Prestige 334W

802.11g Wireless Broadband Router with Firewall

User's Guide

Version 3.60

May 2004

ZyXEL

Unleash Networking Power

Copyright

Copyright © 2004 by ZyXEL Communications Corporation.

Disclaimer

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

This publication is subject to change without notice.

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
This device may not cause harmful interference.
This device must accept any interference received, including interference that may cause undesired operations.
This equipment has been tested and found to comply with the limits for a CLASS B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.
If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
Reorient or relocate the receiving antenna.
Increase the separation between the equipment and the receiver.
Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

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

Certifications

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

FC Tested To Comply
With FCC Standards
FOR HOME OR OFFICE USE

Information for Canadian Users

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

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

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

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

Caution

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

Note

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

ZyXEL Limited Warranty

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

NOTE

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

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

Online Registration

Register your product online at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

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

- Product model and serial number.
- 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[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
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.
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
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
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
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
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

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

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
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
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

Table of Contents

Copyright ii
Federal Communications Commission (FCC) Interference Statement iii
Information for Canadian Users iv
ZyXEL Limited Warranty v
Customer Support vi
List of Figures xxi
List of Tables xxvii
Preface xxxi
Getting Started I
Chapter 1 Getting to Know Your Prestige 1-1
1.1 Prestige Internet Security Gateway Overview 1-1
1.2 Prestige Features 1-1
1.2.1 Physical Features 1-1
1.2.2 Non-Physical Features 1-2
1.3 Applications for the Prestige 1-5
1.3.1 Secure Broadband Internet Access via Cable or DSL Modem 1-6
1.3.2 VPN Application 1-6
1.3.3 Internet Access Application 1-7
Chapter 2 Introducing the Web Configurator 2-1
2.1 Web Configurator Overview 2-1
2.2 Accessing the Prestige Web Configurator 2-1
2.3 Resetting the Prestige 2-2
2.3.1 Procedure To Use The Reset Button 2-2
2.3.2 Navigation Panel 2-3
Chapter 3 Wizard Setup 3-1
3.1 Wizard Setup Overview 3-1
3.2 Wizard Setup: General Setup and System Name 3-1
3.2.1 Domain Name 3-1
3.3 Wizard Setup: Screen 2 3-2
3.4 Wizard Setup: Screen 3 3-3
3.5 Wizard Setup: Screen 4 3-5
3.5.1 Ethernet 3-5
3.5.2 PPPoE Encapsulation 3-7
3.5.3 PPTP Encapsulation 3-9
3.6 Wizard Setup: Screen 5 3-10
3.6.1 WAN IP Address Assignment 3-10
3.6.2 IP Address and Subnet Mask 3-11
3.6.3 DNS Server Address Assignment 3-11

3.6.4 WAN MAC Address 3-12

3.7 Basic Setup Complete 3-14

Chapter 4 Media Bandwidth Management Setup 4-1

4.1 Media Bandwidth Management Setup Overview 4-1

4.2 Media Bandwidth Management Setup 1 4-1

4.3 Media Bandwidth Management Setup 2 4-2

4.4 Media Bandwidth Management Setup 3: 4-3

4.5 Media Bandwidth Management Setup Complete 4-4

System, LAN, WLAN and WAN II

Chapter 5 System Screens 5-1

5.1 System Overview 5-1

5.2 Configuring General Setup 5-1

5.3 Dynamic DNS 5-3

5.3.1 DynDNS Wildcard 5-3

5.4 Configuring Dynamic DNS 5-3

5.5 Configuring Password 5-5

5.6 Configuring Time Zone 5-6

Chapter 6 LAN Screens 6-1

6.1 LAN Overview 6-1

6.2 DHCP Setup 6-1

6.2.1 IP Pool Setup 6-1

6.2.2 System DNS Servers 6-1

6.3 LAN TCP/IP 6-1

6.3.1 Factory LAN Defaults 6-1

6.3.2 IP Address and Subnet Mask 6-2

6.3.3 RIP Setup 6-2

6.3.4 Multicast 6-2

6.4 Any IP 6-3

6.4.1 How Any IP Works 6-4

6.5 Configuring IP 6-4

6.6 Configuring Static DHCP 6-8

6.7 Configuring IP Alias 6-9

Chapter 7 Wireless Configuration and Roaming 7-1

7.1 Wireless LAN Overview 7-1

7.1.1 IBSS 7-1

7.1.2 BSS 7-1

7.1.3 ESS 7-2

7.2 Wireless LAN Basics 7-3

7.2.1 RTS/CTS 7-3

7.2.2 Fragmentation Threshold 7-4

7.3 Configuring Wireless 7-5

7.4 Configuring Roaming 7-6
7.4.1 Requirements for Roaming 7-8
Chapter 8 Wireless Security 8-1
8.1 Wireless Security Overview 8-1
8.2 Security Parameters Summary 8-3
8.3 WEP Overview 8-4
8.3.1 Data Encryption 8-4
8.3.2 Authentication 8-4
8.3.3 Preamble Type 8-6
8.4 Configuring WEP Encryption 8-6
8.5 Introduction to WPA 8-8
8.5.1 User Authentication 8-9
8.5.2 Encryption 8-9
8.5.3 WPA-PSK Application Example 8-9
8.6 Configuring WPA-PSK Authentication 8-10
8.7 Wireless Client WPA Supplicants 8-13
8.7.1 WPA with RADIUS Application Example 8-13
8.8 Configuring WPA Authentication 8-14
8.9 802.1x Overview 8-16
8.10 Dynamic WEP Key Exchange 8-17
8.11 Configuring 802.1x and Dynamic WEP Key Exchange 8-17
8.12 Configuring 802.1x and Static WEP Key Exchange 8-19
8.13 Configuring 802.1x 8-23
8.14 MAC Filter 8-25
8.15 Introduction to Local User Database 8-27
8.16 Configuring Local User Database 8-28
8.17 Introduction to RADIUS 8-29
8.17.1 EAP Authentication Overview 8-30
8.18 Configuring RADIUS 8-31
Chapter 9 WAN Screens 9-1
9.1 WAN Overview 9-1
9.2 TCP/IP Priority (Metric) 9-1
9.3 Configuring Route 9-1
9.4 Configuring WAN ISP 9-2
9.4.1 Ethernet Encapsulation 9-2
9.4.2 PPPoE Encapsulation 9-4
9.4.3 PPTP Encapsulation 9-6
9.5 Configuring WAN IP 9-7
9.6 Configuring WAN MAC 9-11
9.7 Traffic Redirect 9-12
9.8 Configuring Traffic Redirect 9-13

SUA/NAT and Static Route III
Chapter 10 Network Address Translation (NAT) Screens 10-1
10.1 NAT Overview 10-1
10.1.1 NAT Definitions 10-1
10.1.2 What NAT Does 10-2
10.1.3 How NAT Works 10-2
10.1.4 NAT Application 10-3
10.1.5 NAT Mapping Types 10-4
10.2 Using NAT 10-6
10.2.1 SUA (Single User Account) Versus NAT 10-6
10.3 SUA Server 10-6
10.3.1 Port Forwarding: Services and Port Numbers 10-6
10.3.2 Configuring Servers Behind SUA (Example) 10-7
10.4 Configuring SUA Server 10-8
10.5 Configuring Address Mapping 10-10
10.6 Trigger Port Forwarding 10-13
10.6.1 Trigger Port Forwarding Example 10-14
10.6.2 Two Points To Remember About Trigger Ports 10-14
10.7 Configuring Trigger Port Forwarding 10-14
Chapter 11 Static Route Screens 11-1
11.1 Static Route Overview 11-1
11.2 Configuring IP Static Route 11-1
11.2.1 Configuring Route Entry 11-2
UPnP and Firewall IV
Chapter 12 UPnP 12-1
12.1 Universal Plug and Play Overview 12-1
12.1.1 How Do I Know If I'm Using UPnP? 12-1
12.1.2 NAT Traversal 12-1
12.1.3 Cautions with UPnP 12-2
12.2 UPnP and ZyXEL 12-2
12.3 Configuring UPnP 12-2
12.4 Installing UPnP in Windows Example 12-4
12.4.1 Installing UPnP in Windows Me 12-4
12.4.2 Installing UPnP in Windows XP 12-4
12.5 Using UPnP in Windows XP Example 12-6
12.5.1 Auto-discover Your UPnP-enabled Network Device 12-6
12.5.2 Web Configurator Easy Access 12-8
Chapter 13 Firewall 13-1
13.1 Introduction 13-1
13.1.1 Guidelines For Enhancing Security With Your Firewall 13-2
13.2 Firewall Settings Screen 13-3

13.3 The Firewall, NAT and Remote Management 13-5
13.3.1 LAN-to-WAN rules 13-5
13.3.2 WAN-to-LAN rules 13-5
13.4 Configuring Content Filtering 13-6
13.5 Services 13-8
Remote Management and VPN/IPSec V
Chapter 14 Remote Management Screens 14-1
14.1 Remote Management Overview 14-1
14.1.1 Remote Management Limitations 14-2
14.1.2 Remote Management and NAT 14-2
14.1.3 System Timeout 14-2
14.2 Configuring WWW 14-2
14.3 Configuring Telnet 14-4
14.4 Configuring TELNET 14-4
14.5 Configuring FTP 14-6
14.6 SNMP 14-7
14.6.1 Supported MIBs 14-9
14.6.2 SNMP Traps 14-9
14.6.3 Configuring SNMP 14-10
14.7 Configuring DNS 14-11
14.8 Configuring Security 14-13
Chapter 15 Introduction to IPSec 15-1
15.1 VPN Overview 15-1
15.1.1 IPSec 15-1
15.1.2 Security Association 15-1
15.1.3 Other Terminology 15-1
15.1.4 VPN Applications 15-2
15.2 IPSec Architecture 15-3
15.2.1 IPSec Algorithms 15-3
15.2.2 Key Management 15-4
15.3 Encapsulation 15-4
15.3.1 Transport Mode 15-4
15.3.2 Tunnel Mode 15-4
15.4 IPSec and NAT 15-5
Chapter 16 VPN Screens 16-1
16.1 VPN/IPSec Overview 16-1
16.2 IPSec Algorithms 16-1
16.2.1 AH (Authentication Header) Protocol 16-1
16.2.2 ESP (Encapsulating Security Payload) Protocol 16-2
16.3 My IP Address 16-2
16.4 Secure Gateway Address 16-2

16.4.1 Dynamic Secure Gateway Address 16-3
16.5 Summary Screen 16-3
16.6 Keep Alive 16-5
16.7 NAT Traversal 16-6
16.7.1 NAT Traversal Configuration 16-6
16.7.2 Remote DNS Server 16-7
16.8 ID Type and Content 16-8
16.8.1 ID Type and Content Examples 16-9
16.9 Pre-Shared Key 16-10
16.10 Editing VPN Rules 16-10
16.11 IKE Phases 16-15
16.11.1 Negotiation Mode 16-17
16.11.2 Diffie-Hellman (DH) Key Groups 16-17
16.11.3 Perfect Forward Secrecy (PFS) 16-18
16.12 Configuring Advanced IKE Settings 16-18
16.13 Manual Key Setup 16-25
16.13.1 Security Parameter Index (SPI) 16-25
16.14 Configuring Manual Key 16-26
16.15 Viewing SA Monitor 16-30
16.16 Configuring Global Setting 16-32
16.17 Telecommuter VPN/IPSec Examples 16-33
16.17.1 Telecommuters Sharing One VPN Rule Example 16-33
16.17.2 Telecommuters Using Unique VPN Rules Example 16-34
16.18 VPN and Remote Management 16-36
Logs, Media Bandwidth Management and Maintenance VI
Chapter 17 Centralized Logs 17-1
17.1 View Log 17-1
17.2 Log Settings 17-2
Chapter 18 Media Bandwidth Management 18-1
18.1 Bandwidth Management Overview 18-1
18.1.1 Application-based Bandwidth Management Example 18-1
18.1.2 Subnet-based Bandwidth Management Example 18-2
18.1.3 Application and Subnet-based Bandwidth Management Example 18-2
18.1.4 Bandwidth Usage Example 18-3
18.1.5 Bandwidth Management Priorities 18-4
18.1.6 Bandwidth Management Services 18-5
18.1.7 Services 18-6
18.2 Configuration Screen 18-8
18.3 Editing Bandwidth Management Rules 18-11
18.3.1 Bandwidth Borrowing 18-11
18.4 Configuring Bandwidth Management Rules and Services 18-11

18.5 Monitor Screen 18-13
Chapter 19 Maintenance 19-1
19.1 Maintenance Overview 19-1
19.2 Status Screen 19-1
19.2.1 System Statistics 19-2
19.3 DHCP Table Screen 19-4
19.4 Any IP Table 19-5
19.5 Association List 19-5
19.6 F/W Upload Screen 19-6
19.7 Configuration Screen 19-8
19.7.1 Backup Configuration 19-9
19.7.2 Restore Configuration 19-9
19.7.3 Back to Factory Defaults 19-11
19.8 Restart Screen 19-11
SMT General Configuration VII
Chapter 20 Introducing the SMT 20-1
20.1 SMT Introduction 20-1
20.1.1 Procedure for SMT Configuration via Console Port 20-1
20.1.2 Procedure for SMT Configuration via Telnet 20-1
20.1.3 Entering Password 20-1
20.1.4 Prestige SMT Menu Overview 20-2
20.2 Navigating the SMT Interface 20-3
20.2.1 System Management Terminal Interface Summary 20-5
20.3 Changing the System Password 20-6
Chapter 21 Menu 1 General Setup 21-1
21.1 General Setup 21-1
21.2 Procedure To Configure Menu 1 21-1
21.2.1 Procedure to Configure Dynamic DNS 21-3
Chapter 22 Menu 2 WAN Setup 22-1
22.1 Introduction to WAN 22-1
22.2 WAN Setup 22-1
Chapter 23 Menu 3 LAN Setup 23-1
23.1 LAN Setup 23-1
23.1.1 General Ethernet Setup 23-1
23.2 Protocol Dependent Ethernet Setup 23-2
23.3 TCP/IP Ethernet Setup and DHCP 23-2
23.3.1 IP Alias Setup 23-4
23.4 Wireless LAN Setup 23-6
23.4.1 Configuring MAC Address Filter 23-9
23.4.2 Configuring Roaming on the Prestige 23-11
Chapter 24 Internet Access 24-1

24.1 Introduction to Internet Access Setup 24-1
24.2 Ethernet Encapsulation 24-1
24.3 Configuring the PPTP Client 24-3
24.4 Configuring the PPPoE Client 24-4
24.5 Basic Setup Complete 24-5
Chapter 25 Remote Node Configuration 25-1
25.1 Introduction to Remote Node Setup 25-1
25.2 Remote Node Profile Setup 25-1
25.2.1 Ethernet Encapsulation 25-1
25.2.2 PPPoE Encapsulation 25-4
25.2.3 PPTP Encapsulation 25-6
25.3 Edit IP 25-7
25.4 Remote Node Filter 25-9
25.4.1 Traffic Redirect Setup 25-10
Chapter 26 Static Route Setup 26-1
26.1 IP Static Route Setup 26-1
Chapter 27 Dial-in User Setup 27-1
27.1 Dial-in User Setup 27-1
Chapter 28 Network Address Translation (NAT) 28-1
28.1 Using NAT 28-1
28.1.1 SUA (Single User Account) Versus NAT 28-1
28.2 Applying NAT 28-1
28.3 NAT Setup 28-3
28.3.1 Address Mapping Sets 28-4
28.4 Configuring a Server behind NAT 28-9
28.5 General NAT Examples 28-10
28.5.1 Example 1: Internet Access Only 28-10
28.5.2 Example 2: Internet Access with an Inside Server 28-11
28.5.3 Example 3: Multiple Public IP Addresses With Inside Servers 28-12
28.5.4 Example 4: NAT Unfriendly Application Programs 28-16
28.6 Configuring Trigger Port Forwarding 28-18
Chapter 29 Enabling the Firewall 29-1
29.1 Remote Management and the Firewall 29-1
29.2 Access Methods 29-1
29.3 Enabling the Firewall 29-1
SMT Advanced Management VIII
Chapter 30 Filter Configuration 30-1
30.1 Introduction to Filters 30-1
30.1.1 The Filter Structure of the Prestige 30-2
30.2 Configuring a Filter Set 30-4
30.2.1 Configuring a Filter Rule 30-6

30.2.2 Configuring a TCP/IP Filter Rule 30-6
30.2.3 Configuring a Generic Filter Rule 30-11
30.3 Example Filter 30-13
30.4 Filter Types and NAT 30-15
30.5 Firewall Versus Filters 30-16
30.6 Applying a Filter 30-16
30.6.1 Applying LAN Filters 30-17
30.6.2 Applying Remote Node Filters 30-17
Chapter 31 SNMP Configuration 31-1
31.1 About SNMP 31-1
31.2 Supported MIBs 31-2
31.3 SNMP Configuration 31-2
31.4 SNMP Traps 31-4
Chapter 32 System Security 32-1
32.1 System Security 32-1
32.1.1 System Password 32-1
32.1.2 Configuring External RADIUS Server 32-1
32.1.3 802.1x 32-3
Chapter 33 System Information and Diagnosis 33-1
33.1 System Status 33-1
33.2 System Information 33-3
33.2.1 System Information 33-3
33.2.2 Console Port Speed 33-4
33.3 Log and Trace 33-5
33.3.1 Syslog Logging 33-5
33.3.2 Call-Triggering Packet 33-8
33.4 Diagnostic 33-9
33.4.1 WAN DHCP 33-10
Chapter 34 Firmware and Configuration File Maintenance 34-1
34.1 Filename Conventions 34-1
34.2 Backup Configuration 34-2
34.2.1 Backup Configuration 34-3
34.2.2 Using the FTP Command from the Command Line 34-3
34.2.3 Example of FTP Commands from the Command Line 34-4
34.2.4 GUI-based FTP Clients 34-4
34.2.5 TFTP and FTP over WAN Management Limitations 34-4
34.2.6 Backup Configuration Using TFTP 34-5
34.2.7 TFTP Command Example 34-5
34.2.8 GUI-based TFTP Clients 34-6
34.3 Restore Configuration 34-6
34.3.1 Restore Using FTP 34-7

34.3.2 Restore Using FTP Session Example 34-8

34.4 Uploading Firmware and Configuration Files 34-8

34.4.1 Firmware File Upload 34-8

34.4.2 Configuration File Upload 34-9

34.4.3 FTP File Upload Command from the DOS Prompt Example 34-10

34.4.4 FTP Session Example of Firmware File Upload 34-10

34.4.5 TFTP File Upload 34-10

34.4.6 TFTP Upload Command Example 34-11

Chapter 35 System Maintenance 35-1

35.1 Command Interpreter Mode 35-1

35.1.1 Command Syntax 35-1

35.1.2 Command Usage 35-2

35.2 Call Control Support 35-2

35.2.1 Budget Management 35-3

35.2.2 Call History 35-4

35.3 Time and Date Setting 35-4

35.3.1 Resetting the Time 35-6

Chapter 36 Remote Management 36-1

36.1 Remote Management 36-1

36.1.1 Remote Management Limitations 36-2

Chapter 37 Call Scheduling 37-1

37.1 Introduction to Call Scheduling 37-1

SMT VPN/IPSec IX

Chapter 38 VPN/IPSec Setup 38-1

38.1 VPN/IPSec Overview 38-1

38.2 IPSec Summary Screen 38-2

38.3 IPSec Setup 38-5

38.4 IKE Setup 38-10

38.5 Manual Setup 38-13

38.5.1 Active Protocol 38-13

38.5.2 Security Parameter Index (SPI) 38-13

Chapter 39 SA Monitor 39-1

39.1 SA Monitor Overview 39-1

39.2 Using SA Monitor 39-1

Appendices and Index X

Appendix A PPPoE A-1

Appendix B PPTP B-1

Appendix C NetBIOS Filter Commands C-1

Appendix D Log Descriptions D-1

Appendix E Setting up Your Computer's IP Address E-1

Appendix F Wireless LAN and IEEE 802.11 ....F-1

Appendix G Wireless LAN With IEEE 802.1x G-1
Appendix H Types of EAP Authentication H-1
Appendix I Antenna Selection and Positioning Recommendation I-1
Appendix J Brute-Force Password Guessing Protection J-1
Appendix K Triangle Route K-1
Appendix L Index L-1

List of Figures

Figure 1-1 Secure Internet Access via Cable, DSL or Wireless Modem 1-6
Figure 1-2 VPN Application 1-6
Figure 1-3 Internet Access Application Example 1-7
Figure 2-1 Change Password Screen 2-1
Figure 2-2 The MAIN MENU Screen of the Web Configurator 2-3
Figure 3-1 Wizard 1: General Setup 3-2
Figure 3-2 Wizard 2: Wireless LAN Setup 3-2
Figure 3-3 Wizard 3: Wireless LAN Setup: Basic Security 3-4
Figure 3-4 Wizard 3: Wireless LAN Setup: Extend Security 3-5
Figure 3-5 Wizard 4: Ethernet Encapsulation 3-6
Figure 3-6 Wizard 4: PPPoE Encapsulation 3-8
Figure 3-7 Wizard 4: PPTP Encapsulation 3-9
Figure 3-8 Wizard 5: WAN Setup 3-13
Figure 3-9 Wizard Finish 3-15
Figure 4-1 Media Bandwidth Management Setup 1 4-1
Figure 4-2 Media Bandwidth Management Setup 2: Services 4-2
Figure 4-3 Media Bandwidth Management Setup 3: Service Priority 4-3
Figure 4-4 Media Bandwidth Management Setup 4: Finish 4-4
Figure 5-1 System General Setup 5-1
Figure 5-2 DDNS 5-4
Figure 5-3 Password 5-6
Figure 5-4 Time Setting 5-7
Figure 6-1 Any IP Example Application 6-3
Figure 6-2 IP 6-5
Figure 6-3 Static DHCP 6-8
Figure 6-4 IP Alias 6-9
Figure 7-1 IBSS (Ad-hoc) Wireless LAN 7-1
Figure 7-2 Basic Service set 7-2
Figure 7-3 Extended Service Set 7-3
Figure 7-4 RTS/CTS 7-4
Figure 7-5 Wireless 7-5
Figure 7-6 Roaming Example 7-7
Figure 7-7 Roaming 7-8
Figure 8-1 Prestige Wireless Security Levels 8-1
Figure 8-2 Wireless: No Security 8-2
Figure 8-3 WEP Authentication Steps 8-5
Figure 8-4 Wireless: Static WEP Encryption 8-7
Figure 8-5 WPA - PSK Authentication 8-10

Figure 8-6 Wireless: WPA-PSK....8-11
Figure 8-7 WPA with RADIUS Application Example....8-14
Figure 8-8 Wireless: WPA....8-15
Figure 8-9 Wireless: 802.1x and Dynamic WEP....8-18
Figure 8-10 Wireless: 802.1x and Static WEP....8-20
Figure 8-11 Wireless: 802.1x....8-23
Figure 8-12 MAC Address Filter....8-26
Figure 8-13 Local User Database....8-28
Figure 8-14 EAP Authentication....8-30
Figure 8-15 RADIUS....8-31
Figure 9-1 WAN: Route....9-2
Figure 9-2 Ethernet Encapsulation....9-3
Figure 9-3 PPPoE Encapsulation....9-5
Figure 9-4 PPTP Encapsulation....9-6
Figure 9-5 WAN: IP....9-8
Figure 9-6 MAC Setup....9-11
Figure 9-7 Traffic Redirect WAN Setup....9-12
Figure 9-8 Traffic Redirect LAN Setup....9-12
Figure 9-9 WAN: Traffic Redirect....9-13
Figure 10-1 How NAT Works....10-3
Figure 10-2 NAT Application With IP Alias....10-4
Figure 10-3 Multiple Servers Behind NAT Example....10-8
Figure 10-4 SUA/NAT Setup....10-9
Figure 10-5 Address Mapping....10-11
Figure 10-6 Address Mapping Edit....10-12
Figure 10-7 Trigger Port Forwarding Process: Example....10-14
Figure 10-8 Trigger Port....10-15
Figure 11-1 Example of Static Routing Topology....11-1
Figure 11-2 Static Route....11-2
Figure 11-3 Static Route: Edit....11-3
Figure 12-1 Configuring UPnP....12-3
Figure 13-1 Firewall: Settings....13-3
Figure 13-2 Firewall Rule Directions....13-5
Figure 13-3 Firewall: Filter....13-7
Figure 13-4 Firewall: Service....13-9
Figure 14-1 Remote Management: WWW....14-3
Figure 14-2 Telnet Configuration on a TCP/IP Network....14-4
Figure 14-3 Remote Management: Telnet....14-5
Figure 14-4 Remote Management: FTP....14-6
Figure 14-5 SNMP Management Model....14-8
Figure 14-6 Remote Management: SNMP....14-10

Figure 14-7 Remote Management: DNS 14-12
Figure 14-8 Security........ 14-13
Figure 15-1 Encryption and Decryption........ 15-2
Figure 15-2 IPSec Architecture........ 15-3
Figure 15-3 Transport and Tunnel Mode IPSec Encapsulation........ 15-4
Figure 16-1 IPSec Summary Fields 16-3
Figure 16-2 VPN: Summary 16-4
Figure 16-3 NAT Router Between IPSec Routers........ 16-6
Figure 16-4 VPN Host using Intranet DNS Server Example 16-7
Figure 16-5 VPN: Rule Setup (Basic)........16-11
Figure 16-6 Two Phases to Set Up the IPSec SA 16-16
Figure 16-7 VPN IKE: Advanced 16-19
Figure 16-8 Rule Setup: Manual 16-27
Figure 16-9 SA Monitor........ 16-31
Figure 16-10 VPN: Global Setting........ 16-32
Figure 16-11 Telecommuters Sharing One VPN Rule Example 16-34
Figure 16-12 Telecommuters Using Unique VPN Rules Example 16-35
Figure 17-1 View Logs........ 17-1
Figure 17-2 Log Settings........ 17-3
Figure 18-1 Application-based Bandwidth Management Example........ 18-2
Figure 18-2 Subnet-based Bandwidth Management Example 18-2
Figure 18-3 Application and Subnet-based Bandwidth Management Example........ 18-3
Figure 18-4 Bandwidth Usage Example 18-3
Figure 18-5 Maximize Bandwidth Usage Example 18-4
Figure 18-6 Bandwidth Management Configuration 18-9
Figure 18-7 Bandwidth Management Edit........18-11
Figure 18-8 Bandwidth Management Monitor........ 18-14
Figure 19-1 Maintenance Status........ 19-1
Figure 19-2 Maintenance System Statistics 19-3
Figure 19-3 Maintenance DHCP Table 19-4
Figure 19-4 Maintenance Any IP 19-5
Figure 19-5 Maintenance Association List........ 19-6
Figure 19-6 Maintenance Firmware Upload 19-6
Figure 19-7 Upload Warning........ 19-7
Figure 19-8 Network Temporarily Disconnected........ 19-7
Figure 19-9 Upload Error Message........ 19-8
Figure 19-10 Maintenance Configuration........ 19-9
Figure 19-11 Configuration Restore Successful........ 19-10
Figure 19-12 Temporarily Disconnected........ 19-10
Figure 19-13 Configuration Restore Error........19-11
Figure 19-14 Factory Defaults 19-11

Figure 19-15 System Restart..19-12
Figure 20-1 Login Screen..20-2
Figure 20-2 SMT Menu Overview..20-3
Figure 20-3 SMT Main Menu..20-5
Figure 20-4 Menu 23 System Password..20-6
Figure 21-1 Menu 1 General Setup..21-2
Figure 21-2 Menu 1.1 Configure Dynamic DNS..21-4
Figure 22-1 Menu 2 WAN Setup..22-1
Figure 23-1 Menu 3 LAN Setup..23-1
Figure 23-2 Menu 3.1 LAN Port Filter Setup..23-1
Figure 23-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup..23-2
Figure 23-4 Physical Network & Partitioned Logical Networks..23-5
Figure 23-5 Menu 3.2.1: IP Alias Setup..23-5
Figure 23-6 Menu 3.5 Wireless LAN Setup..23-7
Figure 23-7 Menu 3.5 Wireless LAN Setup..23-9
Figure 23-8 Menu 3.5.1 WLAN MAC Address Filter..23-10
Figure 23-9 Menu 3.5 Wireless LAN Setup..23-11
Figure 23-10 Menu 3.5.2 Roaming Configuration..23-12
Figure 24-1 Menu 4 Internet Access Setup..24-1
Figure 24-2 Internet Access Setup (PPTP)..24-4
Figure 24-3 Internet Access Setup (PPPoE)..24-5
Figure 25-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation..25-2
Figure 25-2 Menu 11.1 Remote Node Profile for PPPoE Encapsulation..25-4
Figure 25-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation..25-6
Figure 25-4 Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation..25-7
Figure 25-5 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)..25-9
Figure 25-6 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)..25-10
Figure 25-7 Menu 11.6: Traffic Redirect Setup..25-10
Figure 26-1 Menu 12 IP Static Route Setup..26-1
Figure 26-2 Menu12.1 Edit IP Static Route..26-2
Figure 27-1 Menu 14- Dial-in User Setup..27-1
Figure 27-2 Menu 14.1- Edit Dial-in User..27-1
Figure 28-1 Menu 4 Applying NAT for Internet Access..28-2
Figure 28-2 Menu 11.3 Applying NAT to the Remote Node..28-3
Figure 28-3 Menu 15 NAT Setup..28-4
Figure 28-4 Menu 15.1 Address Mapping Sets..28-4
Figure 28-5 Menu 15.1.255 SUA Address Mapping Rules..28-5
Figure 28-6 Menu 15.1.1 First Set..28-6
Figure 28-7 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set..28-8
Figure 28-8 Menu 15.2.1 NAT Server Setup..28-9
Figure 28-9 Multiple Servers Behind NAT Example..28-10

Figure 28-10 NAT Example 1 28-10
Figure 28-11 Menu 4 Internet Access & NAT Example.......... 28-11
Figure 28-12 NAT Example 2 28-11
Figure 28-13 Menu 15.2.1 Specifying an Inside Server.......... 28-12
Figure 28-14 NAT Example 3 28-13
Figure 28-15 Example 3: Menu 11.3.......... 28-14
Figure 28-16 Example 3: Menu 15.1.1.1 28-14
Figure 28-17 Example 3: Final Menu 15.1.1 28-15
Figure 28-18 NAT Example 4 28-16
Figure 28-19 Example 4: Menu 15.1.1.1 Address Mapping Rule.......... 28-17
Figure 28-20 Example 4: Menu 15.1.1 Address Mapping Rules 28-17
Figure 28-21 Menu 15.3 Trigger Port Setup 28-18
Figure 29-1 Menu 21.2 Firewall Setup 29-2
Figure 30-1 Outgoing Packet Filtering Process 30-2
Figure 30-2 Filter Rule Process.......... 30-3
Figure 30-4 Menu 21: Filter and Firewall Setup.......... 30-4
Figure 30-5 Menu 21.1: Filter Set Configuration.......... 30-4
Figure 30-6 Menu 21.1.1.1 TCP/IP Filter Rule.......... 30-7
Figure 30-7 Executing an IP Filter.......... 30-10
Figure 30-8 Menu 21.1.4.1 Generic Filter Rule.......... 30-11
Figure 30-9 Telnet Filter Example 30-13
Figure 30-10 Example Filter: Menu 21.1.3.1.......... 30-14
Figure 30-11 Example Filter Rules Summary: Menu 21.1.3.......... 30-15
Figure 30-12 Protocol and Device Filter Sets 30-16
Figure 30-13 Filtering LAN Traffic 30-17
Figure 30-14 Filtering Remote Node Traffic 30-18
Figure 31-1 SNMP Management Model.......... 31-1
Figure 31-2 Menu 22 SNMP Configuration.......... 31-3
Figure 32-1 Menu 23 System Security.......... 32-1
Figure 32-2 Menu 23 System Security.......... 32-1
Figure 32-3 Menu 23.2 System Security : RADIUS Server 32-2
Figure 32-4 Menu 23 System Security.......... 32-3
Figure 32-5 Menu 23.4 System Security : IEEE802.1x 32-4
Figure 33-1 Menu 24 System Maintenance 33-1
Figure 33-2 Menu 24.1 System Maintenance : Status.......... 33-2
Figure 33-3 Menu 24.2 System Information and Console Port Speed.......... 33-3
Figure 33-4 Menu 24.2.1 System Maintenance : Information 33-4
Figure 33-5 Menu 24.2.2 System Maintenance : Change Console Port Speed.......... 33-5
Figure 33-6 Menu 24.3.2 System Maintenance : Syslog Logging 33-5
Figure 33-7 Call-Triggering Packet Example 33-9
Figure 33-8 Menu 24.4 System Maintenance : Diagnostic 33-10

Figure 33-9 LAN & WAN DHCP.....33-10
Figure 34-1 Telnet in Menu 24.5.....34-3
Figure 34-2 FTP Session Example.....34-4
Figure 34-3 Telnet into Menu 24.6.....34-7
Figure 34-4 Restore Using FTP Session Example.....34-8
Figure 34-5 Telnet Into Menu 24.7.1 Upload System Firmware.....34-9
Figure 34-6 Telnet Into Menu 24.7.2 System Maintenance.....34-9
Figure 34-7 FTP Session Example of Firmware File Upload.....34-10
Figure 35-1 Command Mode in Menu 24.....35-1
Figure 35-2 Valid Commands.....35-2
Figure 35-3 Menu 24.9 System Maintenance : Call Control.....35-2
Figure 35-4 Budget Management.....35-3
Figure 35-5 Call History.....35-4
Figure 35-6 Menu 24: System Maintenance.....35-5
Figure 35-7 Menu 24.10 System Maintenance: Time and Date Setting.....35-5
Figure 36-1 Menu 24.11 – Remote Management Control.....36-1
Figure 37-1 Menu 26 Schedule Setup.....37-1
Figure 37-2 Menu 26.1 Schedule Set Setup.....37-2
Figure 37-3 Applying Schedule Set(s) to a Remote Node (PPPoE).....37-4
Figure 38-1 VPN SMT Menu Tree.....38-1
Figure 38-2 Menu 27 VPN/IPSec Setup.....38-2
Figure 38-3 Menu 27.1 IPSec Summary.....38-2
Figure 38-4 Menu 27.1.1 IPSec Setup.....38-6
Figure 38-5 Menu 27.1.1.1 IKE Setup.....38-11
Figure 38-6 Menu 27.1.1.2 Manual Setup.....38-14
Figure 39-1 Menu 27.2 SA Monitor.....39-1

List of Tables

Table 2-1 Screens Summary 2-3
Table 3-1 Wizard 2: Wireless LAN Setup 3-3
Table 3-2 Wizard 3: Wireless LAN Setup: Basic Security 3-4
Table 3-3 Wizard 3: Wireless LAN Setup: Extend Security 3-5
Table 3-4 Wizard 4: Ethernet Encapsulation 3-6
Table 3-5 Wizard 4: PPPoE Encapsulation 3-8
Table 3-6 Wizard 4: PPTP Encapsulation 3-10
Table 3-7 Private IP Address Ranges 3-11
Table 3-8 Example of Network Properties for LAN Servers with Fixed IP Addresses 3-12
Table 3-9 Wizard 5: WAN Setup 3-13
Table 4-1 Media Bandwidth Management Setup 1 4-2
Table 4-2 Media Bandwidth Management Setup 2: Services 4-3
Table 4-3 Media Bandwidth Management Setup 3: Service Priority 4-4
Table 5-1 System General Setup 5-2
Table 5-2 DDNS 5-4
Table 5-3 Password 5-6
Table 5-4 Time Setting 5-7
Table 6-1 IP 6-5
Table 6-2 Static DHCP 6-9
Table 6-3 IP Alias 6-10
Table 7-1 Wireless 7-5
Table 7-2 Roaming 7-8
Table 8-1 Wireless: No Security 8-2
Table 8-2 Wireless Security Relational Matrix 8-3
Table 8-3 Wireless: Static WEP Encryption 8-7
Table 8-4 Wireless: WPA-PSK 8-11
Table 8-5 Wireless: WPA 8-15
Table 8-6 Wireless: 802.1x and Dynamic WEP 8-18
Table 8-7 Wireless: 802.1x and Static WEP 8-20
Table 8-8 Wireless: 802.1x and No WEP 8-24
Table 8-9 MAC Address Filter 8-26
Table 8-10 Local User Database 8-29
Table 8-11 RADIUS 8-31
Table 9-1 WAN: Route 9-2
Table 9-2 Ethernet Encapsulation 9-3
Table 9-3 PPPoE Encapsulation 9-5
Table 9-4 PPTP Encapsulation 9-7
Table 9-5 WAN: IP 9-8

Table 9-6 WAN: Traffic Redirect 9-13
Table 10-1 NAT Definitions....................10-1
Table 10-2 NAT Mapping Types....................10-5
Table 10-3 Services and Port Numbers....................10-7
Table 10-4 SUA/NAT Setup 10-9
Table 10-5 Address Mapping....................10-11
Table 10-6 Address Mapping Edit 10-13
Table 10-7 Trigger Port....................10-15
Table 11-1 Static Route....................11-2
Table 11-2 Static Route: Edit....................11-3
Table 12-1 Configuring UPnP 12-3
Table 13-1 Firewall: Settings....................13-3
Table 13-2 Firewall: Filter 13-7
Table 13-3 Firewall: Service....................13-9
Table 14-1 Remote Management: WWW....................14-3
Table 14-2 Remote Management: Telnet 14-5
Table 14-3 Remote Management: FTP 14-6
Table 14-4 SNMP Traps....................14-9
Table 14-5 Remote Management: SNMP 14-11
Table 14-6 Remote Management: DNS....................14-12
Table 14-7 Security....................14-13
Table 15-1 VPN and NAT....................15-5
Table 16-1 AH and ESP 16-2
Table 16-2 VPN: Summary....................16-4
Table 16-3 Local ID Type and Content Fields 16-8
Table 16-4 Peer ID Type and Content Fields 16-9
Table 16-5 Matching ID Type and Content Configuration Example 16-9
Table 16-6 Mismatching ID Type and Content Configuration Example....................16-9
Table 16-7 VPN: Rule Setup (Basic) 16-12
Table 16-8 VPN IKE: Advanced....................16-20
Table 16-9 Rule Setup: Manual 16-28
Table 16-10 SA Monitor 16-31
Table 16-11 VPN: Global Setting 16-32
Table 16-12 Telecommuter and Headquarters Configuration Example 16-33
Table 17-1 View Logs....................17-2
Table 17-2 log Settings 17-4
Table 18-1 Application and Subnet-based Bandwidth Management Example 18-2
Table 18-2 Media Bandwidth Management Priorities 18-5
Table 18-3 Commonly Used Services....................18-6
Table 18-4 Bandwidth Management Configuration....................18-10
Table 18-5 Bandwidth Management Edit 18-12

Table 19-1 Maintenance Status 19-2
Table 19-2 Maintenance System Statistics 19-3
Table 19-3 Maintenance DHCP Table 19-4
Table 19-4 Maintenance Any IP 19-5
Table 19-5 Maintenance Association List 19-6
Table 19-6 Maintenance Firmware Upload 19-7
Table 19-7 Maintenance Restore Configuration 19-10
Table 20-1 Main Menu Commands 20-4
Table 20-2 Main Menu Summary 20-5
Table 21-1 Menu 1 General Setup 21-2
Table 21-2 Menu 1.1 Configure Dynamic DNS 21-4
Table 22-1 Menu 2 WAN Setup 22-1
Table 23-1 Menu 3.2: DHCP Ethernet Setup Fields 23-2
Table 23-2 Menu 3.2: LAN TCP/IP Setup Fields 23-4
Table 23-3 Menu 3.2.1: IP Alias Setup 23-6
Table 23-4 Menu 3.5 Wireless LAN Setup 23-7
Table 23-5 Menu 3.5.1 WLAN MAC Address Filter 23-10
Table 23-6 Menu 3.5.2 Roaming Configuration 23-12
Table 24-1 Menu 4: Internet Access Setup (Ethernet) 24-2
Table 24-2 New Fields in Menu 4 (PPTP) Screen 24-4
Table 24-3 New Fields in Menu 4 (PPPoE) screen 24-5
Table 25-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation 25-2
Table 25-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific) 25-5
Table 25-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation 25-6
Table 25-4 Remote Node Network Layer Options 25-7
Table 25-5 Menu 11.6: Traffic Redirect Setup 25-10
Table 26-1 Menu12.1 Edit IP Static Route 26-2
Table 27-1 Menu 14.1- Edit Dial-in User 27-2
Table 28-1 Applying NAT in Menus 4 & 11.3 28-3
Table 28-2 SUA Address Mapping Rules 28-5
Table 28-3 Menu 15.1.1 First Set 28-7
Table 28-4 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set 28-8
Table 28-5 Menu 15.3 Trigger Port Setup 28-18
Table 30-1 Abbreviations Used in the Filter Rules Summary Menu 30-5
Table 30-2 Rule Abbreviations Used 30-6
Table 30-3 TCP/IP Filter Rule 30-7
Table 30-4 Generic Filter Rule Menu Fields 30-11
Table 31-1 Menu 22 SNMP Configuration 31-3
Table 31-2 SNMP Traps 31-4
Table 31-3 Ports and Permanent Virtual Circuits 31-4
Table 32-1 Menu 23.2 System Security : RADIUS Server 32-2

Table 32-2 Menu 23.4 System Security : IEEE802.1x 32-4
Table 33-1 System Maintenance: Status Menu Fields 33-2
Table 33-2 Menu 24.2.1 System Maintenance : Information....................33-4
Table 33-3 Menu 24.3.2 System Maintenance : Syslog and Accounting....................33-5
Table 33-4 System Maintenance Menu Diagnostic 33-11
Table 34-1 Filename Conventions 34-2
Table 34-2 General Commands for GUI-based FTP Clients 34-4
Table 34-3 General Commands for GUI-based TFTP Clients 34-6
Table 35-1 Budget Management....................35-3
Table 35-2 Call History Fields....................35-4
Table 35-3 Time and Date Setting Fields....................35-6
Table 36-1 Menu 24.11 – Remote Management Control....................36-2
Table 37-1 Menu 26.1 Schedule Set Setup 37-2
Table 38-1 Menu 27.1 IPSec Summary 38-2
Table 38-2 Menu 27.1.1 IPSec Setup....................38-6
Table 38-3 Menu 27.1.1.1 IKE Setup 38-11
Table 38-4 Active Protocol: Encapsulation and Security Protocol 38-13
Table 38-5 Menu 27.1.1.2 Manual Setup....................38-14
Table 39-1 Menu 27.2 SA Monitor....................39-2
Table C-1 NetBIOS Filter Default Settings C-2

Preface

About This User's Manual

Congratulations on your purchase of the Prestige 334 802.11g Wireless Broadband Router with Firewall. This manual is designed to guide you through the configuration of your Prestige for its various applications.

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.

The web configurator parts of this guide contain background information on features configurable by the web configurator and the SMT. The SMT parts of this guide contain background information solely on features not configurable by the web configurator.

This manual may refer to the Prestige 334W or 802.11g Wireless Broadband Router with Firewall as the Prestige.

Related Documentation

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

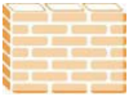
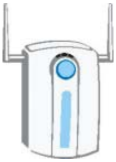
User's Guide Feedback

Help us help you. E-mail all User's 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

- The version number on the title page is the latest firmware version that is documented in this *User's Guide*. Earlier versions may also be included.
- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one of the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. 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.
- The choices of a menu item are in **Bold Arial** font.
- 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	Modem	 Firewall
Telephone	Switch	Router
DSLAM	 Wireless Access Point	Wireless Signal

The following section offers some background information on DSL. Skip to *Chapter 1* if you wish to begin working with your router right away.

Part I:

Getting Started

This part helps you get to know your Prestige, introduces the web configurator and covers how to configure the Wizard Setup screens.

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 embedded web configurator is easy to operate.

1.2 Prestige Features

The following sections describe Prestige features.

1.2.1 Physical Features

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.

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

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

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.

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.

Reset Button

The Prestige reset button is built into the rear panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33.

1.2.2 Non-Physical Features

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.

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.

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.

IEEE 802.1x Network Security

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.

Content Filtering

The Prestige can also block access to web sites containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude a range of users on the LAN from content filtering.

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.

802.11b Wireless LAN Standard

The Prestige, complies with the 802.11b wireless standard.
The 802.11g data rate and corresponding modulation techniques are as follows. The modulation technique defines how bits are encoded onto radio waves.

IEEE 802.11b	
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)

The Prestige may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

802.11g Wireless LAN Standard

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:

IEEE 802.11g	
Data Rate (Mbps)	Modulation
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Packet Filtering

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

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.

Call Scheduling

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

PPPoE

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

PPTP Encapsulation

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

Dynamic DNS Support

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

IP Multicast

Deliver IP packets to a specific group of hosts using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the Prestige supports both versions 1 and 2.

IP Alias

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

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).

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).

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.

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The 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. The Prestige can also act as a surrogate DHCP server (**DHCP Relay**) where it relays IP address assignment from the actual real DHCP server to the clients.

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.

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.

RoadRunner Support

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

Logging and Tracing

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

Upgrade Prestige Firmware via LAN

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

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.

Wireless Association List

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.

Wireless LAN Channel Usage

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 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.

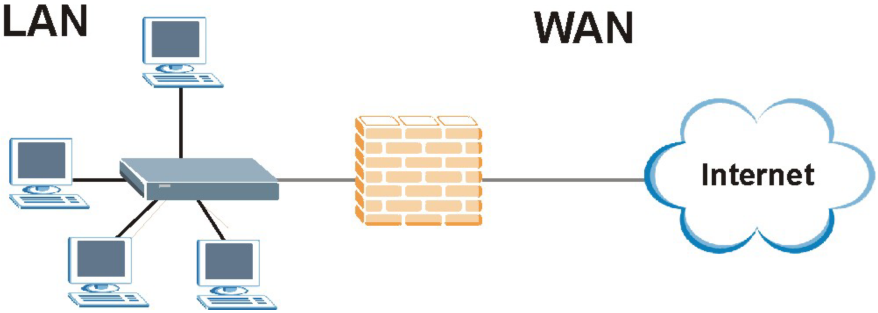


Figure 1-1 Secure Internet Access via Cable, DSL or Wireless Modem

1.3.2 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.

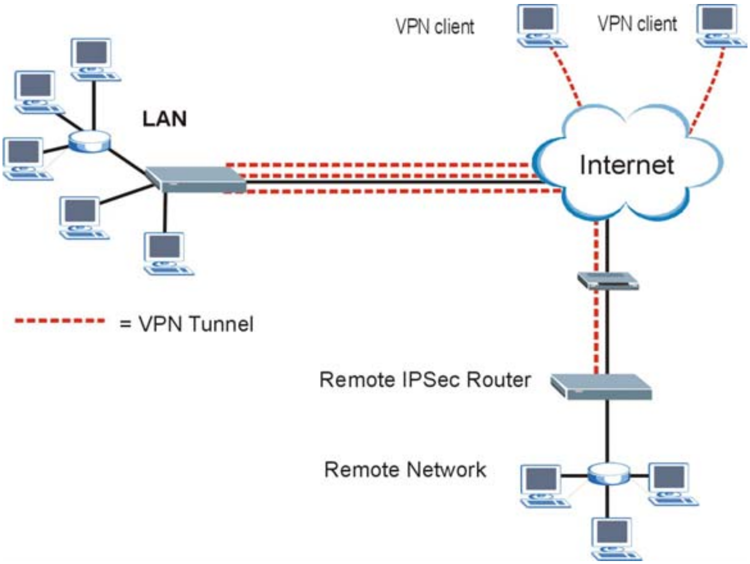


Figure 1-2 VPN Application

1.3.3 Internet Access Application

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.

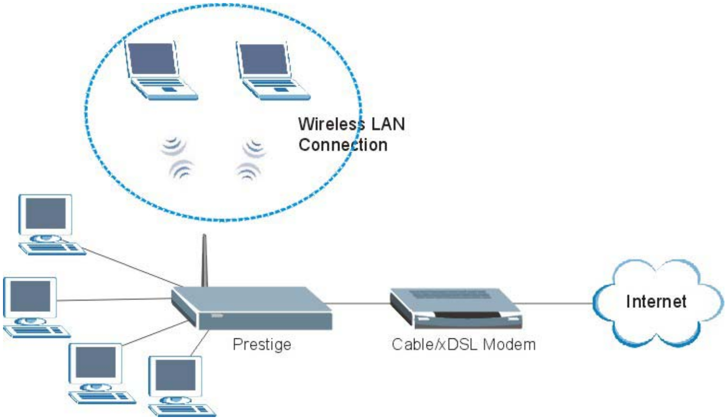


Figure 1-3 Internet Access Application Example

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 embedded web configurator allows you to manage the Prestige from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels. The screens you see in the web configurator may vary somewhat from the ones shown in this document due to differences between individual Prestige models or firmware versions.

2.2 Accessing the Prestige Web Configurator

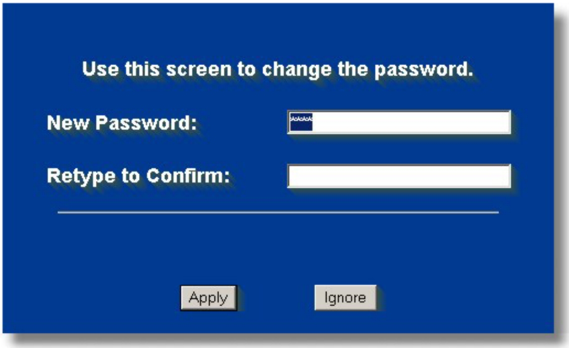
Step 1. Make sure your Prestige hardware is properly connected and prepare your computer/computer network to connect to the Prestige (refer to the *Quick Start Guide*).

Step 2. Launch your web browser.

Step 3. Type "192.168.1.1" as the URL.

Step 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**.

Step 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**.



Use this screen to change the password.

New Password:

Retype to Confirm:

Figure 2-1 Change Password Screen

Step 6. You should now see the **MAIN MENU** screen (see *Figure 2-2*).

