact Information **7**
Firewall **183**, **184**
   Access Methods **333**
   Remote Management **333**
   SMT Menus **333**
Firmware File
   Maintenance **270**, **273**
Fragmentation Threshold **480**
Fragmentation threshold **480**
France, Contact Information **7**
FTP **81**, **87**, **147**, **148**, **197**, **201**, **390**
FTP File Transfer **378**
FTP Restrictions **197**, **374**, **390**
FTP Server **328**

G

Gateway **316**
Gateway IP Addr **310**
Gateway IP Address **302**
General Setup **79**
Germany, Contact Information **7**
Global **143**

H

Hidden Menus **281**
Hidden node **479**
Hop Count **316**
Host **83**
HTTP **148**, **403**

I

IBSS **477**
Idle Timeout **308**
IEEE 802.11g **481**
IGMP **88**, **89**
Independent Basic Service Set **477**
initialization vector (IV) **487**
Inside **143**
Inside Global Address **143**
Inside Local Address **143**
Internet Access **301**
   ISP's Name **301**
Internet access **301**
Internet Access Setup **301**, **317**, **414**
Introduction to Filters **335**
IP Address **88**, **92**, **147**, **149**, **150**, **293**, **302**, **310**, **316**, **361**
IP Address Assignment **310**
IP Pool **91**, **293**
IP Pool Setup **87**
IP Ports **403**
IP Static Route Setup **315**

J

Java **193**