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

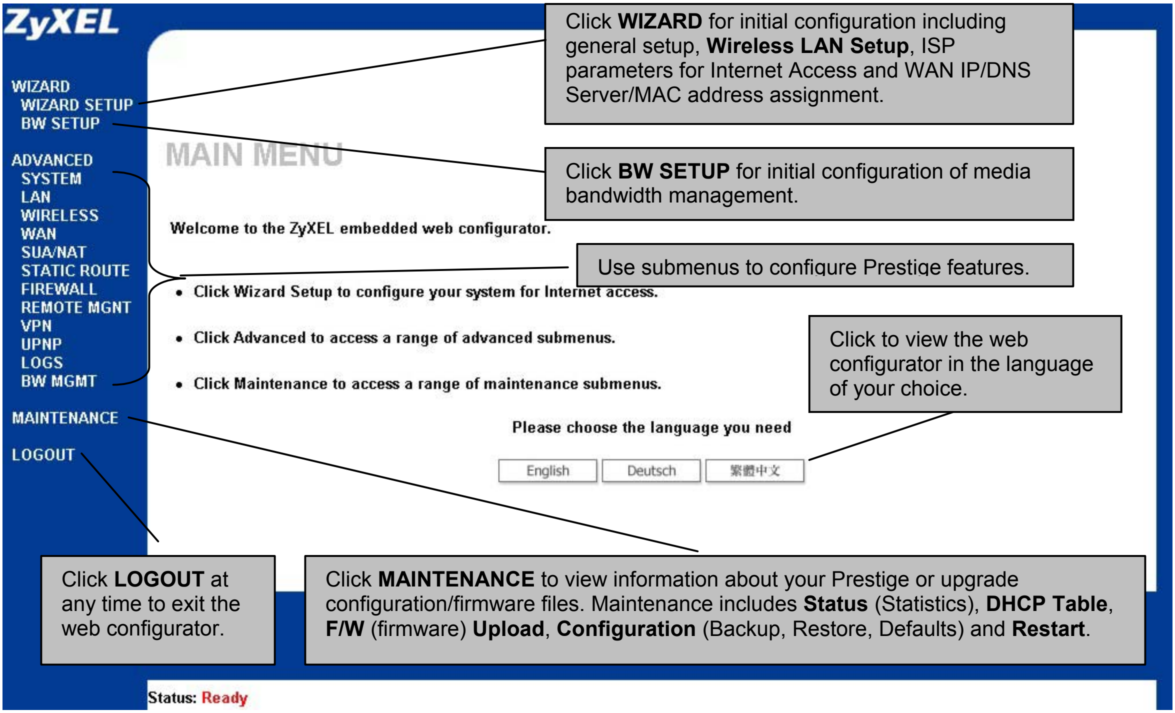
If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the Prestige to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

2.3.1 Procedure To Use The Reset Button

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

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

Step 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.



MAIN MENU

Welcome to the ZyXEL embedded web configurator.

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

Please choose the language you need

Status: Ready

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 **BW SETUP** for initial configuration of media bandwidth management.

Use submenus to configure Prestige features.

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 2-2 The MAIN MENU Screen of the Web Configurator

2.3.2 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 2-1 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.
BW SETUP		Use these screens for initial configuration of media bandwidth management.
SYSTEM	General	This screen contains administrative and system-related information.

Table 2-1 Screens Summary

LINK	TAB	FUNCTION
	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	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.
	802.1x/WPA	This screen allows you to configure 802.1x enhanced security method for both the authentication of wireless stations and encryption key management.
	Local User Database	This screen allows you to configure a database internal to the Prestige.
	RADIUS	This screen allows you to configure an external RADIUS server for an unlimited number of users.
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.

Table 2-1 Screens Summary

LINK	TAB	FUNCTION
FIREWALL	Settings	Use this screen to activate/deactivate the firewall and log packets related to firewall rules.
	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.
	Services	Use this screen to enable service blocking.
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.
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.
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.
MAINTENANCE	Status	This screen contains administrative and system-related information.

Table 2-1 Screens Summary

LINK	TAB	FUNCTION
	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 3
Wizard Setup

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

3.1 Wizard Setup Overview

The web configurator’s setup wizard helps you configure your device to access the Internet. The second screen has three variations depending on what encapsulation type you use. Refer to your ISP 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

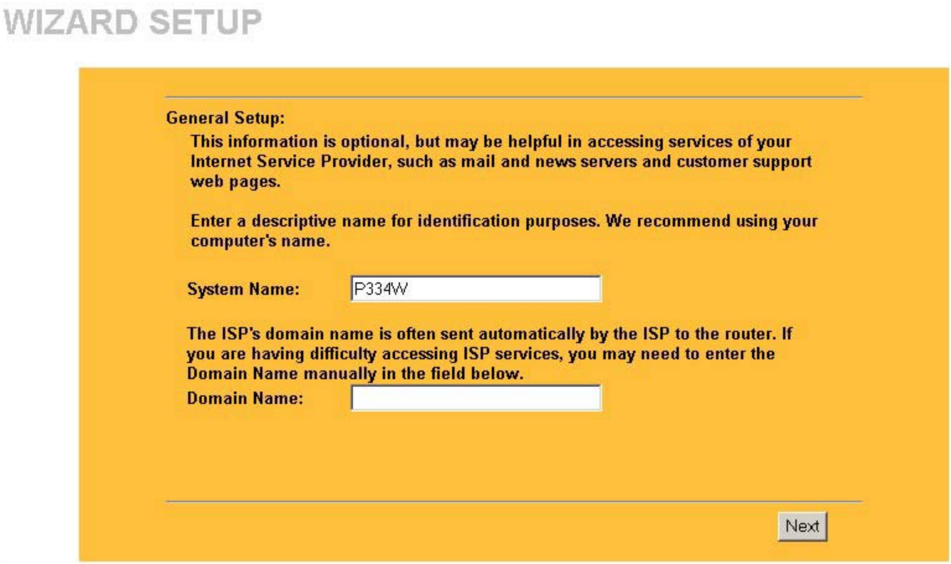
General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- 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.



WIZARD SETUP

General Setup:

This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.

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

System Name: P334W

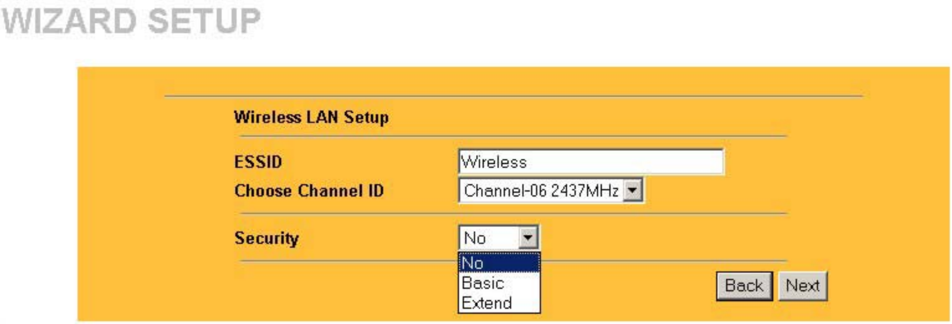
The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.

Domain Name:

Figure 3-1 Wizard 1: General Setup

3.3 Wizard Setup: Screen 2

Set up your wireless LAN using the second wizard screen.



WIZARD SETUP

Wireless LAN Setup

ESSID: Wireless

Choose Channel ID: Channel-06 2437MHz

Security: No

Figure 3-2 Wizard 2: Wireless LAN Setup

The following table describes the fields in this screen.

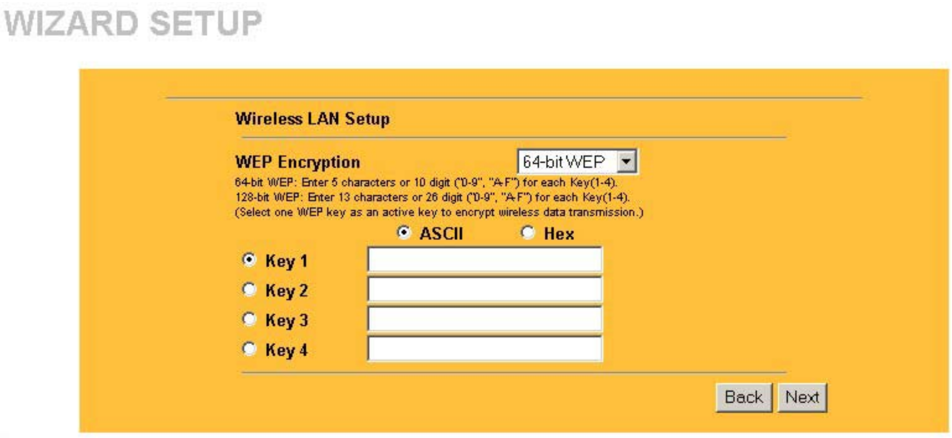
Table 3-1 Wizard 2: Wireless LAN Setup

LABEL	DESCRIPTION
ESSID	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 ESSID 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.
	The level of **Security** can be selected as none, basic or extended. Choose **No** security to have no wireless LAN security configured and proceed to the **ISP Parameters for Internet Access** screen. Choose **Basic** security if you want to configure **WEP Encryption** parameters. Choose **Extend** 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.

The wireless stations and Prestige must use the same ESSID, channel ID and WEP encryption key (if WEP is enabled) for wireless communication.

3.4 Wizard Setup: Screen 3

If you choose **Basic**, you can setup WEP Encryption parameters.



WIZARD SETUP

Wireless LAN Setup

WEP Encryption: 64-bit WEP

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

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

Figure 3-3 Wizard 3: Wireless LAN Setup: Basic Security

The following table describes the labels in this screen.

Table 3-2 Wizard 3: Wireless LAN Setup: Basic Security

WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding “0x” is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the 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"). You must configure all four keys, but 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.

If you choose **Extend** security in the Wireless LAN Setup screen, you can set up a **Pre-Shared Key**.

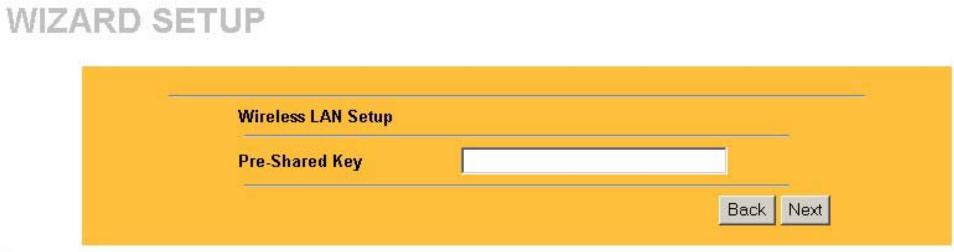


Figure 3-4 Wizard 3: Wireless LAN Setup: Extend Security

The following table describes the labels in this screen.

Table 3-3 Wizard 3: Wireless LAN Setup: Extend Security

Pre-Shared Key	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.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

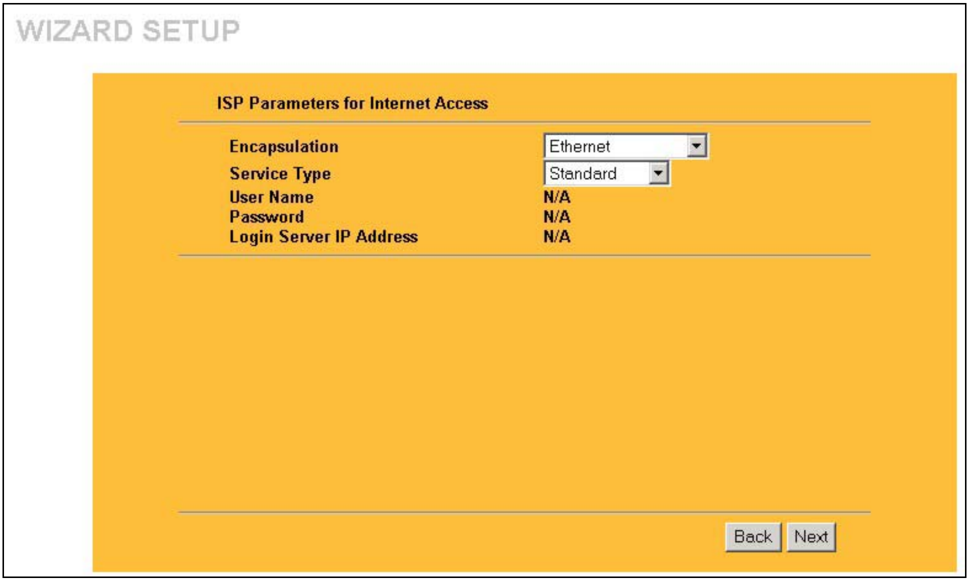
Refer to the chapter on wireless LAN for more information.

3.5 Wizard Setup: Screen 4

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.



WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation: Ethernet

Service Type: Standard

User Name: N/A

Password: N/A

Login Server IP Address: N/A

Figure 3-5 Wizard 4: Ethernet Encapsulation

The following table describes the fields in this screen.

Table 3-4 Wizard 4: 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".

Table 3-4 Wizard 4: Ethernet Encapsulation

LABEL	DESCRIPTION
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.

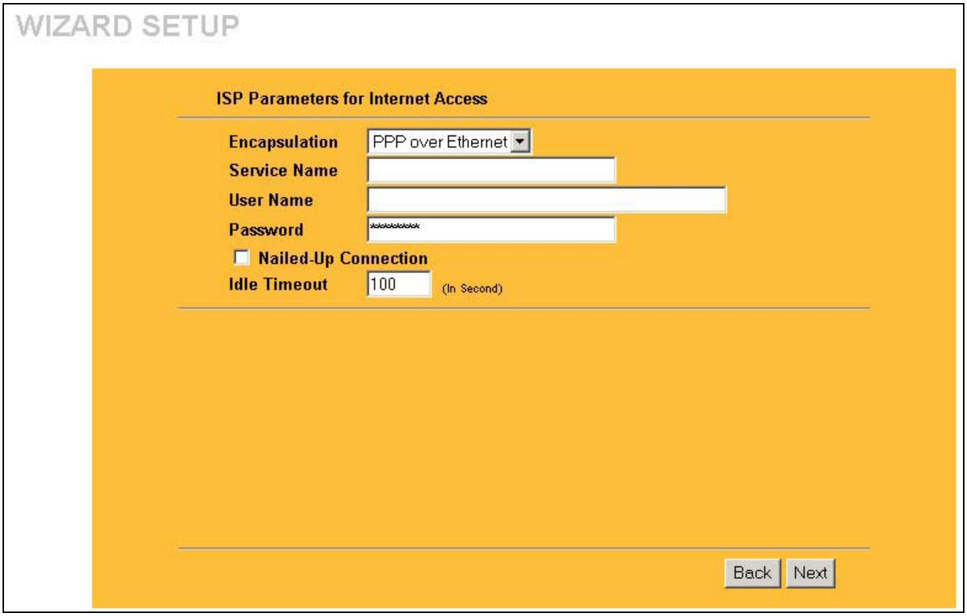
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires 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.



WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation: PPP over Ethernet

Service Name:

User Name:

Password: *********

□ Nailed-Up Connection

Idle Timeout: 100 (In Second)

Figure 3-6 Wizard 4: PPPoE Encapsulation

The following table describes the fields in this screen.

Table 3-5 Wizard 4: 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.

Table 3-5 Wizard 4: PPPoE Encapsulation

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

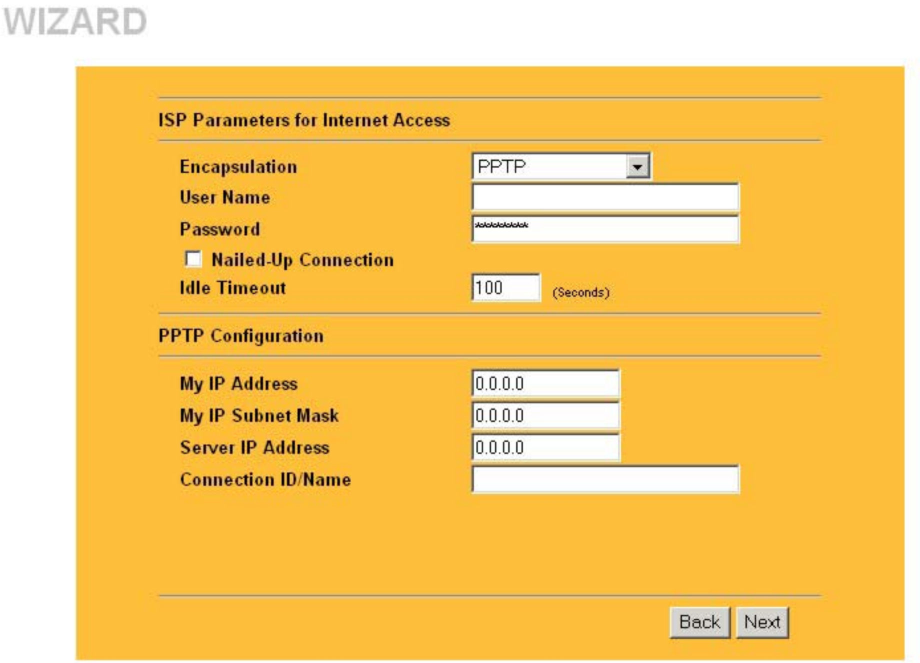
3.5.3 PPTP Encapsulation

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.

The PRESTIGE supports one PPTP server connection at any given time.



WIZARD

ISP Parameters for Internet Access

Encapsulation: PPTP

User Name:

Password: *********

□ Nailed-Up Connection

Idle Timeout: 100 (Seconds)

PPTP Configuration

My IP Address: 0.0.0.0

My IP Subnet Mask: 0.0.0.0

Server IP Address: 0.0.0.0

Connection ID/Name:

Figure 3-7 Wizard 4: PPTP Encapsulation

The following table describes the fields in this screen.

Table 3-6 Wizard 4: 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.
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: Screen 5

The fifth wizard screen allows 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 3-7 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

3.6.2 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.

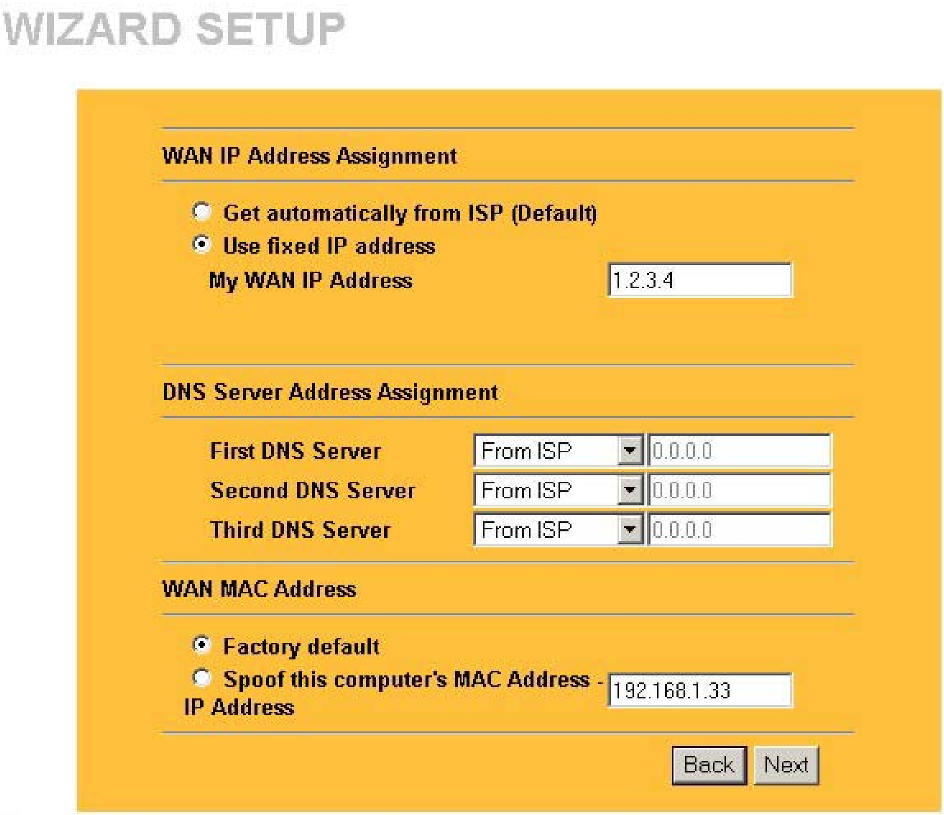
You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload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

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

Table 3-8 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 fifth wizard screen varies according to the type of encapsulation that you select in the third wizard screen.



WIZARD SETUP

WAN IP Address Assignment

○ Get automatically from ISP (Default)

● Use fixed IP address

My WAN IP Address: 1.2.3.4

DNS Server Address Assignment

First DNS Server	From ISP	0.0.0.0
Second DNS Server	From ISP	0.0.0.0
Third DNS Server	From ISP	0.0.0.0

WAN MAC Address

● Factory default

○ Spoof this computer's MAC Address - IP Address: 192.168.1.33

Figure 3-8 Wizard 5: WAN Setup

The following table describes the fields in this screen.

Table 3-9 Wizard 5: WAN Setup

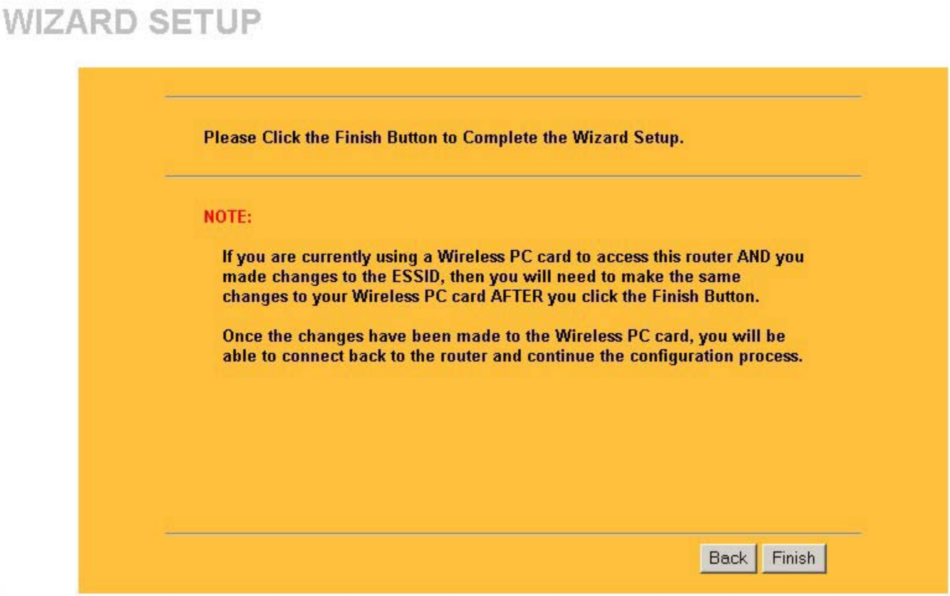
LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**

Table 3-9 Wizard 5: WAN Setup

LABEL	DESCRIPTION
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.
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 Basic Setup Complete

Click **Back** to return to the previous screen or click **Finish** to complete and save the wizard setup.



WIZARD SETUP

Please Click the Finish Button to Complete the Wizard Setup.

NOTE:

If you are currently using a Wireless PC card to access this router AND you made changes to the ESSID, then you will need to make the same changes to your Wireless PC card AFTER you click the Finish Button.

Once the changes have been made to the Wireless PC card, you will be able to connect back to the router and continue the configuration process.

Figure 3-9 Wizard Finish

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.

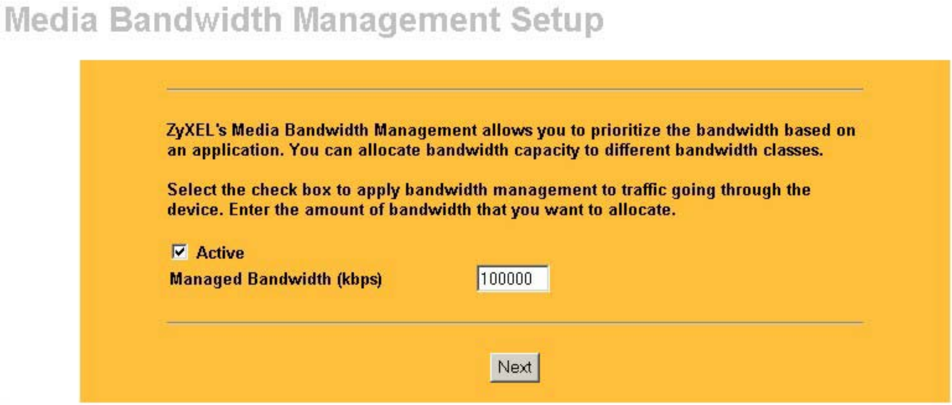
The Prestige applies bandwidth management to traffic that it forwards out through an interface. The Prestige does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router through the interface, 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.

4.2 Media Bandwidth Management Setup 1

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



Media Bandwidth Management Setup

ZyXEL's Media Bandwidth Management allows you to prioritize the bandwidth based on an application. You can allocate bandwidth capacity to different bandwidth classes.

Select the check box to apply bandwidth management to traffic going through the device. Enter the amount of bandwidth that you want to allocate.

☑ Active

Managed Bandwidth (kbps) 100000

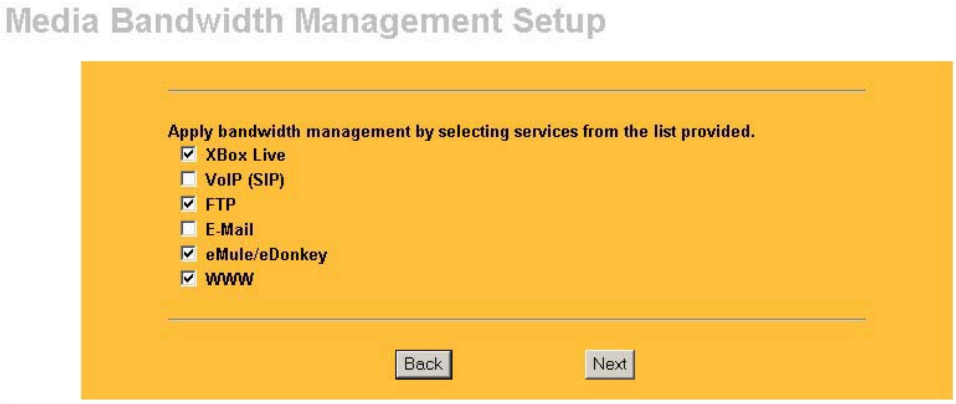
Figure 4-1 Media Bandwidth Management Setup 1

Table 4-1 Media Bandwidth Management Setup 1

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 2

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



Media Bandwidth Management Setup

Apply bandwidth management by selecting services from the list provided.

☑ XBox Live
□ VoIP (SIP)
☑ FTP
□ E-Mail
☑ eMule/eDonkey
☑ WWW

Figure 4-2 Media Bandwidth Management Setup 2: Services

The following table describes the fields in this screen.

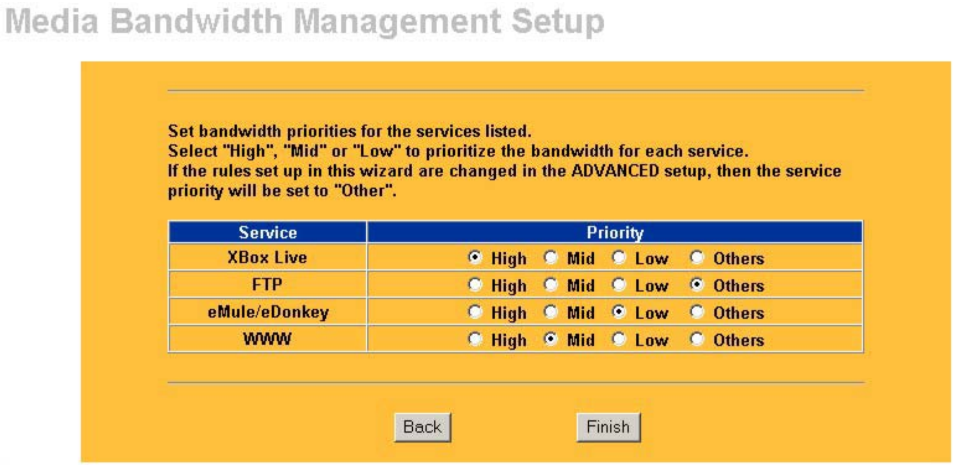
Table 4-2 Media Bandwidth Management Setup 2: Services

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.

Refer to the chapter on Media Bandwidth Management for more information.

4.4 Media Bandwidth Management Setup 3:

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



Media Bandwidth Management Setup

Set bandwidth priorities for the services listed.
Select "High", "Mid" or "Low" to prioritize the bandwidth for each service.
If the rules set up in this wizard are changed in the ADVANCED setup, then the service priority will be set to "Other".

Service	Priority
XBox Live	● High ○ Mid ○ Low ○ Others
FTP	○ High ○ Mid ○ Low ● Others
eMule/eDonkey	○ High ○ Mid ● Low ○ Others
WWW	○ High ● Mid ○ Low ○ Others

Figure 4-3 Media Bandwidth Management Setup 3: Service Priority

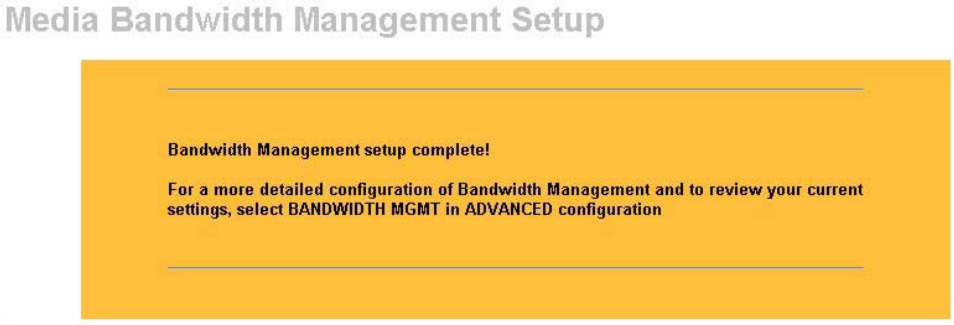
The following table describes the fields in this screen.

Table 4-3 Media Bandwidth Management Setup 3: Service Priority

LABEL	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.



Media Bandwidth Management Setup

Bandwidth Management setup complete!

For a more detailed configuration of Bandwidth Management and to review your current settings, select BANDWIDTH MGMT in ADVANCED configuration

Figure 4-4 Media Bandwidth Management Setup 4: Finish

Part II:

System, LAN, WLAN and WAN

This part covers configuration of the system, LAN, WLAN and WAN screens.

Chapter 5
System Screens

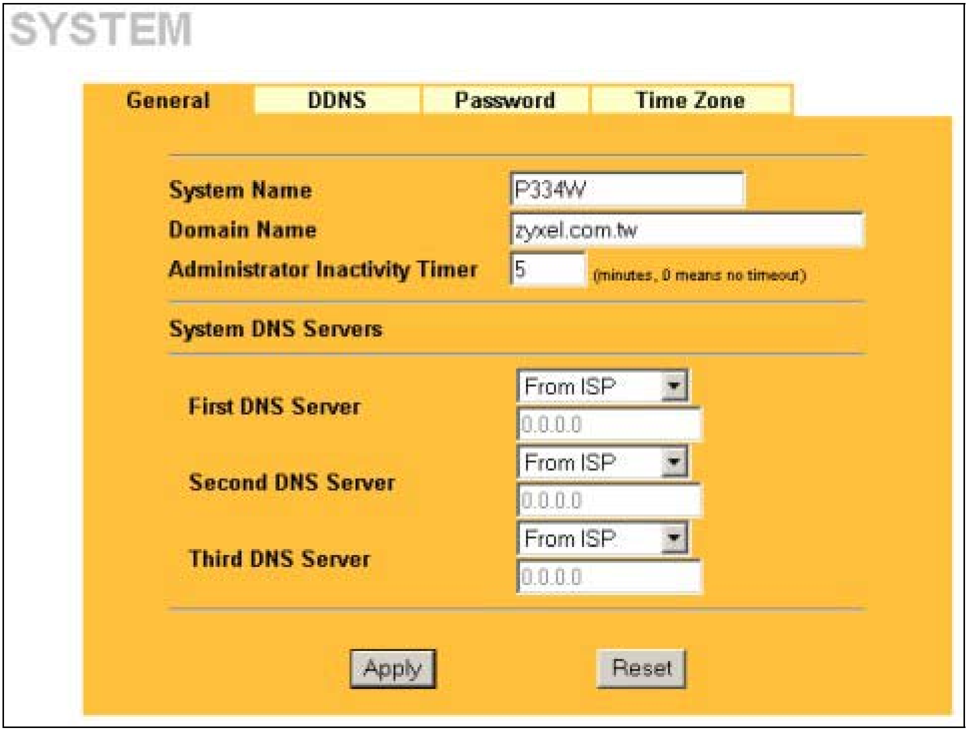
This chapter provides information on the System screens.

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.



System Name: P334W

Domain Name: zyxel.com.tw

Administrator Inactivity Timer: 5 (minutes, 0 means no timeout)

System DNS Servers

First DNS Server: From ISP, 0.0.0.0

Second DNS Server: From ISP, 0.0.0.0

Third DNS Server: From ISP, 0.0.0.0

Figure 5-1 System General Setup

The following table describes the labels in this screen.

Table 5-1 System General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. 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.	
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.

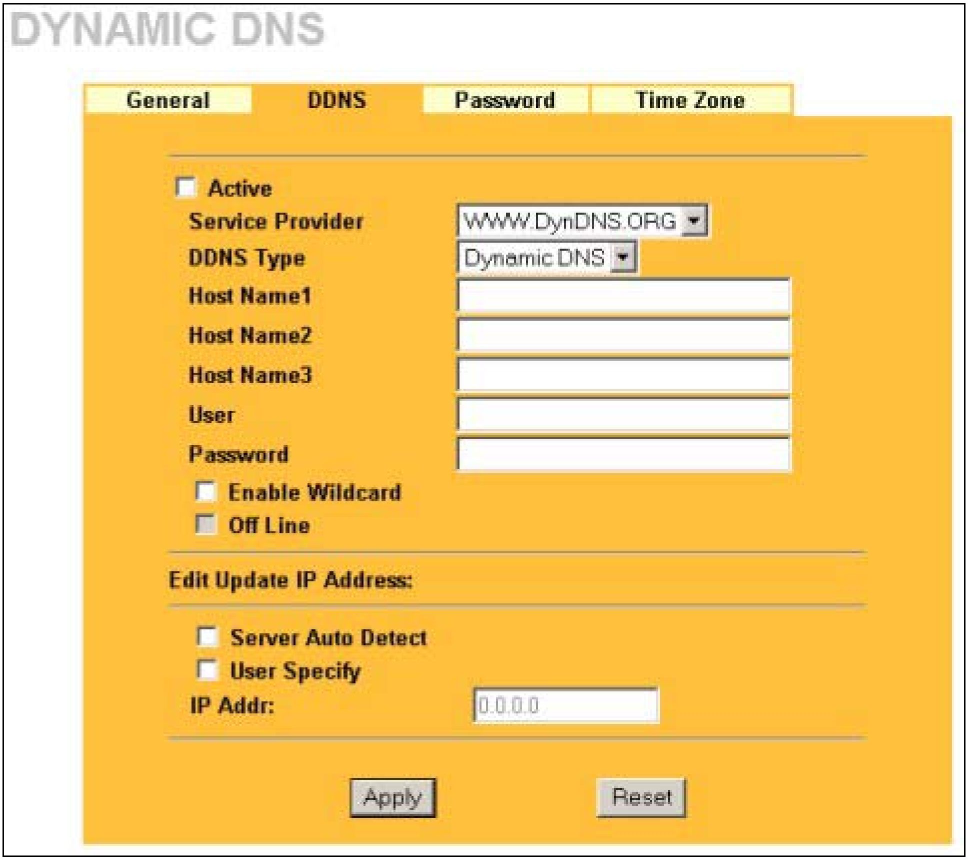
5.3.1 DynDNS Wildcard

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.

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.



Service Provider: WWW.DynDNS.ORG

DDNS Type: Dynamic DNS

IP Addr: 0.0.0.0

Figure 5-2 DDNS

The following table describes the labels in this screen.

Table 5-2 DDNS

LABEL	DESCRIPTION
Active	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.

Table 5-2 DDNS

LABEL	DESCRIPTION
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	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard	Select the check box to enable DynDNS Wildcard.
Off Line	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.
Edit Update IP Address:	
Server Auto Detect	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.
User Specify	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
IP Addr	Enter the IP address if you select the **User Specify** option.
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.

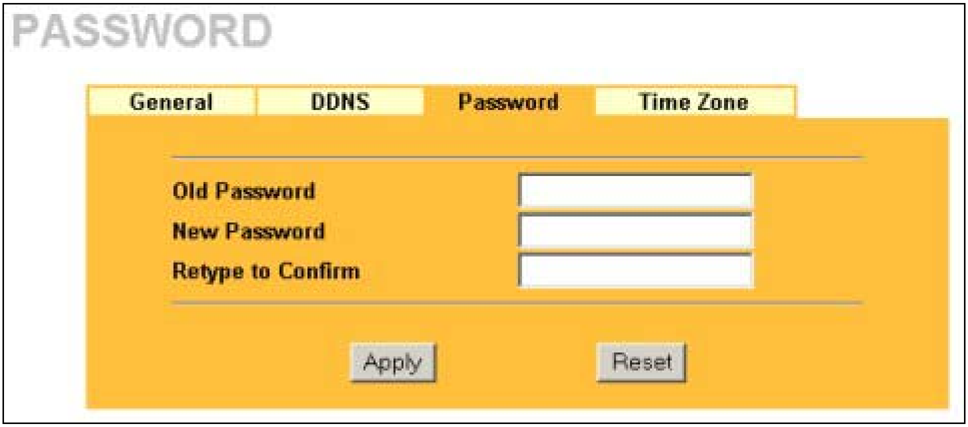


Figure 5-3 Password

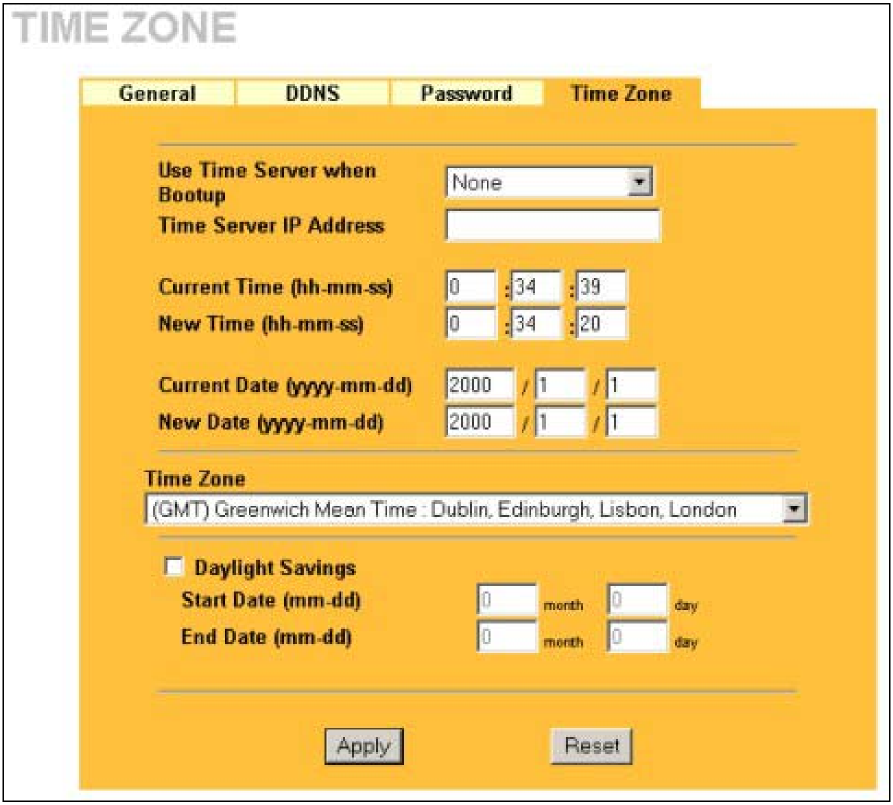
The following table describes the labels in this screen.

Table 5-3 Password

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

5.6 Configuring Time Zone

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



TIME ZONE

Use Time Server when Bootup: None

Time Server IP Address:

Current Time (hh-mm-ss): 0 : 34 : 39

New Time (hh-mm-ss): 0 : 34 : 20

Current Date (yyyy-mm-dd): 2000 / 1 / 1

New Date (yyyy-mm-dd): 2000 / 1 / 1

Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

□ Daylight Savings

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

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

Figure 5-4 Time Setting

The following table describes the labels in this screen.

Table 5-4 Time Setting

LABEL	DESCRIPTION
Use Time Server when Bootup	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.

Table 5-4 Time Setting

LABEL	DESCRIPTION
Time Server IP Address	Enter the IP address 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**.
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.

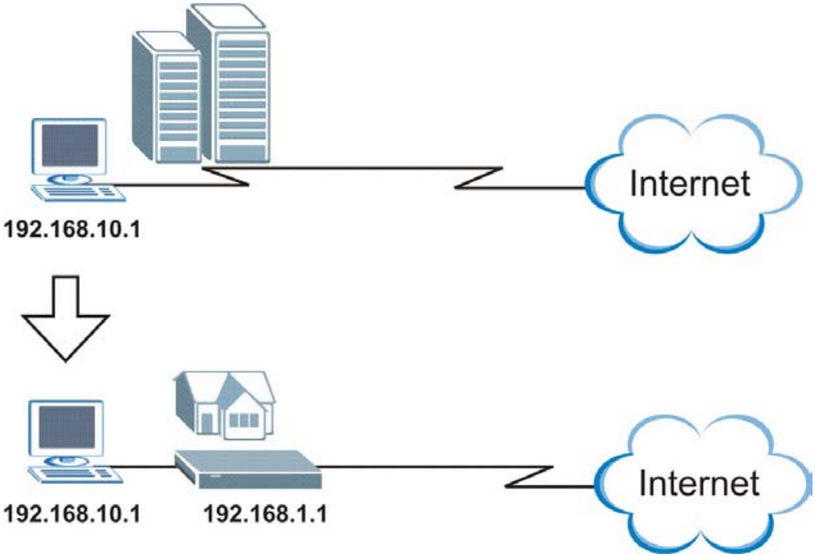


Figure 6-1 Any IP Example Application

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.

You *must* enable NAT/SUA 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.

Step 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.

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

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

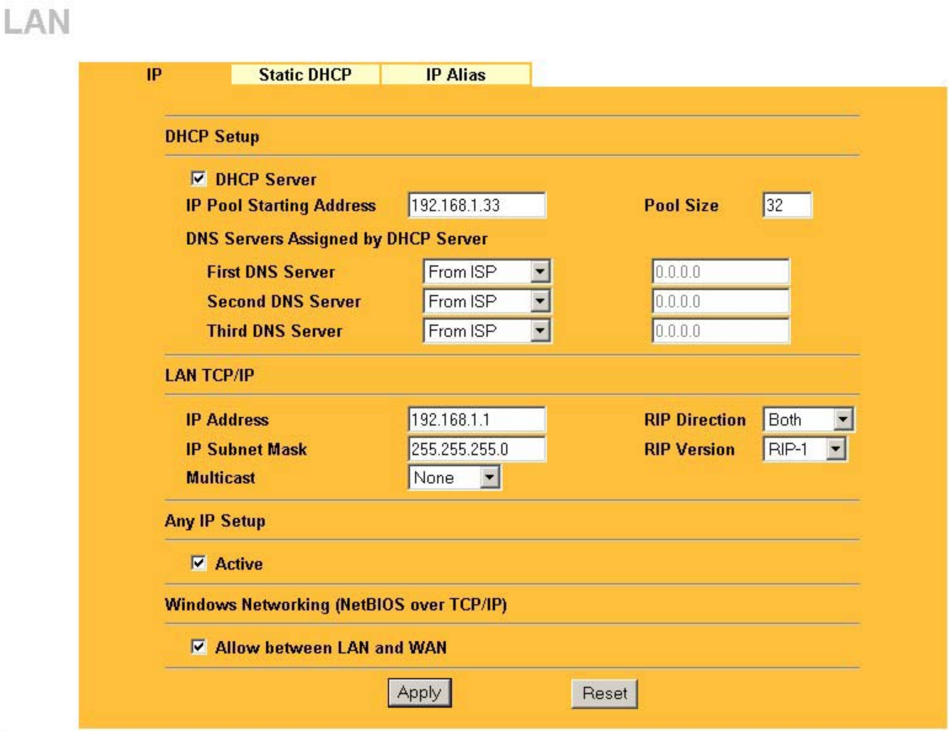
Step 4. The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the Prestige.

Step 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.



DHCP Setup

☑ DHCP Server

IP Pool Starting Address: 192.168.1.33 — Pool Size: 32

DNS Servers Assigned by DHCP Server

First DNS Server	From ISP	0.0.0.0
Second DNS Server	From ISP	0.0.0.0
Third DNS Server	From ISP	0.0.0.0

LAN TCP/IP

IP Address	192.168.1.1	RIP Direction	Both
IP Subnet Mask	255.255.255.0	RIP Version	RIP-1
Multicast	None		

Any IP Setup

☑ Active

Windows Networking (NetBIOS over TCP/IP)

☑ Allow between LAN and WAN

Figure 6-2 IP

The following table describes the fields in this screen.

Table 6-1 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.

Table 6-1 IP

LABEL	DESCRIPTION
Pool Size	This field specifies the size, or count of the IP address pool.
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.

Table 6-1 IP

LABEL	DESCRIPTION
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.
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 subnet 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.	

Table 6-1 IP

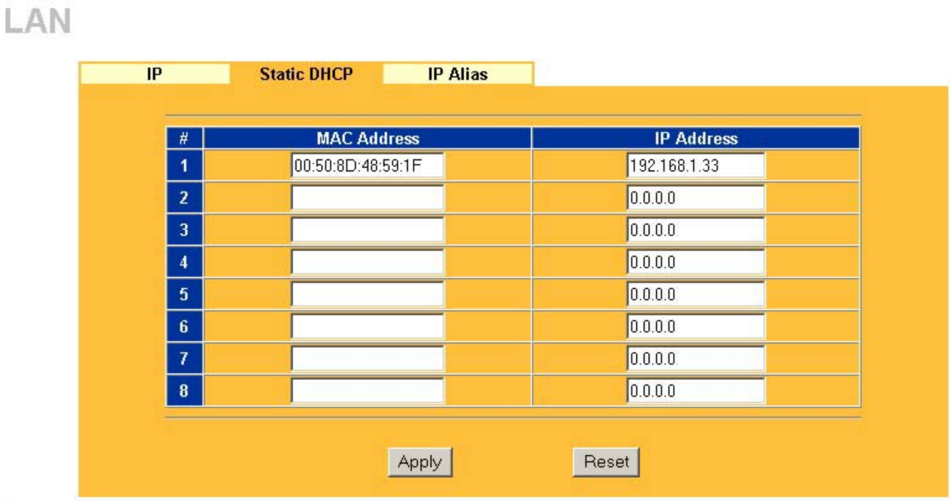
LABEL	DESCRIPTION
Allow from LAN to WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards 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.



#	MAC Address	IP Address
1	00:50:8D:48:59:1F	192.168.1.33
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

Figure 6-3 Static DHCP

The following table describes the labels in this screen.

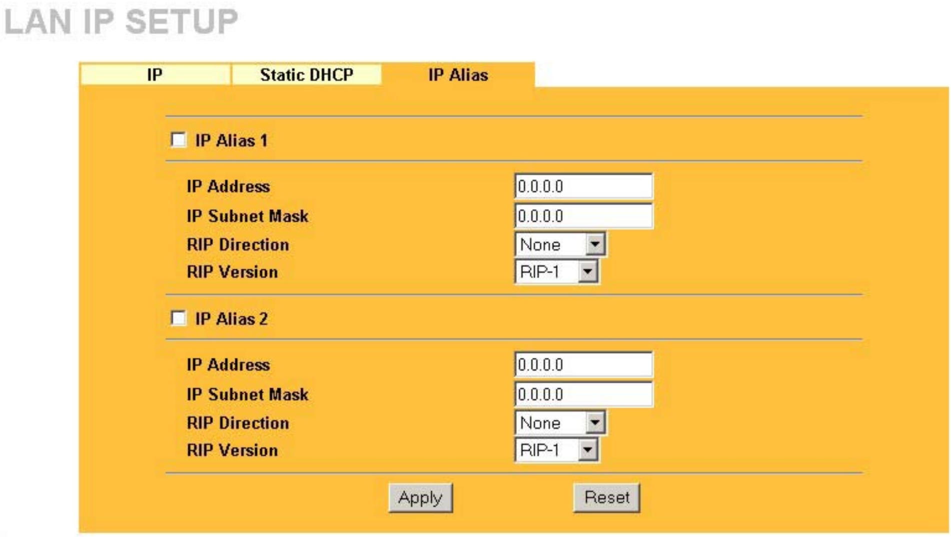
Table 6-2 Static DHCP

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	This field specifies the size, or count of the IP address pool.
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.



LAN IP SETUP

☐ IP Alias 1

IP Address: 0.0.0.0
IP Subnet Mask: 0.0.0.0
RIP Direction: None
RIP Version: RIP-1

☐ IP Alias 2

IP Address: 0.0.0.0
IP Subnet Mask: 0.0.0.0
RIP Direction: None
RIP Version: RIP-1

Figure 6-4 IP Alias

The following table describes the labels in this screen.

Table 6-3 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.

Chapter 7 Wireless Configuration and Roaming

This chapter discusses how to configure the *Wireless* and *Roaming* screen*s on the Prestige.*

7.1 Wireless LAN Overview

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

7.1.1 IBSS

An Independent Basic Service Set (IBSS), also called an Ad-hoc network, is the simplest WLAN configuration. An IBSS is defined as two or more computers with wireless adapters within range of each other that from an independent (wireless) network without the need of an access point (AP).

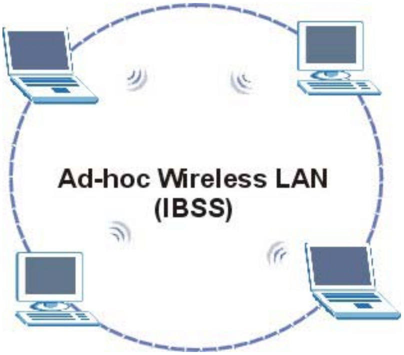


Figure 7-1 IBSS (Ad-hoc) Wireless LAN

7.1.2 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.

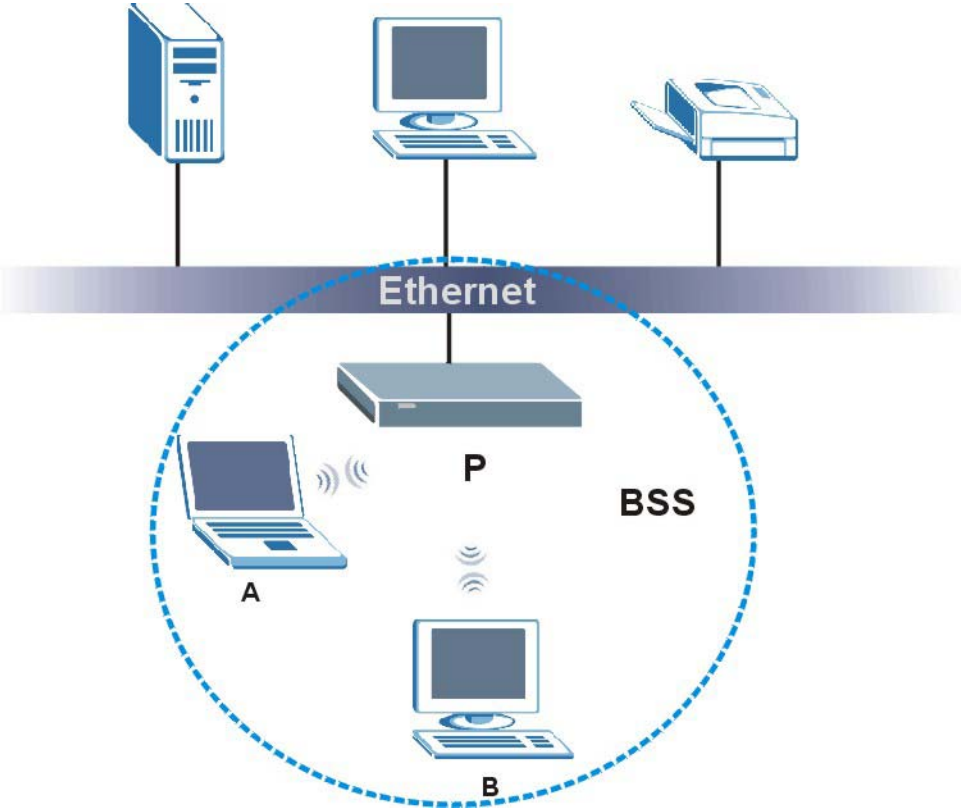


Figure 7-2 Basic Service set

7.1.3 ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS). An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

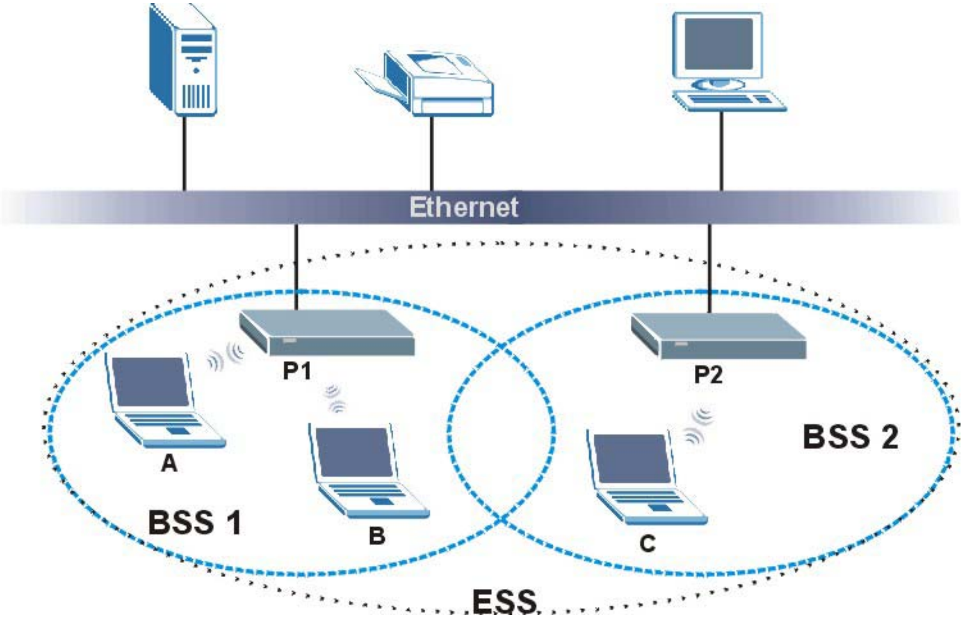


Figure 7-3 Extended Service Set

7.2 Wireless LAN Basics

Refer also to the *Wizard Setup* chapter for more background information on Wireless LAN features, such as channels.

7.2.1 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.

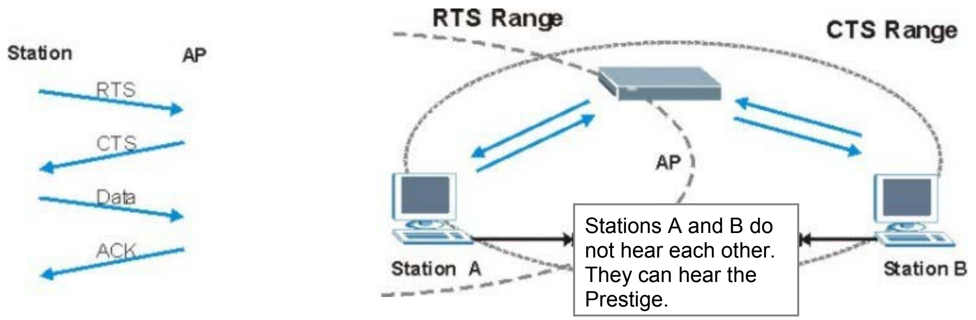

Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the Prestige.

Figure 7-4 RTS/CTS

When station A sends data to the Prestige, it might not know that station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

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

7.2.2 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 Prestige will fragment the packet into smaller data frames.

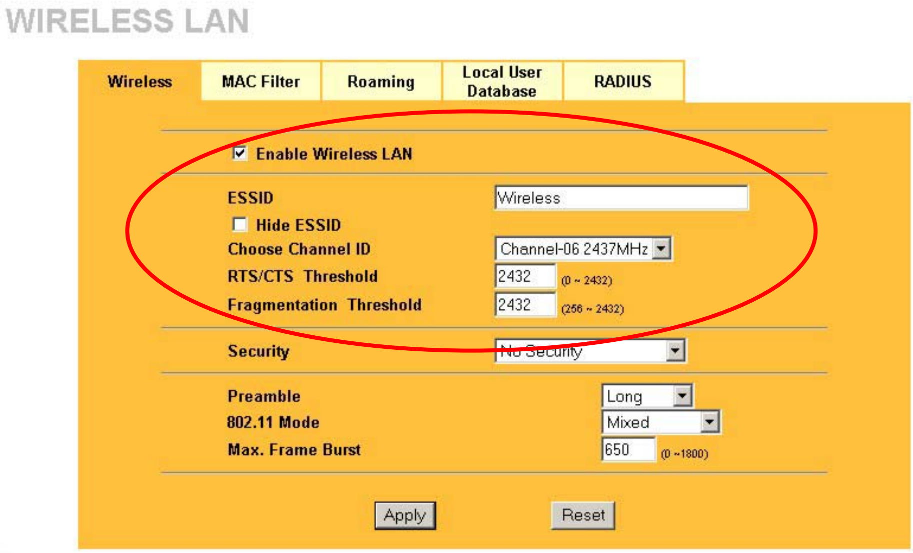
A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

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.

7.3 Configuring Wireless

If you are configuring the Prestige from a computer connected to the wireless LAN and you change the Prestige's ESSID 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.



☑ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: No Security

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

Figure 7-5 Wireless

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

Table 7-1 Wireless

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.

Table 7-1 Wireless

LABEL	DESCRIPTION
ESSID	(Extended Service Set IDentity) The ESSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. **If you are configuring the Prestige from a computer connected to the wireless LAN and you change the Prestige's ESSID 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.**
Hide ESSID	Select this check box to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID 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. The default is **2432**.
Fragmentation Threshold	Enter a value between 256 and 2432. The default is **2432**. It is the maximum data fragment size that can be sent.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

See the *Wireless Security* chapter for information on the other labels in this screen.

7.4 Configuring Roaming

A wireless station is a device with an IEEE 802.11mode 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 *Figure 7-6*.

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.

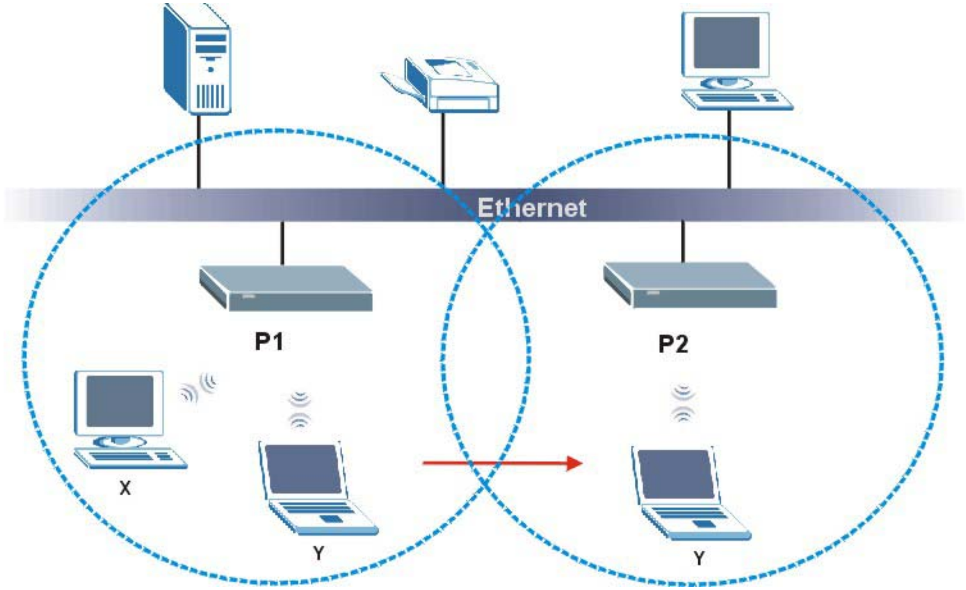


Figure 7-6 Roaming Example

The steps below describe the roaming process.

Step 1. As wireless station **Y** moves from the coverage area of access point **P1** to that of access point **P2**, it scans and uses the signal of access point **P2**.

Step 2. Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.

Step 3. Access point **P1** updates the new position of wireless station.

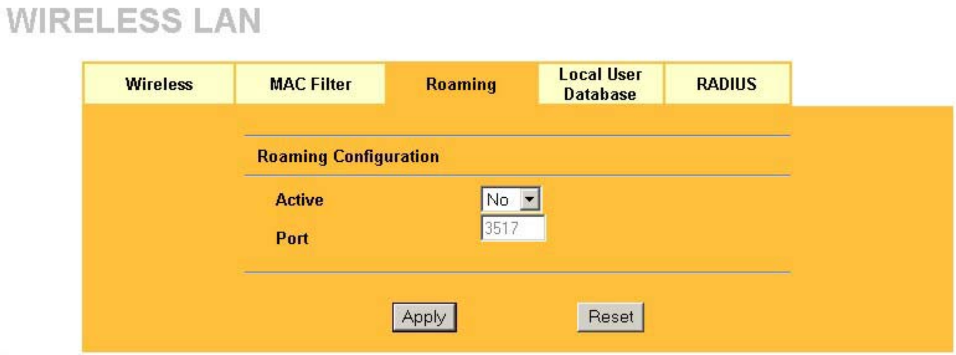
Step 4. Wireless station **Y** sends a request to access point **P2** for re-authentication.

7.4.1 Requirements for Roaming

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

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

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



Roaming Configuration

Active: No

Port: 3517

Figure 7-7 Roaming

The following table describes the labels in this screen.

Table 7-2 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. **All APs on the same subnet and the wireless stations must have the same ESSID to allow roaming.**

Table 7-2 Roaming

LABEL	DESCRIPTION
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.

Chapter 8
Wireless Security

This Chapter describes how to use the MAC Filter, 802.1x, Local User Database and RADIUS to configure wireless security on your Prestige.

8.1 Wireless Security Overview

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

The figure below shows the possible wireless security levels on your Prestige. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

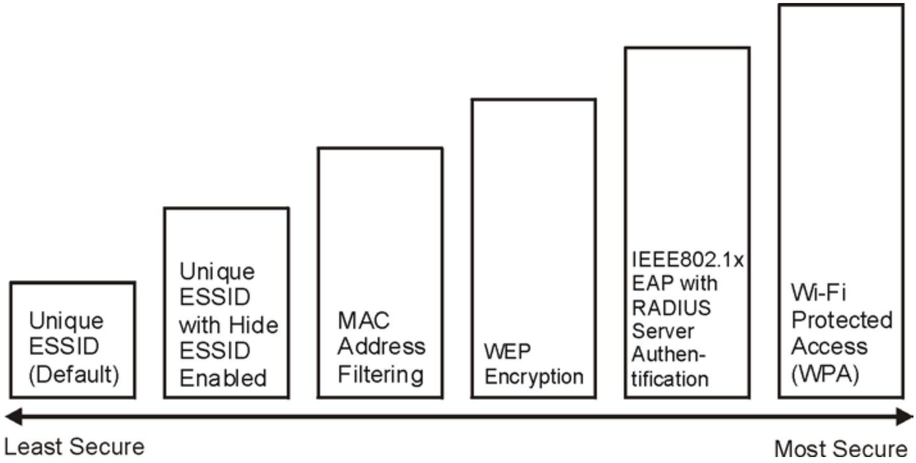
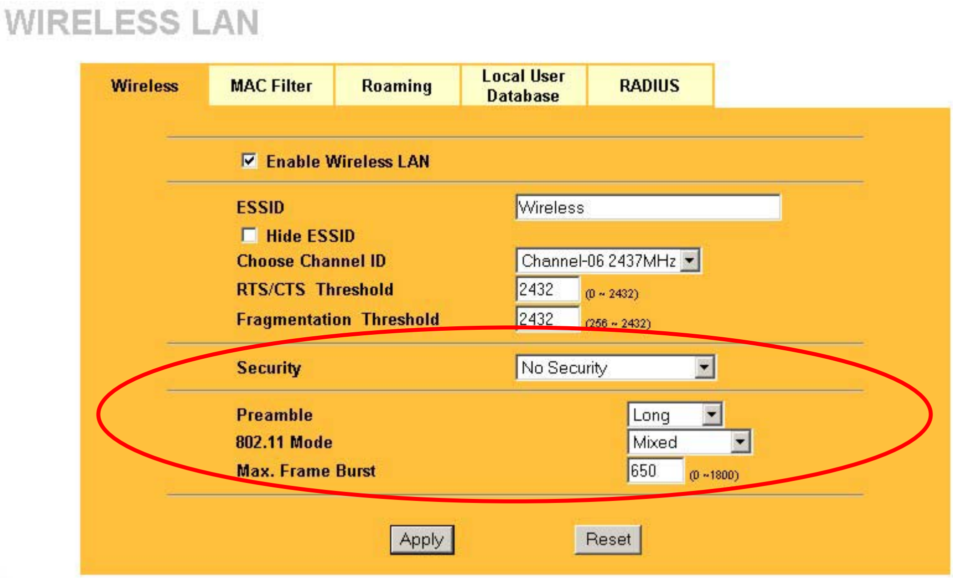

Unique ESSID (Default)
Unique ESSID with Hide ESSID Enabled
MAC Address Filtering
WEP Encryption
IEEE802.1x EAP with RADIUS Server Authen-tification
Wi-Fi Protected Access (WPA)
Least Secure
Most Secure

Figure 8-1 Prestige Wireless Security Levels

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

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



☑ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: No Security

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

Figure 8-2 Wireless: No Security

The following table describes the labels in this screen.

Table 8-1 Wireless: No Security

LABEL	DESCRIPTION
Security	Choose from one of the security features listed in the drop-down box. ➢ No Security ➢ Static WEP ➢ WPA-PSK ➢ WPA ➢ 802.1x + Dynamic WEP ➢ 802.1x + Static WEP ➢ 802.1x + No WEP
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 8-1 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.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the Prestige transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

8.2 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP** or **128-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

Table 8-2 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key

Table 8-2 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Enable
WPA	TKIP	No	Enable
WPA-PSK	WEP	Yes	Enable
WPA-PSK	TKIP	Yes	Enable

8.3 WEP Overview

WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication.

8.3.1 Data Encryption

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your Prestige allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be enabled at any one time.

8.3.2 Authentication

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.

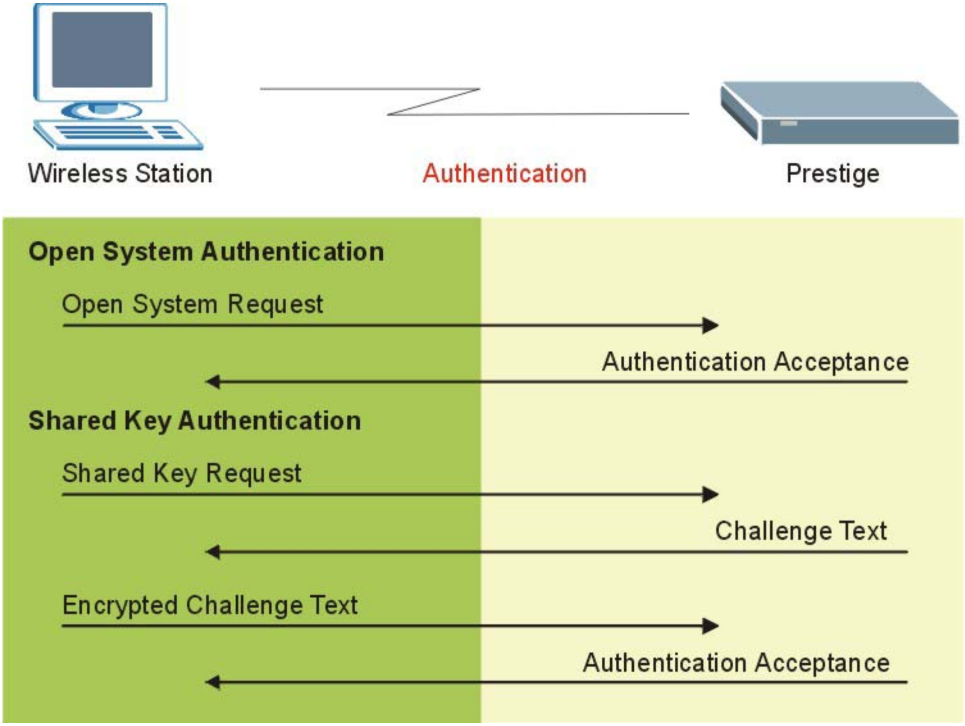


Figure 8-3 WEP Authentication Steps

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 Prestige's 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 Prestige will accept either type of authentication request and the Prestige will fall back to use open authentication if the shared key does not match.

8.3.3 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 clients support it.

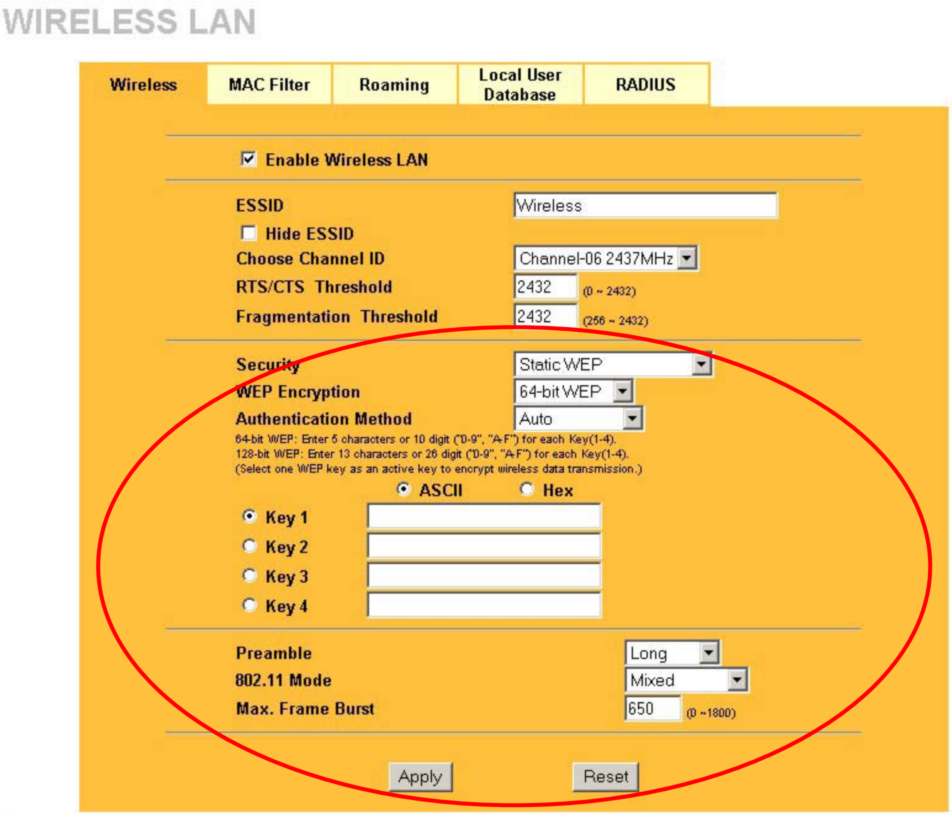
Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless clients support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the Prestige and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the Prestige automatically use short preamble when all wireless clients support it, otherwise the Prestige uses long preamble.

The Prestige and the wireless stations MUST use the same preamble mode in order to communicate.

8.4 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.



WIRELESS LAN

☑ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: Static WEP

WEP Encryption: 64-bit WEP

Authentication Method: Auto

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

● ASCII ○ Hex

● Key 1

○ Key 2

○ Key 3

○ Key 4

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

Figure 8-4 Wireless: Static WEP Encryption

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

Table 8-3 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	This field is activated when you select **64-bit WEP** or **128-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.

Table 8-3 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
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"). You must configure all four keys, but 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.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the Prestige transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

8.5 Introduction to WPA

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

8.5.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can't use the Prestige's Local User Database for WPA authentication purposes since the Local User Database uses EAP MD5, which cannot be used to generate keys. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS and EAP.

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

8.5.2 Encryption

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

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

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

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

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

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

8.5.3 WPA-PSK Application Example

A WPA-PSK application looks as follows.

Step 1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).

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

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

Step 4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

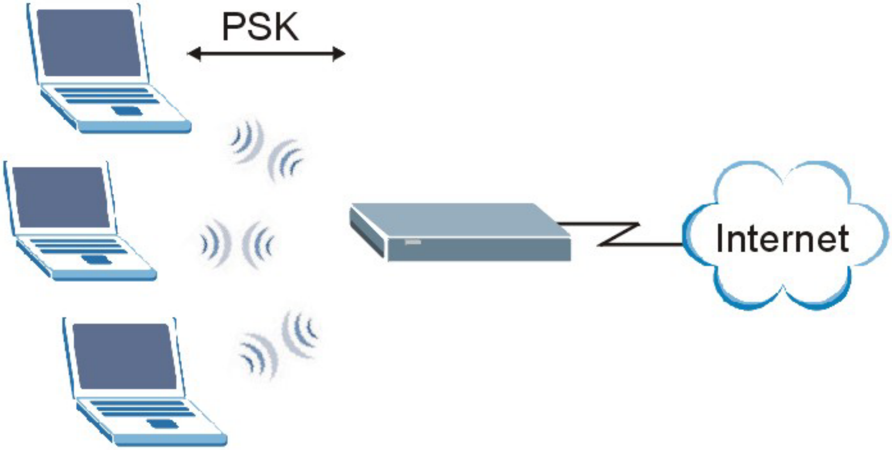
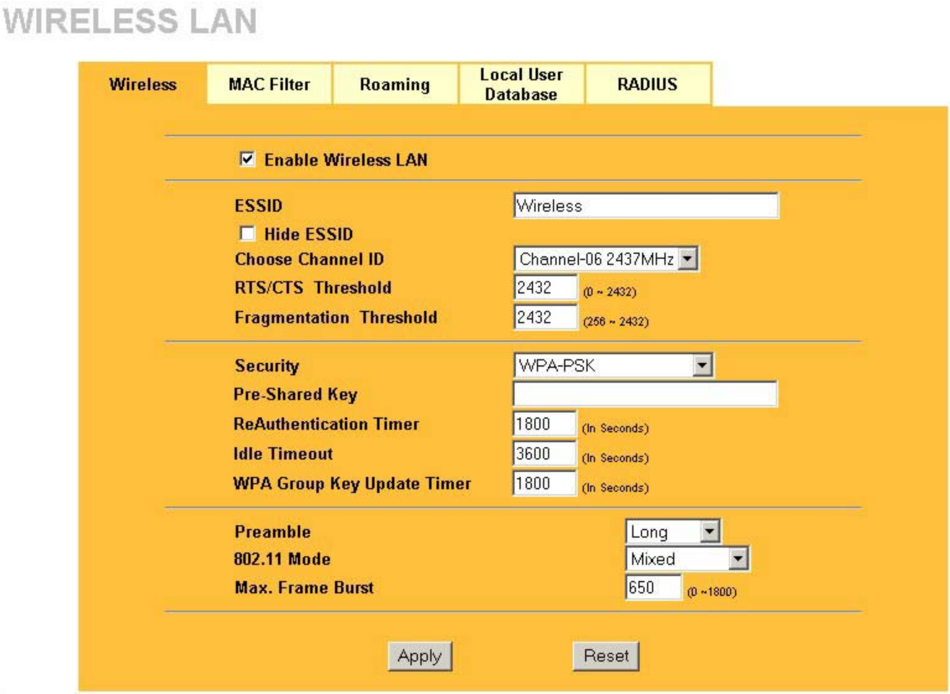


Figure 8-5 WPA - PSK Authentication

8.6 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.



WIRELESS LAN

☑ Enable Wireless LAN

ESSID	Wireless	
□ Hide ESSID		
Choose Channel ID	Channel-06 2437MHz	
RTS/CTS Threshold	2432	(0 ~ 2432)
Fragmentation Threshold	2432	(256 ~ 2432)
Security	WPA-PSK	
Pre-Shared Key		
ReAuthentication Timer	1800	(In Seconds)
Idle Timeout	3600	(In Seconds)
WPA Group Key Update Timer	1800	(In Seconds)
Preamble	Long	
802.11 Mode	Mixed	
Max. Frame Burst	650	(0 ~1800)

Figure 8-6 Wireless: WPA-PSK

The following table describes the labels in this screen.

Table 8-4 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).

Table 8-4 Wireless: WPA-PSK

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). **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).
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.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the Prestige transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

8.7 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 supplicants are the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

The AEGIS client is bundled free (at the time of writing) with the Prestige client adaptor(s). The XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it. Funk's client runs supports a wider variety of authentication protocols than the Windows XP patch, but you need to buy it.

8.7.1 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.

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

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

Step 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.

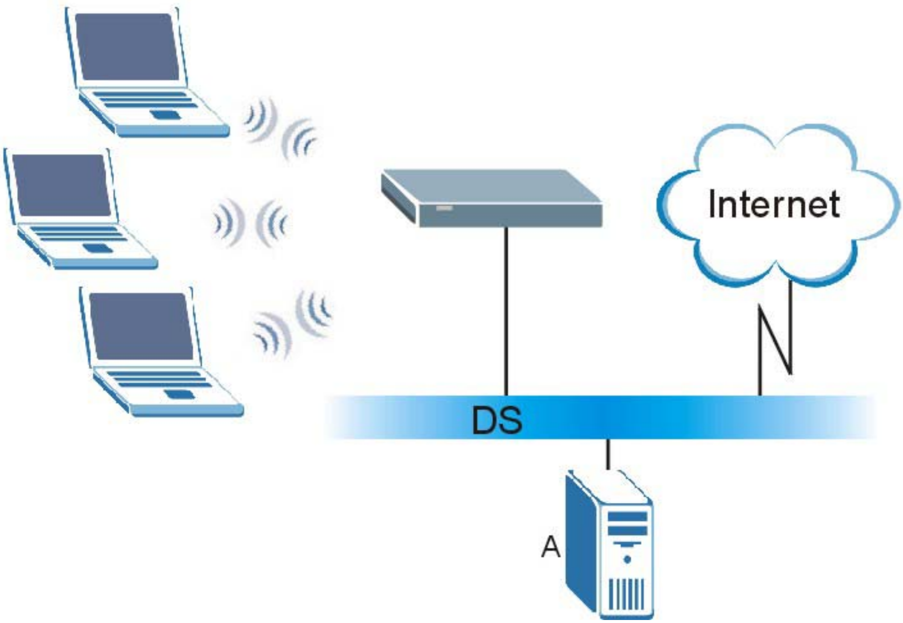
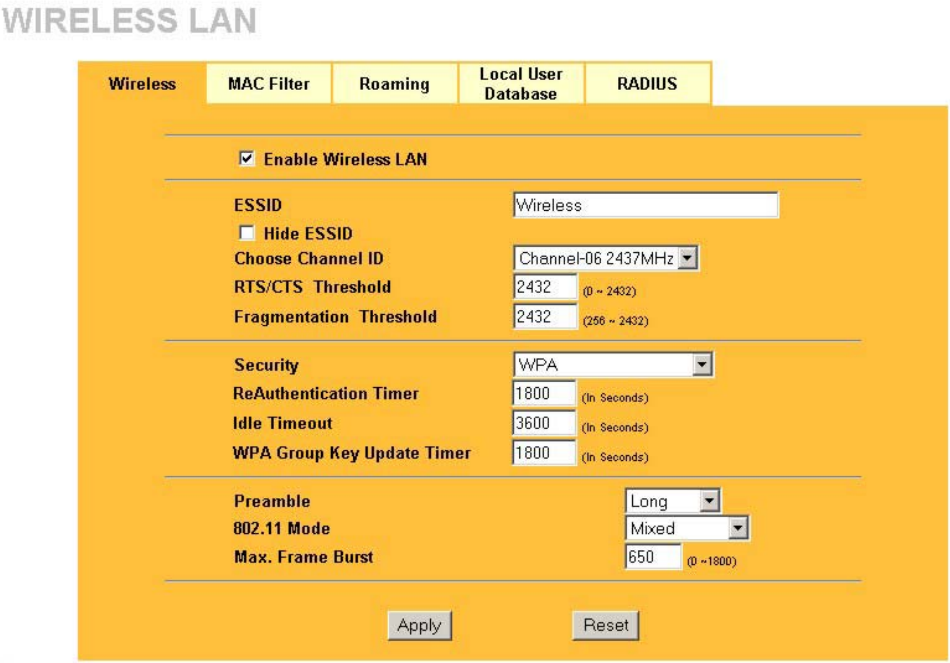


Figure 8-7 WPA with RADIUS Application Example

8.8 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.



WIRELESS LAN

☑ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: WPA

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

WPA Group Key Update Timer: 1800 (In Seconds)

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

Figure 8-8 Wireless: WPA

The following table describes the labels in this screen.

Table 8-5 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). **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).

Table 8-5 Wireless: WPA

LABEL	DESCRIPTION
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.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the Prestige transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

8.9 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the local user database internal to the Prestige (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

See also the section on RADIUS in this *User's Guide*.

8.10 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.

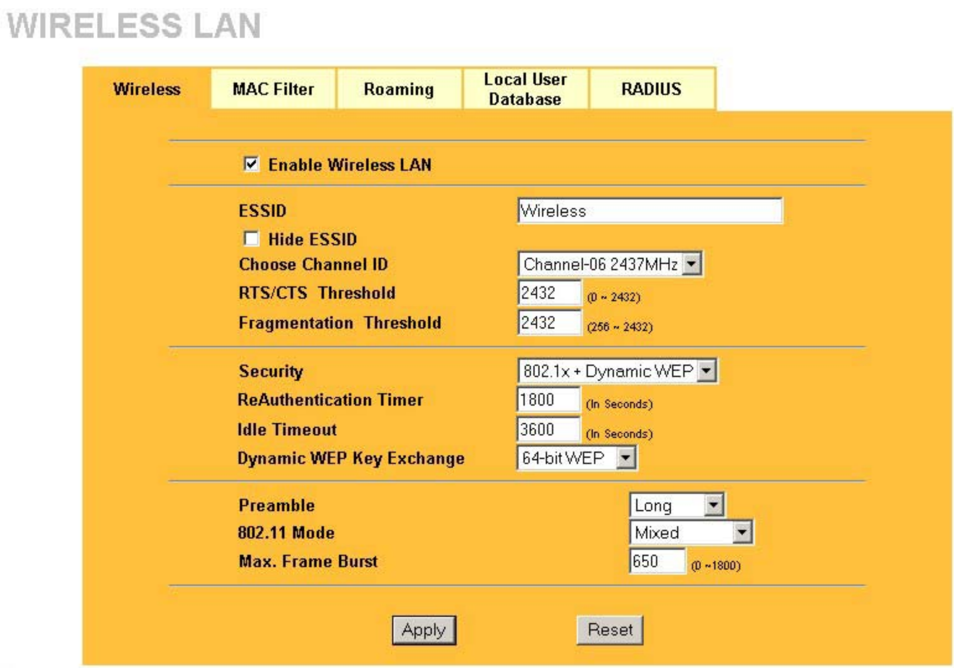
To use Dynamic WEP, enable and configure the RADIUS server (see *section 8.17*) and enable Dynamic WEP Key Exchange in the Wireless screen. Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP

EAP-MD5 cannot be used with Dynamic WEP Key Exchange.

8.11 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.



WIRELESS LAN

☑ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: 802.1x + Dynamic WEP

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Dynamic WEP Key Exchange: 64-bit WEP

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

Figure 8-9 Wireless: 802.1x and Dynamic WEP

The following table describes the labels in this screen.

Table 8-6 Wireless: 802.1x and Dynamic WEP

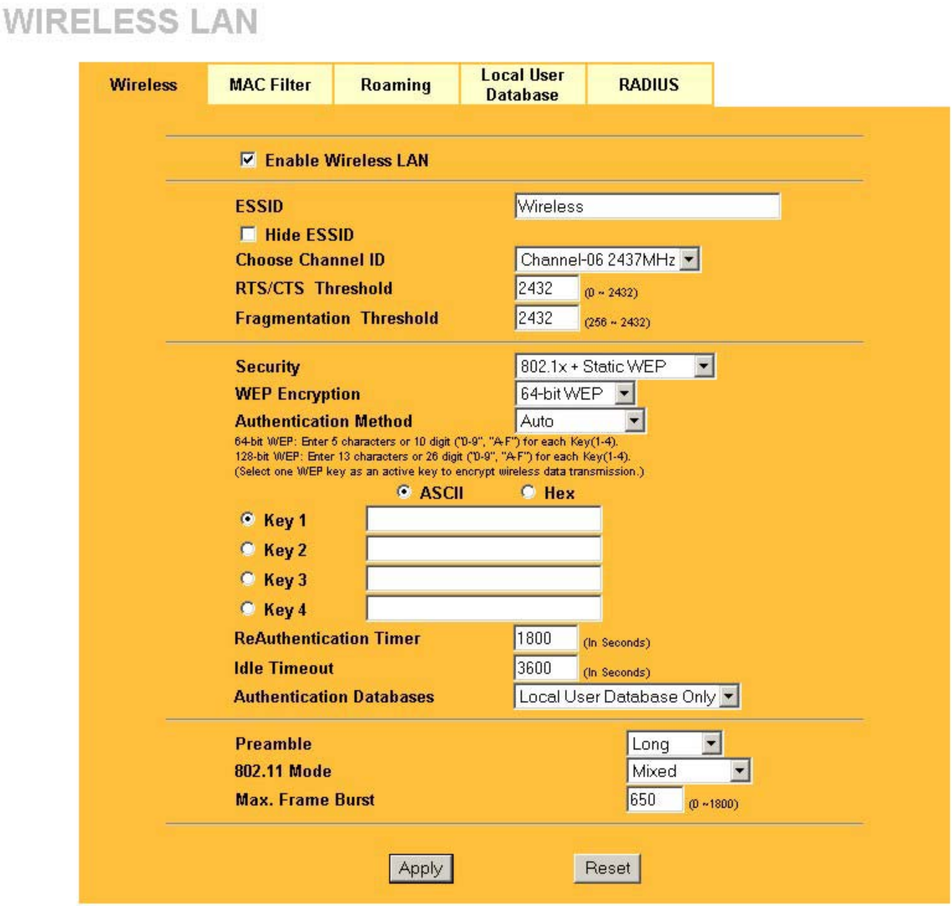
LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). **If wireless station authentication 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).

Table 8-6 Wireless: 802.1x and Dynamic WEP

LABEL	DESCRIPTION
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**.
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.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the Prestige transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

8.12 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.



WIRELESS LAN

☑ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: 802.1x + Static WEP

WEP Encryption: 64-bit WEP

Authentication Method: Auto

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

● ASCII ○ Hex

● Key 1

○ Key 2

○ Key 3

○ Key 4

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Authentication Databases: Local User Database Only

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

Figure 8-10 Wireless: 802.1x and Static WEP

The following table describes the labels in this screen.

Table 8-7 Wireless: 802.1x and Static WEP

LABEL	DESCRIPTION
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	This field is activated when you select **64-bit WEP** or **128-bit WEP** in the WEP Encryption field. Select Auto, Open System or Shared Key from the drop-down list box.

Table 8-7 Wireless: 802.1x and Static WEP

LABEL	DESCRIPTION
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"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
ReAuthentication Timer (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). **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).

Table 8-7 Wireless: 802.1x and Static WEP

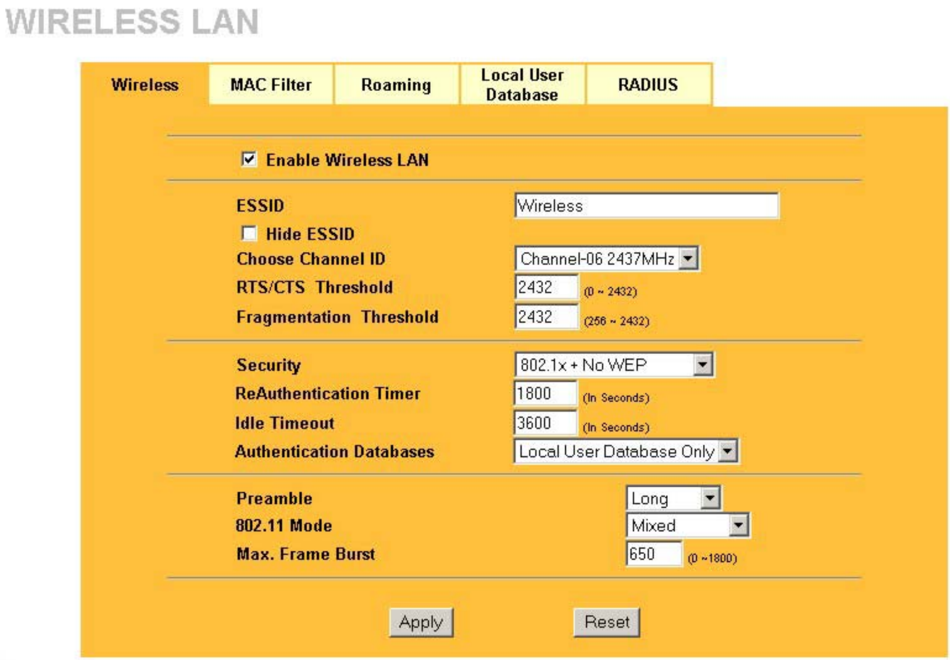
LABEL	DESCRIPTION
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this drop-down list box to select which database the Prestige should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password. 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. Select **Local first, then RADIUS** to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails.
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.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the Prestige transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.

Table 8-7 Wireless: 802.1x and Static WEP

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

8.13 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.



☑ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: 802.1x + No WEP

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Authentication Databases: Local User Database Only

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

Figure 8-11 Wireless: 802.1x

The following table describes the labels in this screen.

Table 8-8 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). **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 Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this drop-down list box to select which database the Prestige should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password. 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. Select **Local first, then RADIUS** to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails.
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.

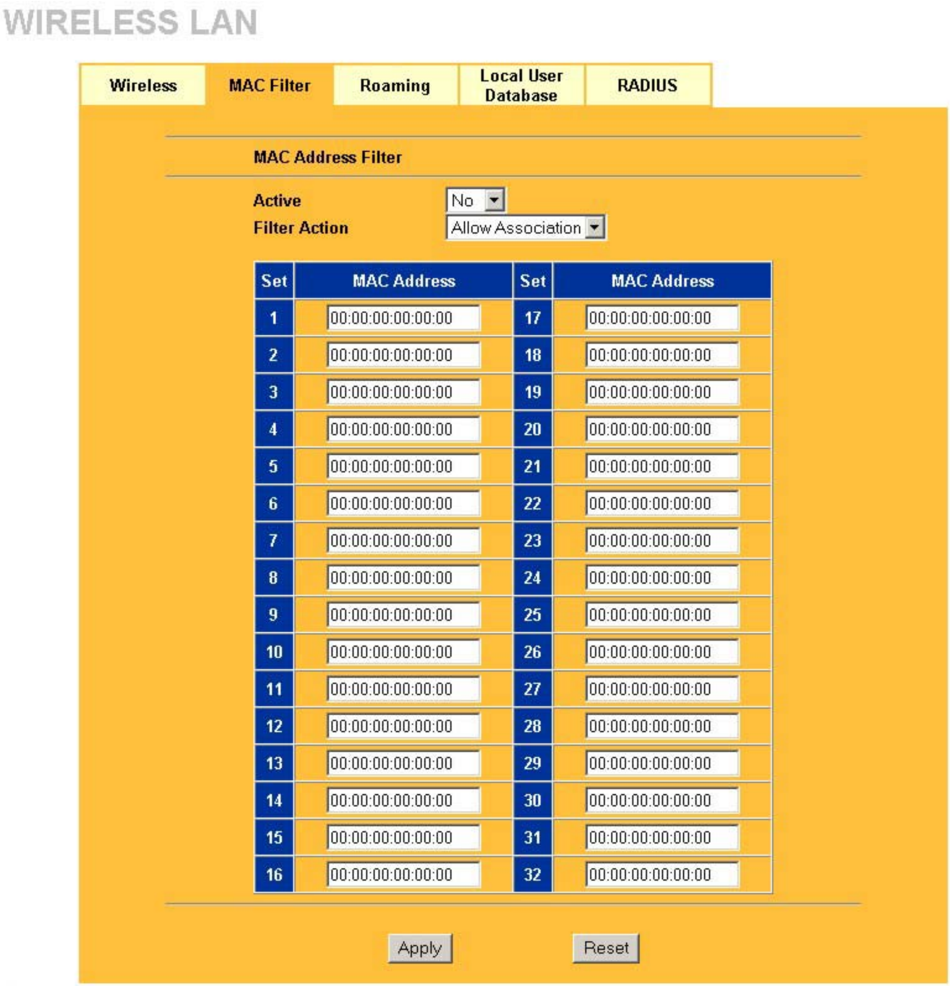
Table 8-8 Wireless: 802.1x and No WEP

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.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the Prestige transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

8.14 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.



MAC Address Filter

Active: No

Filter Action: Allow Association

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

Figure 8-12 MAC Address Filter

The following table describes the labels in this menu.

Table 8-9 MAC Address Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.

Table 8-9 MAC Address Filter

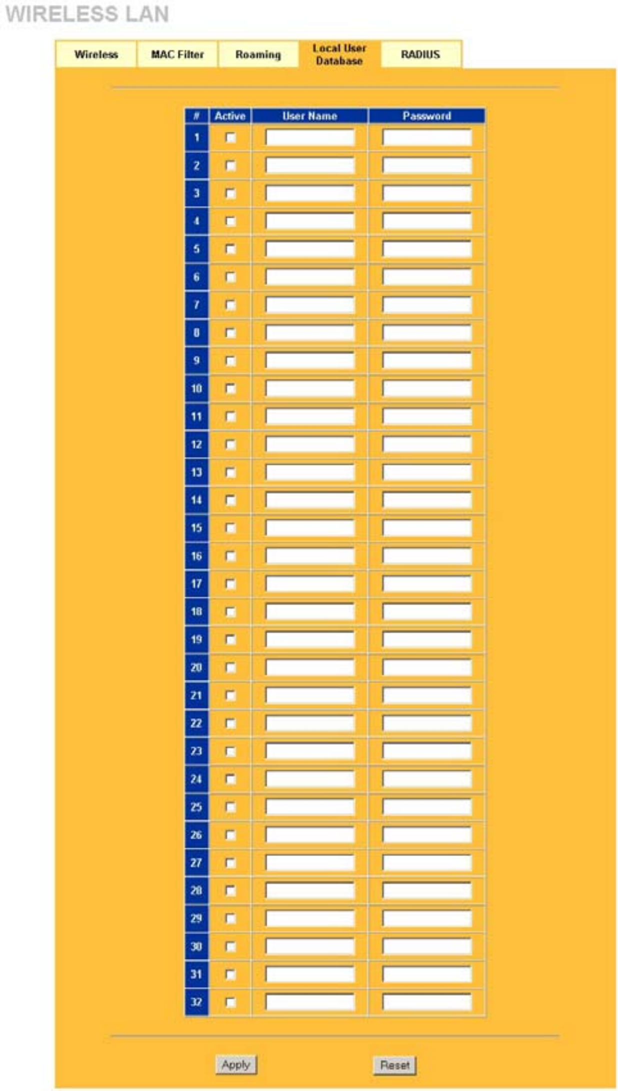
LABEL	DESCRIPTION
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny Association** to block access to the Prestige, MAC addresses not listed will be allowed to access the Prestige Select **Allow Association** to permit access to the Prestige, MAC addresses not listed will be denied access to the Prestige.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the Prestige in these address fields.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

8.15 Introduction to Local User Database

By storing user profiles locally on the Prestige, your Prestige is able to authenticate wireless users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way. You can only use **Local User Database** with 802.1x key management protocol.

8.16 Configuring Local User Database

To change your Prestige's local user database, click the **WIRELESS** link under **ADVANCED** and then the **Local User Database** tab. The screen appears as shown.



#	Active	User Name	Password
1	□		
2	□		
3	□		
4	□		
5	□		
6	□		
7	□		
8	□		
9	□		
10	□		
11	□		
12	□		
13	□		
14	□		
15	□		
16	□		
17	□		
18	□		
19	□		
20	□		
21	□		
22	□		
23	□		
24	□		
25	□		
26	□		
27	□		
28	□		
29	□		
30	□		
31	□		
32	□		

Figure 8-13 Local User Database

The following table describes the labels in this screen.

Table 8-10 Local User Database

LABEL	DESCRIPTION
Active	Select this option to activate the user profile.
User Name	Enter the username (up to 31 characters) for this user profile.
Password	Type a password (up to 31 characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

8.17 Introduction to RADIUS

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

- **Authentication**

  Determines the identity of the users.

- **Accounting**

  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your Prestige 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 wired network from unauthorized access.

8.17.1 EAP Authentication Overview

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

The type of authentication you use depends on the RADIUS server or the AP. The Prestige supports EAP-TLS, EAP-TTLS and DEAP with RADIUS. Refer to the *Types of EAP Authentication* appendix for descriptions on the four common types.

Your Prestige supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database and RADIUS.

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

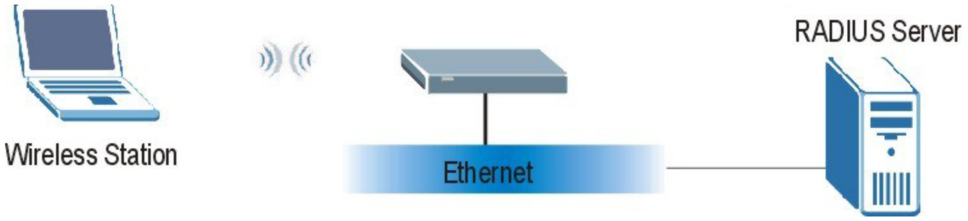


Figure 8-14 EAP Authentication

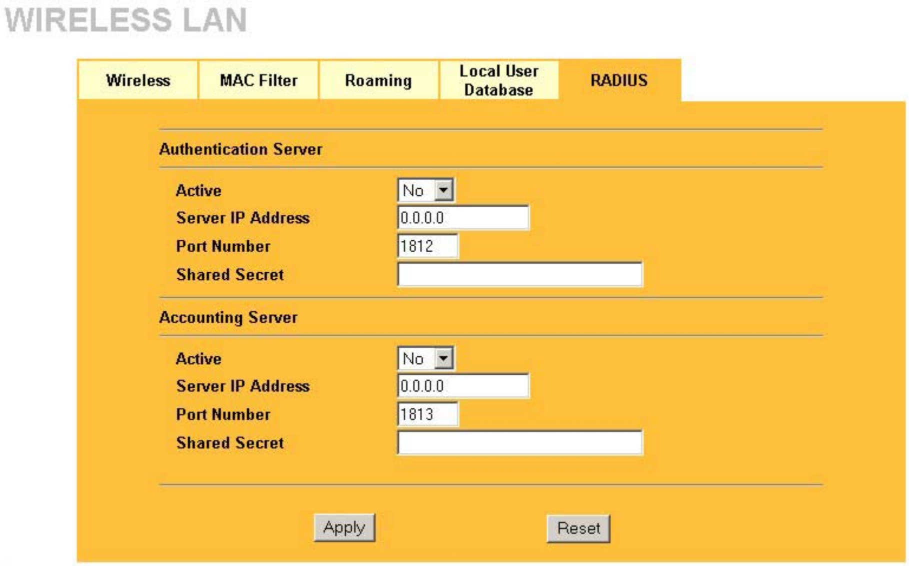
The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

- The wireless station sends a “start” message to the Prestige.
- The Prestige sends a “request identity” message to the wireless station for identity information.
- 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.

8.18 Configuring RADIUS

Configure the RADIUS screen if you want to authenticate wireless users using an external server.

To specify a RADIUS server, click the **WIRELESS** link under **ADVANCED** and then the **RADIUS** tab. The screen appears as shown.



Authentication Server

Active	No
Server IP Address	0.0.0.0
Port Number	1812
Shared Secret	

Accounting Server

Active	No
Server IP Address	0.0.0.0
Port Number	1813
Shared Secret	

Figure 8-15 RADIUS

The following table describes the labels in this screen.

Table 8-11 RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select **Yes** from the drop down list box to enable user authentication through an external authentication server.

Table 8-11 RADIUS

LABEL	DESCRIPTION
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.
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.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

Chapter 9
WAN Screens

This chapter describes how to configure WAN settings.

9.1 WAN Overview

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

9.2 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".

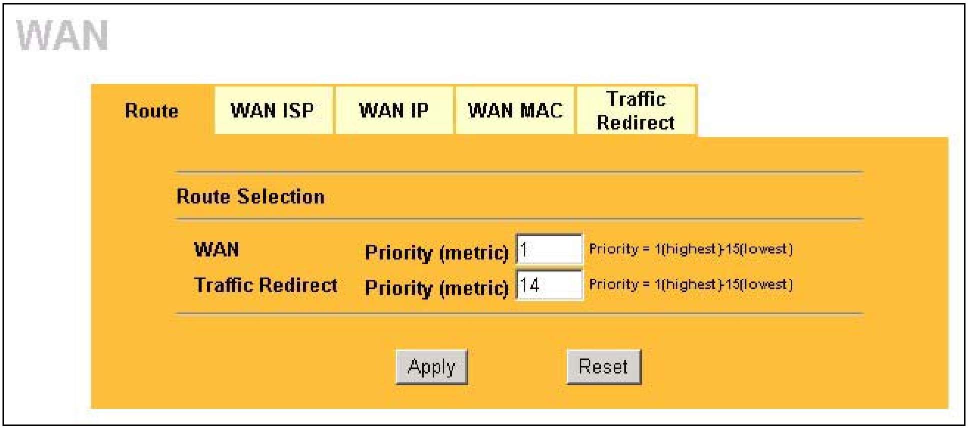
The metric sets the priority for the Prestige's routes to the Internet. If the routes have the same metric, the Prestige uses the following pre-defined priorities:

1. **WAN**: designated by the ISP (see *Section 9.5*) or a static route (see the IP Static Route Setup chapter)
2. **Traffic Redirect** (see *Section 9.8*)

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.

9.3 Configuring Route

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



Route Selection

WAN Priority (metric) 1 Priority = 1(highest)-15(lowest)

Traffic Redirect Priority (metric) 14 Priority = 1(highest)-15(lowest)

Figure 9-1 WAN: Route

The following table describes the labels in this screen.

Table 9-1 WAN: Route

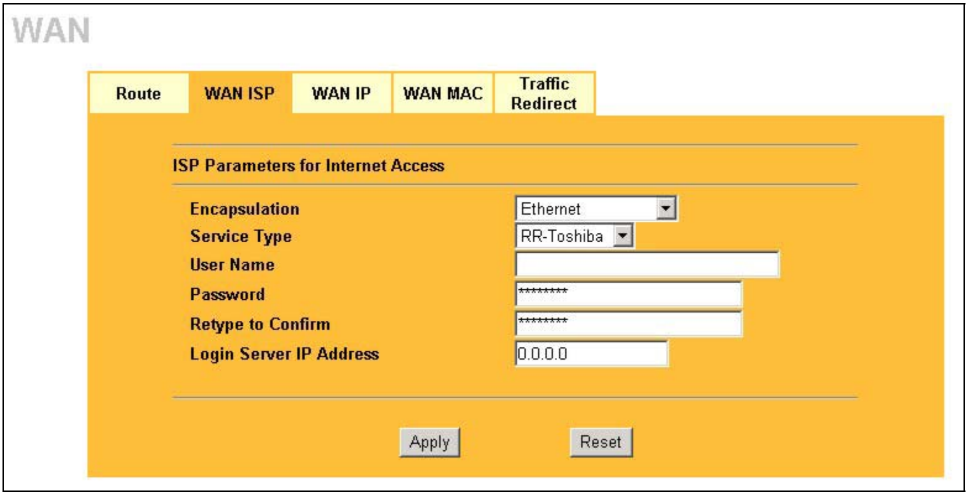
LABEL	DESCRIPTION
WAN Traffic Redirect	The default WAN connection is "1' as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is **WAN** and then **Traffic Redirect**.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

9.4 Configuring WAN ISP

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

9.4.1 Ethernet Encapsulation

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



ISP Parameters for Internet Access

Encapsulation: Ethernet

Service Type: RR-Toshiba

User Name:

Password: ********

Retype to Confirm: ********

Login Server IP Address: 0.0.0.0

Figure 9-2 Ethernet Encapsulation

The following table describes the labels in this screen.

Table 9-2 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 Typ**e 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.

Table 9-2 Ethernet Encapsulation

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

9.4.2 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.

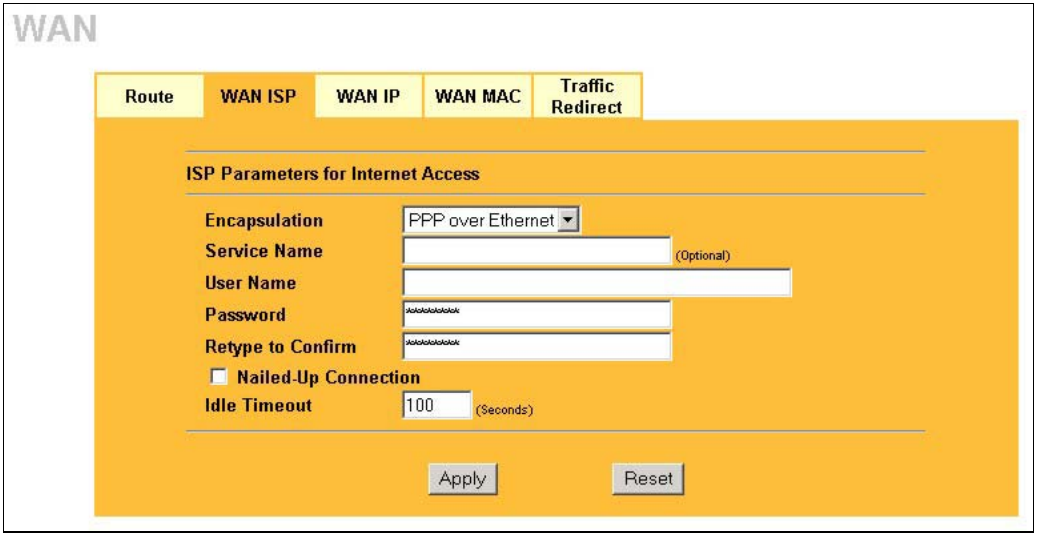
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning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



WAN

ISP Parameters for Internet Access

Encapsulation: PPP over Ethernet

Service Name: (Optional)

User Name:

Password: *********

Retype to Confirm: *********

□ Nailed-Up Connection

Idle Timeout: 100 (Seconds)

Figure 9-3 PPPoE Encapsulation

The following table describes the labels in this screen.

Table 9-3 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.

Table 9-3 PPPoE Encapsulation

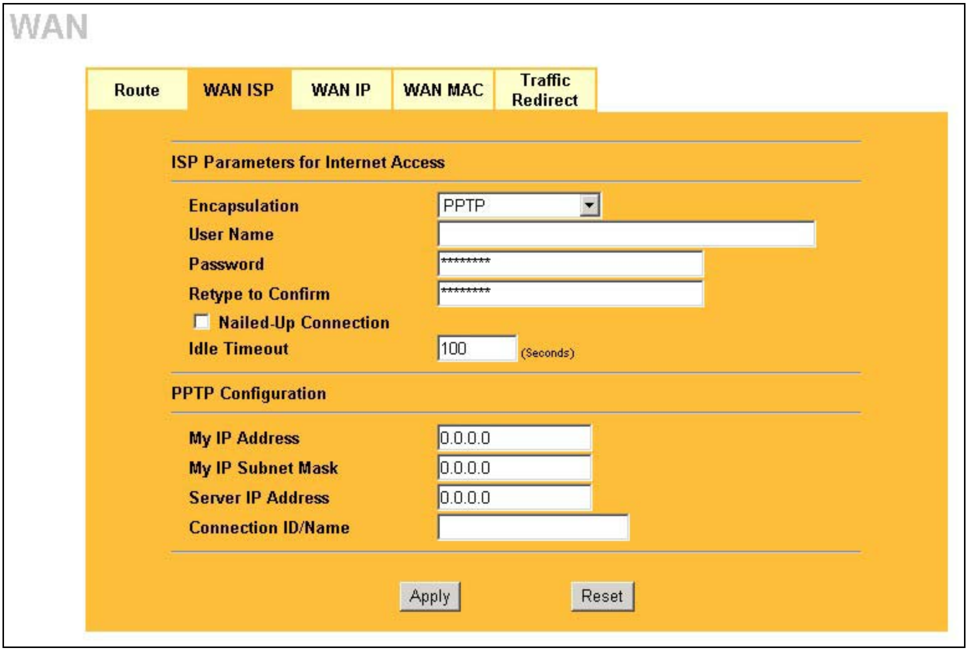
LABEL	DESCRIPTION
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

9.4.3 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.



ISP Parameters for Internet Access

Encapsulation: PPTP
User Name:
Password: ********
Retype to Confirm: ********
□ Nailed-Up Connection
Idle Timeout: 100 (Seconds)

PPTP Configuration

My IP Address: 0.0.0.0
My IP Subnet Mask: 0.0.0.0
Server IP Address: 0.0.0.0
Connection ID/Name:

Figure 9-4 PPTP Encapsulation

The following table describes the labels in this screen.

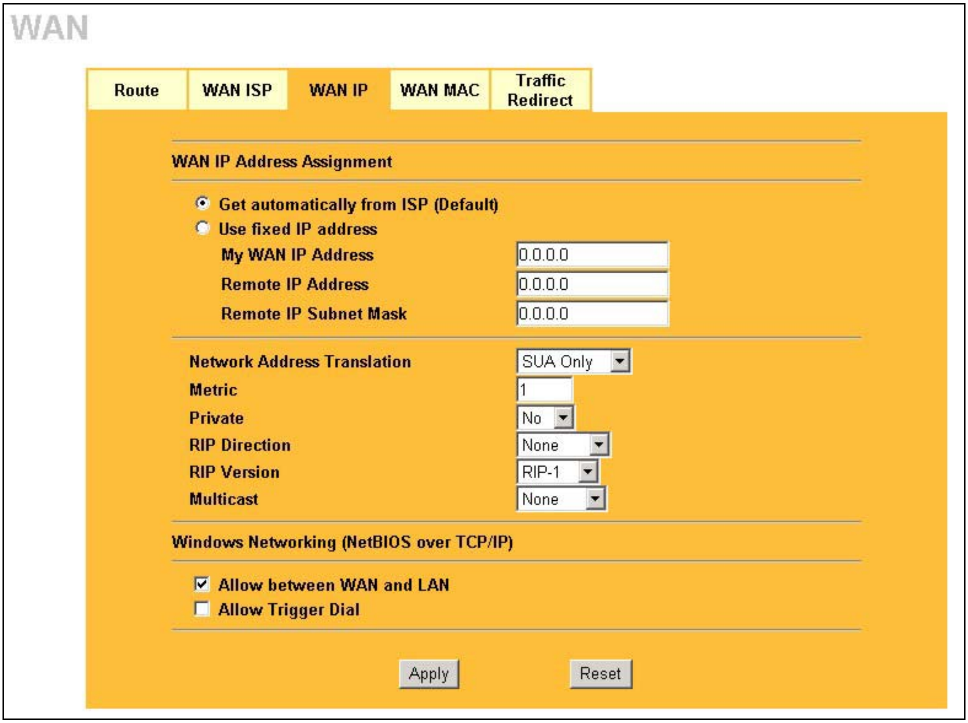
Table 9-4 PPTP Encapsulation

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.
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.

9.5 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.



WAN IP Address Assignment

● Get automatically from ISP (Default)

○ Use fixed IP address

My WAN IP Address	0.0.0.0
Remote IP Address	0.0.0.0
Remote IP Subnet Mask	0.0.0.0
Network Address Translation	SUA Only
Metric	1
Private	No
RIP Direction	None
RIP Version	RIP-1
Multicast	None

Windows Networking (NetBIOS over TCP/IP)

☑ Allow between WAN and LAN

□ Allow Trigger Dial

Figure 9-5 WAN: IP

The following table describes the labels in this screen.

Table 9-5 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.

Table 9-5 WAN: IP

LABEL	DESCRIPTION
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**.
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*.
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.

Table 9-5 WAN: IP

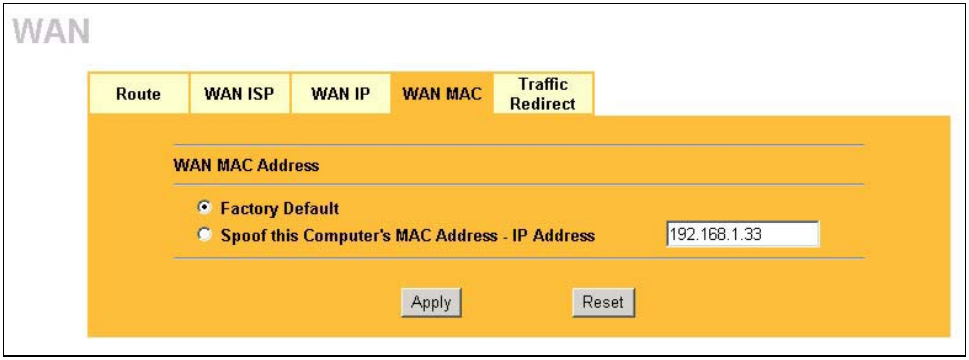
LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, 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**.
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.	

Table 9-5 WAN: IP

LABEL	DESCRIPTION
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.

9.6 Configuring WAN MAC

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



WAN MAC Address

● Factory Default
○ Spoof this Computer's MAC Address - IP Address 192.168.1.33

Figure 9-6 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.

9.7 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.

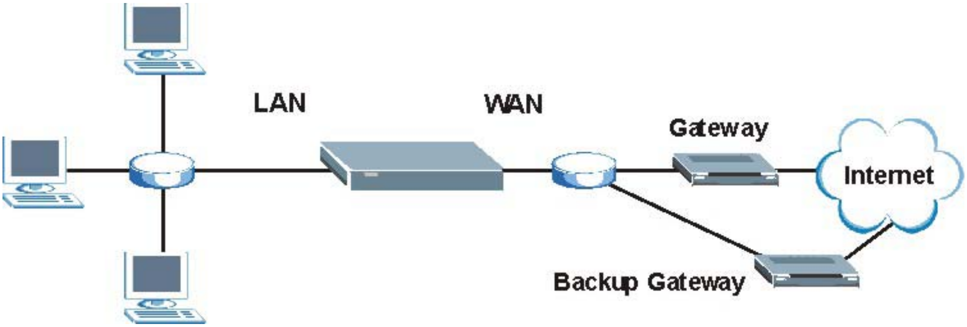


Figure 9-7 Traffic Redirect WAN Setup

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).

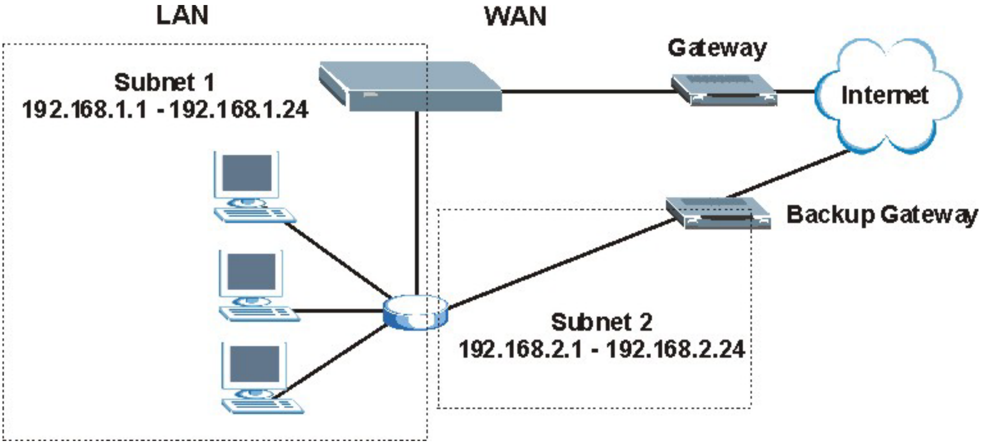
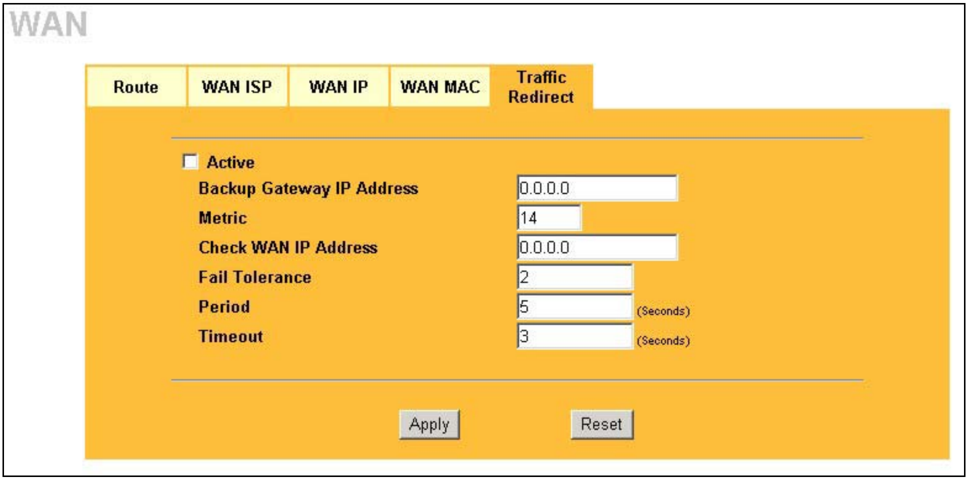


Figure 9-8 Traffic Redirect LAN Setup

9.8 Configuring Traffic Redirect

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



□ Active

Backup Gateway IP Address 0.0.0.0

Metric 14

Check WAN IP Address 0.0.0.0

Fail Tolerance 2

Period 5 (Seconds)

Timeout 3 (Seconds)

Figure 9-9 WAN: Traffic Redirect

The following table describes the labels in this screen.

Table 9-6 WAN: 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".

Table 9-6 WAN: Traffic Redirect

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

Part III:

SUA/NAT and Static Route

This part covers Network Address Translation and setting up static routes.

Chapter 10
Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Prestige.

10.1 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.

10.1.1 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 10-1 NAT Definitions

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

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

10.1.2 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)*.

10.1.3 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.

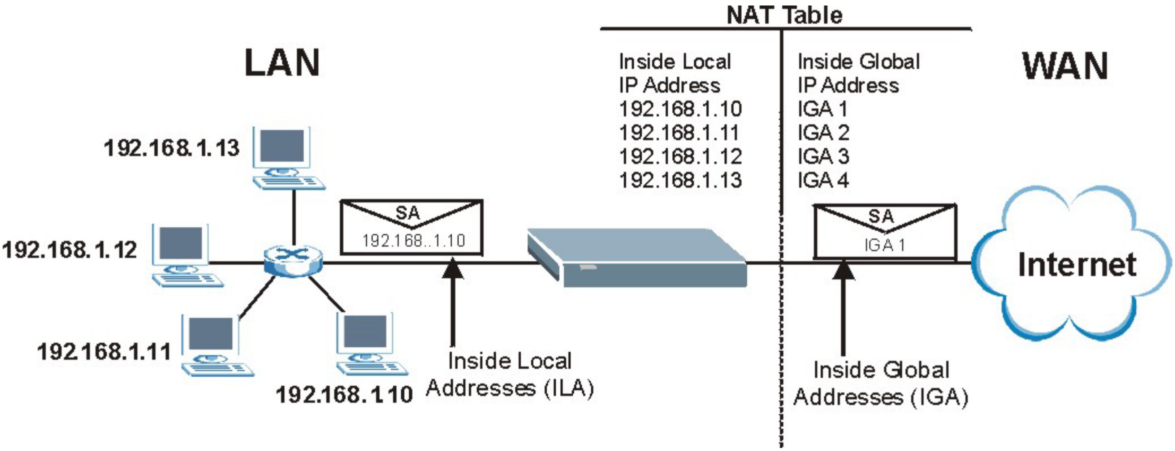


Figure 10-1 How NAT Works

10.1.4 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.

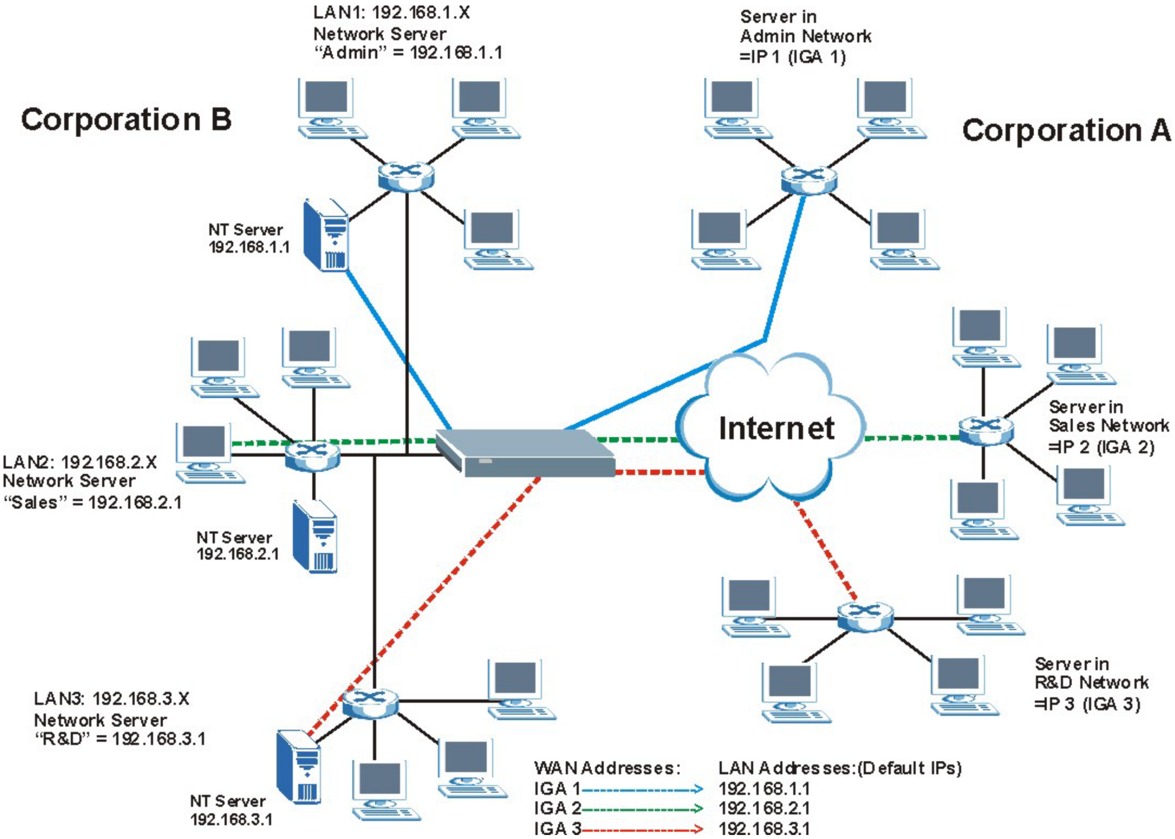


Figure 10-2 NAT Application With IP Alias

10.1.5 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.

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

The following table summarizes these types.

Table 10-2 NAT Mapping Types

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

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

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

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

10.2 Using NAT

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

10.2.1 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.

10.3 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.

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.

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.**

10.3.1 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.

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 10-3 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

10.3.2 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.

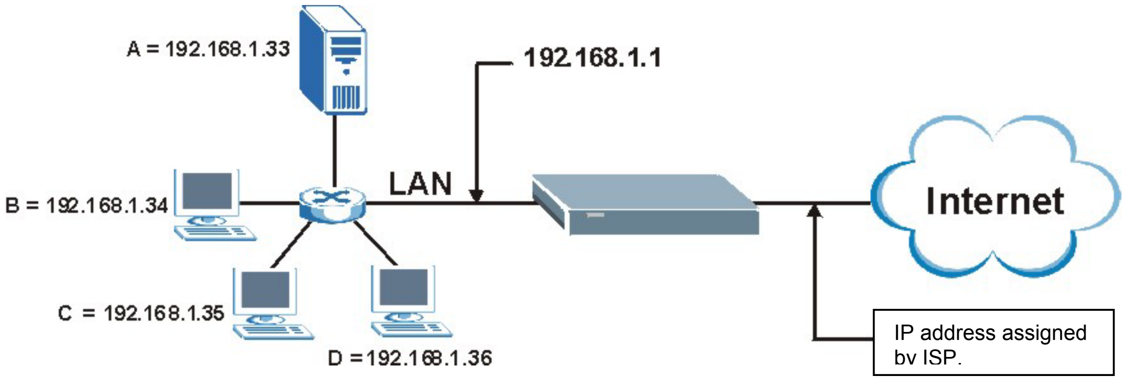


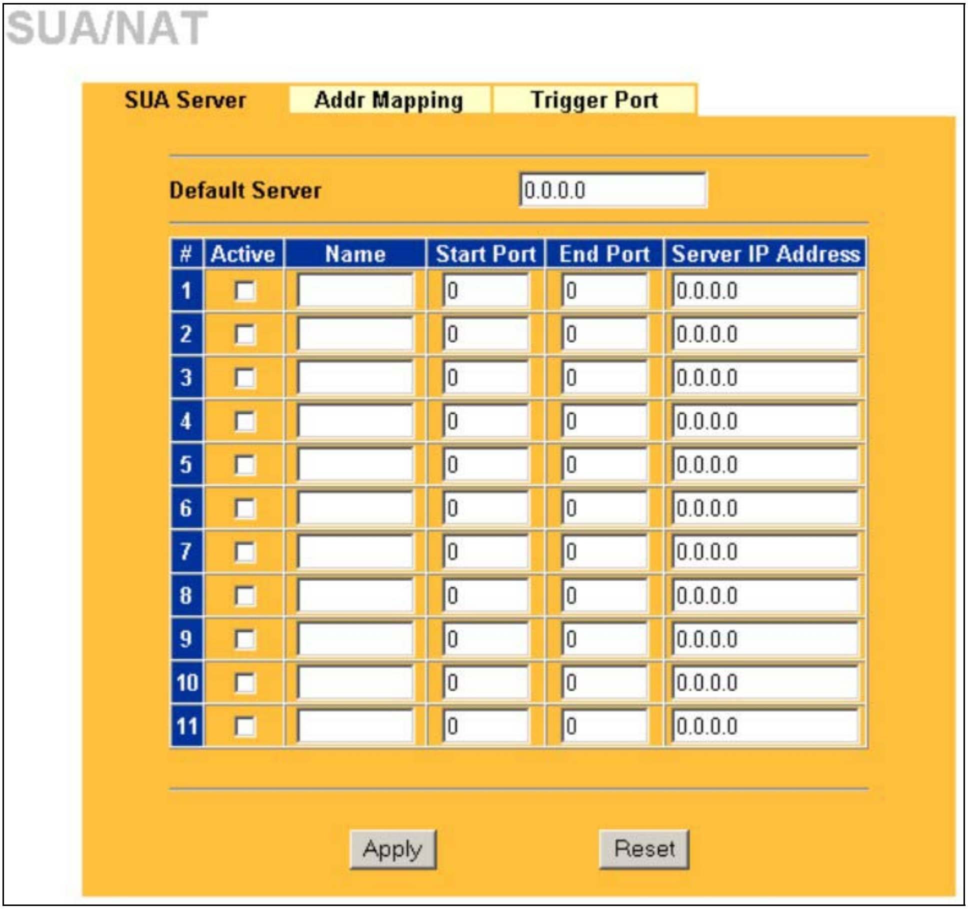
Figure 10-3 Multiple Servers Behind NAT Example

10.4 Configuring SUA Server

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 10-3* for port numbers commonly used for particular services.



Default Server 0.0.0.0

#	Active	Name	Start Port	End Port	Server IP Address
1	□		0	0	0.0.0.0
2	□		0	0	0.0.0.0
3	□		0	0	0.0.0.0
4	□		0	0	0.0.0.0
5	□		0	0	0.0.0.0
6	□		0	0	0.0.0.0
7	□		0	0	0.0.0.0
8	□		0	0	0.0.0.0
9	□		0	0	0.0.0.0
10	□		0	0	0.0.0.0
11	□		0	0	0.0.0.0

Figure 10-4 SUA/NAT Setup

The following table describes the labels in this screen.

Table 10-4 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.

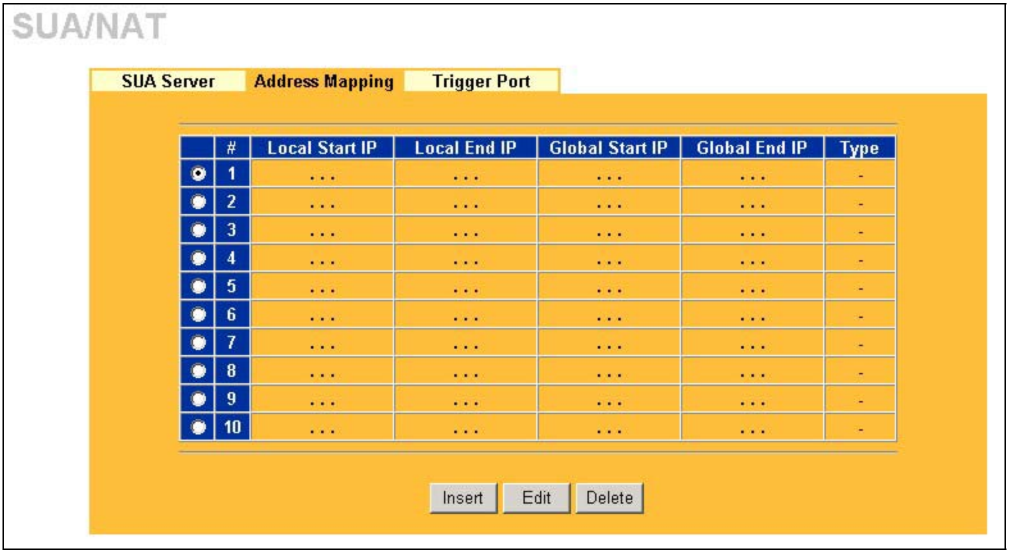
Table 10-4 SUA/NAT Setup

LABEL	DESCRIPTION
#	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.

10.5 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.



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

Figure 10-5 Address Mapping

The following table describes the labels in this screen.

Table 10-5 Address Mapping

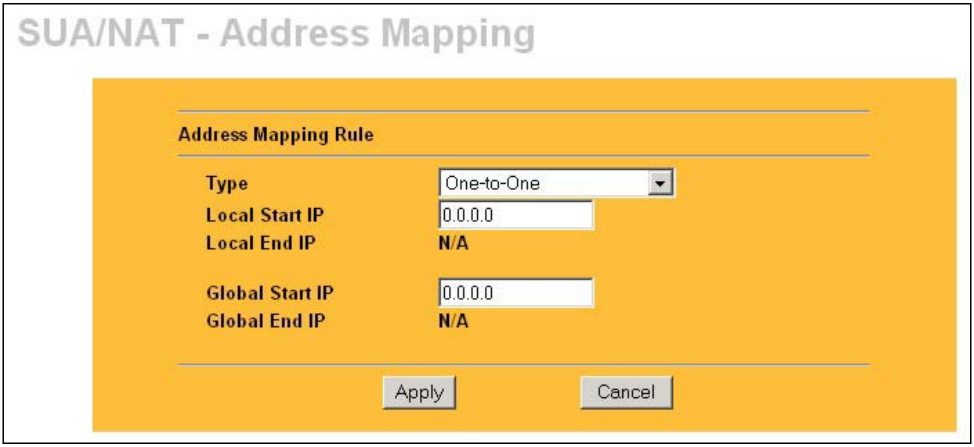
LABEL	DESCRIPTION
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address. Local IP addresses are **N/A** for **Server** port mapping.
Local End 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 10-5 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.

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.



SUA/NAT - Address Mapping

Address Mapping Rule

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

Figure 10-6 Address Mapping Edit

The following table describes the labels in this screen.

Table 10-6 Address Mapping Edit

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.

10.6 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.

10.6.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

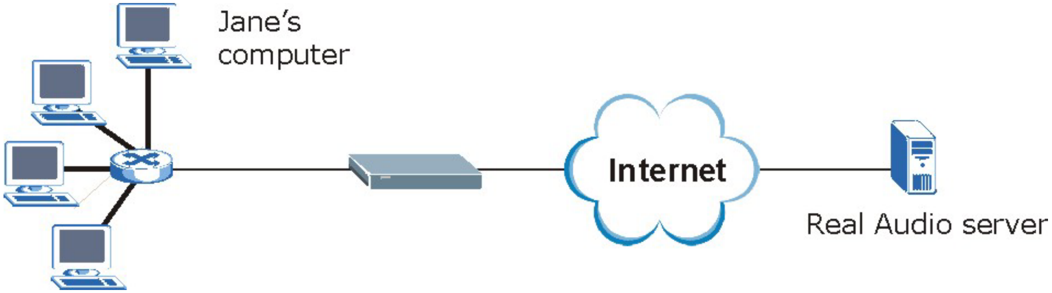


Figure 10-7 Trigger Port Forwarding Process: Example

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).

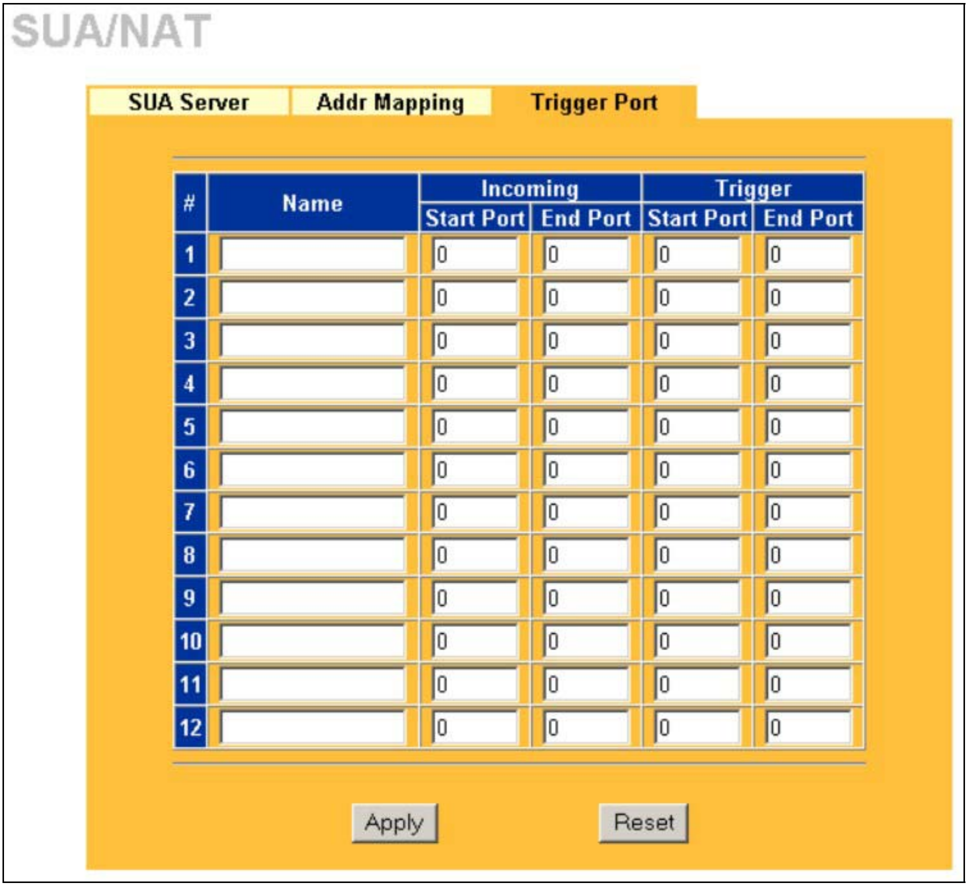
10.6.2 Two Points To Remember About Trigger Ports

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.

10.7 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.

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



#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1		0	0	0	0
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

Figure 10-8 Trigger Port

The following table describes the labels in this screen.

Table 10-7 Trigger Port

LABEL	DESCRIPTION
#	This is the rule index number (read-only).

Table 10-7 Trigger Port

LABEL	DESCRIPTION
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 11
Static Route Screens

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

11.1 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.

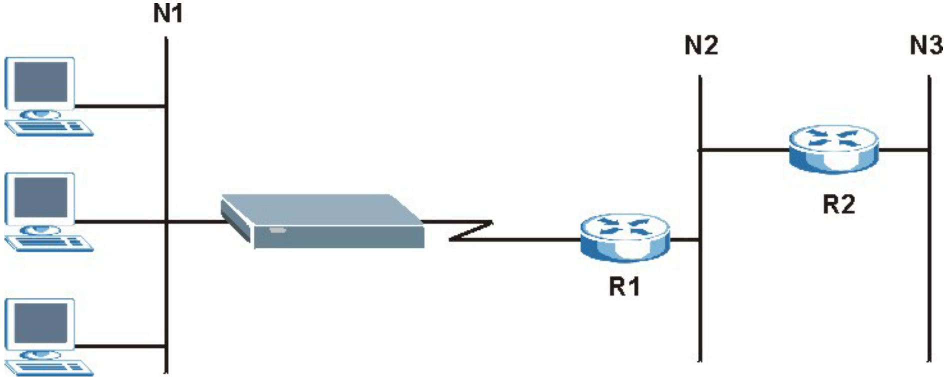
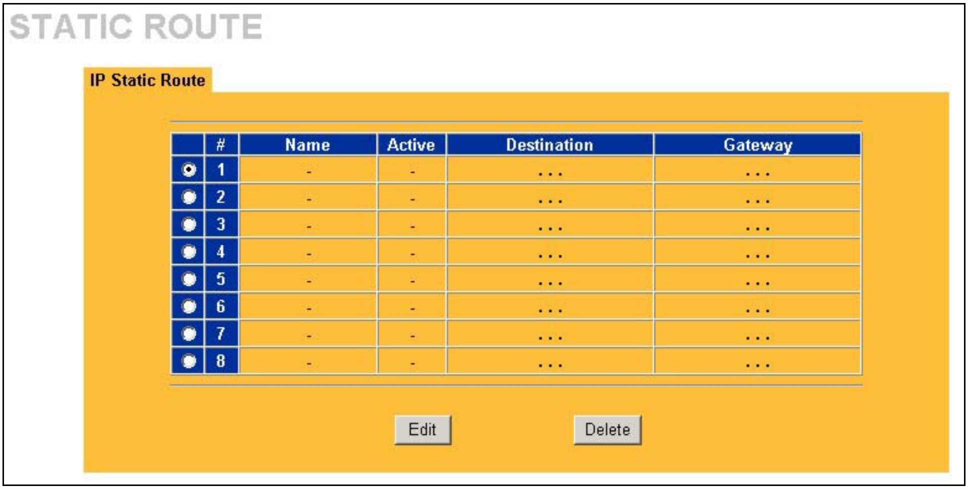


Figure 11-1 Example of Static Routing Topology

11.2 Configuring IP Static Route

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



	#	Name	Active	Destination	Gateway
●	1	-	-	. . .	. . .
○	2	-	-	. . .	. . .
○	3	-	-	. . .	. . .
○	4	-	-	. . .	. . .
○	5	-	-	. . .	. . .
○	6	-	-	. . .	. . .
○	7	-	-	. . .	. . .
○	8	-	-	. . .	. . .

Figure 11-2 Static Route

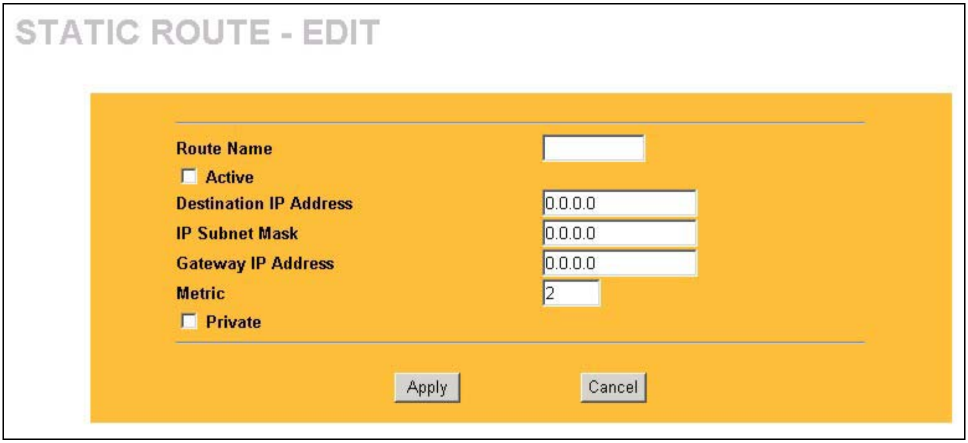
The following table describes the labels in this screen.

Table 11-1 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.

11.2.1 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.



STATIC ROUTE - EDIT

Route Name

□ Active

Destination IP Address 0.0.0.0

IP Subnet Mask 0.0.0.0

Gateway IP Address 0.0.0.0

Metric 2

□ Private

Figure 11-3 Static Route: Edit

The following table describes the labels in this screen.

Table 11-2 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.

Table 11-2 Static Route: Edit

LABEL	DESCRIPTION
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.

Part IV:

UPnP and Firewall

This part provides information and configuration instructions for configuration of Universal Plug and Play, firewall and content filtering.

Chapter 12
UPnP

This chapter introduces the Universal Plug and Play feature.

12.1 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.

12.1.1 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.

12.1.2 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:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

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

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

12.1.3 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.

12.2 UPnP and ZyXEL

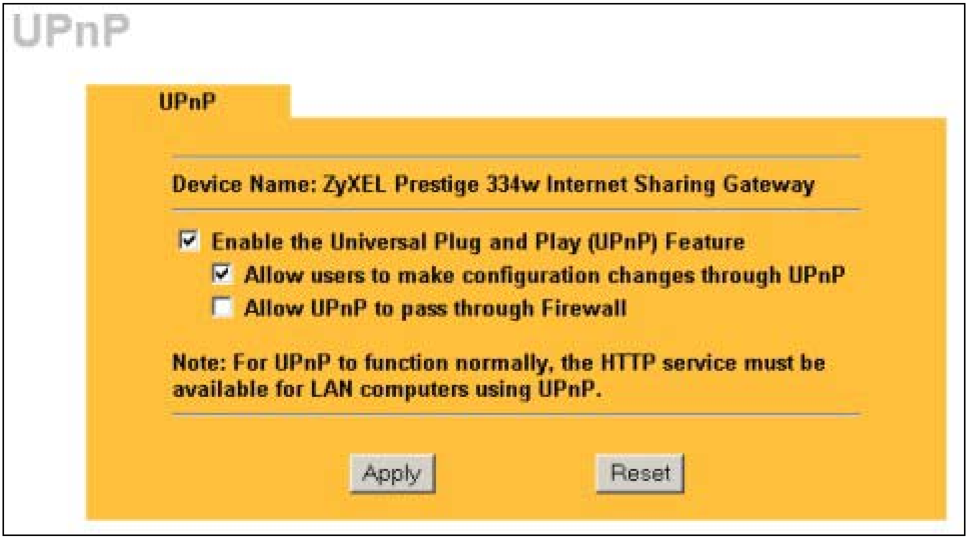
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 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.

12.3 Configuring UPnP

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



Device Name: ZyXEL Prestige 334w Internet Sharing Gateway

☑ Enable the Universal Plug and Play (UPnP) Feature

☑ Allow users to make configuration changes through UPnP

□ Allow UPnP to pass through Firewall

Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

Figure 12-1 Configuring UPnP

The following table describes the labels in this screen.

Table 12-1 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	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all 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.

12.4 Installing UPnP in Windows Example

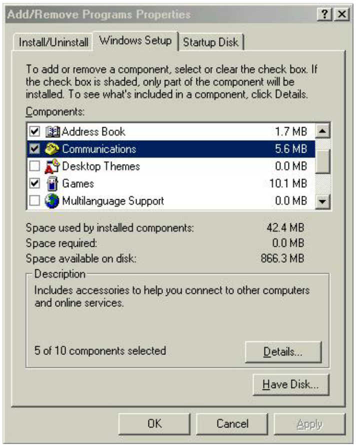
This section shows how to install UPnP in Windows Me and Windows XP.

12.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

Step 1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

Step 2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ Address Book	1.7 MB
☑ Communications	5.6 MB
□ Desktop Themes	0.0 MB
☑ Games	10.1 MB
□ Multilanguage Support	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description

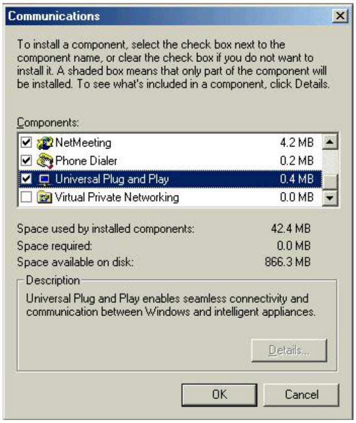
Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

Step 3. In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Step 4. Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

Step 5. Restart the computer when prompted.



To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ NetMeeting	4.2 MB
☑ Phone Dialer	0.2 MB
☑ Universal Plug and Play	0.4 MB
□ Virtual Private Networking	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

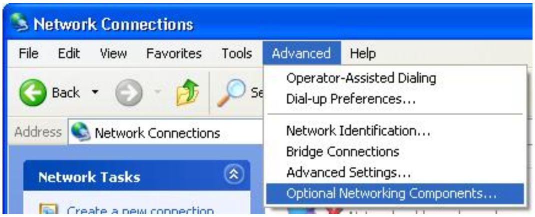
12.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

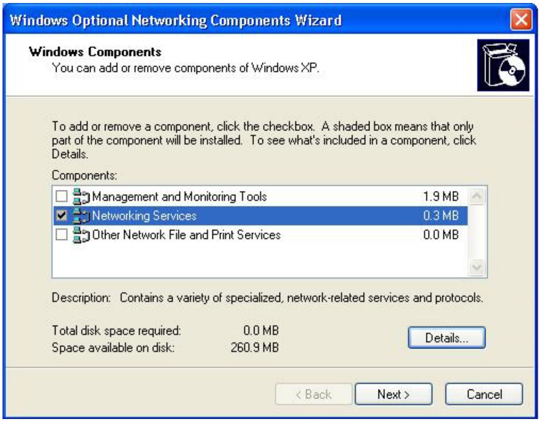
Step 1. Click **Start** and **Control Panel**.

Step 2. Double-click **Network Connections**.

Step 3. In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**
The **Windows Optional Networking Components Wizard** window displays.



Step 4. Select **Networking Service** in the **Components** selection box and click **Details**.



You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

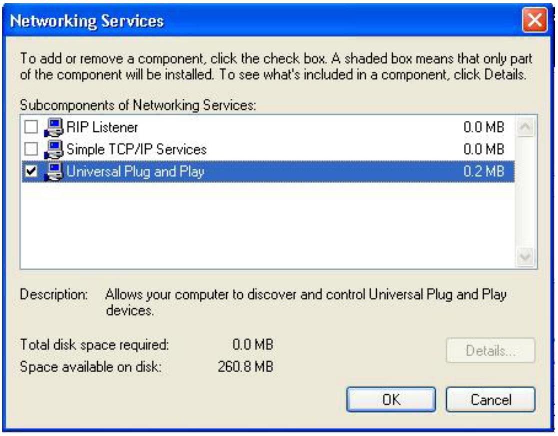
□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 260.9 MB

Step 5. In the **Networking Services** window, select the **Universal Plug and Play** check box.

Step 6. Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□	RIP Listener	0.0 MB
□	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB
Space available on disk: 260.8 MB

12.5 Using UPnP in Windows XP Example

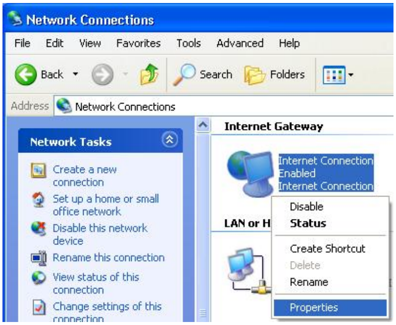
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

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

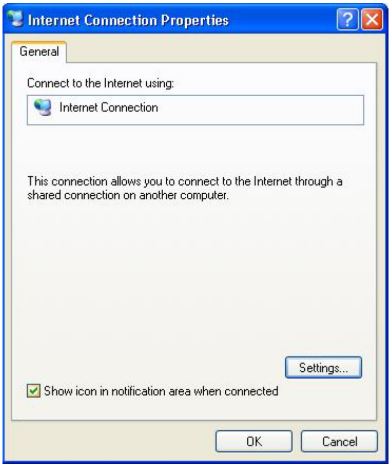
12.5.1 Auto-discover Your UPnP-enabled Network Device

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

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



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



Internet Connection Properties

General

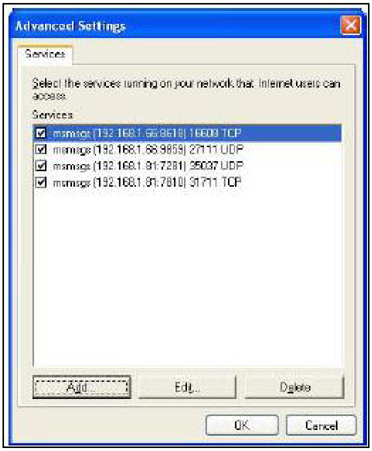
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

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



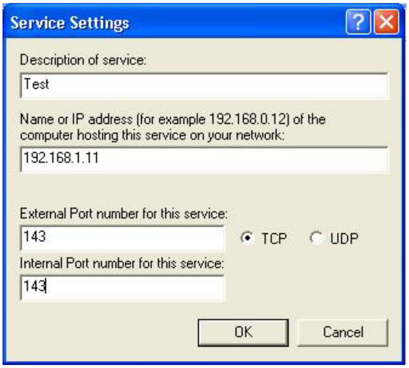
Advanced Settings

Services

Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:8618) 16608 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP



Service Settings

Description of service:
Test

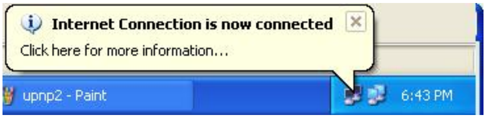
Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

External Port number for this service:
143 ● TCP ○ UDP

Internal Port number for this service:
143

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

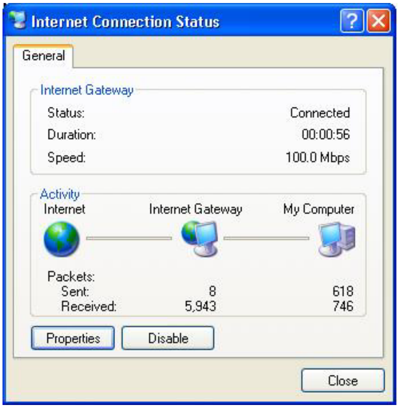
Step 5. Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray



Internet Connection is now connected

Click here for more information...

Step 6. Double-click the icon to display your current Internet connection status.



Internet Connection Status

General

Internet Gateway

Status:	Connected
Duration:	00:00:56
Speed:	100.0 Mbps

Activity

	Internet Gateway	My Computer
Packets:		
Sent:	8	618
Received:	5,943	746

12.5.2 Web Configurator Easy Access

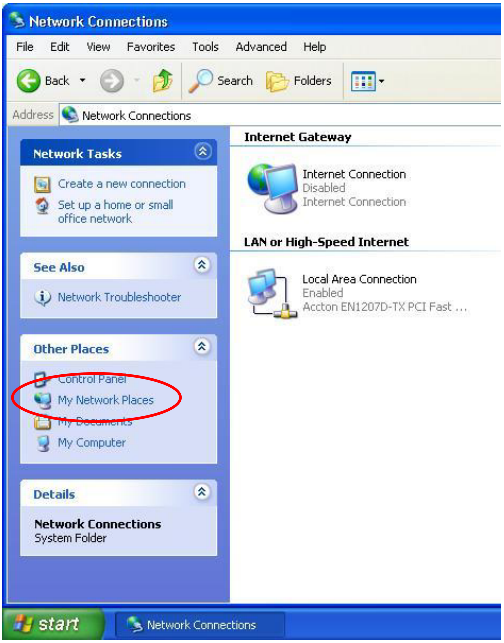
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

Step 1. Click **Start** and then **Control Panel**.

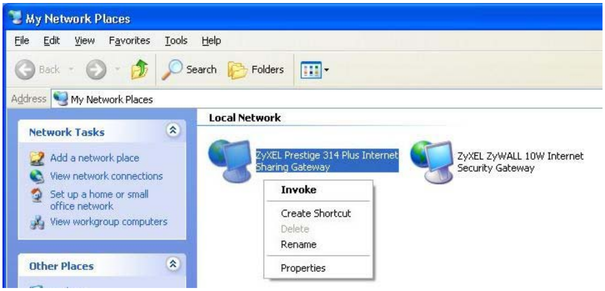
Step 2. Double-click **Network Connections**.

Step 3. Select **My Network Places** under **Other Places**.

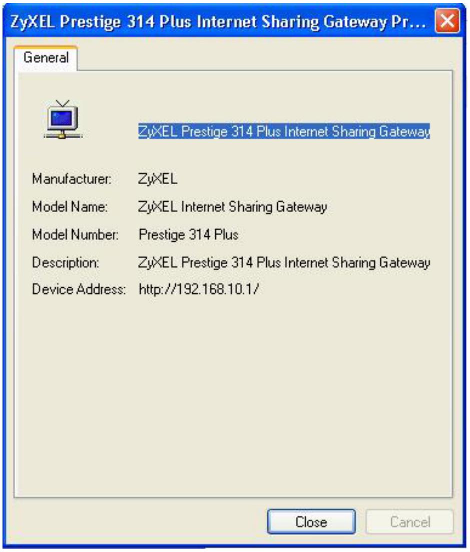


Step 4. An icon with the description for each UPnP-enabled device displays under **Local Network**.

Step 5. Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.


My Network Places
File Edit View Favorites Tools Help
Back Search Folders
Address My Network Places
Network Tasks
Add a network place
View network connections
Set up a home or small office network
View workgroup computers
Other Places
Local Network
ZyXEL Prestige 314 Plus Internet Sharing Gateway
ZyXEL ZyWALL 10W Internet Security Gateway
Invoke
Create Shortcut
Delete
Rename
Properties

Step 6. Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.



ZyXEL Prestige 314 Plus Internet Sharing Gateway Pr...

ZyXEL Prestige 314 Plus Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: Prestige 314 Plus

Description: ZyXEL Prestige 314 Plus Internet Sharing Gateway

Device Address: http://192.168.10.1/

Chapter 13
Firewall

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

13.1 Introduction

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.

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.

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.

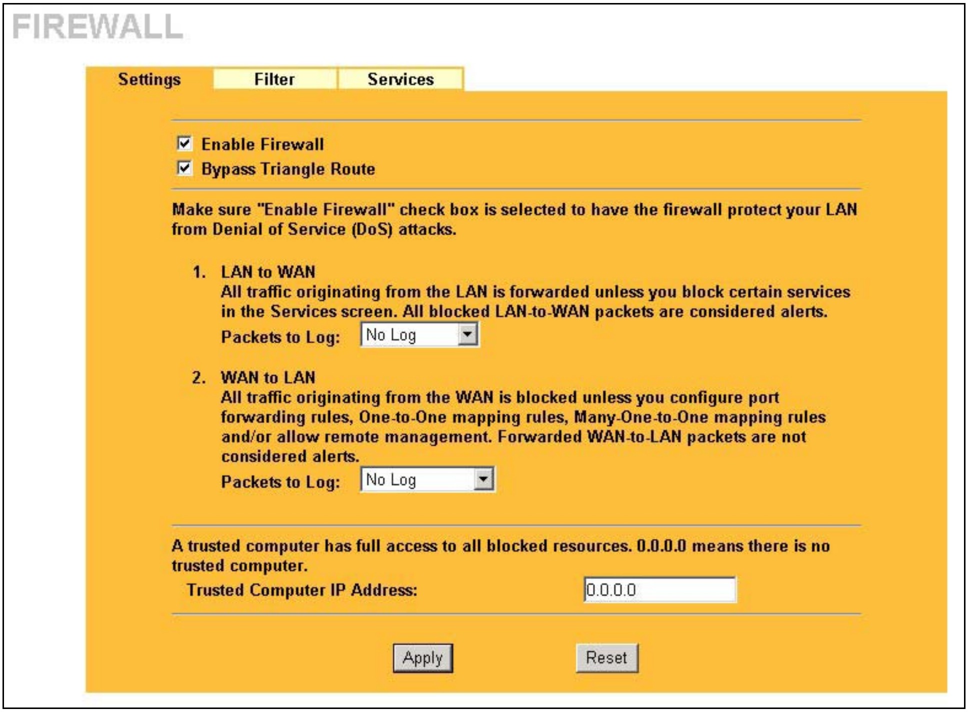
The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

13.1.1 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.



☑ Enable Firewall
☑ Bypass Triangle Route

Make sure "Enable Firewall" check box is selected to have the firewall protect your LAN from Denial of Service (DoS) attacks.

1. LAN to WAN
   All traffic originating from the LAN is forwarded unless you block certain services in the Services screen. All blocked LAN-to-WAN packets are considered alerts.
   Packets to Log: No Log
2. WAN to LAN
   All traffic originating from the WAN is blocked unless you configure port forwarding rules, One-to-One mapping rules, Many-One-to-One mapping rules and/or allow remote management. Forwarded WAN-to-LAN packets are not considered alerts.
   Packets to Log: No Log

A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.

Trusted Computer IP Address: 0.0.0.0

Figure 13-1 Firewall: Settings

The following table describes the labels in this screen.

Table 13-1 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.

Table 13-1 Firewall: Settings

LABEL	DESCRIPTION
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.
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

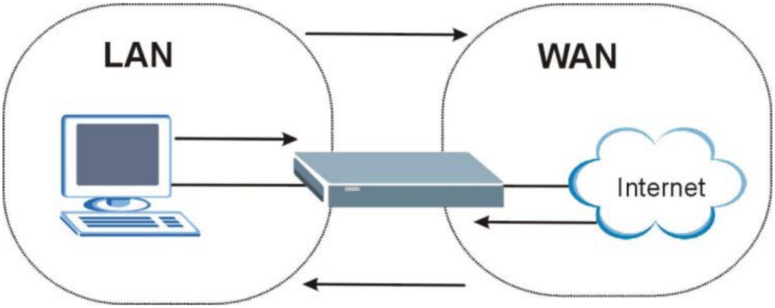


Figure 13-2 Firewall Rule Directions

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:

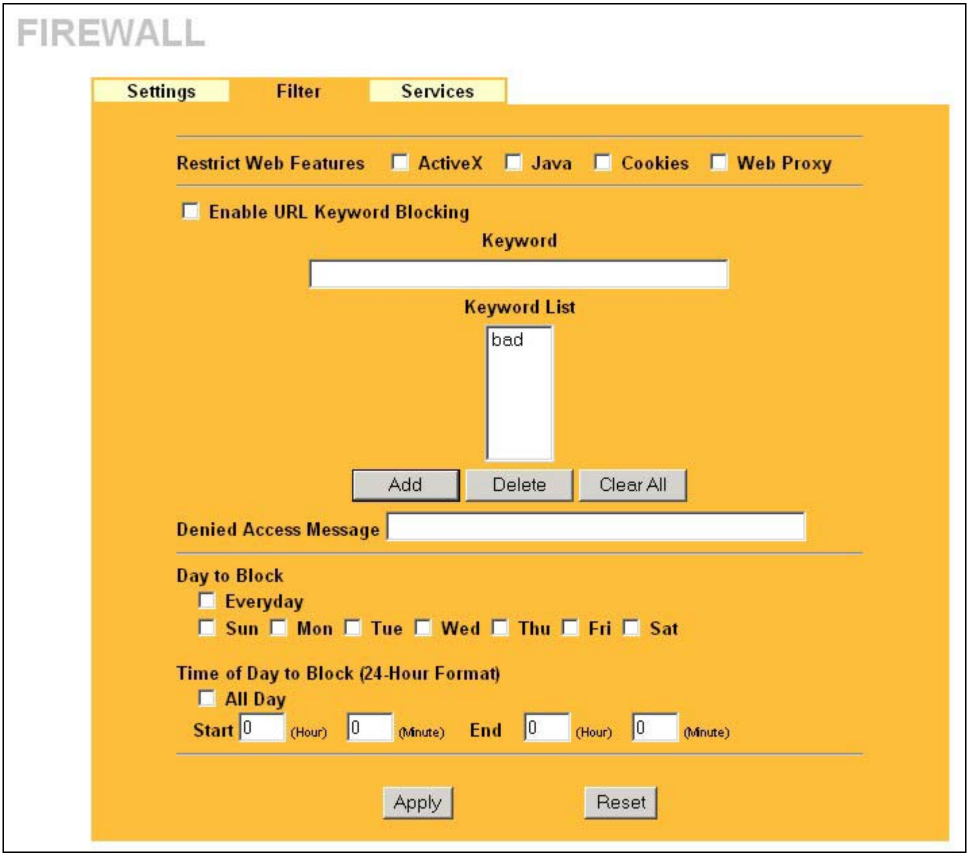
- Configuring NAT port forwarding rules in the web configurator **SUA Server** screen or SMT NAT menus.
- Configuring **One-to-One** and **Many-One-to-One** NAT mapping rules in the web configurator **Address Mapping** screen or SMT NAT menus.
- Configuring **WAN** or **LAN & WAN** access for services 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 Configuring Content Filtering

Content filtering allows you to block web sites by URL keywords that you specify, for example, you can block access to all web sites with the word "bad" in the URL by specifying "bad' as a keyword. You can also block access to web proxies and pages containing Active X components, Java applets and cookies. Finally you can schedule when the Prestige performs content filtering by day and time.

Click on the **Filter** tab. The screen appears as shown next. Use this screen to restrict web features (Active X, Java, Cookies, Web Proxy), enable URL keyword blocking, enter/delete/modify keywords you want to block and the date/time you want to block them.



Restrict Web Features □ ActiveX □ Java □ Cookies □ Web Proxy

□ Enable URL Keyword Blocking

Keyword

Keyword List
bad

Denied Access Message

Day to Block
□ Everyday
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Time of Day to Block (24-Hour Format)
□ All Day
Start 0 (Hour) 0 (Minute) End 0 (Hour) 0 (Minute)

Figure 13-3 Firewall: Filter

The following table describes the labels in this screen.

Table 13-2 Firewall: Filter

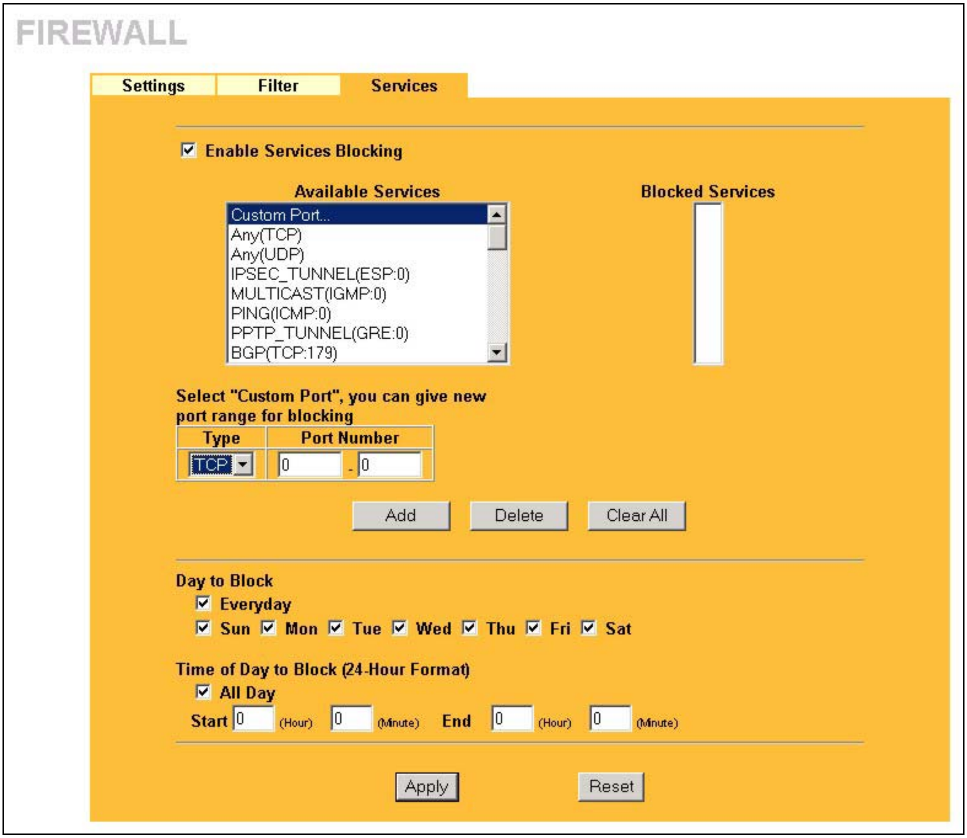
LABEL	DESCRIPTION
Restricted Web Features	
ActiveX	ActiveX is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.

Table 13-2 Firewall: Filter

LABEL	DESCRIPTION
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Web servers that track usage and provide service based on ID use cookies.
Web Proxy	This is 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	Select this option to block the URL containing the keywords in the keyword list.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.
Keyword List	This is a list of keywords that will be inaccessible to computers on your LAN once you enable URL keyword blocking.
Add	Type a keyword in the **Keyword** field and click then **Add** to add a keyword to the Keyword List.
Delete	Select a keyword from the **Keyword List** and then click **Delete** to remove this keyword from the list.
Clear All	Click **Clear All** to empty the **Keyword List**.
Denied Access Message	Enter a message to be displayed when a user tries to access a restricted web site.
Date to Block	Select everyday or the day(s) of the week to activate blocking.
Time of Day to Block	Select **All Day** or enter the start and end times in the hour-minute format to activate blocking.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

13.5 Services

Click on the **Service** 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.



FIREWALL

☑ Enable Services Blocking

Available Services

- Custom Port...
- Any(TCP)
- Any(UDP)
- IPSEC_TUNNEL(ESP:0)
- MULTICAST(IGMP:0)
- PING(ICMP:0)
- PPTP_TUNNEL(GRE:0)
- BGP(TCP:179)

Blocked Services

Select "Custom Port", you can give new port range for blocking

Type	Port Number
TCP	0 - 0

Day to Block

☑ Everyday

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Block (24-Hour Format)

☑ All Day

Start 0 (Hour) 0 (Minute) End 0 (Hour) 0 (Minute)

Figure 13-4 Firewall: Service

The following table describes the labels in this screen.

Table 13-3 Firewall: Service

ABEL	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.

Table 13-3 Firewall: Service

ABEL	DESCRIPTION
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**.
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.

Part V:

Remote Management and VPN/IPSec

This part provides information and configuration instructions for configuration of remote management and VPN/IPSec.

Chapter 14
Remote Management Screens

This chapter provides information on the Remote Management screens.

14.1 Remote Management Overview

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

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).

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. Console port
2. Telnet
3. HTTP

14.1.1 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.

14.1.2 Remote Management and NAT

When NAT is enabled:

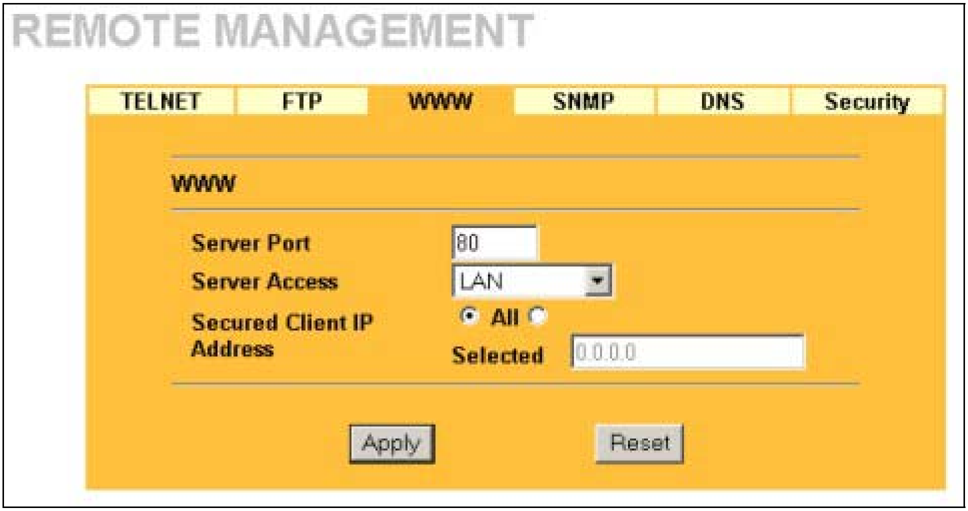
- Use the Prestige's WAN IP address when configuring from the WAN.
- Use the Prestige's LAN IP address when configuring from the LAN.

14.1.3 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

14.2 Configuring WWW

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



Server Port 80

Server Access LAN

Secured Client IP Address ● All ○ Selected 0.0.0.0

Figure 14-1 Remote Management: WWW

The following table describes the labels in this screen.

Table 14-1 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.

14.3 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.

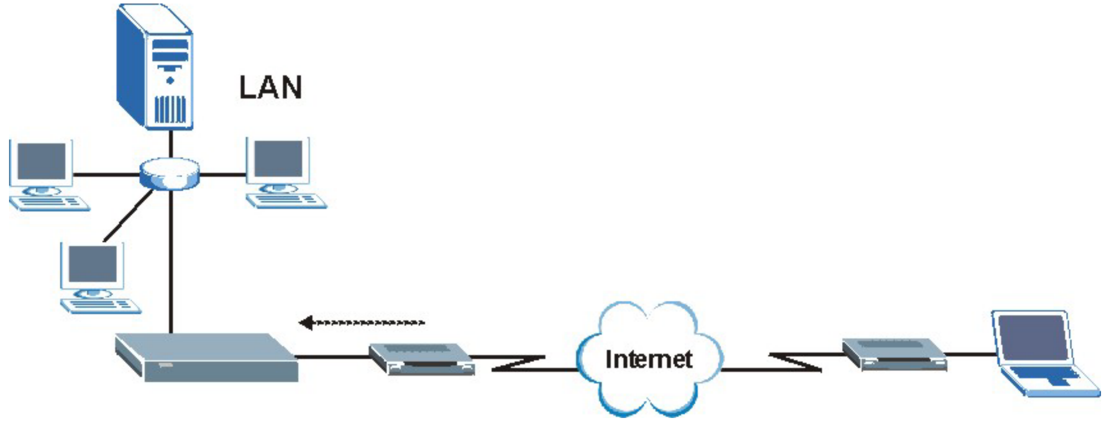
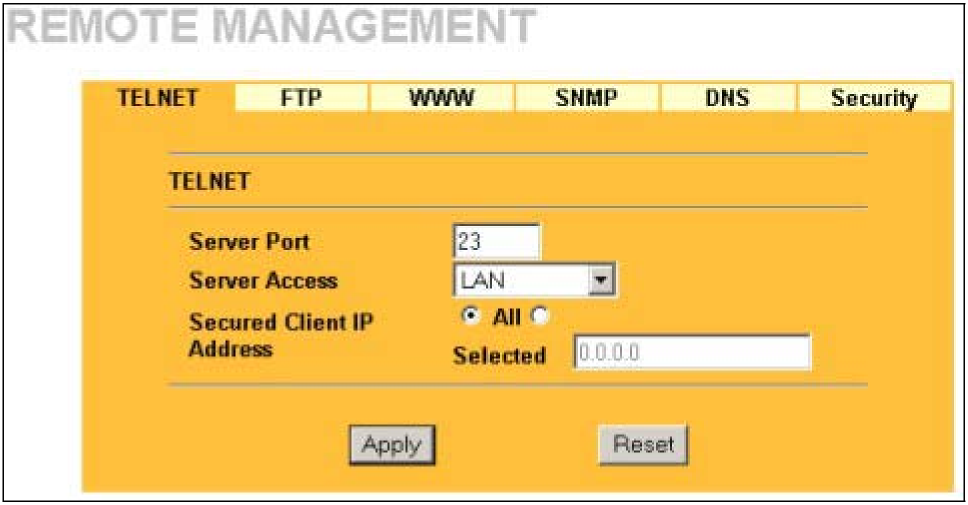


Figure 14-2 Telnet Configuration on a TCP/IP Network

14.4 Configuring TELNET

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



TELNET

Server Port: 23

Server Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Figure 14-3 Remote Management: Telnet

The following table describes the labels in this screen.

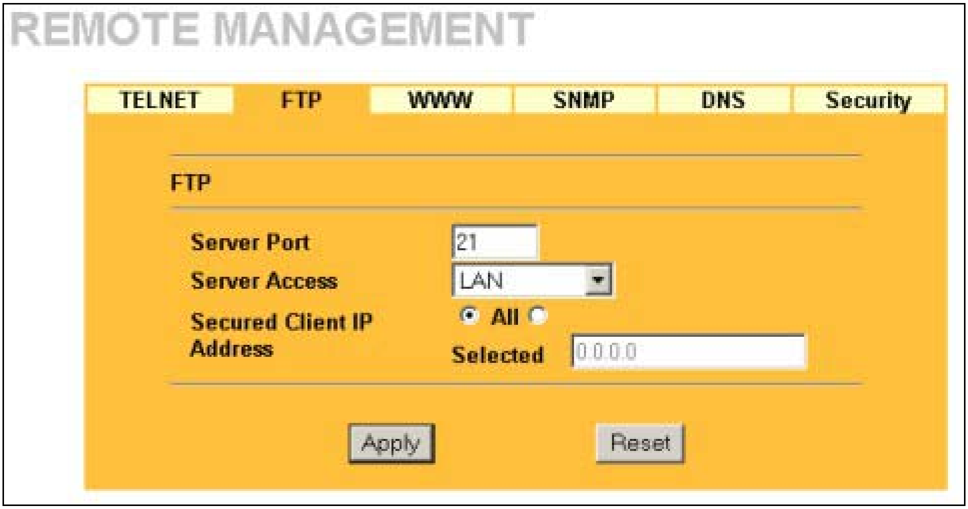
Table 14-2 Remote Management: Telnet

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

14.5 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.



Server Port 21

Server Access LAN

Secured Client IP Address ● All ○ Selected 0.0.0.0

Figure 14-4 Remote Management: FTP

The following table describes the labels in this screen.

Table 14-3 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.

Table 14-3 Remote Management: FTP

LABEL	DESCRIPTION
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.

14.6 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.

SNMP is only available if TCP/IP is configured.

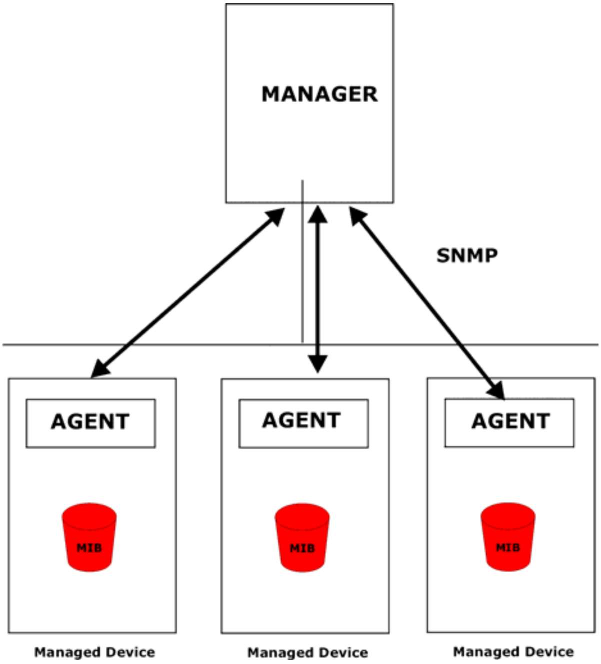


Figure 14-5 SNMP Management Model

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.

14.6.1 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.

14.6.2 SNMP Traps

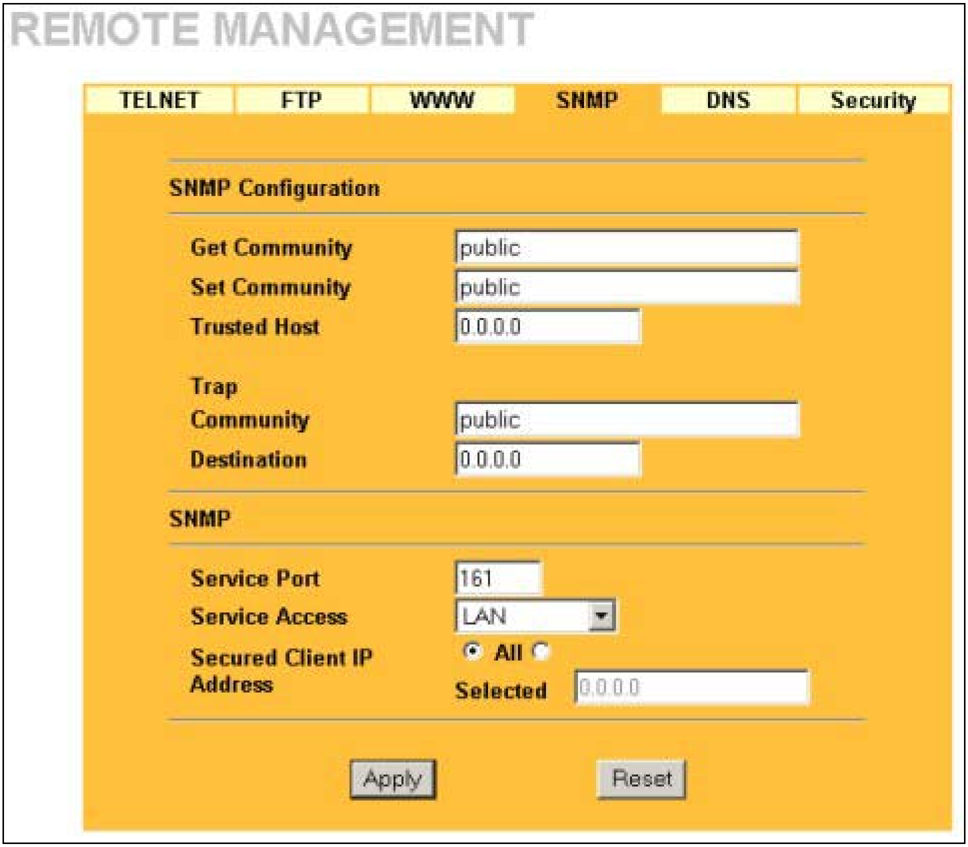
The Prestige will send traps to the SNMP manager when any one of the following events occurs:

Table 14-4 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.

14.6.3 Configuring SNMP

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



SNMP Configuration

Get Community: public

Set Community: public

Trusted Host: 0.0.0.0

Trap

Community: public

Destination: 0.0.0.0

SNMP

Service Port: 161

Service Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Figure 14-6 Remote Management: SNMP

The following table describes the labels in this screen.

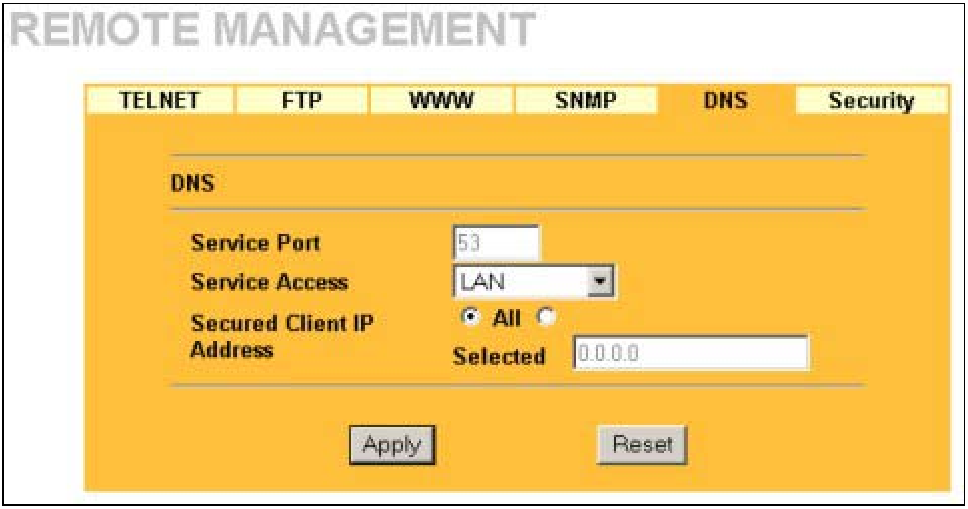
Table 14-5 Remote Management: SNMP

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

14.7 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.



REMOTE MANAGEMENT

DNS

Service Port: 53

Service Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Figure 14-7 Remote Management: DNS

The following table describes the labels in this screen.

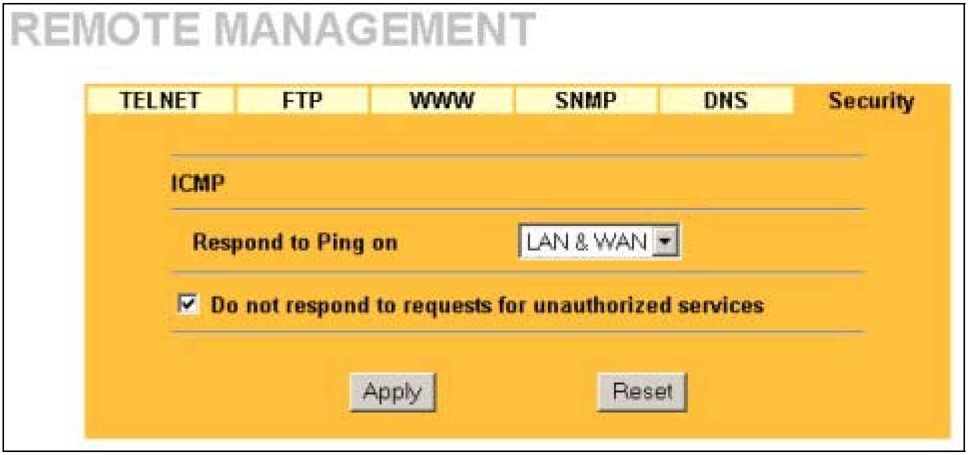
Table 14-6 Remote Management: DNS

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.

14.8 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.



Respond to Ping on: LAN & WAN

☑ Do not respond to requests for unauthorized services

Figure 14-8 Security

The following table describes the labels in this screen.

Table 14-7 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.

Table 14-7 Security

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

Chapter 15
Introduction to IPSec

This chapter introduces the basics of IPSec VPNs

15.1 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.

15.1.1 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.

15.1.2 Security Association

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

15.1.3 Other Terminology

- **Encryption**

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

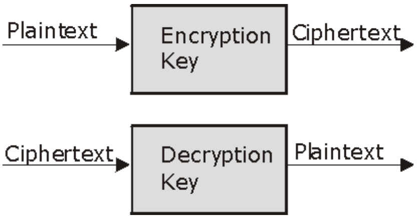


Figure 15-1 Encryption and Decryption

- **Data Confidentiality**

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

- **Data Integrity**

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

- **Data Origin Authentication**

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

15.1.4 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.

15.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

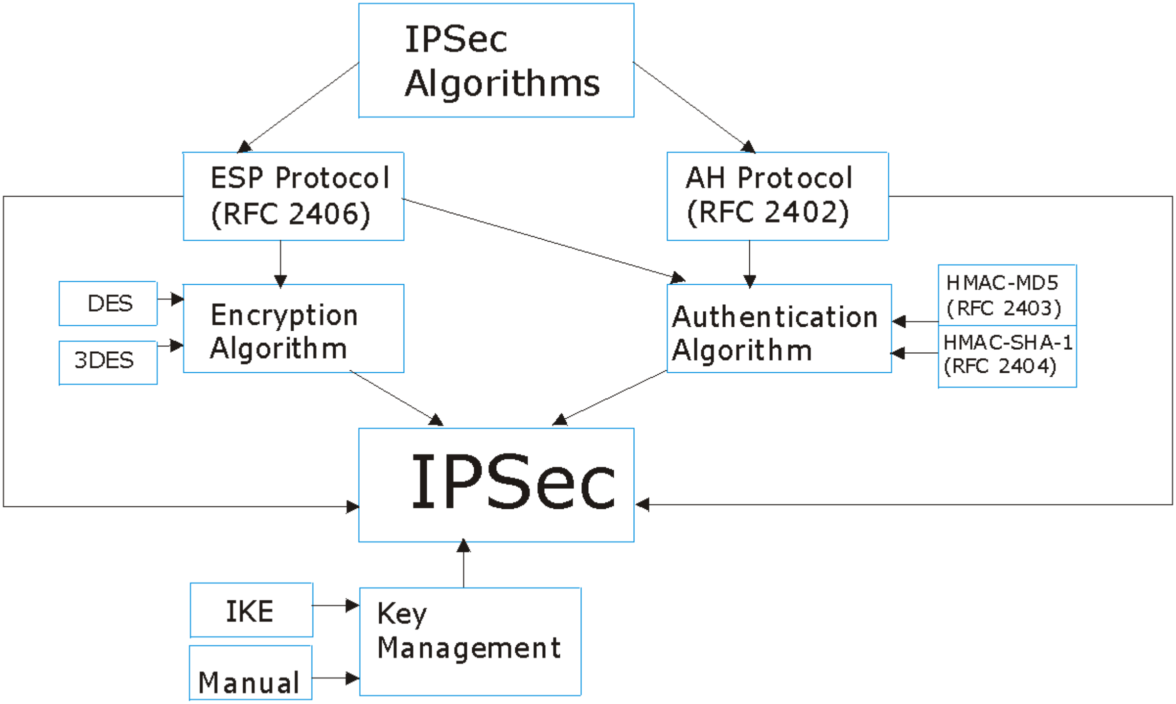


Figure 15-2 IPSec Architecture

15.2.1 IPSec Algorithms

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

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

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Please see *Section 16.2* for more information.

15.2.2 Key Management

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

15.3 Encapsulation

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

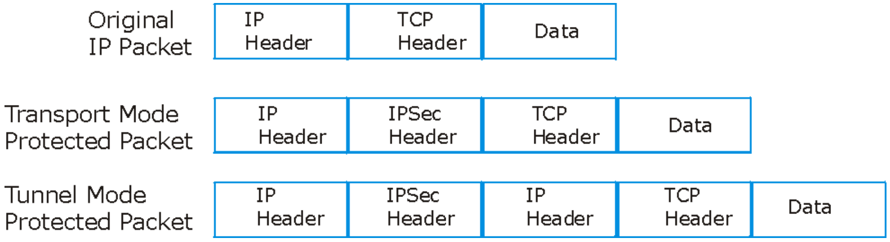


Figure 15-3 Transport and Tunnel Mode IPSec Encapsulation

15.3.1 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.

15.3.2 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.

15.4 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 (see *section 16.7* for details).

Table 15-1 VPN and NAT

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

Chapter 16
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.

16.1 VPN/IPSec Overview

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

16.2 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.

16.2.1 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.

16.2.2 ESP (Encapsulating Security Payload) Protocol

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

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

Table 16-1 AH and ESP

ESP	AH
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.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
Select **DES** for minimal security and **3DES** for maximum.	Select **MD5** for minimal security and **SHA-1** for maximum security.

16.3 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.

16.4 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).

16.4.1 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. See *section 16.17* for configuration examples.

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

16.5 Summary Screen

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

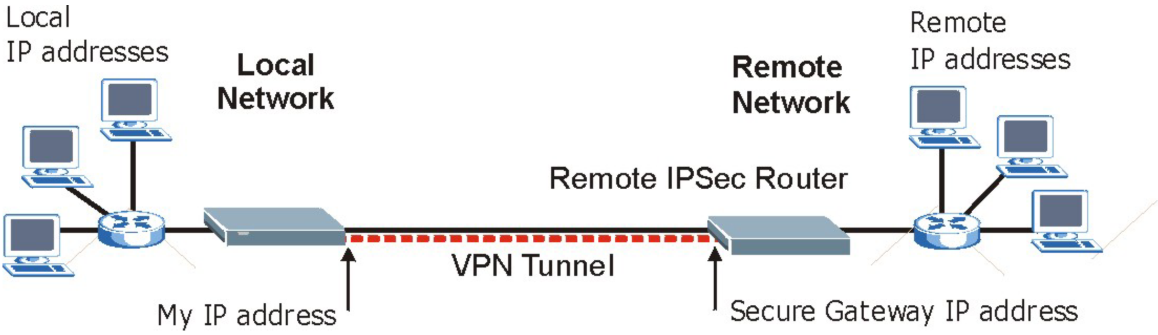
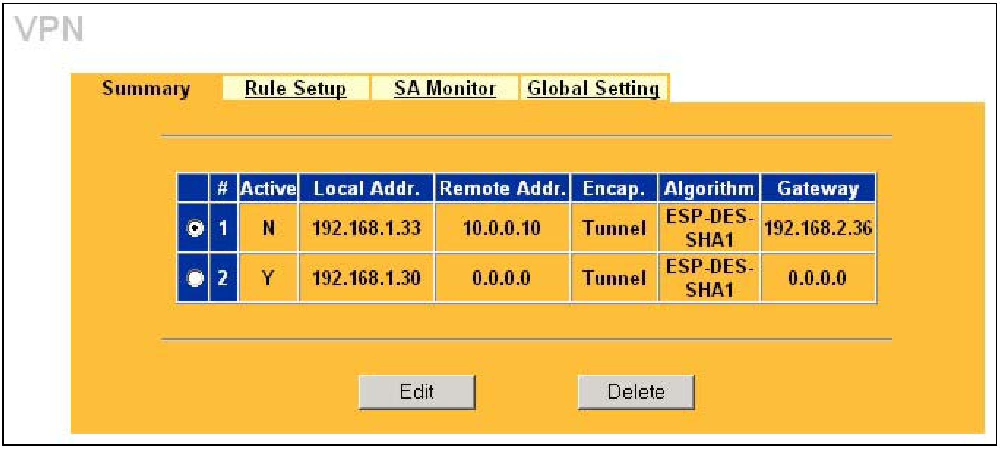


Figure 16-1 IPSec Summary Fields

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.



	#	Active	Local Addr.	Remote Addr.	Encap.	Algorithm	Gateway
●	1	N	192.168.1.33	10.0.0.10	Tunnel	ESP-DES-SHA1	192.168.2.36
○	2	Y	192.168.1.30	0.0.0.0	Tunnel	ESP-DES-SHA1	0.0.0.0

Figure 16-2 VPN: Summary

The following table describes the labels in this screen.

Table 16-2 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.

Table 16-2 VPN: Summary

LABEL	DESCRIPTION
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.	

16.6 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 (see *Section 16.11* 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.

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

16.7 NAT Traversal

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

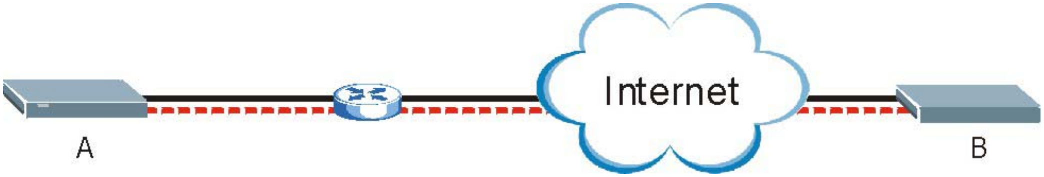


Figure 16-3 NAT Router Between IPSec Routers

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.

16.7.1 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.

16.7.2 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.

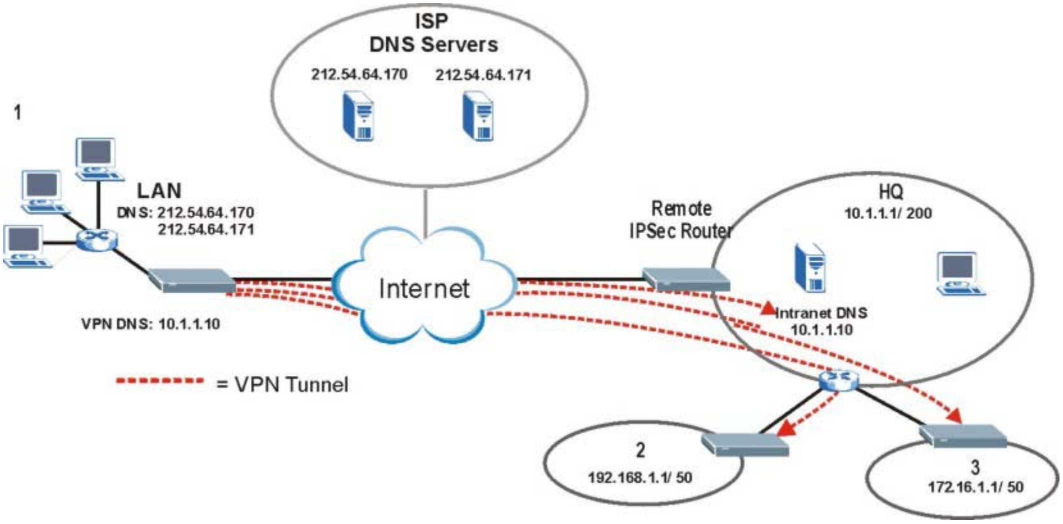


Figure 16-4 VPN Host using Intranet DNS Server Example

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.

16.8 ID Type and Content

With aggressive negotiation mode (see *Section 16.11.1*), 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 *Section 16.17.2* for a telecommuter configuration example).

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 16.11.1*), 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 (see *Section 16.12*). 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 16-3 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 16-4 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.
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.	

16.8.1 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 16-5 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.

Table 16-6 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

Table 16-6 Mismatching ID Type and Content Configuration Example

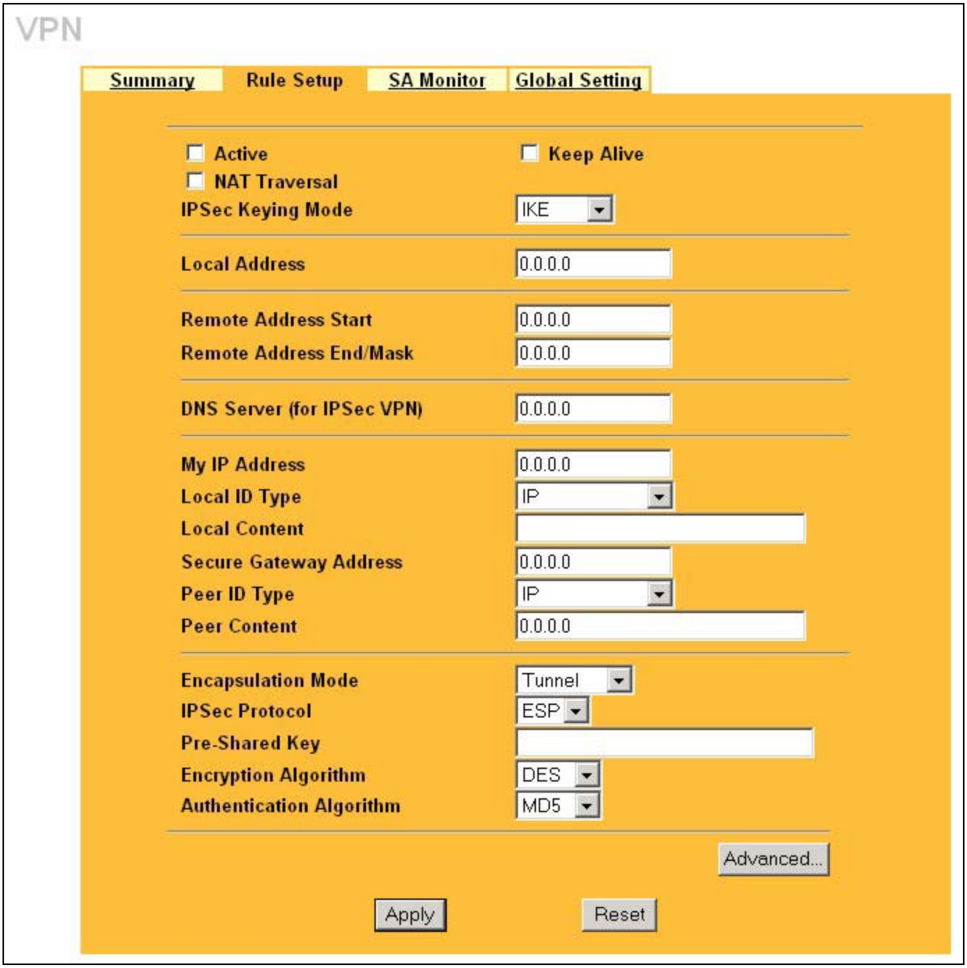
PRESTIGE A	PRESTIGE B
Peer ID content: aa@yahoo.com	Peer ID content: N/A

16.9 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see *Section 16.11* 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.

16.10 Editing VPN Rules

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



☐ Active
☐ Keep Alive
☐ NAT Traversal

IPSec Keying Mode	IKE
Local Address	0.0.0.0
Remote Address Start	0.0.0.0
Remote Address End/Mask	0.0.0.0
DNS Server (for IPSec VPN)	0.0.0.0
My IP Address	0.0.0.0
Local ID Type	IP
Local Content	
Secure Gateway Address	0.0.0.0
Peer ID Type	IP
Peer Content	0.0.0.0
Encapsulation Mode	Tunnel
IPSec Protocol	ESP
Pre-Shared Key	
Encryption Algorithm	DES
Authentication Algorithm	MD5

Figure 16-5 VPN: Rule Setup (Basic)

The following table describes the labels in this screen.

Table 16-7 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.
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.

Table 16-7 VPN: Rule Setup (Basic)

LABEL	DESCRIPTION
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 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.

Table 16-7 VPN: Rule Setup (Basic)

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.
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 16-7 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.

16.11 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.

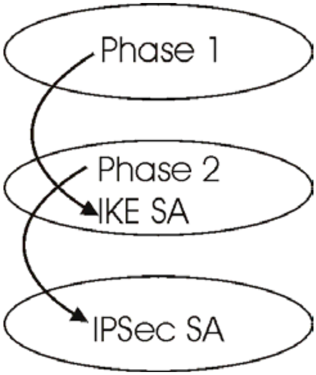


Figure 16-6 Two Phases to Set Up the IPSec SA

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 16.11.3*. 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.

16.11.1 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.

16.11.2 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.

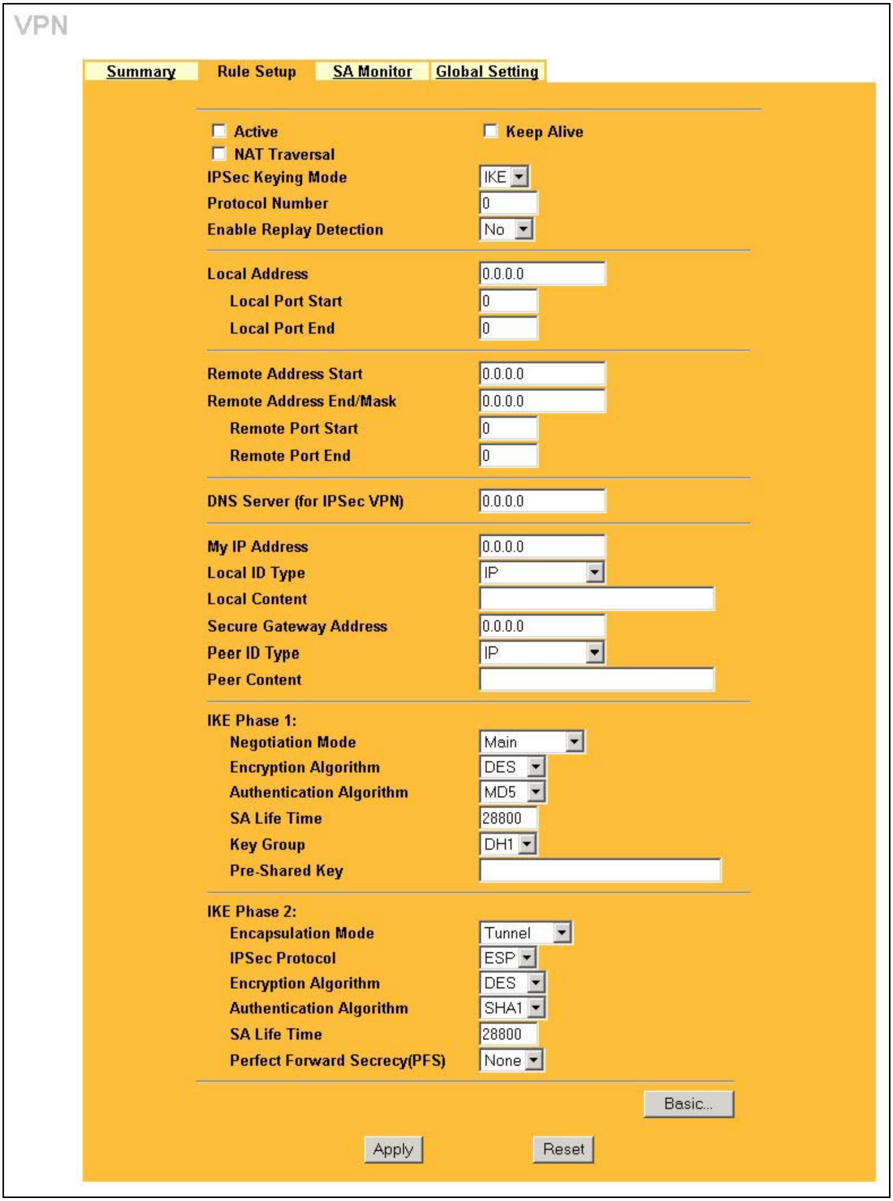
16.11.3 Perfect Forward Secrecy (PFS)

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).

16.12 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.



□ Active	□ Keep Alive
□ NAT Traversal	
IPSec Keying Mode	IKE
Protocol Number	0
Enable Replay Detection	No
Local Address	0.0.0.0
Local Port Start	0
Local Port End	0
Remote Address Start	0.0.0.0
Remote Address End/Mask	0.0.0.0
Remote Port Start	0
Remote Port End	0
DNS Server (for IPSec VPN)	0.0.0.0
My IP Address	0.0.0.0
Local ID Type	IP
Local Content	
Secure Gateway Address	0.0.0.0
Peer ID Type	IP
Peer Content	
IKE Phase 1:	
Negotiation Mode	Main
Encryption Algorithm	DES
Authentication Algorithm	MD5
SA Life Time	28800
Key Group	DH1
Pre-Shared Key	
IKE Phase 2:	
Encapsulation Mode	Tunnel
IPSec Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA Life Time	28800
Perfect Forward Secrecy(PFS)	None

Figure 16-7 VPN IKE: Advanced

The following table describes the labels in this screen.

Table 16-8 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

Table 16-8 VPN IKE: Advanced

LABEL	DESCRIPTION
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.
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.

Table 16-8 VPN IKE: Advanced

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 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 16-8 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.

Table 16-8 VPN IKE: Advanced

LABEL	DESCRIPTION
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.
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.

Table 16-8 VPN IKE: Advanced

LABEL	DESCRIPTION
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.

16.13 Manual Key Setup

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

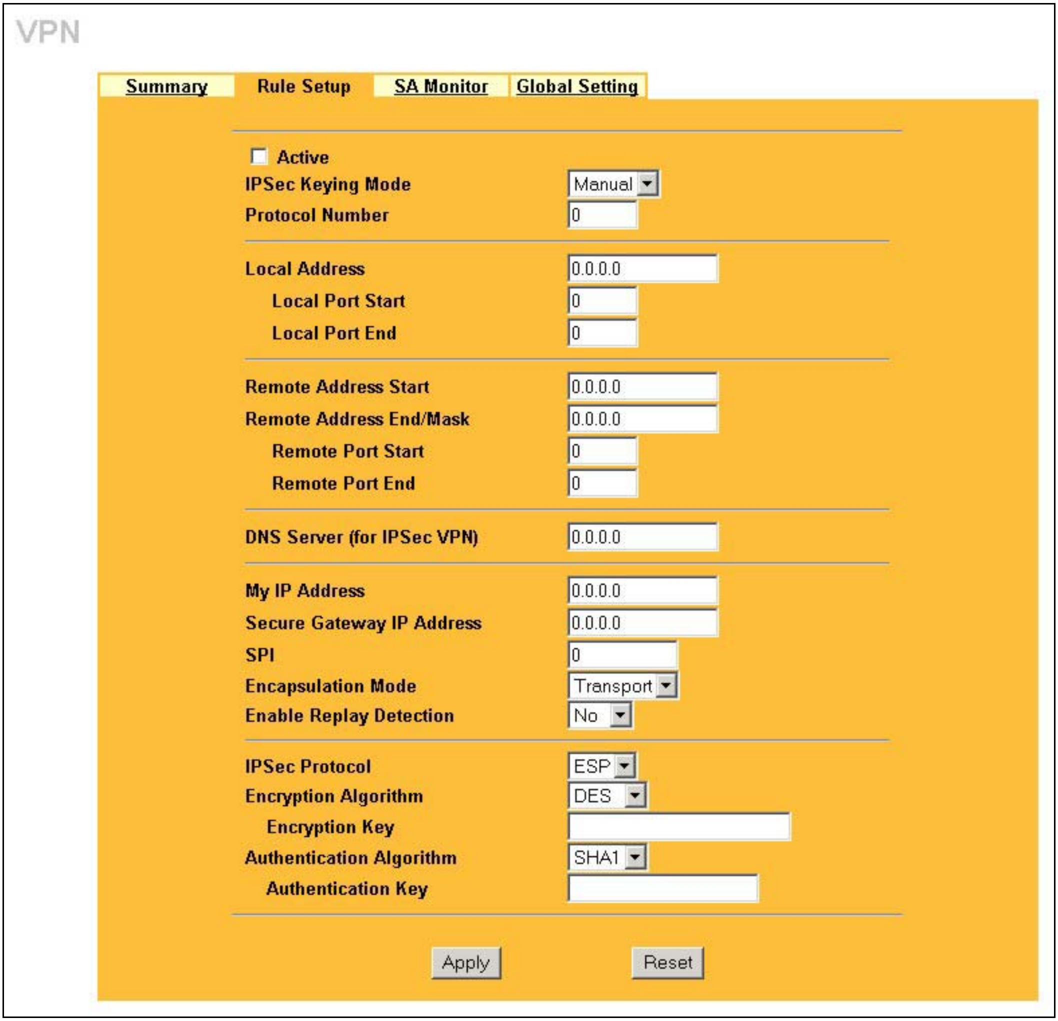
16.13.1 Security Parameter Index (SPI)

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.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

16.14 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.



VPN

☐ Active

IPSec Keying Mode	Manual
Protocol Number	0
Local Address	0.0.0.0
Local Port Start	0
Local Port End	0
Remote Address Start	0.0.0.0
Remote Address End/Mask	0.0.0.0
Remote Port Start	0
Remote Port End	0
DNS Server (for IPSec VPN)	0.0.0.0
My IP Address	0.0.0.0
Secure Gateway IP Address	0.0.0.0
SPI	0
Encapsulation Mode	Transport
Enable Replay Detection	No
IPSec Protocol	ESP
Encryption Algorithm	DES
Encryption Key	
Authentication Algorithm	SHA1
Authentication Key	

Figure 16-8 Rule Setup: Manual

The following table describes the labels in this screen.

Table 16-9 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.
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.

Table 16-9 Rule Setup: Manual

LABEL	DESCRIPTION
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.
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.

Table 16-9 Rule Setup: Manual

LABEL	DESCRIPTION
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.

16.15Viewing 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.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See *section 16.6* on keep alive to have the Prestige renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

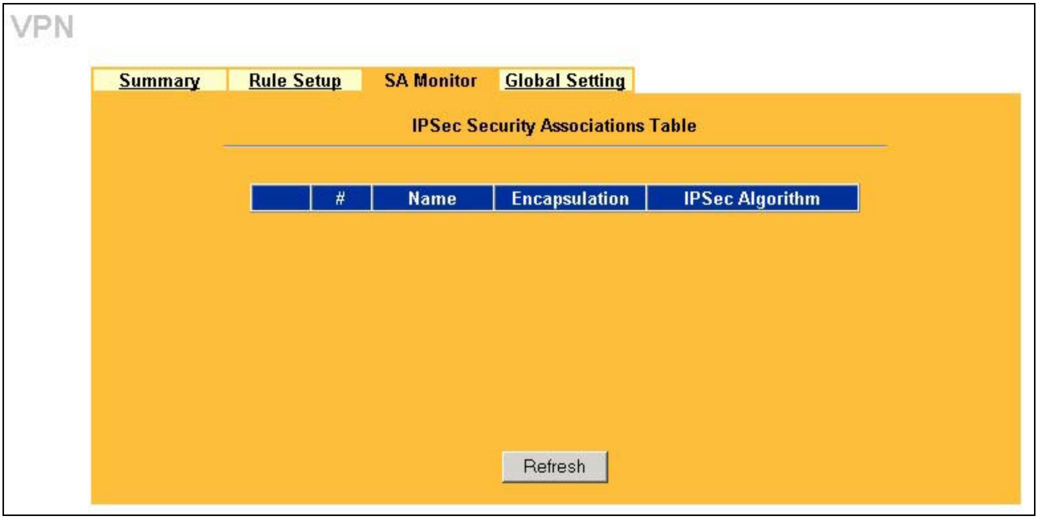


Figure 16-9 SA Monitor

The following table describes the labels in this screen.

Table 16-10 SA Monitor

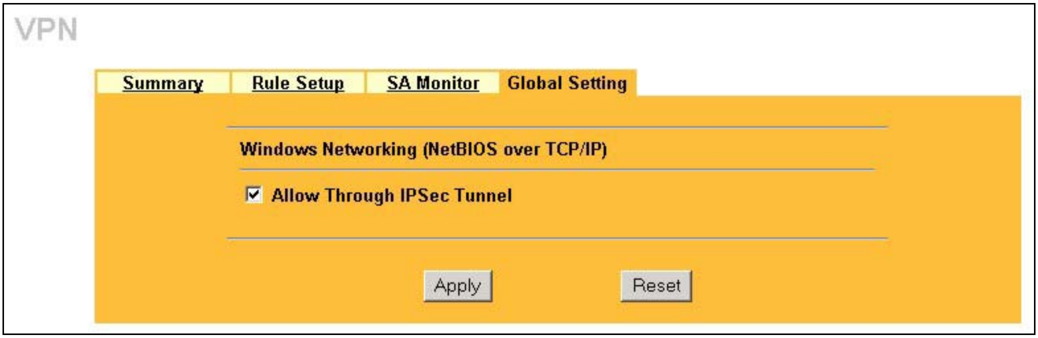
LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays Tunnel or Transport mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase Prestige processing requirements and communications latency (delay).

Table 16-10 SA Monitor

LABEL	DESCRIPTION
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.

16.16 Configuring Global Setting

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



Windows Networking (NetBIOS over TCP/IP)

☑ Allow Through IPSec Tunnel

Figure 16-10 VPN: Global Setting

The following table describes the labels in this screen.

Table 16-11 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.

Table 16-11 VPN: Global Setting

LABEL	DESCRIPTION
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.

16.17 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.

16.17.1 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 *section 16.17.2* for an example).

Table 16-12 Telecommuter and Headquarters Configuration Example

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

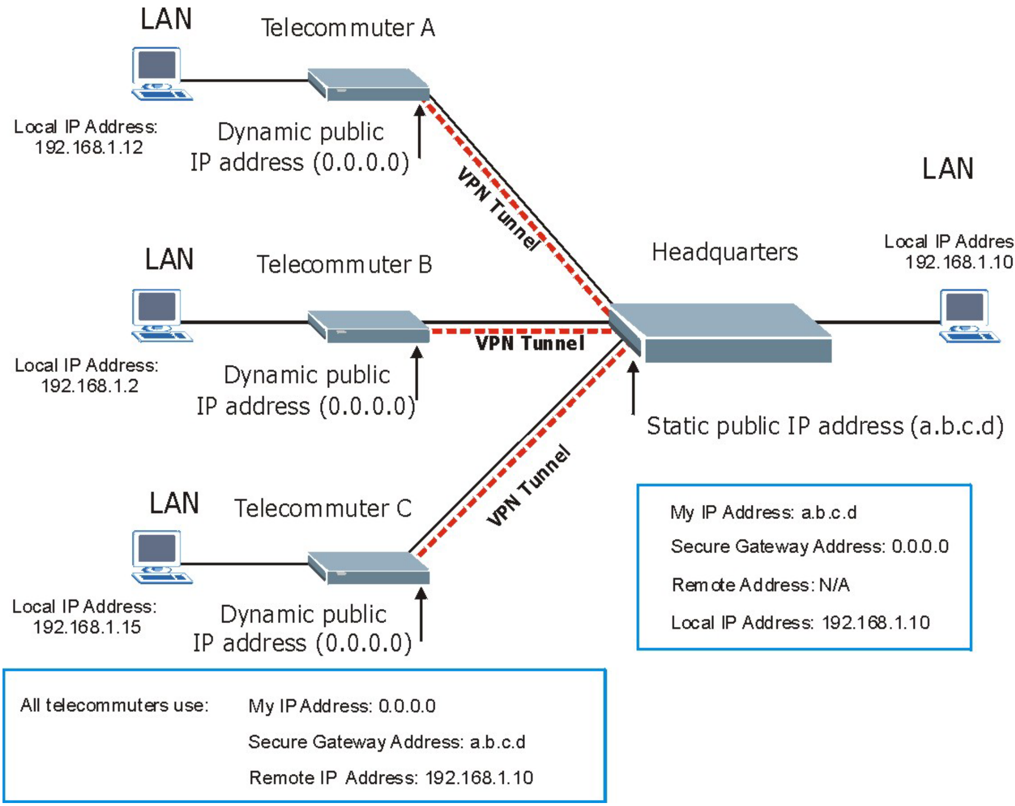
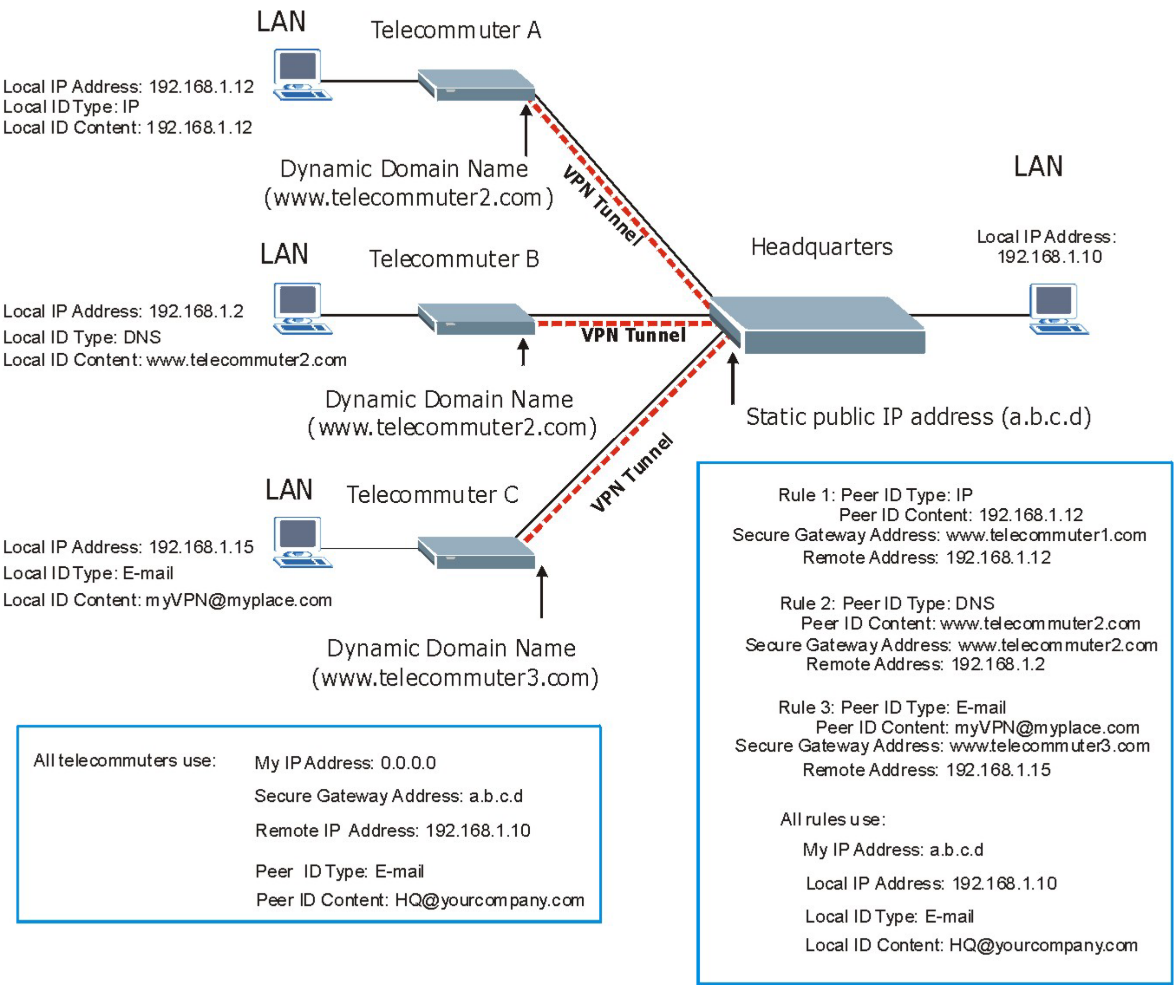

LAN
Telecommuter A
Local IP Address: 192.168.1.12
Dynamic public IP address (0.0.0.0)
VPN Tunnel
LAN
Telecommuter B
Local IP Address: 192.168.1.2
Dynamic public IP address (0.0.0.0)
VPN Tunnel
LAN
Telecommuter C
Local IP Address: 192.168.1.15
Dynamic public IP address (0.0.0.0)
VPN Tunnel
Headquarters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

Figure 16-11 Telecommuters Sharing One VPN Rule Example

16.17.2 Telecommuters Using Unique VPN Rules Example

With aggressive negotiation mode (see *section 16.11.1*), 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.



Local IP Address: 192.168.1.12
Local ID Type: IP
Local ID Content: 192.168.1.12

Local IP Address: 192.168.1.2
Local ID Type: DNS
Local ID Content: www.telecommuter2.com

Local IP Address: 192.168.1.15
Local ID Type: E-mail
Local ID Content: myVPN@myplace.com

Local IP Address:
192.168.1.10

All telecommuters use:
My IP Address: 0.0.0.0
Secure Gateway Address: a.b.c.d
Remote IP Address: 192.168.1.10
Peer ID Type: E-mail
Peer ID Content: HQ@yourcompany.com

Rule 1: Peer ID Type: IP
Peer ID Content: 192.168.1.12
Secure Gateway Address: www.telecommuter1.com
Remote Address: 192.168.1.12

Rule 2: Peer ID Type: DNS
Peer ID Content: www.telecommuter2.com
Secure Gateway Address: www.telecommuter2.com
Remote Address: 192.168.1.2

Rule 3: Peer ID Type: E-mail
Peer ID Content: myVPN@myplace.com
Secure Gateway Address: www.telecommuter3.com
Remote Address: 192.168.1.15

All rules use:
My IP Address: a.b.c.d
Local IP Address: 192.168.1.10
Local ID Type: E-mail
Local ID Content: HQ@yourcompany.com

Figure 16-12 Telecommuters Using Unique VPN Rules Example

16.18 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**.

Part VI:

Logs, Media Bandwidth Management and Maintenance

This part covers the centralized logs, media bandwidth management and maintenance screens.

Chapter 17
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.

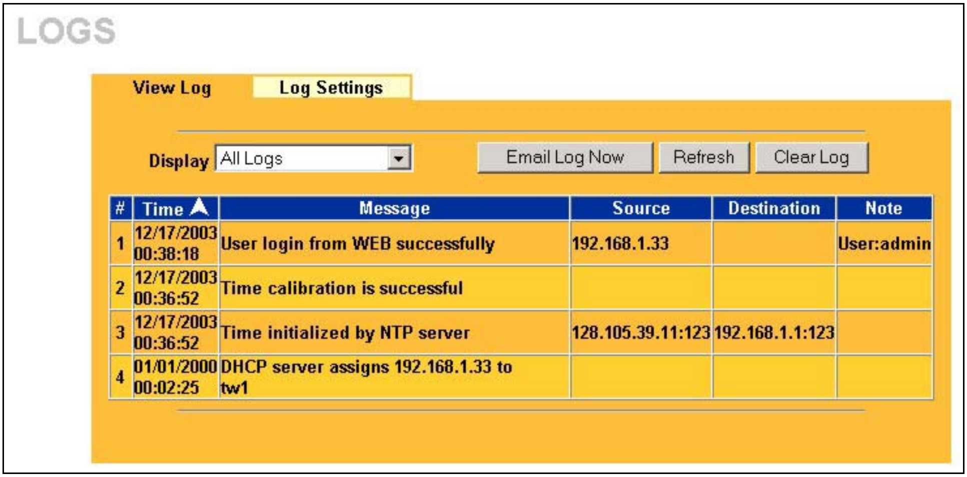
17.1 View Log

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 *section 17.2*). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

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



#	Time ▲	Message	Source	Destination	Note
1	12/17/2003 00:38:18	User login from WEB successfully	192.168.1.33		User:admin
2	12/17/2003 00:36:52	Time calibration is successful			
3	12/17/2003 00:36:52	Time initialized by NTP server	128.105.39.11:123	192.168.1.1:123	
4	01/01/2000 00:02:25	DHCP server assigns 192.168.1.33 to tw1			

Figure 17-1 View Logs

The following table describes the labels in this screen.

Table 17-1 View Logs

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see *section 17.2*) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the 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.
Note	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**, see *section 17.2*).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

17.2 Log Settings

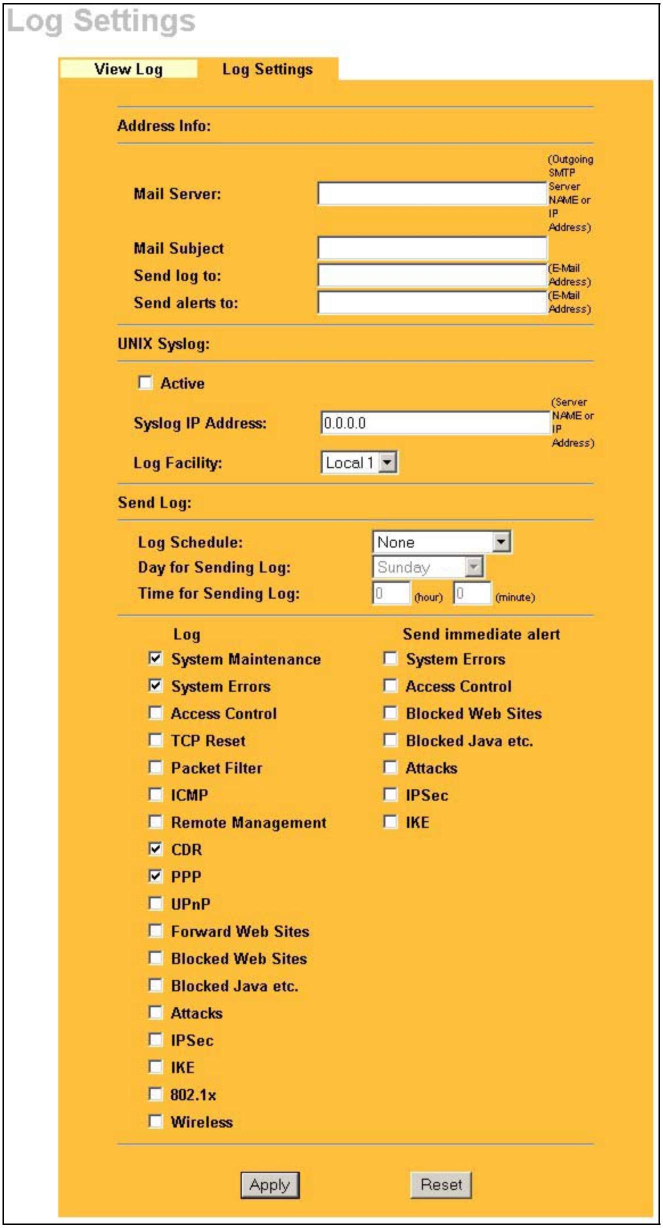
You can configure the Prestige's general log settings in one location.

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



Log Settings

View Log | Log Settings

Address Info:

Mail Server: ______ (Outgoing SMTP Server NAME or IP Address)

Mail Subject ______

Send log to: ______ (E-Mail Address)

Send alerts to: ______ (E-Mail Address)

UNIX Syslog:

□ Active

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

Log Facility: Local 1

Send Log:

Log Schedule: None

Day for Sending Log: Sunday

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

Log	Send immediate alert
☑ System Maintenance	□ System Errors
☑ System Errors	□ Access Control
□ Access Control	□ Blocked Web Sites
□ TCP Reset	□ Blocked Java etc.
□ Packet Filter	□ Attacks
□ ICMP	□ IPSec
□ Remote Management	□ IKE
☑ CDR	
☑ PPP	
□ UPnP	
□ Forward Web Sites	
□ Blocked Web Sites	
□ Blocked Java etc.	
□ Attacks	
□ IPSec	
□ IKE	
□ 802.1x	
□ Wireless	

Figure 17-2 Log Settings

The following table describes the labels in this screen.

Table 17-2 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	

Table 17-2 log Settings

LABEL	DESCRIPTION
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • **Daily** • **Weekly** • **Hourly** • **When Log is Full** • **None.** If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select 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 18 Media Bandwidth Management

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

18.1 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).

18.1.1 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.

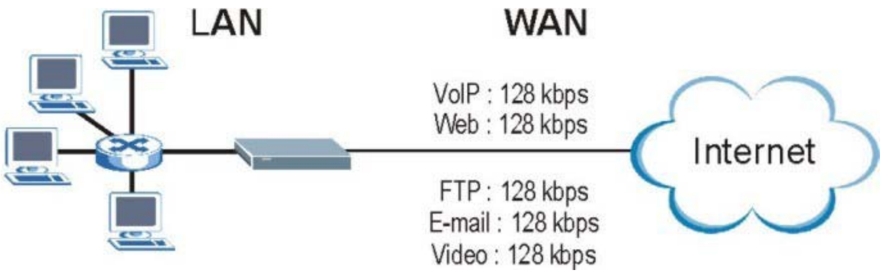


Figure 18-1 Application-based Bandwidth Management Example

18.1.2 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.

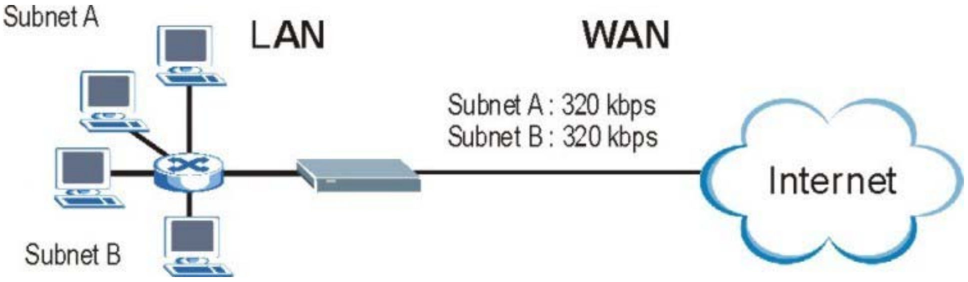


Figure 18-2 Subnet-based Bandwidth Management Example

18.1.3 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).

Table 18-1 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

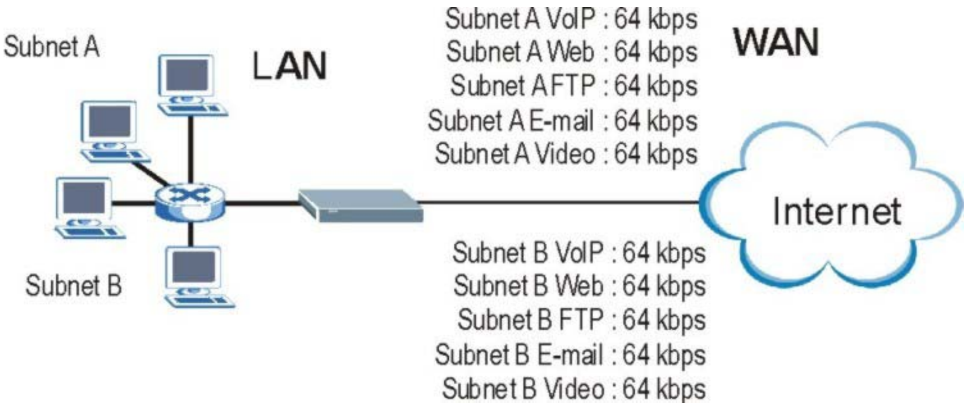


Figure 18-3 Application and Subnet-based Bandwidth Management Example

18.1.4 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 not defined to go out when you do not select the **Use All Managed Bandwidth** option.

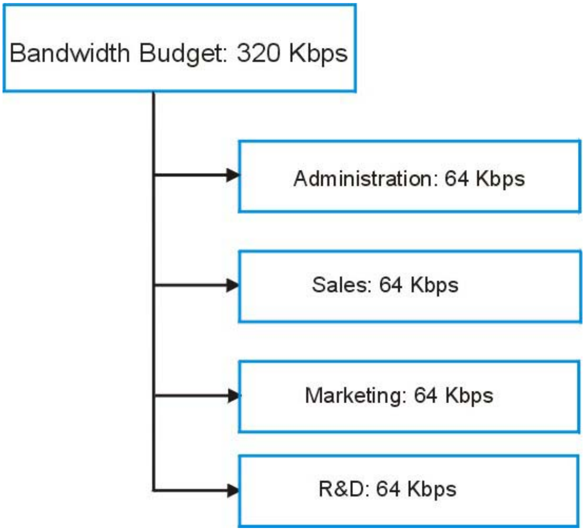


Figure 18-4 Bandwidth Usage Example

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.

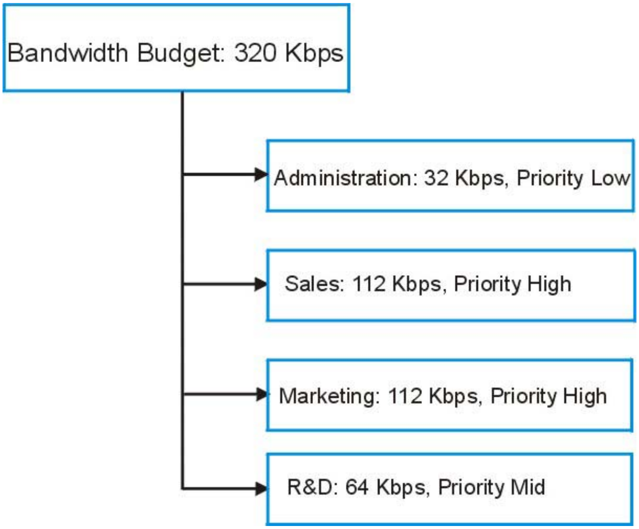

Bandwidth Budget: 320 Kbps
Administration: 32 Kbps, Priority Low
Sales: 112 Kbps, Priority High
Marketing: 112 Kbps, Priority High
R&D: 64 Kbps, Priority Mid

Figure 18-5 Maximize Bandwidth Usage Example

18.1.5 Bandwidth Management Priorities

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

Table 18-2 Media Bandwidth 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.

18.1.6 Bandwidth Management Services

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

- **Xbox Live**

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

- **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.

- **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.

- **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

- **eMule/eDonkey**

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

- **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.

18.1.7 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 18-3 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.

Table 18-3 Commonly Used Services

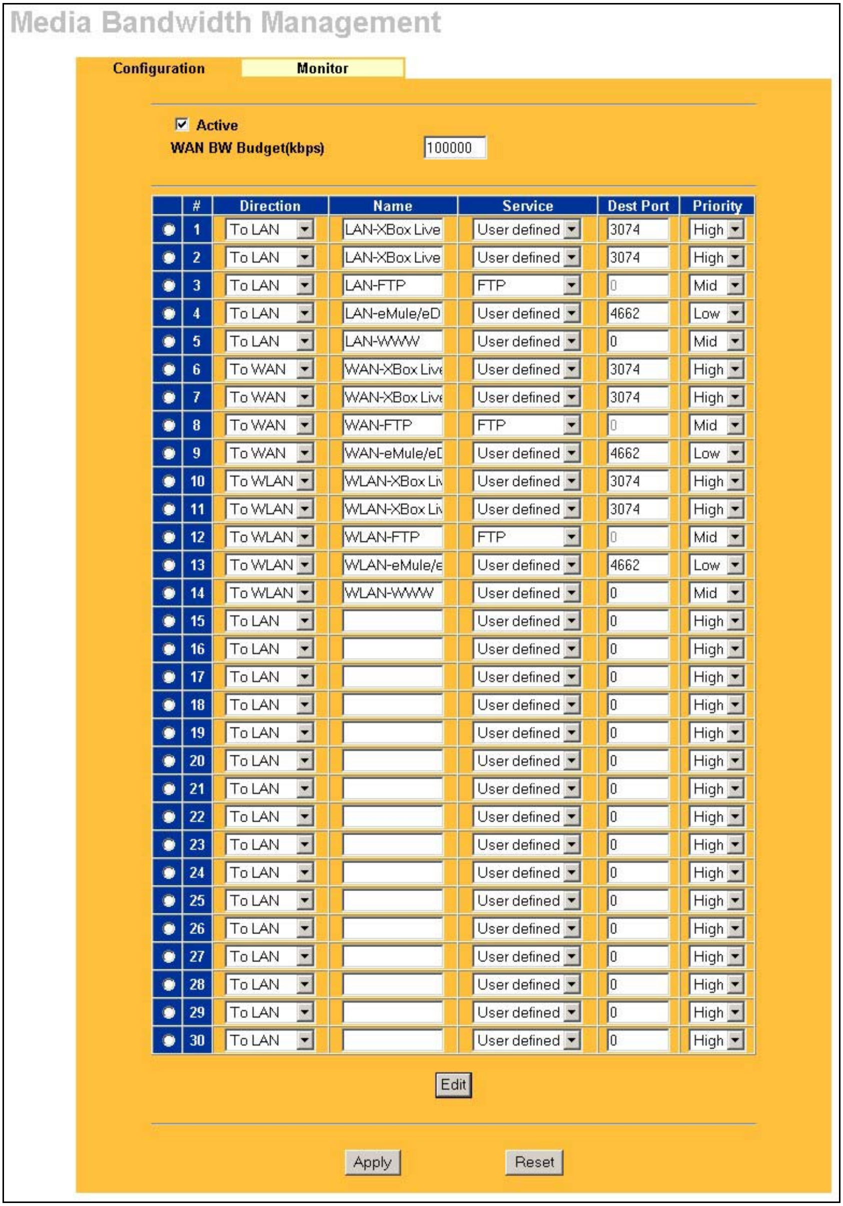
SERVICE	DESCRIPTION
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
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.

Table 18-3 Commonly Used Services

SERVICE	DESCRIPTION
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.

18.2 Configuration Screen

Click **ADVANCED** and then **BW MGMT** to open the media bandwidth management **Configuration** screen, where you can configure your Prestige.



Media Bandwidth Management

☑ Active

WAN BW Budget(kbps) 100000

	#	Direction	Name	Service	Dest Port	Priority
●	1	To LAN	LAN-XBox Live	User defined	3074	High
●	2	To LAN	LAN-XBox Live	User defined	3074	High
●	3	To LAN	LAN-FTP	FTP	0	Mid
●	4	To LAN	LAN-eMule/eD	User defined	4662	Low
●	5	To LAN	LAN-WWW	User defined	0	Mid
●	6	To WAN	WAN-XBox Live	User defined	3074	High
●	7	To WAN	WAN-XBox Live	User defined	3074	High
●	8	To WAN	WAN-FTP	FTP	0	Mid
●	9	To WAN	WAN-eMule/eD	User defined	4662	Low
●	10	To WLAN	WLAN-XBox Li	User defined	3074	High
●	11	To WLAN	WLAN-XBox Li	User defined	3074	High
●	12	To WLAN	WLAN-FTP	FTP	0	Mid
●	13	To WLAN	WLAN-eMule/e	User defined	4662	Low
●	14	To WLAN	WLAN-WWW	User defined	0	Mid
●	15	To LAN		User defined	0	High
●	16	To LAN		User defined	0	High
●	17	To LAN		User defined	0	High
●	18	To LAN		User defined	0	High
●	19	To LAN		User defined	0	High
●	20	To LAN		User defined	0	High
●	21	To LAN		User defined	0	High
●	22	To LAN		User defined	0	High
●	23	To LAN		User defined	0	High
●	24	To LAN		User defined	0	High
●	25	To LAN		User defined	0	High
●	26	To LAN		User defined	0	High
●	27	To LAN		User defined	0	High
●	28	To LAN		User defined	0	High
●	29	To LAN		User defined	0	High
●	30	To LAN		User defined	0	High

Figure 18-6 Bandwidth Management Configuration

The following table describes the labels in this screen.

Table 18-4 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 18-3* for a table 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.

18.3 Editing Bandwidth Management Rules

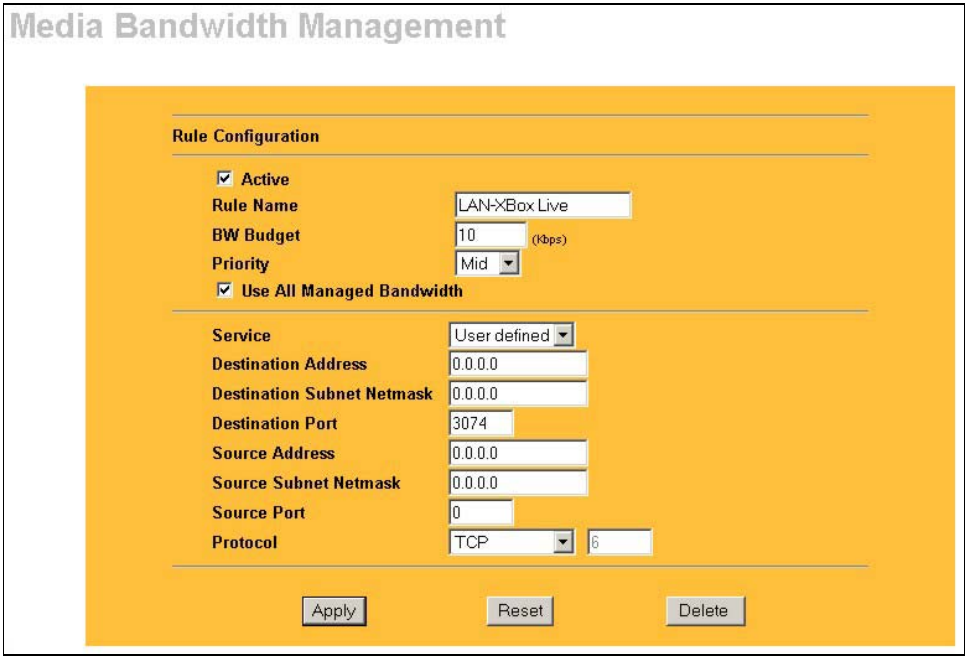
Use the **Bandwidth Management Configuration Edit** screen to configure a bandwidth management rule. Use bandwidth rules to allocate specific amounts of bandwidth capacity (bandwidth budgets) to specific applications and/or subnets.

18.3.1 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.

18.4 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.



Media Bandwidth Management

Rule Configuration

☑ Active

Rule Name: LAN-XBox Live

BW Budget: 10 (Kbps)

Priority: Mid

☑ Use All Managed Bandwidth

Service: User defined

Destination Address: 0.0.0.0

Destination Subnet Netmask: 0.0.0.0

Destination Port: 3074

Source Address: 0.0.0.0

Source Subnet Netmask: 0.0.0.0

Source Port: 0

Protocol: TCP 6

Figure 18-7 Bandwidth Management Edit

The following table describes the labels in this screen.

Table 18-5 Bandwidth Management Edit

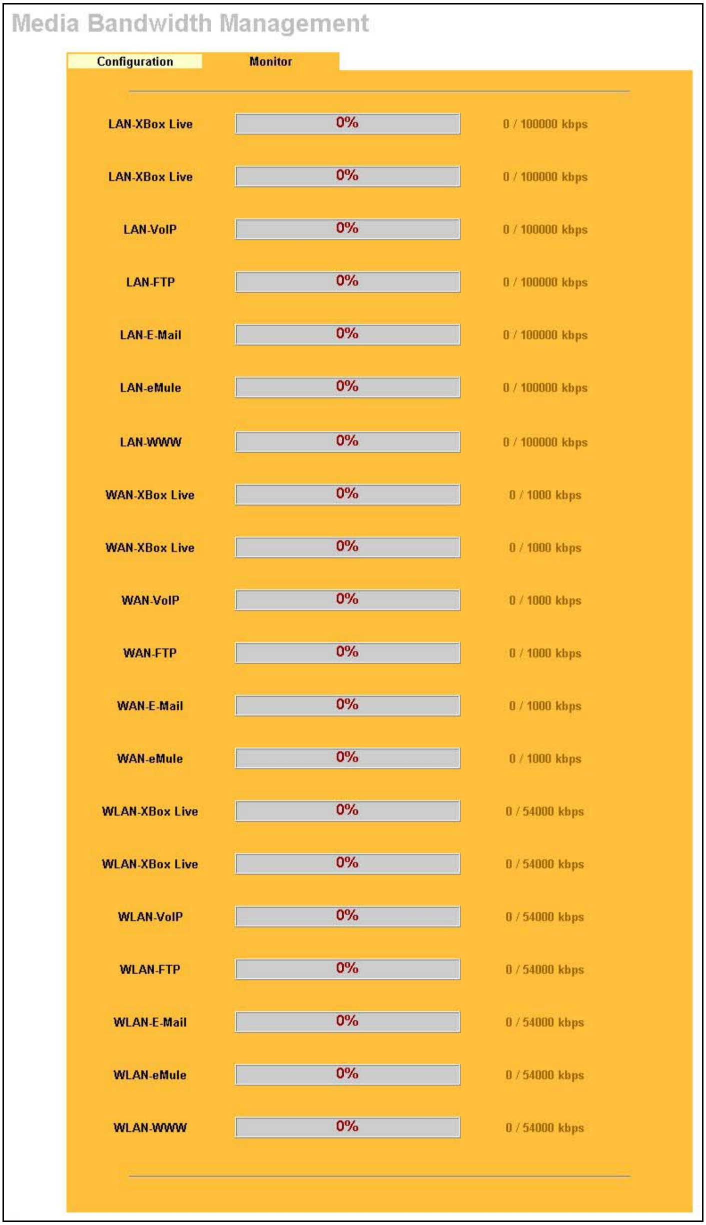
LABEL	DESCRIPTION
Active	Select this check box to have the Prestige apply this bandwidth management rule. Enable a bandwidth management rule to give traffic that matches the rule priority over traffic that does not match the rule.
Rule Name	Use the auto-generated name or enter a descriptive name of up 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.
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 IP Address**. Refer to the appendices for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See *Table 18-3* for some 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 IP Address**. Refer to the appendices for more information on IP subnetting.
Source Port	Enter the port number of the source. See *Table 18-3* for some common services and port numbers.

Table 18-5 Bandwidth Management Edit

LABEL	DESCRIPTION
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.

18.5 Monitor Screen

Select 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.



Media Bandwidth Management

LAN-XBox Live	0%	0 / 100000 kbps
LAN-XBox Live	0%	0 / 100000 kbps
LAN-VoIP	0%	0 / 100000 kbps
LAN-FTP	0%	0 / 100000 kbps
LAN-E-Mail	0%	0 / 100000 kbps
LAN-eMule	0%	0 / 100000 kbps
LAN-WWW	0%	0 / 100000 kbps
WAN-XBox Live	0%	0 / 1000 kbps
WAN-XBox Live	0%	0 / 1000 kbps
WAN-VoIP	0%	0 / 1000 kbps
WAN-FTP	0%	0 / 1000 kbps
WAN-E-Mail	0%	0 / 1000 kbps
WAN-eMule	0%	0 / 1000 kbps
WLAN-XBox Live	0%	0 / 54000 kbps
WLAN-XBox Live	0%	0 / 54000 kbps
WLAN-VoIP	0%	0 / 54000 kbps
WLAN-FTP	0%	0 / 54000 kbps
WLAN-E-Mail	0%	0 / 54000 kbps
WLAN-eMule	0%	0 / 54000 kbps
WLAN-WWW	0%	0 / 54000 kbps

Figure 18-8 Bandwidth Management Monitor

Chapter 19 Maintenance

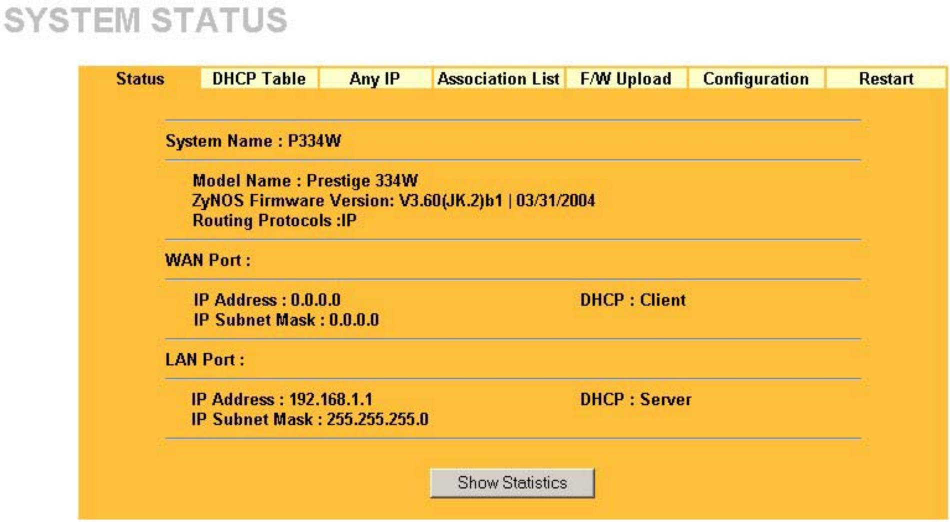
This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

19.1 Maintenance Overview

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

19.2 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.


SYSTEM STATUS

System Name : P334W

Model Name : Prestige 334W
ZyNOS Firmware Version: V3.60(JK.2)b1 | 03/31/2004
Routing Protocols :IP

WAN Port :

IP Address : 0.0.0.0 DHCP : Client
IP Subnet Mask : 0.0.0.0

LAN Port :

IP Address : 192.168.1.1 DHCP : Server
IP Subnet Mask : 255.255.255.0

Figure 19-1 Maintenance Status

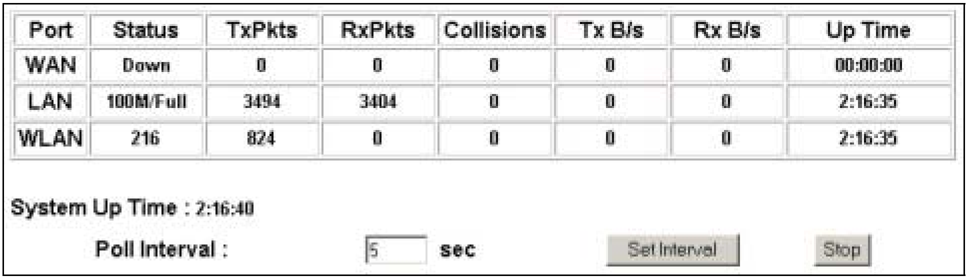
The following table describes the labels in this screen.

Table 19-1 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 19.2.1* for more information.

19.2.1 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.



Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	3494	3404	0	0	0	2:16:35
WLAN	216	824	0	0	0	0	2:16:35

System Up Time : 2:16:40

Poll Interval : 5 sec

Figure 19-2 Maintenance System Statistics

The following table describes the labels in this screen.

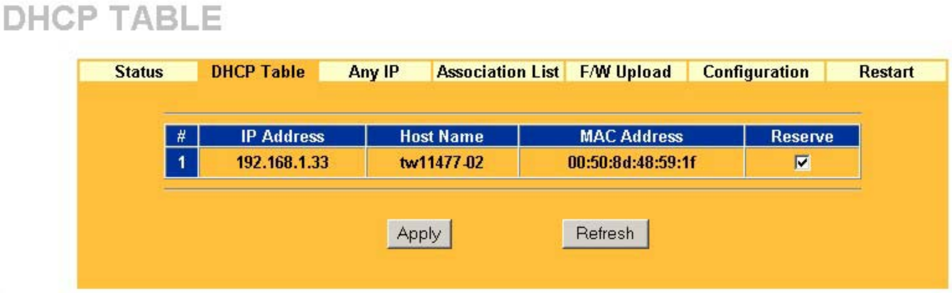
Table 19-2 Maintenance System Statistics

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**.

19.3 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.



#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	tw11477-02	00:50:8d:48:59:1f	☑

Figure 19-3 Maintenance DHCP Table

The following table describes the labels in this screen.

Table 19-3 Maintenance DHCP Table

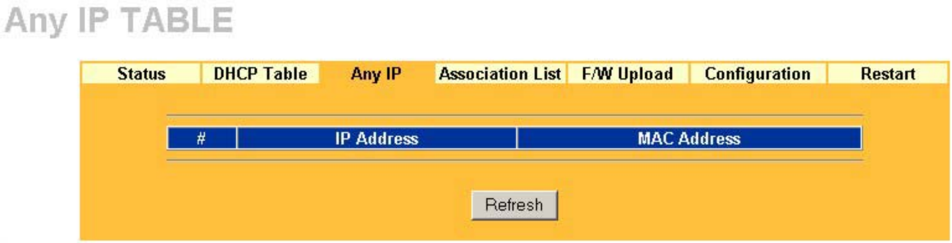
LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** 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).

Table 19-3 Maintenance DHCP Table

LABEL	DESCRIPTION
Refresh	Click **Refresh** to renew the screen.

19.4 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.



#	IP Address	MAC Address

Figure 19-4 Maintenance Any IP

The following table describes the labels in this screen.

Table 19-4 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.

19.5 Association List

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

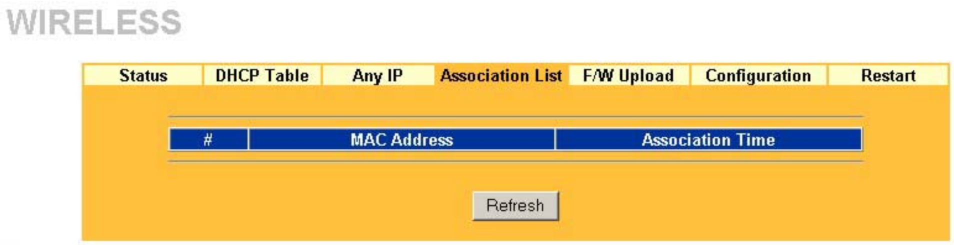


Figure 19-5 Maintenance Association List

The following table describes the labels in this screen.

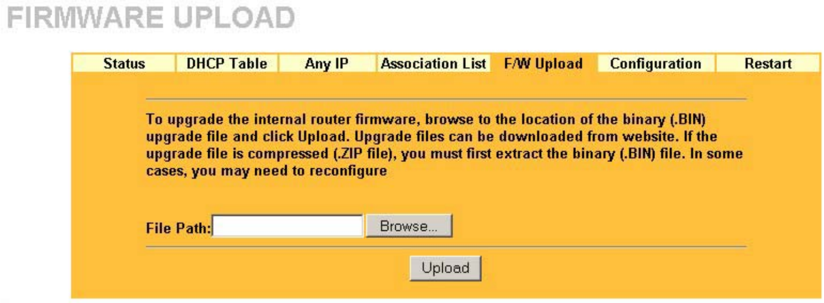
Table 19-5 Maintenance Association List

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.

19.6 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.



To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure

Figure 19-6 Maintenance Firmware Upload

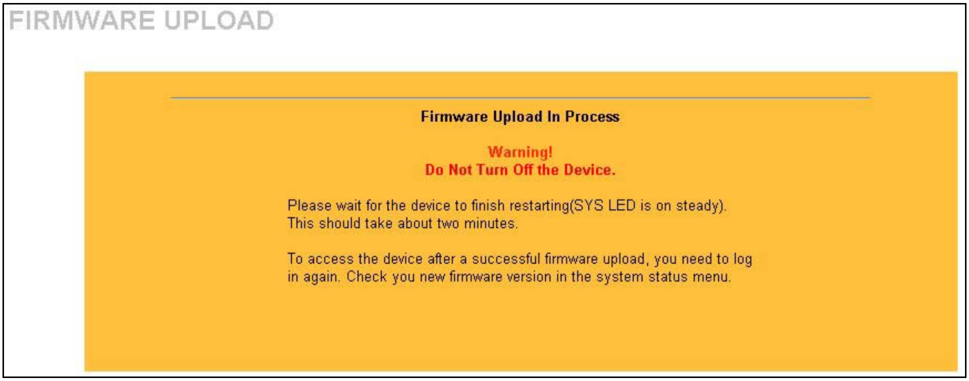
The following table describes the labels in this screen.

Table 19-6 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.

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.



FIRMWARE UPLOAD

Firmware Upload In Process

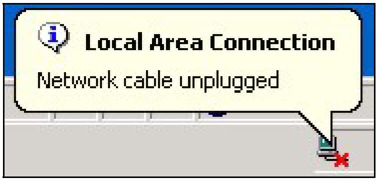
Warning!
Do Not Turn Off the Device.

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

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

Figure 19-7 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.



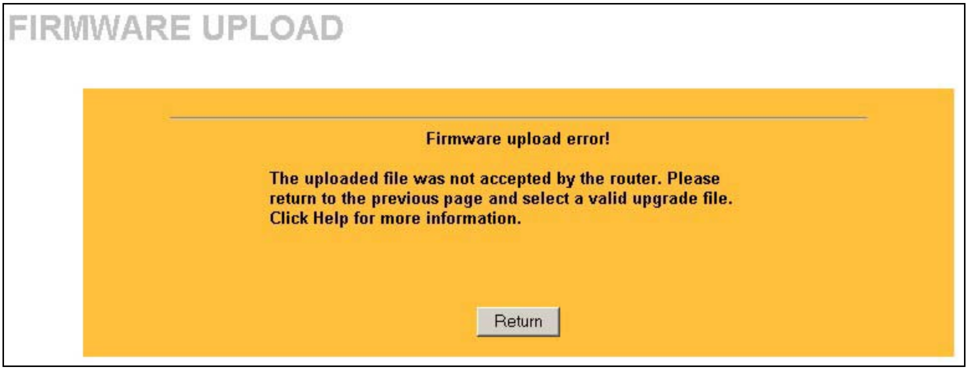
Local Area Connection

Network cable unplugged

Figure 19-8 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.



Firmware upload error!

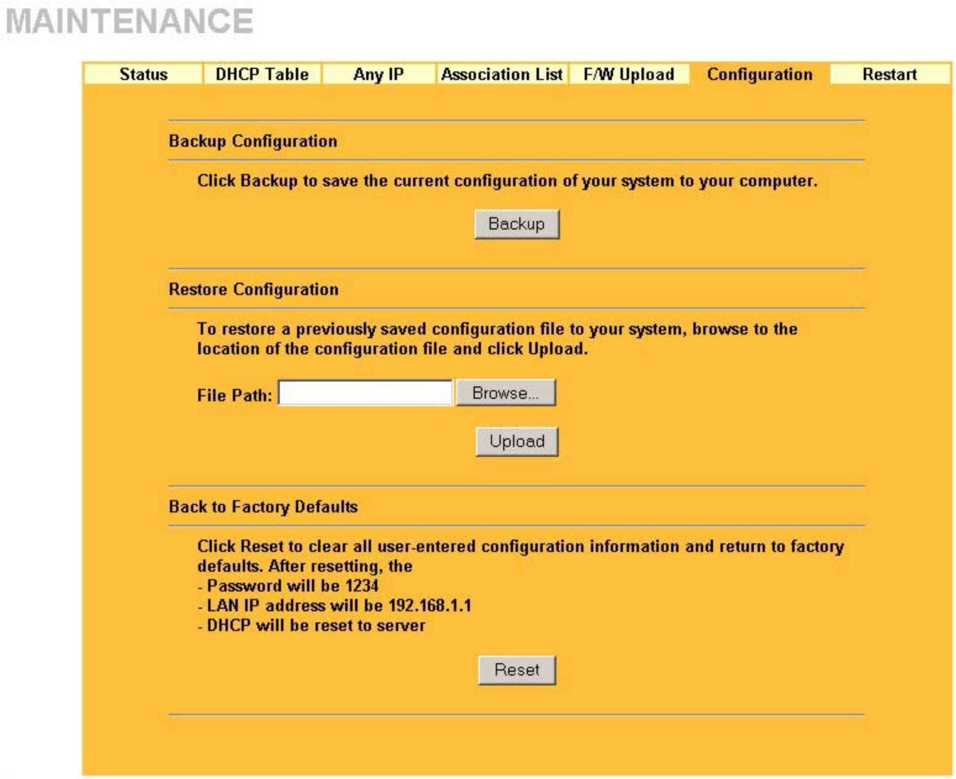
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

Figure 19-9 Upload Error Message

19.7 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.



MAINTENANCE

Backup Configuration

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

Restore Configuration

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

File Path:

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

Figure 19-10 Maintenance Configuration

19.7.1 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

19.7.2 Restore Configuration

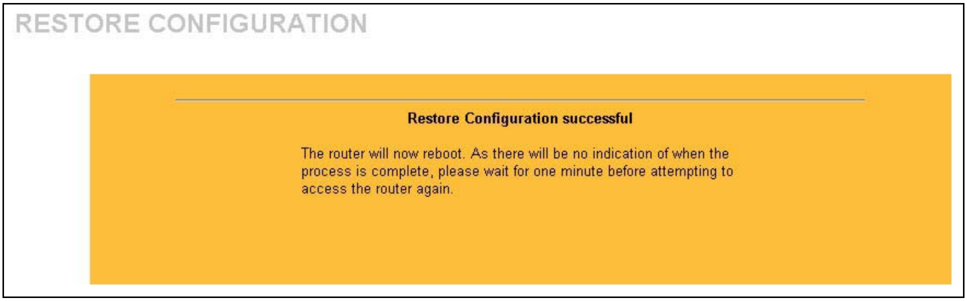
Restore configuration allows you to upload a new or previously saved configuration file from your computer to your Prestige.

Table 19-7 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.

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.



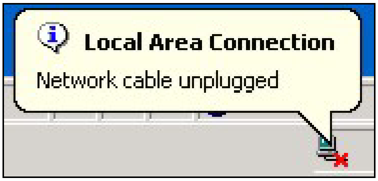
RESTORE CONFIGURATION

Restore Configuration successful

The router will now reboot. As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

Figure 19-11 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.



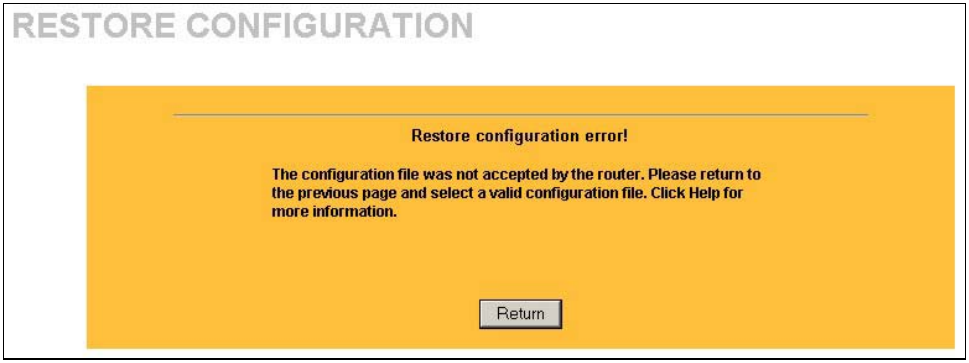
Local Area Connection

Network cable unplugged

Figure 19-12 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.



RESTORE CONFIGURATION

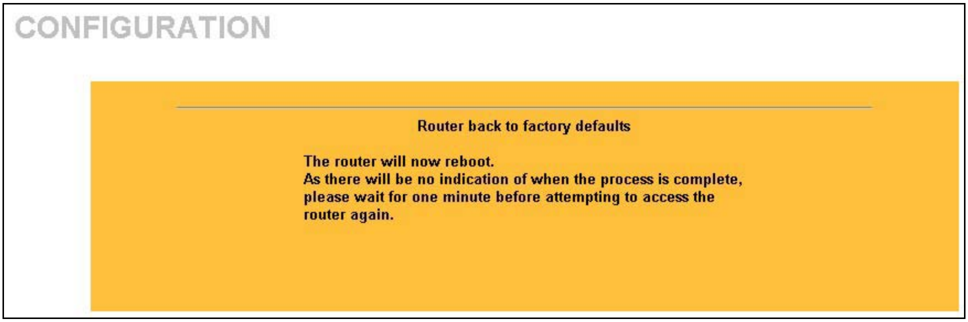
Restore configuration error!

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

Figure 19-13 Configuration Restore Error

19.7.3 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 as shown on the screen. The following warning screen will appear.



CONFIGURATION

Router back to factory defaults

The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

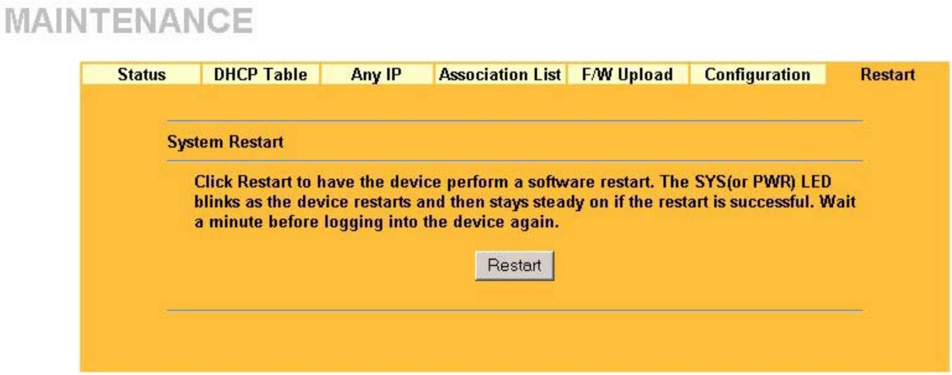
Figure 19-14 Factory Defaults

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

19.8 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.



System Restart

Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.

Figure 19-15 System Restart

Part VII:

SMT General Configuration

This part covers System Management Terminal configuration for general setup, WAN setup, LAN setup, WLAN setup, Internet access, remote node, static route, NAT and enabling the firewall.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 20
Introducing the SMT

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

20.1 SMT Introduction

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

20.1.1 Procedure for SMT Configuration via Console Port

Follow the steps below to access your Prestige via the console port.

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

Press [ENTER] to display the SMT password screen. The default password is "1234".

20.1.2 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your Prestige.

Step 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**.

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

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

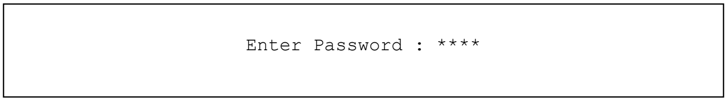
Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again.

20.1.3 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.



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

Figure 20-1 Login Screen

20.1.4 Prestige SMT Menu Overview

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

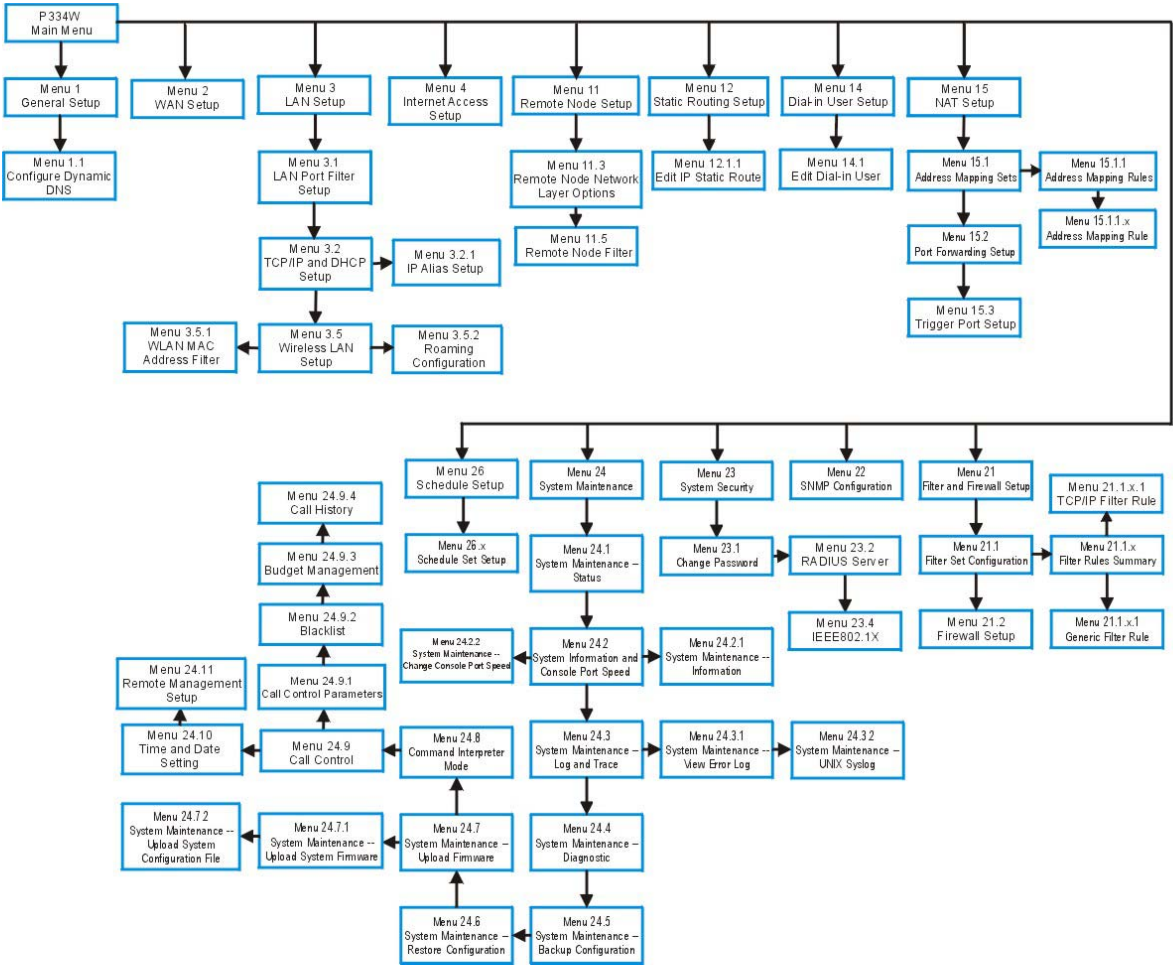

P334W Main Menu
Menu 1 General Setup
Menu 1.1 Configure Dynamic DNS
Menu 2 WAN Setup
Menu 3 LAN Setup
Menu 3.1 LAN Port Filter Setup
Menu 3.2 TCP/IP and DHCP Setup
Menu 3.2.1 IP Alias Setup
Menu 3.5 Wireless LAN Setup
Menu 3.5.1 WLAN MAC Address Filter
Menu 3.5.2 Roaming Configuration
Menu 4 Internet Access Setup
Menu 11 Remote Node Setup
Menu 11.3 Remote Node Network Layer Options
Menu 11.5 Remote Node Filter
Menu 12 Static Routing Setup
Menu 12.1.1 Edit IP Static Route
Menu 14 Dial-in User Setup
Menu 14.1 Edit Dial-in User
Menu 15 NAT Setup
Menu 15.1 Address Mapping Sets
Menu 15.1.1 Address Mapping Rules
Menu 15.1.1.x Address Mapping Rule
Menu 15.2 Port Forwarding Setup
Menu 15.3 Trigger Port Setup
Menu 26 Schedule Setup
Menu 26.x Schedule Set Setup
Menu 24 System Maintenance
Menu 24.1 System Maintenance – Status
Menu 24.2 System Information and Console Port Speed
Menu 24.2.1 System Maintenance -- Information
Menu 24.2.2 System Maintenance -- Change Console Port Speed
Menu 24.3 System Maintenance – Log and Trace
Menu 24.3.1 System Maintenance -- View Error Log
Menu 24.3.2 System Maintenance – UNIX Syslog
Menu 24.4 System Maintenance – Diagnostic
Menu 24.5 System Maintenance – Backup Configuration
Menu 24.6 System Maintenance – Restore Configuration
Menu 24.7 System Maintenance – Upload Firmware
Menu 24.7.1 System Maintenance -- Upload System Firmware
Menu 24.7.2 System Maintenance -- Upload System Configuration File
Menu 24.8 Command Interpreter Mode
Menu 24.9 Call Control
Menu 24.9.1 Call Control Parameters
Menu 24.9.2 Blacklist
Menu 24.9.3 Budget Management
Menu 24.9.4 Call History
Menu 24.10 Time and Date Setting
Menu 24.11 Remote Management Setup
Menu 23 System Security
Menu 23.1 Change Password
Menu 23.2 RADIUS Server
Menu 23.4 IEEE802.1X
Menu 22 SNMP Configuration
Menu 21 Filter and Firewall Setup
Menu 21.1 Filter Set Configuration
Menu 21.1.x Filter Rules Summary
Menu 21.1.x.1 TCP/IP Filter Rule
Menu 21.1.x.1 Generic Filter Rule
Menu 21.2 Firewall Setup

Figure 20-2 SMT Menu Overview

20.2 Navigating the SMT Interface

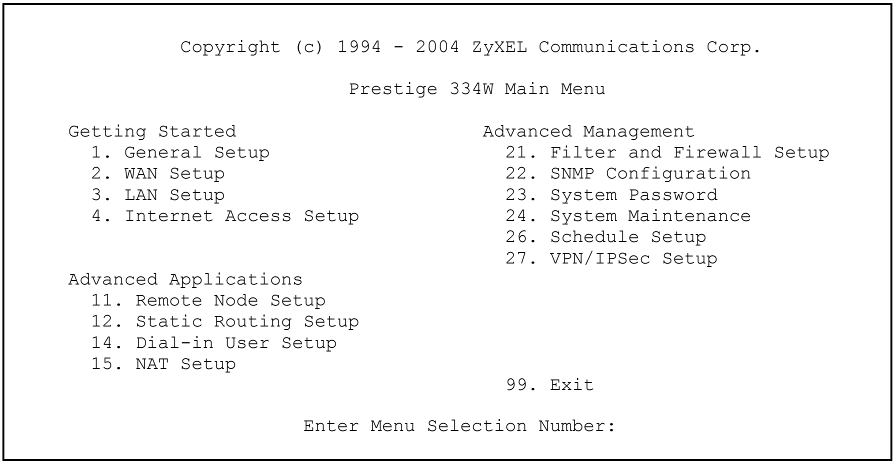
The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

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

Table 20-1 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.



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

                           Prestige 334W 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
       14. Dial-in User Setup
       15. NAT Setup
                                            99. Exit

                         Enter Menu Selection Number:
```

Figure 20-3 SMT Main Menu

20.2.1 System Management Terminal Interface Summary

Table 20-2 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.
14	Dial-in User Setup	Use this menu to set up local user profiles on the Prestige.
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.

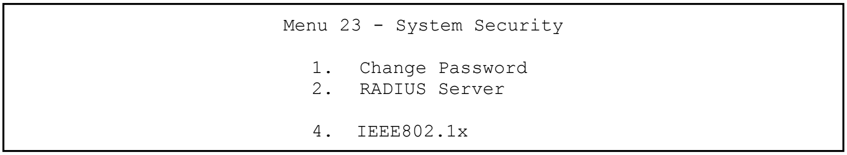
Table 20-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
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.

20.3 Changing the System Password

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

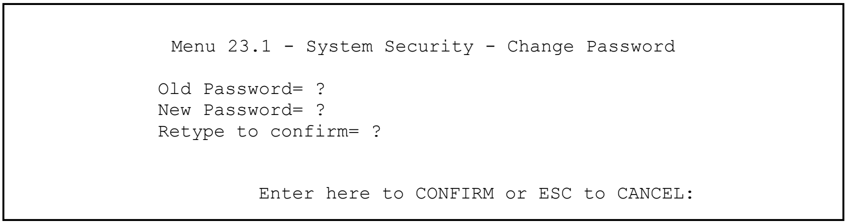
Step 1. Enter 23 in the main menu to display **Menu 23 - System Security** as shown next.



```
                    Menu 23 - System Security

                      1.  Change Password
                      2.  RADIUS Server

                      4.  IEEE802.1x
```

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

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



```
            Menu 23.1 - System Security - Change Password

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


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

Figure 20-4 Menu 23 System Password

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

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

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

Chapter 21
Menu 1 General Setup

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

21.1 General Setup

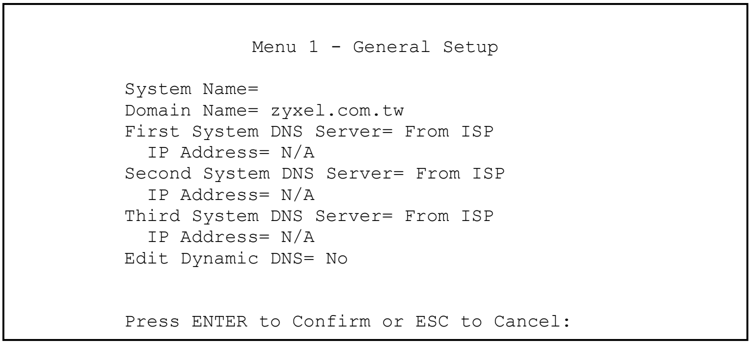
Menu 1 — General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- 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.

21.2 Procedure To Configure Menu 1

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



```
                    Menu 1 - General Setup

           System Name=
           Domain Name= zyxel.com.tw
           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:
```

Figure 21-1 Menu 1 General Setup

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

Table 21-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
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].	zyxel.com.tw

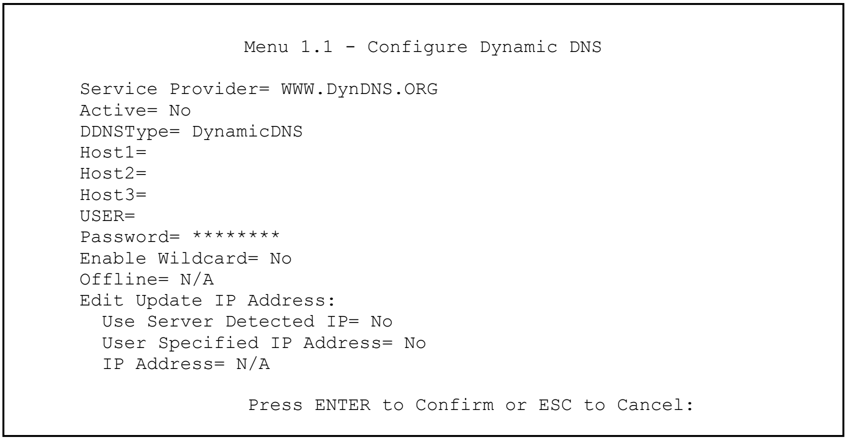
Table 21-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
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.	**From ISP**
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next.	**No** (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

21.2.1 Procedure to Configure Dynamic DNS

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

Step 1. 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.



```
                 Menu 1.1 - Configure Dynamic DNS

  Service Provider= WWW.DynDNS.ORG
  Active= No
  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:
```

Figure 21-2 Menu 1.1 Configure Dynamic DNS

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

Table 21-2 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
DDNS Type	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have a dynamic IP address(es). Select **StaticDNS** if you have a static IP address(s). Select **CustomDNS** to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.	**DynamicDNS** (default)
Host1-3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.	me.dyndns.org
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	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.	**No**

Table 21-2 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION	EXAMPLE
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).	**Yes**
Edit Update IP Address: You can select **Yes** in either the **Use Server Detected IP** field (recommended) or the **User Specified IP Addr** field, but not both. With the **Use Server Detected IP** and **User Specified IP Addr** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the 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.	**Yes**
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.	**No**
IP Address	Enter the static public IP address if you select **Yes** in the **User Specified IP Addr** field.	**N/A**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

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

Chapter 22
Menu 2 WAN Setup

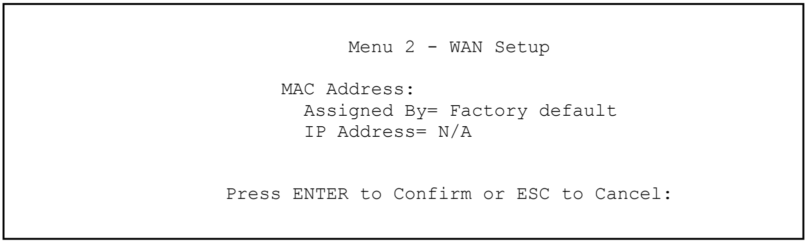
This chapter describes how to configure the WAN using menu 2.

22.1 Introduction to WAN

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

22.2 WAN Setup

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



```
                    Menu 2 - WAN Setup

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


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

Figure 22-1 Menu 2 WAN Setup

The following table describes the fields in this menu.

Table 22-1 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.

Table 22-1 Menu 2 WAN Setup

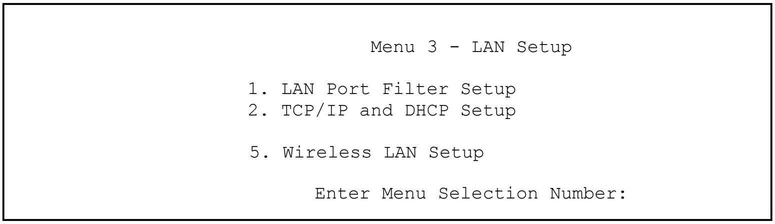
FIELD	DESCRIPTION
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

Chapter 23
Menu 3 LAN Setup

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

23.1 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.

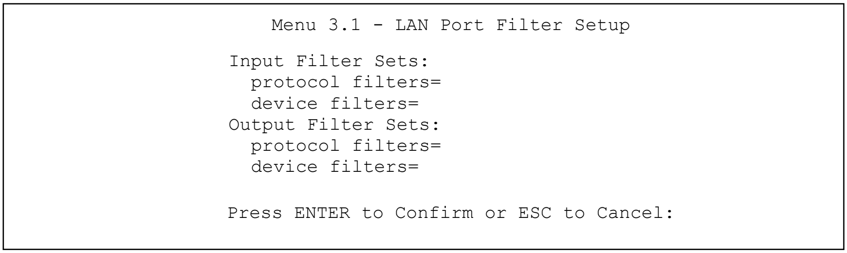


```
                     Menu 3 - LAN Setup

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

           5. Wireless LAN Setup

                Enter Menu Selection Number:
```

Figure 23-1 Menu 3 LAN Setup

23.1.1 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.



```
    Menu 3.1 - LAN Port Filter Setup

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

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

Figure 23-2 Menu 3.1 LAN Port Filter Setup

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

23.2 Protocol Dependent Ethernet Setup

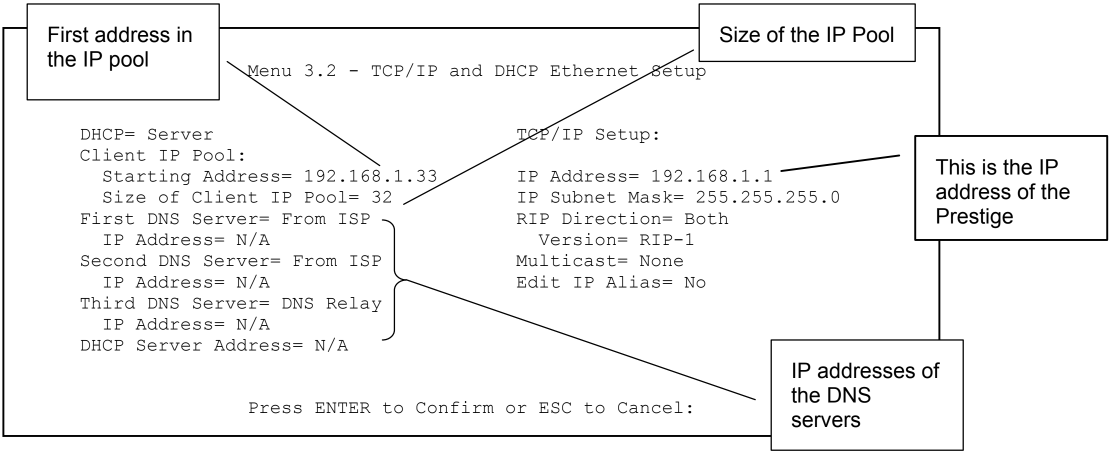
Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

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

23.3 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:



```
                    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:
```

First address in the IP pool

Size of the IP Pool

This is the IP address of the Prestige

IP addresses of the DNS servers

Figure 23-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup

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

Table 23-1 Menu 3.2: DHCP Ethernet Setup Fields

FIELD	DESCRIPTION	EXAMPLE
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:	**Server**

Table 23-1 Menu 3.2: DHCP Ethernet Setup Fields

FIELD	DESCRIPTION	EXAMPLE
Client IP Pool:		
Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	128
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.	**From ISP**
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 23-2 Menu 3.2: LAN TCP/IP Setup Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup:		
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.1.1 (default)
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.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The 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.	**None**
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	**No**
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

23.3.1 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.

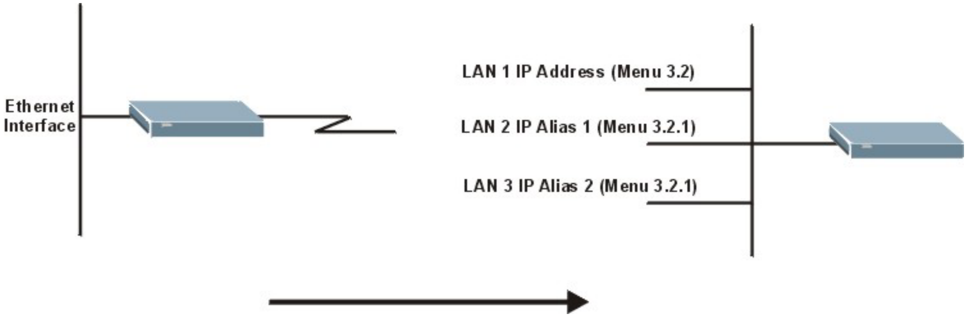
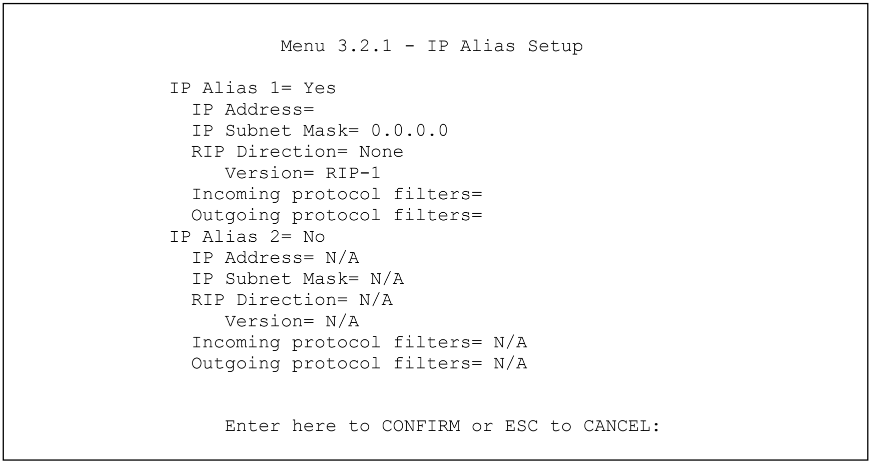

Ethernet Interface
LAN 1 IP Address (Menu 3.2)
LAN 2 IP Alias 1 (Menu 3.2.1)
LAN 3 IP Alias 2 (Menu 3.2.1)

Figure 23-4 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.



```
                    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:
```

Figure 23-5 Menu 3.2.1: IP Alias Setup

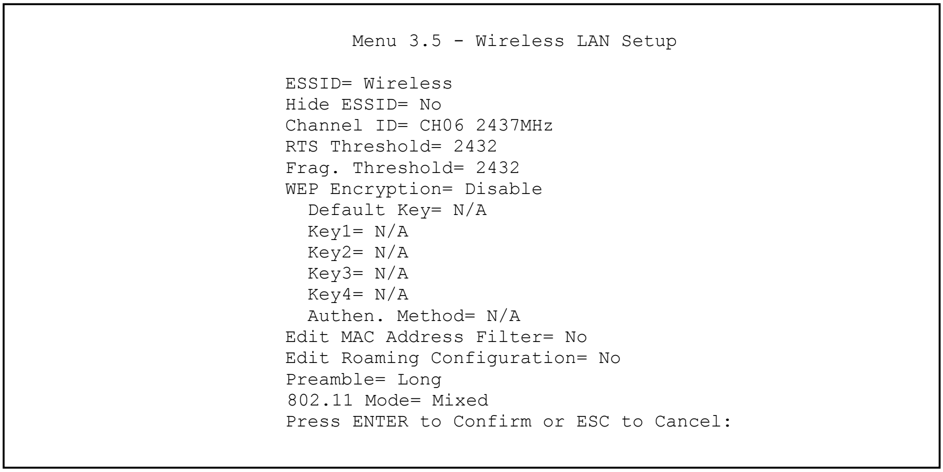
Use the instructions in the following table to configure IP alias parameters.

Table 23-3 Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION	EXAMPLE
IP Alias 1, 2	Choose **Yes** to configure the LAN network for the Prestige.	**Yes**
IP Address	Enter the IP address of your Prestige in dotted decimal notation.	192.168.1.1
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.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only, Out Only** or **None**.	**None**
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	1
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	2
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

23.4 Wireless LAN Setup

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.



```
                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:
```

Figure 23-6 Menu 3.5 Wireless LAN Setup

The following table describes the fields in this menu.

Table 23-4 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXAMPLE
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.	**Wireless**
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.	**No**
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.	**CH06 2437MHz**
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.	**2432**
Fragment Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.	**2432**
WEP	Select **Disable** to allow wireless stations to communicate with the access points without any data encryption.	**Disable**

Table 23-4 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXAMPLE
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.	**Disable**
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.	**1**
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"). **Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key.**	**0x12345abcde**
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**.	**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.	**Long**
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.	**Mixed**

Table 23-4 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXAMPLE
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

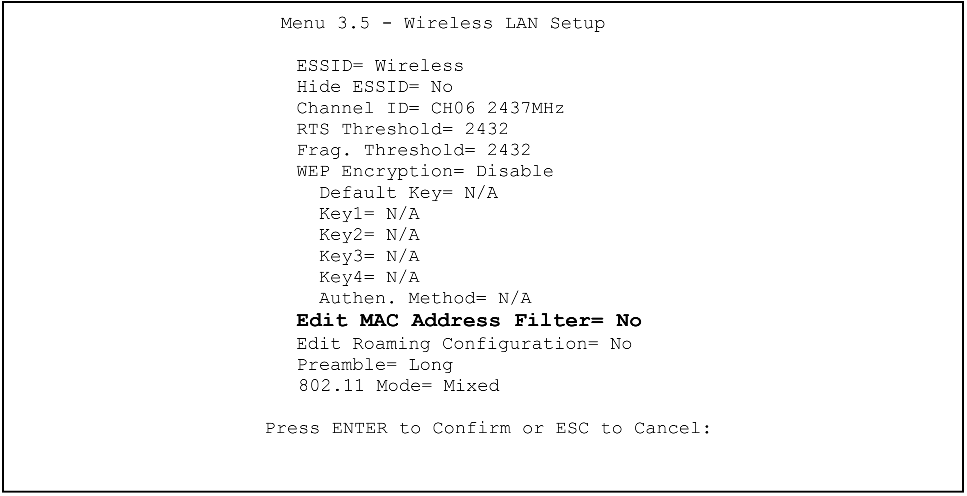
23.4.1 Configuring MAC Address Filter

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.

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

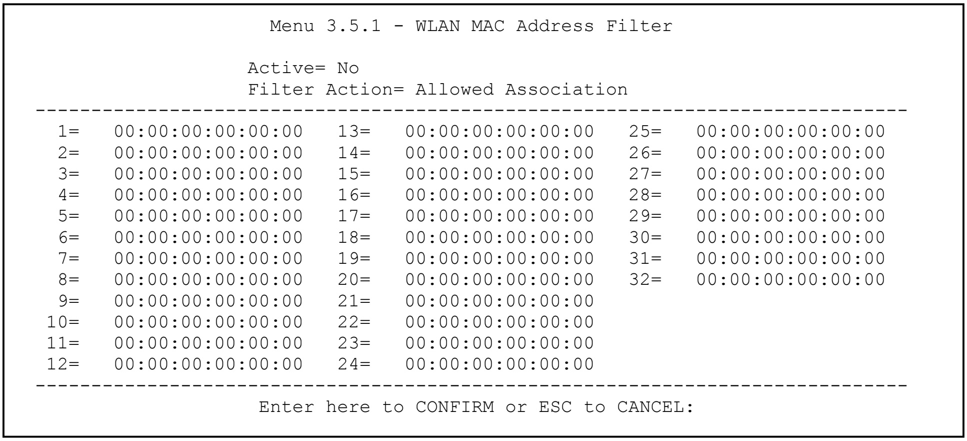
Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.



```
                         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:
```

Figure 23-7 Menu 3.5 Wireless LAN Setup

Step 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.



```
                       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:
```

Figure 23-8 Menu 3.5.1 WLAN MAC Address Filter

The following table describes the fields in this menu.

Table 23-5 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.

Table 23-5 Menu 3.5.1 WLAN MAC Address Filter

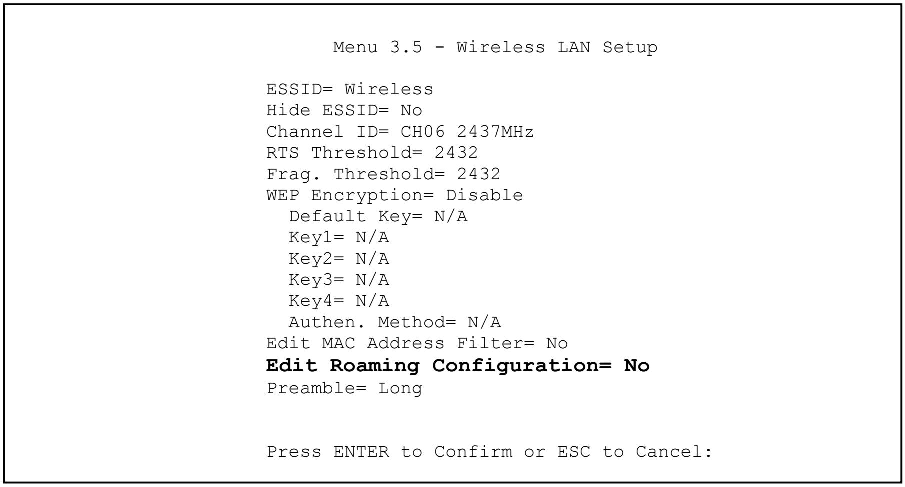
FIELD	DESCRIPTION
MAC Address Filter	
1..32	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the Prestige in these address fields.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

23.4.2 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.

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

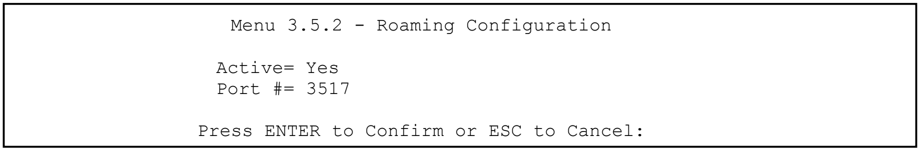
Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.



```
                         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:
```

Figure 23-9 Menu 3.5 Wireless LAN Setup

Step 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.



```
                    Menu 3.5.2 - Roaming Configuration

                   Active= Yes
                   Port #= 3517

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

Figure 23-10 Menu 3.5.2 Roaming Configuration

The following table describes the fields in this menu.

Table 23-6 Menu 3.5.2 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 24
Internet Access

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

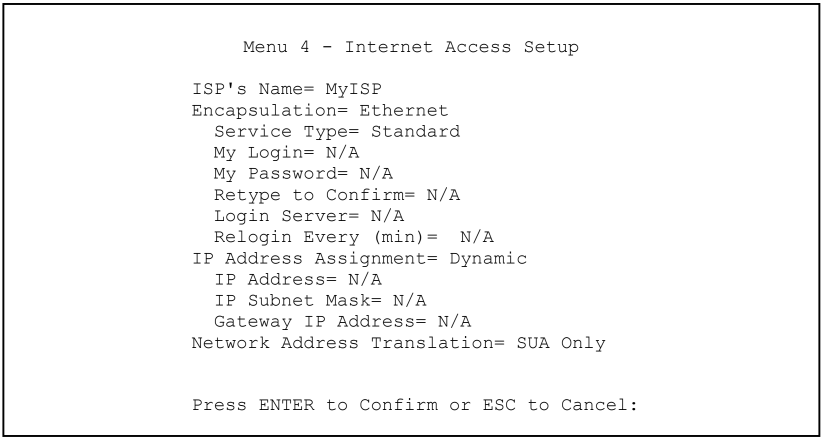
24.1 Introduction to Internet Access Setup

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.

24.2 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.



```
         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:
```

Figure 24-1 Menu 4 Internet Access Setup

The following table describes the fields in this menu.

Table 24-1 Menu 4: 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.
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.

Table 24-1 Menu 4: Internet Access Setup (Ethernet)

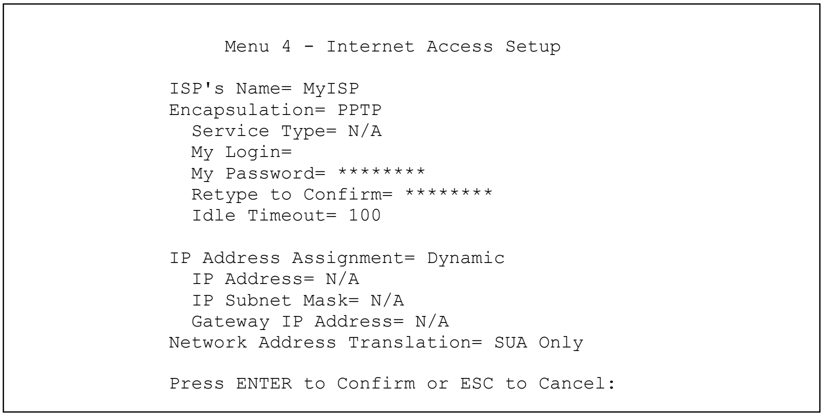
FIELD	DESCRIPTION
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address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

24.3 Configuring the PPTP Client

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.



```
          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:
```

Figure 24-2 Internet Access Setup (PPTP)

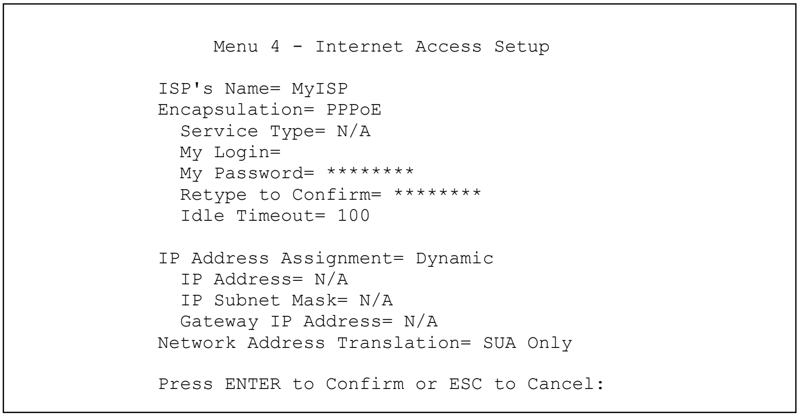
The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

Table 24-2 New Fields in Menu 4 (PPTP) Screen

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

24.4 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.



```
                  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:
```

Figure 24-3 Internet Access Setup (PPPoE)

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

Table 24-3 New Fields in Menu 4 (PPPoE) screen

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

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

24.5 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.

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 25
Remote Node Configuration

This chapter covers remote node configuration.

25.1 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**.

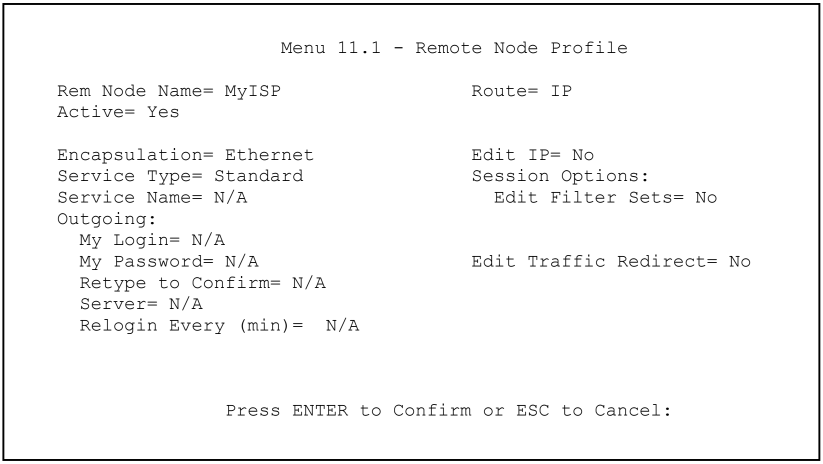
25.2 Remote Node Profile Setup

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.

25.2.1 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.



```
                    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:
```

Figure 25-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

The following table describes the fields in this menu.

Table 25-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

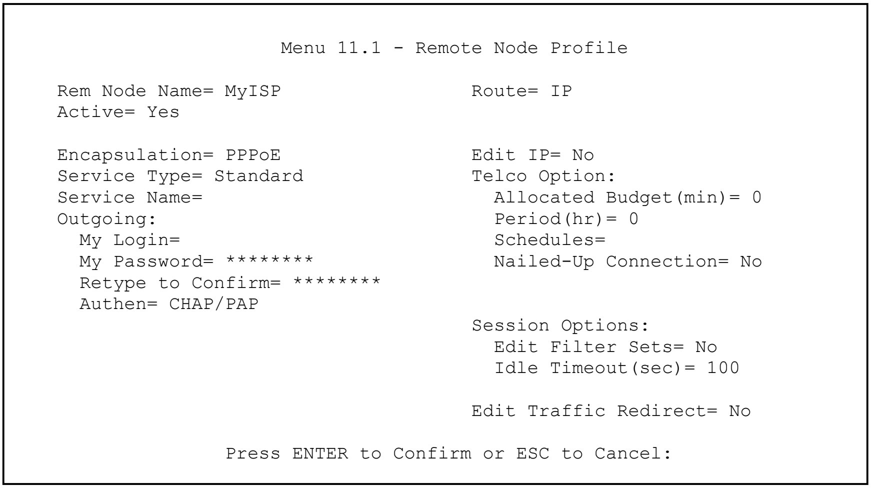
FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node).	**Yes**
Encapsulation	**Ethernet** is the default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

Table 25-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION	EXAMPLE
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.	**IP**
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**.	**No** (default)
Session Options		
Edit Filter Sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.	**No** (default)
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.		

25.2.2 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.



```
                    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:
```

Figure 25-2 Menu 11.1 Remote Node Profile for PPPoE Encapsulation

Outgoing Authentication Protocol

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

Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The 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.

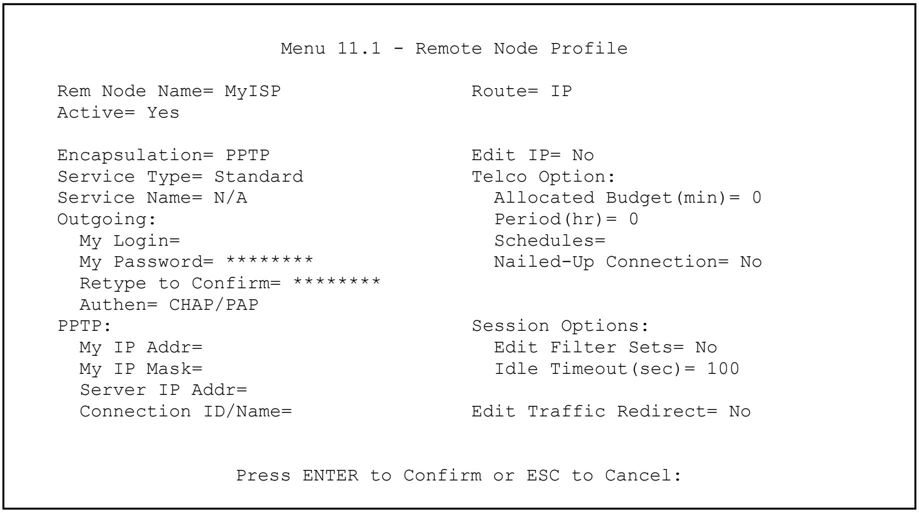
The following table describes the fields not already described in *Table 25-1*.

Table 25-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION	EXAMPLE
Service Name	If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation.	poellc
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.	**CHAP/PAP**
Telco Option		
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period(hr)** is 1 (hour).	0 (default)
Schedules	You can apply up to four schedule sets here. For more details please refer to the *Call Schedule Setup* chapter.	
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	**No** (default)
Session Options		
Idle Timeout	Type the length of idle time (when there is no traffic from the 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.	100 seconds (default)

25.2.3 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.



```
                         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:
```

Figure 25-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation

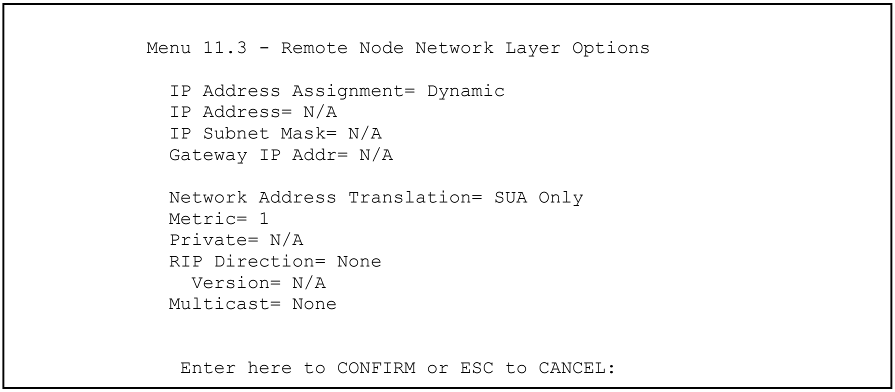
The next table shows how to configure fields in menu 11.1 not previously discussed.

Table 25-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **PPTP**. You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.	**PPTP**
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
My IP Mask	Enter the subnet mask of the WAN Ethernet port.	255.255.255.0
Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/Name	Enter the connection ID or connection name in the ANT. It must follow the "c:id" and "n:name" format. This field is optional and depends on the requirements of your DSL modem.	N:My ISP

25.3 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**.



```
            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:
```

Figure 25-4 Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation

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 25-4 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.	**Dynamic** (default)
(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.	

Table 25-4 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
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.	**SUA Only** (default)
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.	1
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.	**No**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. See the *LAN Setup* chapter for more information on RIP. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting.	**None** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/**RIP-2M** or **None**.	N/A

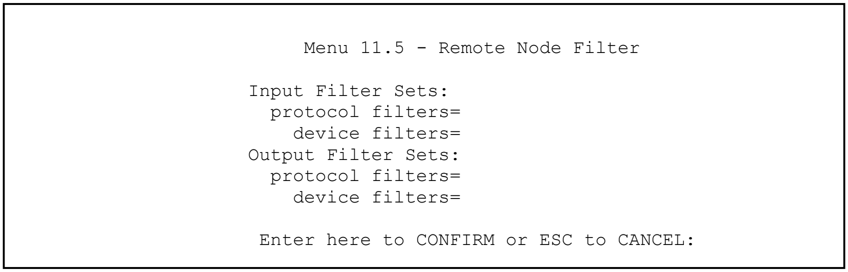
Table 25-4 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
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.	**None** (default)
Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

25.4 Remote Node Filter

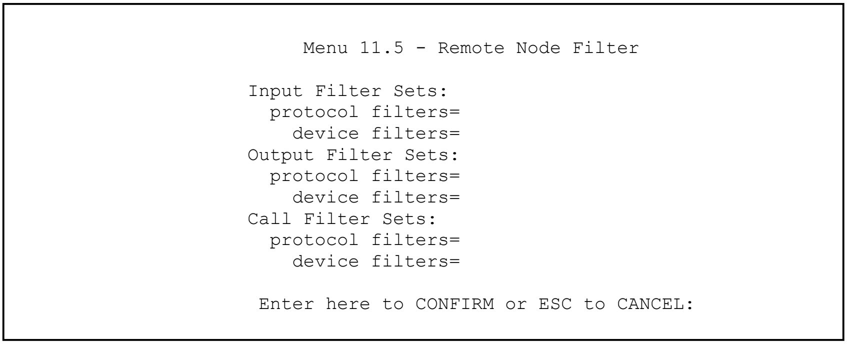
Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

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.



```
               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 25-5 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)

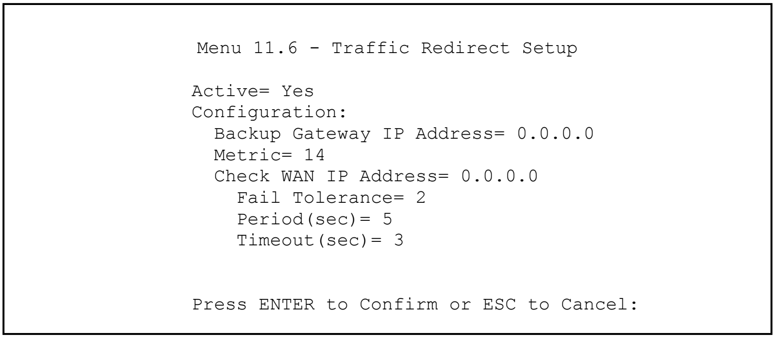


```
                    Menu 11.5 - Remote Node Filter

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

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

Figure 25-6 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)

25.4.1 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**.



```
                Menu 11.6 - Traffic Redirect Setup

                Active= Yes
                Configuration:
                  Backup Gateway IP Address= 0.0.0.0
                  Metric= 14
                  Check WAN IP Address= 0.0.0.0
                    Fail Tolerance= 2
                    Period(sec)= 5
                    Timeout(sec)= 3


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

Figure 25-7 Menu 11.6: Traffic Redirect Setup

The following table describes the fields in this screen.

Table 25-5 Menu 11.6: Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup. The default is **No**.	**Yes**

Table 25-5 Menu 11.6: Traffic Redirect Setup

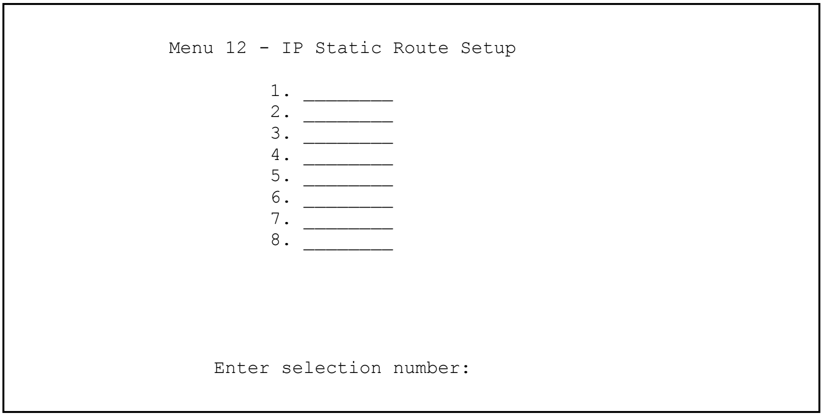
FIELD	DESCRIPTION	EXAMPLE
Configuration:		
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.	0.0.0.0
Metric	Enter a number from 1 to 15 to set 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.	15 (default)
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your 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.	0.0.0.0
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.	2
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.	5
Timeout (sec)	Enter the number of seconds the 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.	3
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

Chapter 26
Static Route Setup

This chapter shows how to setup IP static routes.

26.1 IP Static Route Setup

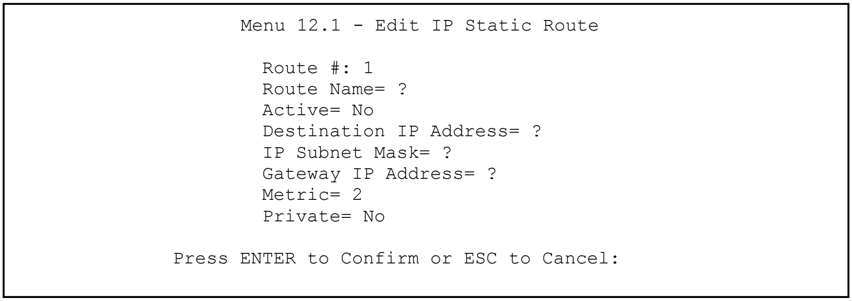
Step 1. To configure an IP static route, use **Menu 12** – **Static Routing Setup** (shown next).



```
              Menu 12 - IP Static Route Setup

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




                  Enter selection number:
```

Figure 26-1 Menu 12 IP Static Route Setup

Step 2. Now, type the route number of a static route you want to configure.



```
                     Menu 12.1 - Edit IP Static Route

                       Route #: 1
                       Route Name= ?
                       Active= No
                       Destination IP Address= ?
                       IP Subnet Mask= ?
                       Gateway IP Address= ?
                       Metric= 2
                       Private= No

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

Figure 26-2 Menu12.1 Edit IP Static Route

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

Table 26-1 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.
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.

Table 26-1 Menu12.1 Edit IP Static Route

FIELD	DESCRIPTION
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 27
Dial-in User Setup

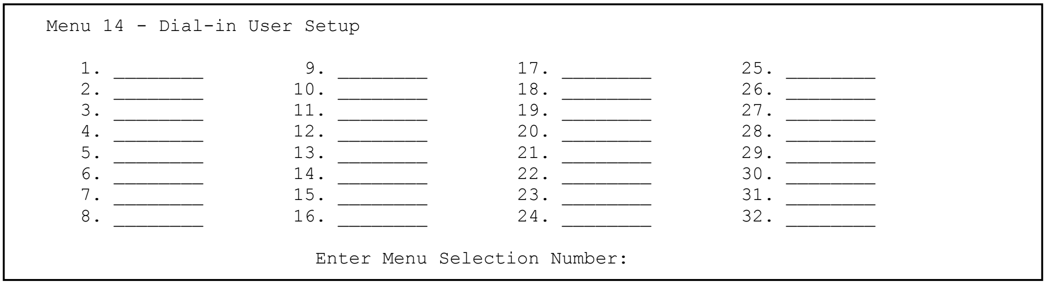
This chapter shows you how to create user accounts on the ZyAIR.

27.1 Dial-in User Setup

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

Follow the steps below to set up user profiles on your ZyAIR.

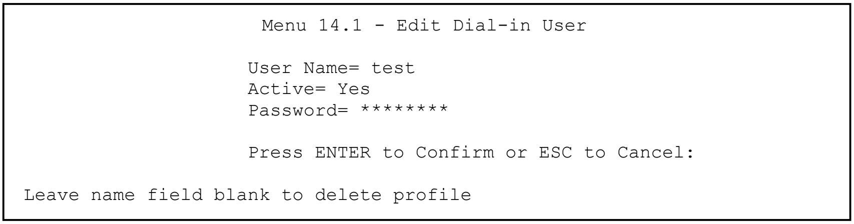
Step 1. From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.



```
  Menu 14 - Dial-in User Setup

     1. ________         9. ________        17. ________        25. ________
     2. ________        10. ________        18. ________        26. ________
     3. ________        11. ________        19. ________        27. ________
     4. ________        12. ________        20. ________        28. ________
     5. ________        13. ________        21. ________        29. ________
     6. ________        14. ________        22. ________        30. ________
     7. ________        15. ________        23. ________        31. ________
     8. ________        16. ________        24. ________        32. ________

                        Enter Menu Selection Number:
```

Figure 27-1 Menu 14- Dial-in User Setup

Step 2. Type a number and press [ENTER] to edit the user profile.



```
                     Menu 14.1 - Edit Dial-in User

                    User Name= test
                    Active= Yes
                    Password= ********

                    Press ENTER to Confirm or ESC to Cancel:

Leave name field blank to delete profile
```

Figure 27-2 Menu 14.1- Edit Dial-in User

The following table describes the fields in this screen.

Table 27-1 Menu 14.1- Edit Dial-in User

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 28
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

28.1 Using NAT

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

28.1.1 SUA (Single User Account) Versus NAT

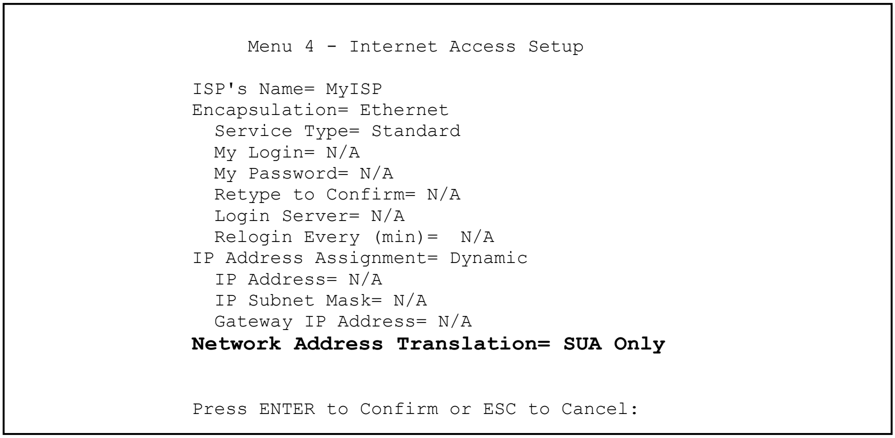
SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See *section 28.3.1* for a detailed description of the NAT set for SUA. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

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

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

28.2 Applying NAT

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



```
          Menu 4 - Internet Access Setup

     ISP's Name= MyISP
     Encapsulation= Ethernet
       Service Type= Standard
       My Login= N/A
       My Password= N/A
       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:
```

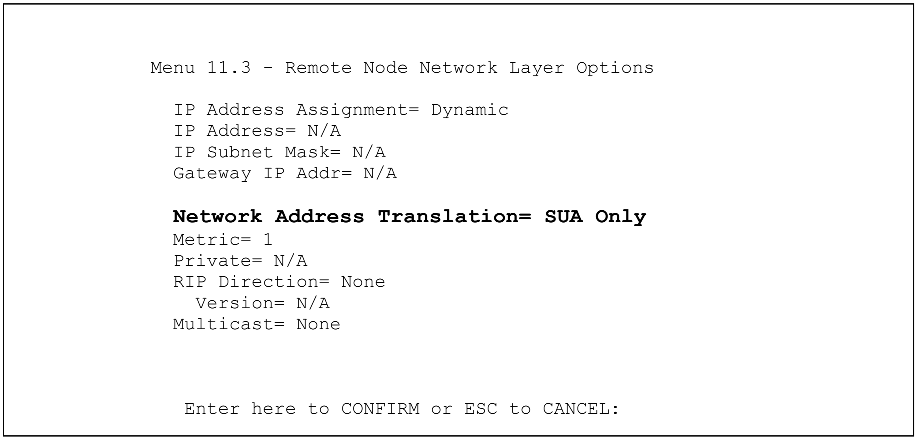
Figure 28-1 Menu 4 Applying NAT for Internet Access

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

Step 1. Enter 11 from the main menu.

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

Step 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.**



```
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:
```

Figure 28-2 Menu 11.3 Applying NAT to the Remote Node

The following table describes the options for Network Address Translation.

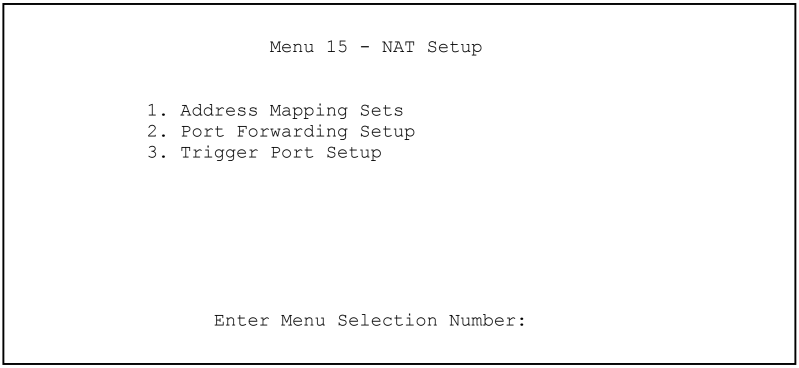
Table 28-1 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION	EXAMPLE
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 *28.3.1*).	**Full Feature**
	Select **None** to disable NAT.	**None**
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (menu 15.1 - see section *28.3.1*). Choose **SUA Only** if you have just one public WAN IP address for your Prestige.	**SUA Only**

28.3 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.

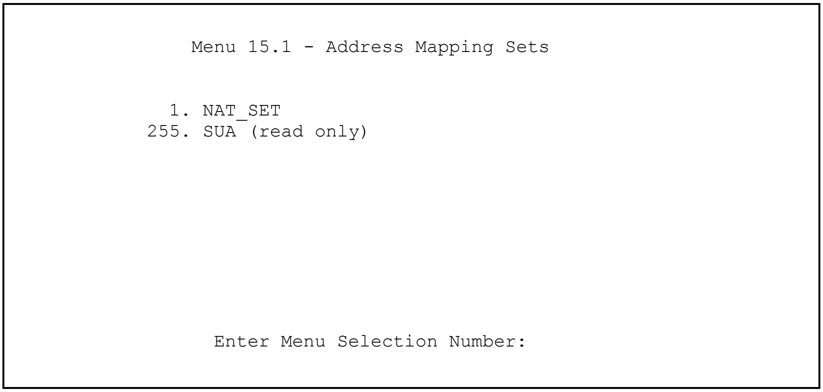


```
                   Menu 15 - NAT Setup


          1. Address Mapping Sets
          2. Port Forwarding Setup
          3. Trigger Port Setup








              Enter Menu Selection Number:
```

Figure 28-3 Menu 15 NAT Setup

28.3.1 Address Mapping Sets

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

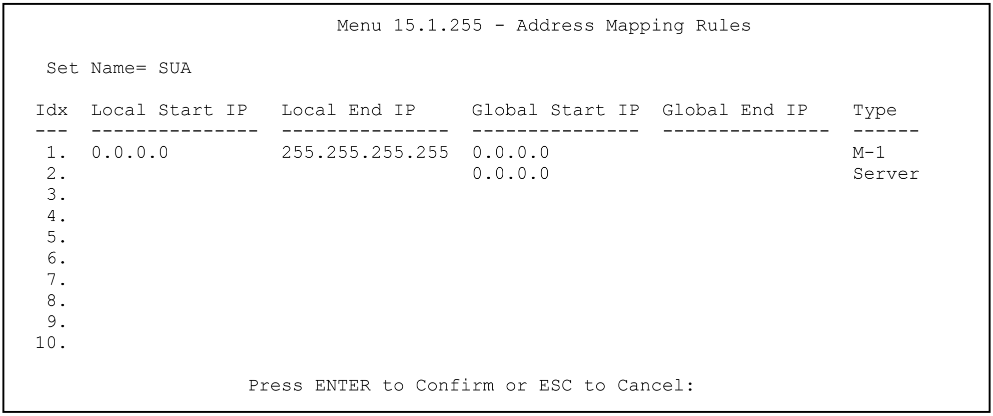


```
              Menu 15.1 - Address Mapping Sets


            1. NAT_SET
          255. SUA (read only)








              Enter Menu Selection Number:
```

Figure 28-4 Menu 15.1 Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 28.1.1)*. The fields in this menu cannot be changed.



```
                        Menu 15.1.255 - Address Mapping Rules

 Set Name= SUA

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  0.0.0.0          255.255.255.255  0.0.0.0                           M-1
 2.                                    0.0.0.0                           Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

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

Figure 28-5 Menu 15.1.255 SUA Address Mapping Rules

The following table explains the fields in this menu.

Menu 15.1.255 is read-only.

Table 28-2 SUA Address Mapping Rules

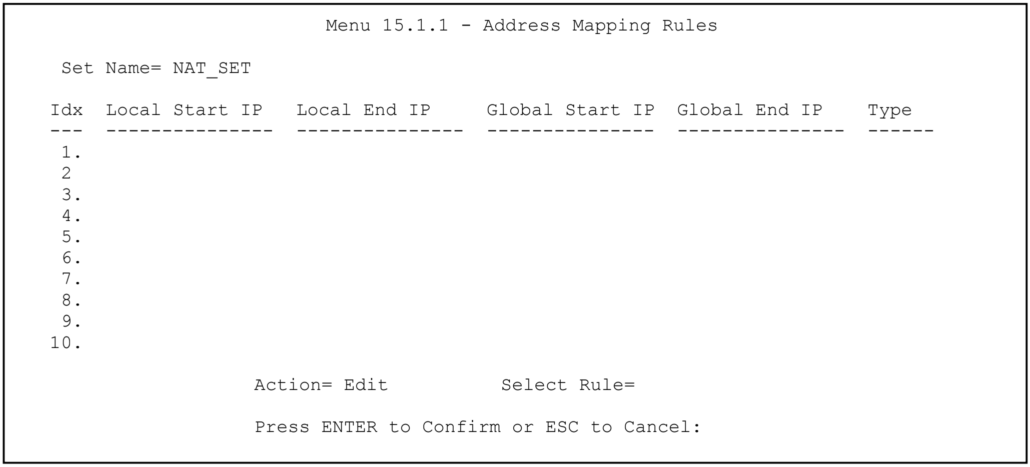
FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP	**Local Start IP** is the starting local IP address (ILA).	0.0.0.0
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	
Type	These are the mapping types. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server

Table 28-2 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
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.		

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.



```
                             Menu 15.1.1 - Address Mapping Rules

     Set Name= NAT_SET

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

                       Action= Edit          Select Rule=

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

Figure 28-6 Menu 15.1.1 First Set

If the Set Name **field is left blank, the entire set will be deleted.**

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

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.

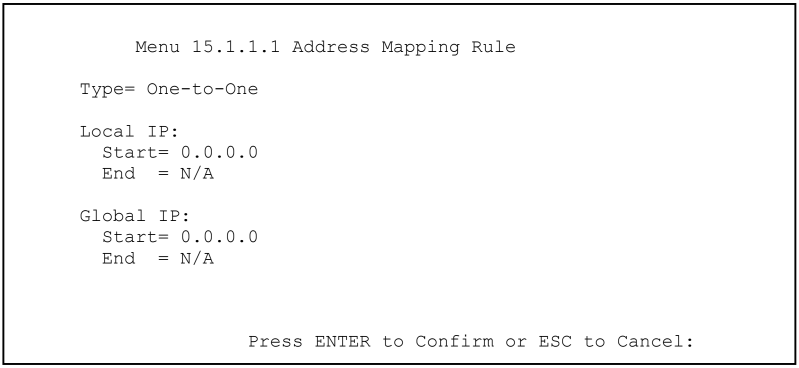
Table 28-3 Menu 15.1.1 First Set

FIELD	DESRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.	**Edit**
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

You must press [ENTER] **at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.**

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

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



```
     Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start= 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:
```

Figure 28-7 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

The following table explains the fields in this menu.

Table 28-4 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

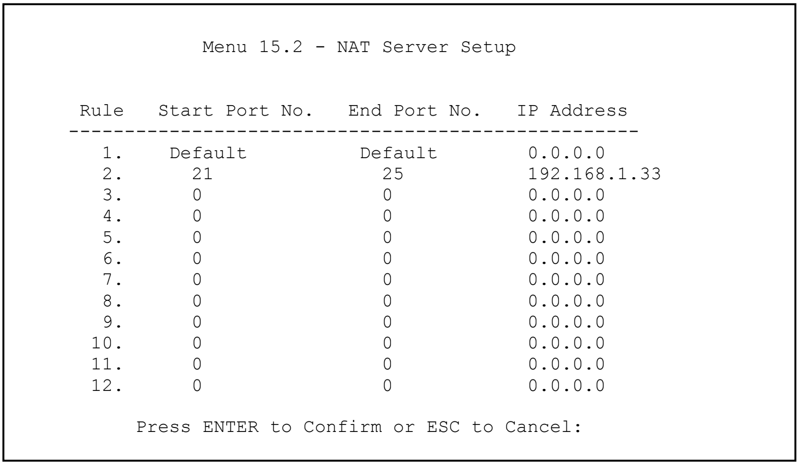
FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 28.5.3* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	This is the starting local IP address (ILA).	0.0.0.0
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.	N/A
Global IP		
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.	0.0.0.0
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**.	N/A
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

28.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

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

Step 2. Enter 2 to display **Menu 15.2 - NAT Server Setup** as shown next.



```
            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:
```

Figure 28-8 Menu 15.2.1 NAT Server Setup

Step 3. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

Step 4. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

Step 5. Press [ENTER] at the “Press ENTER to confirm …” prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

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.

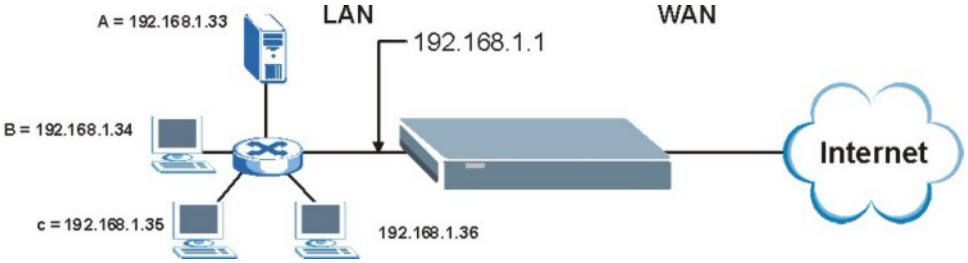


Figure 28-9 Multiple Servers Behind NAT Example

28.5 General NAT Examples

The following are some examples of NAT configuration.

28.5.1 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.

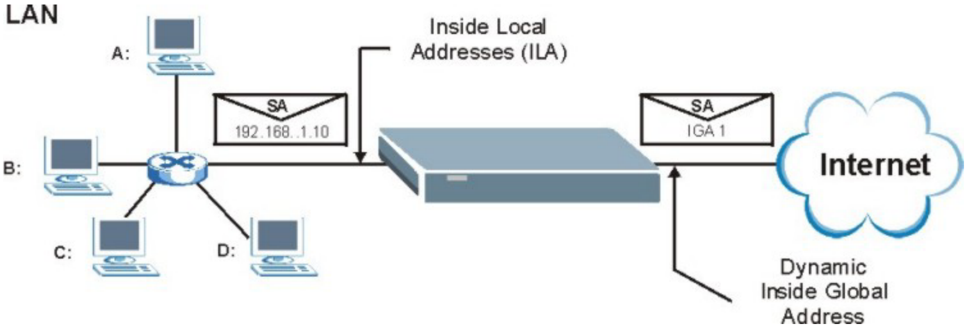
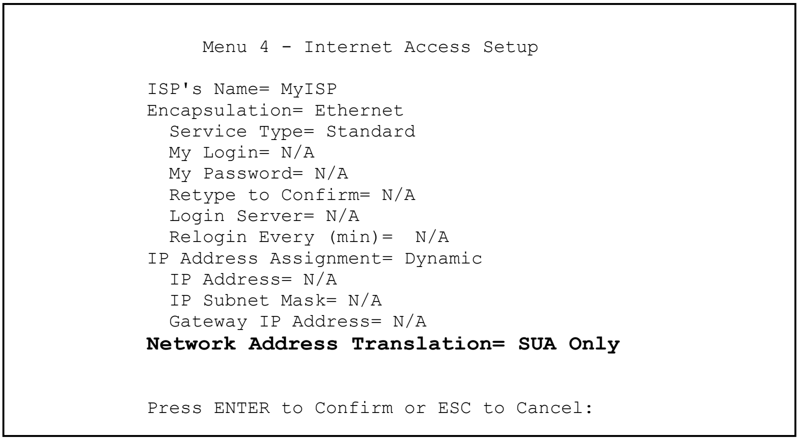


Figure 28-10 NAT Example 1



```
     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:
```

Figure 28-11 Menu 4 Internet Access & NAT Example

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 28.5.* The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

28.5.2 Example 2: Internet Access with an Inside Server

The dynamic Inside Global Address is assigned by the ISP.

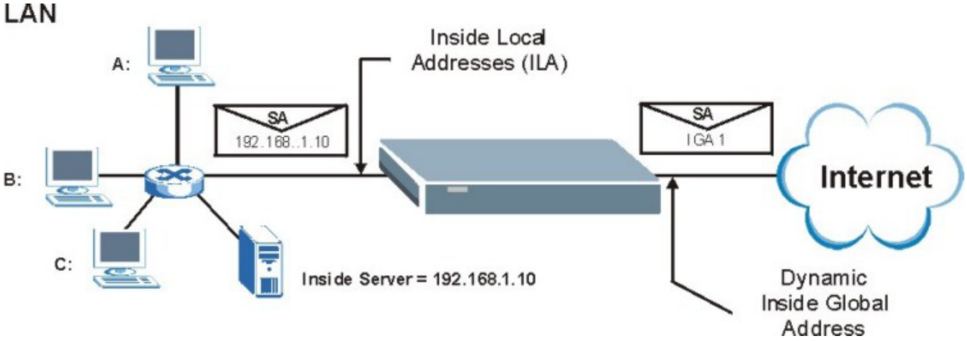
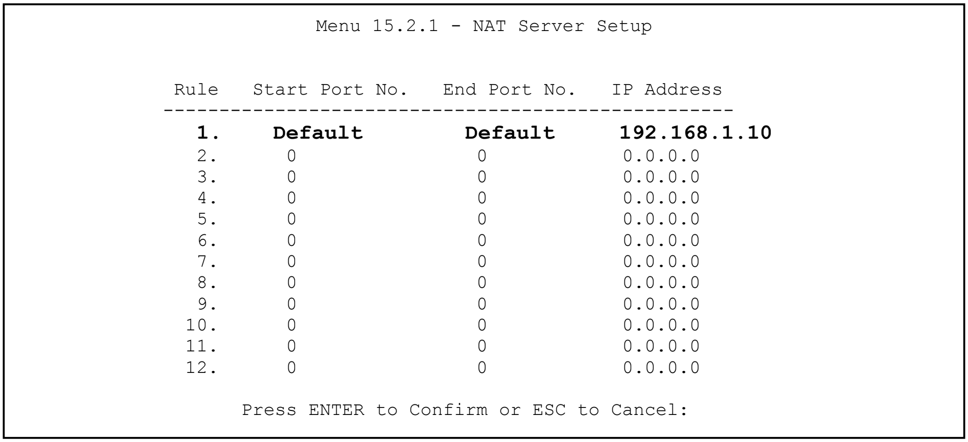

LAN
A:
B:
C:
Inside Local Addresses (ILA)
SA
192.168.1.10
SA
IGA 1
Internet
Inside Server = 192.168.1.10
Dynamic Inside Global Address

Figure 28-12 NAT Example 2

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



```
                        Menu 15.2.1 - 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:
```

Figure 28-13 Menu 15.2.1 Specifying an Inside Server

28.5.3 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.

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

Rule 2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

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

Rule 4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

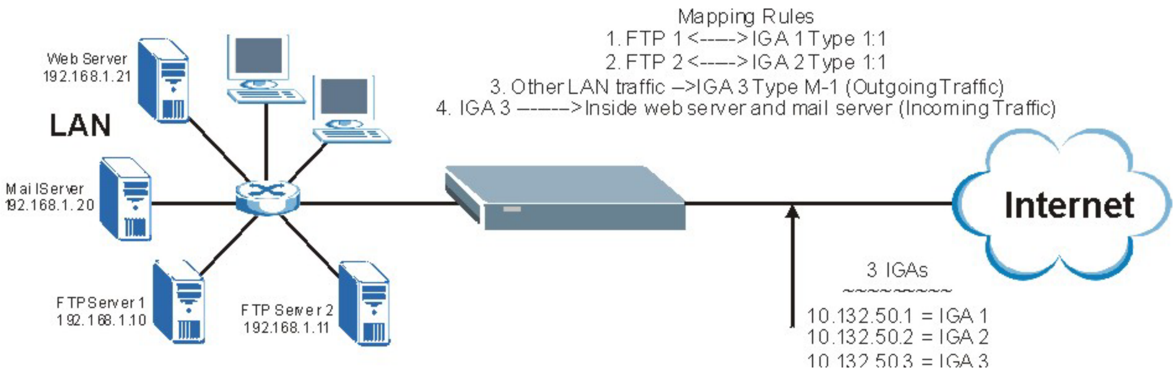


Figure 28-14 NAT Example 3

Step 1. In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in *Figure 28-15*.

Step 2. Then enter 15 from the main menu.

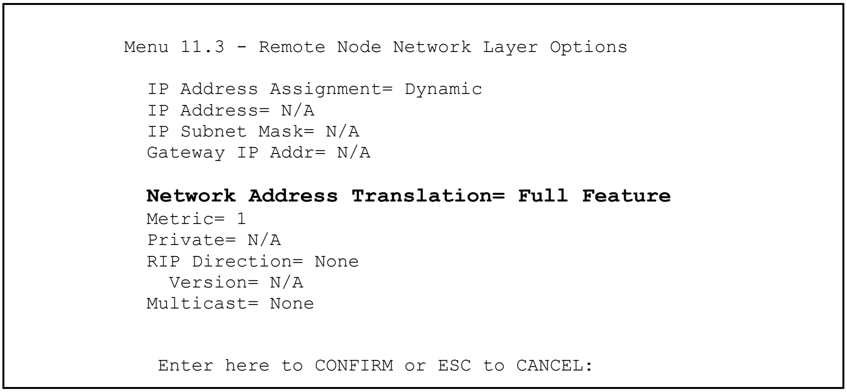
Step 3. Enter 1 to configure the Address Mapping Sets.

Step 4. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

Step 5. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 28-16).*

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

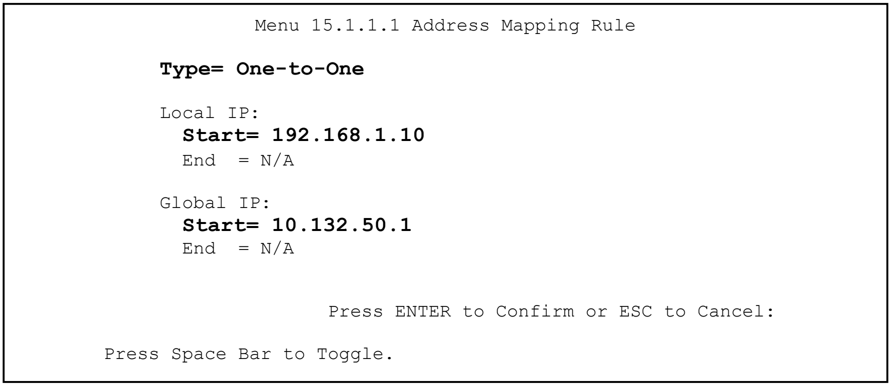
Step 7. When finished, menu 15.1.1.1 should look like as shown in *Figure 28-17.*



```
          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:
```

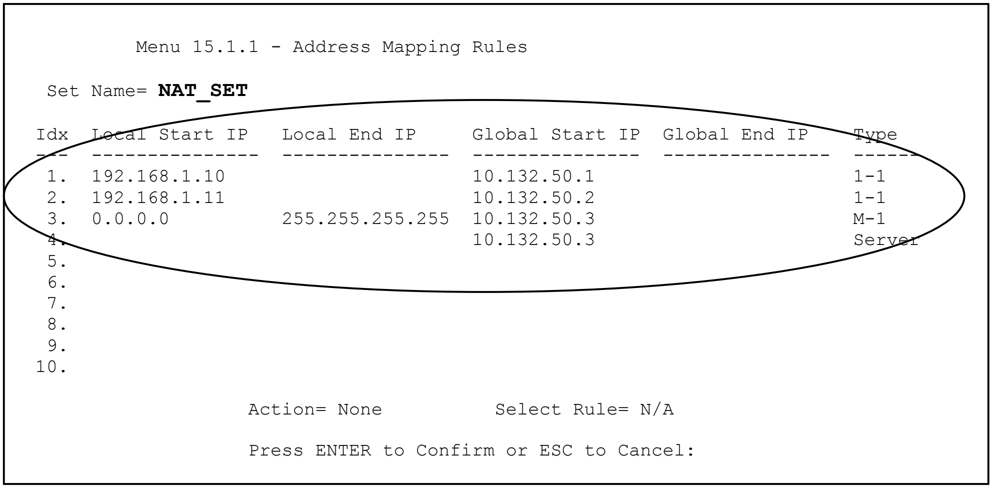
Figure 28-15 Example 3: Menu 11.3

The following figures show how to configure the first rule.



```
                      Menu 15.1.1.1 Address Mapping Rule

              Type= One-to-One

              Local IP:
                Start= 192.168.1.10
                End  = N/A

              Global IP:
                Start= 10.132.50.1
                End  = N/A


                             Press ENTER to Confirm or ESC to Cancel:

         Press Space Bar to Toggle.
```

Figure 28-16 Example 3: Menu 15.1.1.1



```
         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:
```

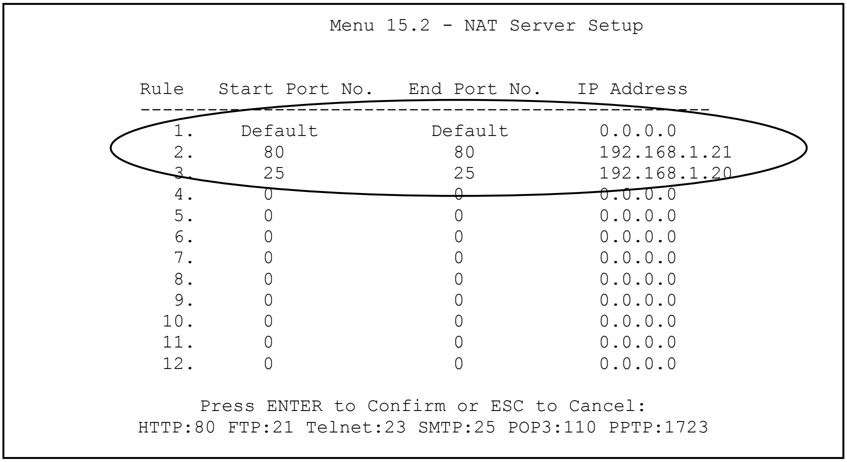
Figure 28-17 Example 3: Final Menu 15.1.1

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

Step 8. Enter 15 from the main menu.

Step 9. Enter 2 in **Menu 15 - NAT Setup**.

Step 10. Enter 1 in **Menu 15.2 - NAT Server Setup** to see the following menu. Configure it as shown.



```
                     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
```

Example 3: Menu 15.2

28.5.4 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.

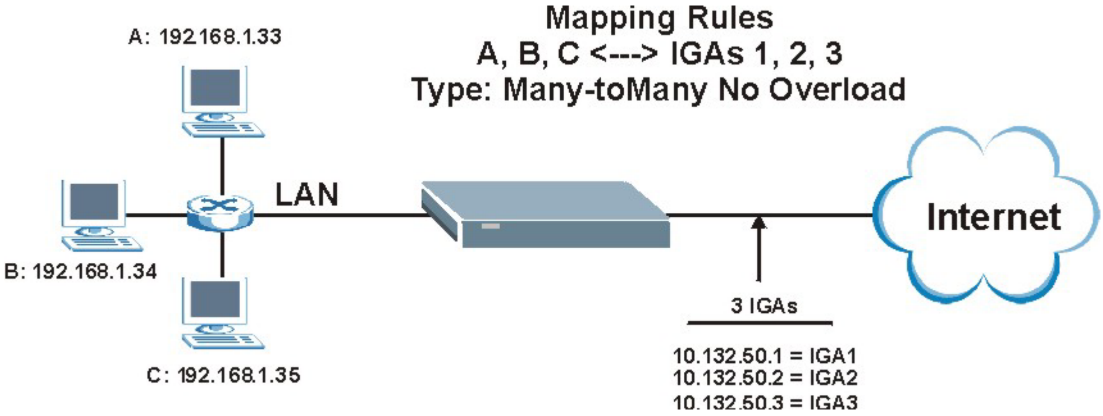
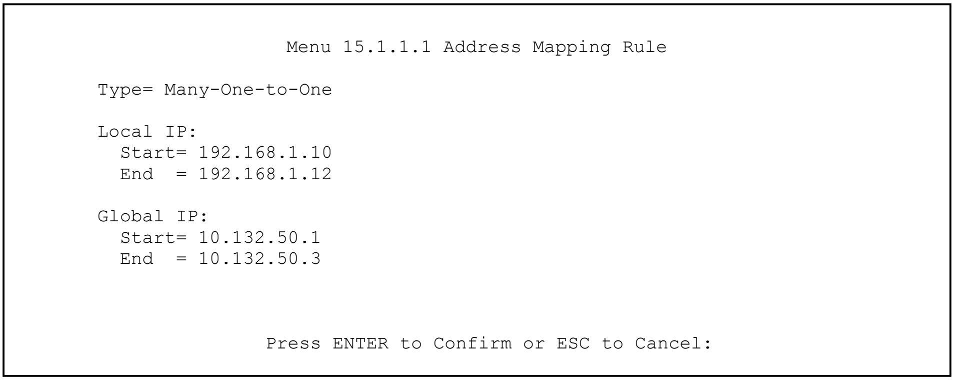


Figure 28-18 NAT Example 4

Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won’t work through NAT even when using One-to-One **and** Many-to-Many No Overload **mapping types.**

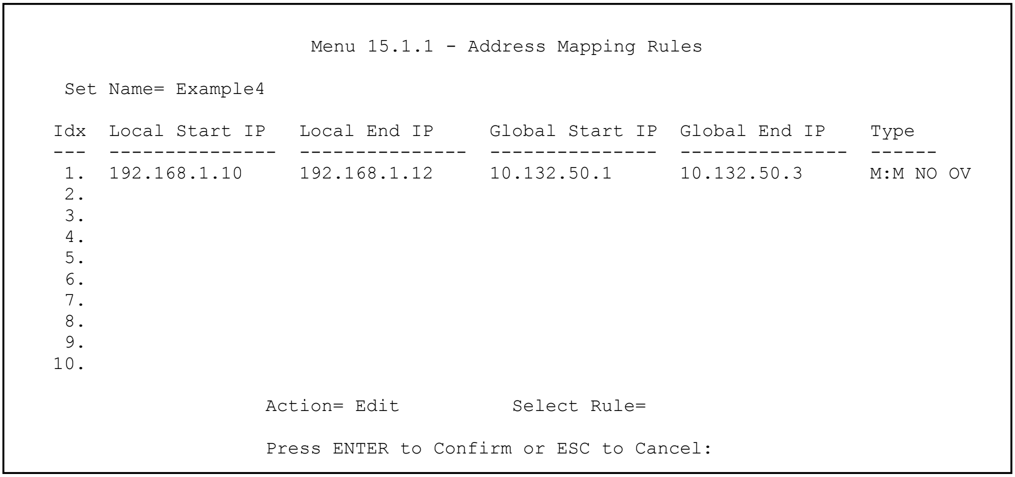
Follow the steps outlined in example 3 to configure these two menus as follows.



```
                        Menu 15.1.1.1 Address Mapping Rule

       Type= Many-One-to-One

       Local IP:
         Start= 192.168.1.10
         End  = 192.168.1.12

       Global IP:
         Start= 10.132.50.1
         End  = 10.132.50.3



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

Figure 28-19 Example 4: Menu 15.1.1.1 Address Mapping Rule

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



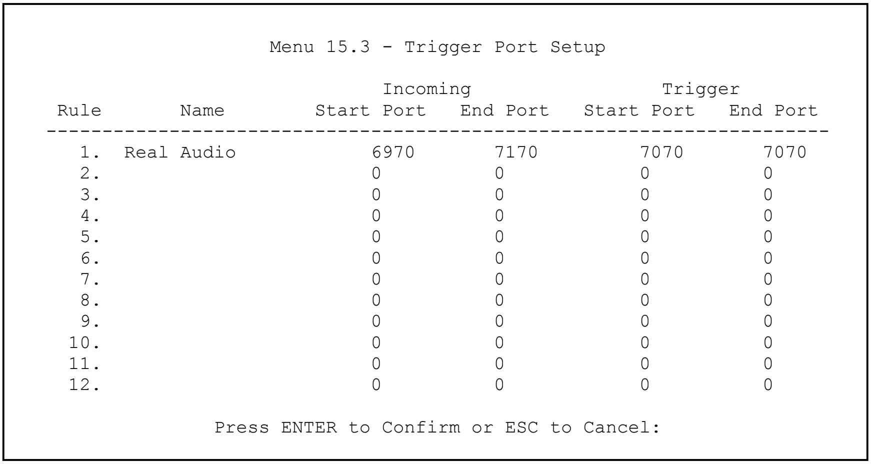
```
                         Menu 15.1.1 - Address Mapping Rules

   Set Name= Example4

  Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
  ---  ---------------  ---------------  ---------------  ---------------  ------
   1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M:M NO OV
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
  10.
                    Action= Edit          Select Rule=

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

Figure 28-20 Example 4: Menu 15.1.1 Address Mapping Rules

28.6 Configuring Trigger Port Forwarding

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

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



```
                        Menu 15.3 - Trigger Port Setup

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

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

Figure 28-21 Menu 15.3 Trigger Port Setup

The following table describes the fields in this screen.

Table 28-5 Menu 15.3 Trigger Port Setup

FIELD	DESCRIPTION	EXAMPLE
Rule	This is the rule index number.	1
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.	Real Audio
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The 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.	6970
End Port	Enter a port number or the ending port number in a range of port numbers.	7170
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the 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.	7070

Table 28-5 Menu 15.3 Trigger Port Setup

FIELD	DESCRIPTION	EXAMPLE
End Port	Enter a port number or the ending port number in a range of port numbers.	7070
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

Chapter 29
Enabling the Firewall

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

29.1 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.

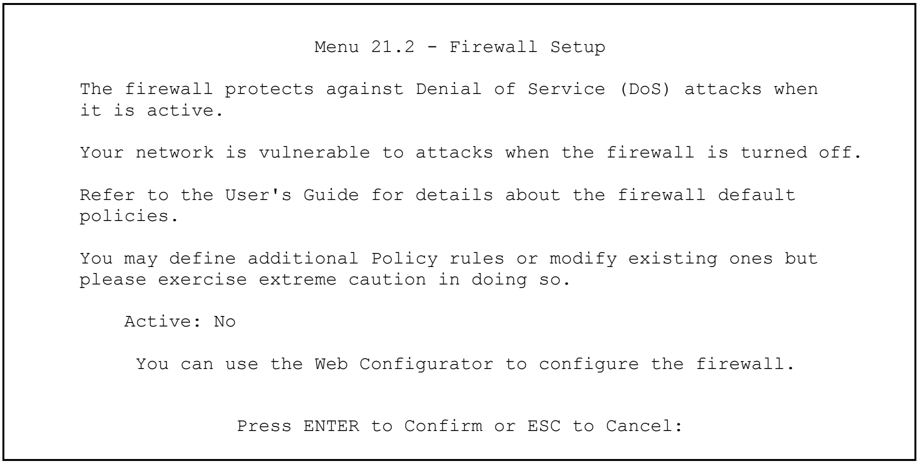
29.2 Access Methods

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.

29.3 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.



```
                    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:
```

Figure 29-1 Menu 21.2 Firewall Setup

Use the web configurator or the command interpreter to configure the firewall rules.

Part VIII:

SMT Advanced Management

This part discusses filtering setup, SNMP, system security, system information and diagnosis, firmware and configuration file maintenance, system maintenance, remote management and call scheduling.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 30
Filter Configuration

This chapter shows you how to create and apply filters.

30.1 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.

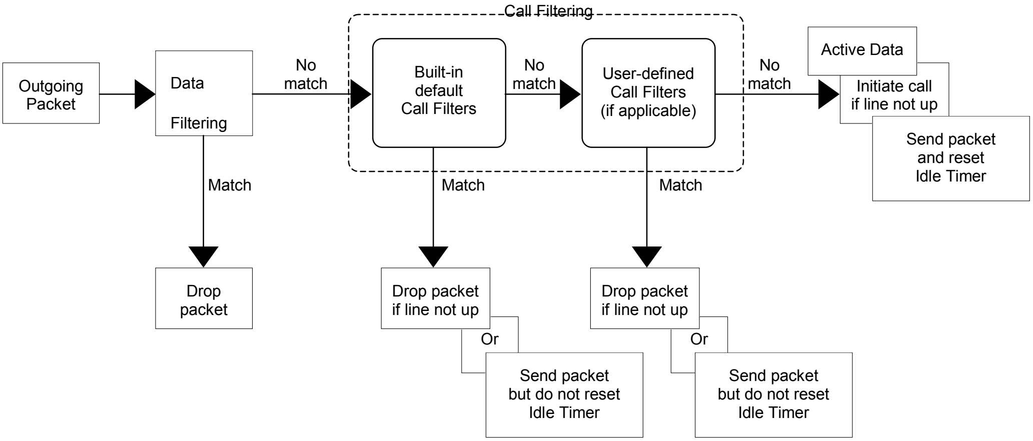

Call Filtering
Outgoing Packet
Data Filtering
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not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

Figure 30-1 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.

30.1.1 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 cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also *Figure 30-7* for the logic flow when executing an IP filter.

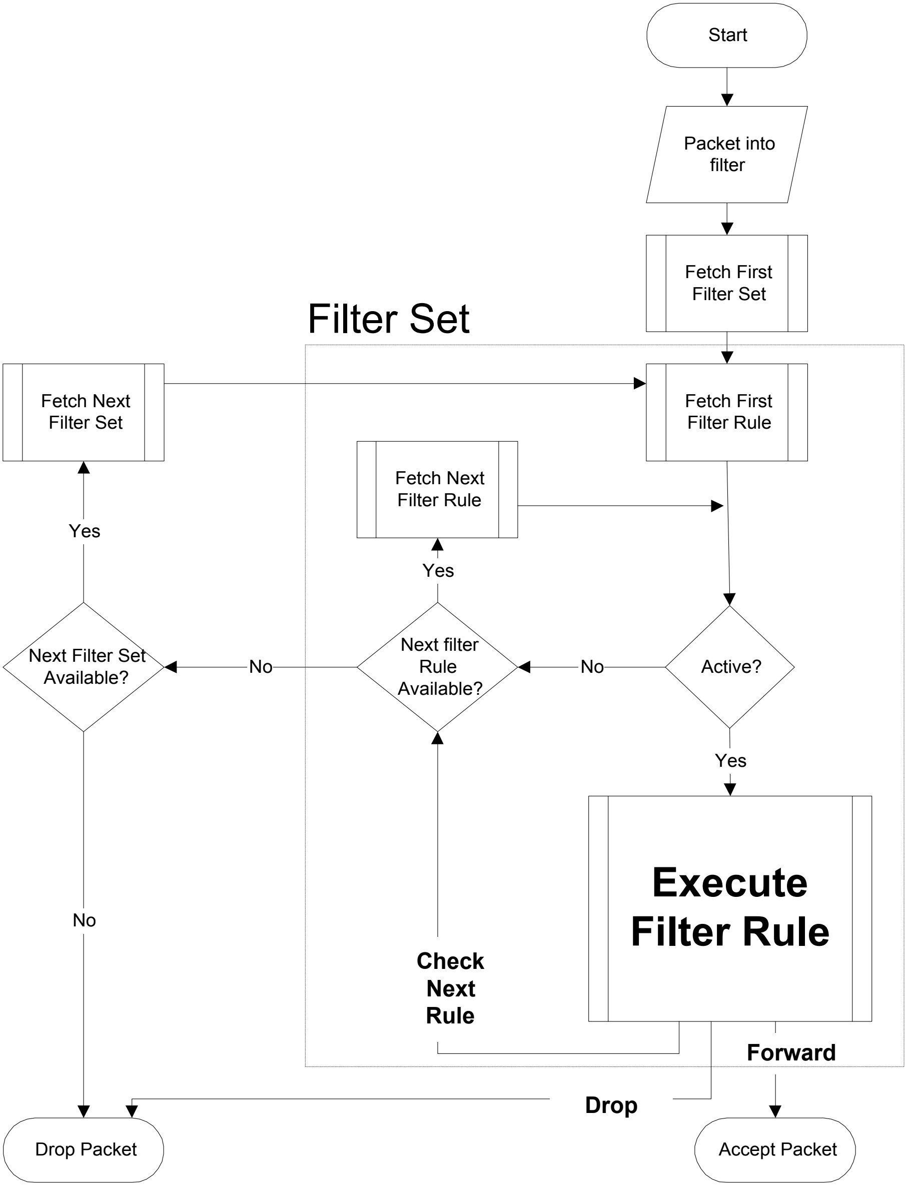


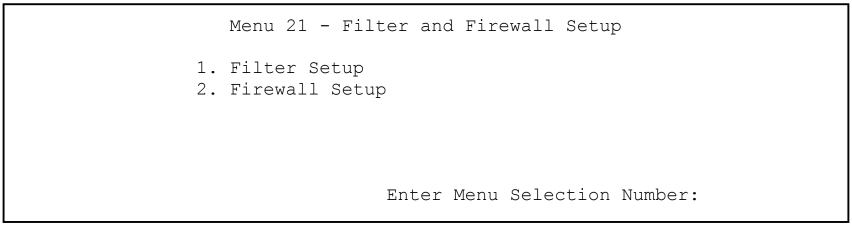
Figure 30-2 Filter Rule Process

You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

30.2 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.

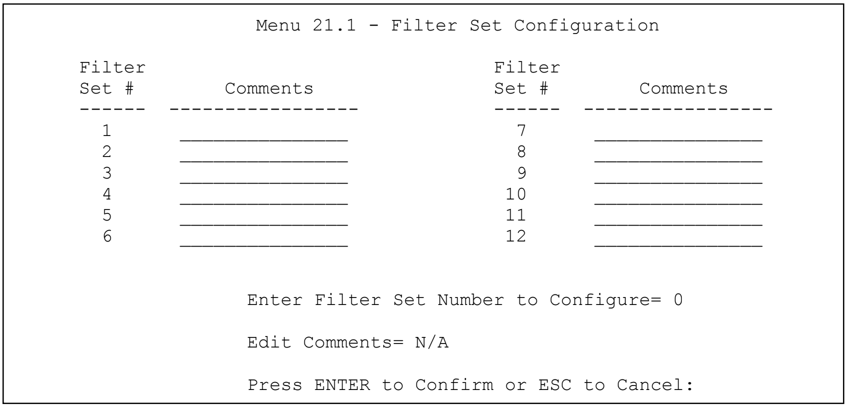
Step 1. Enter 21 in the main menu to open menu 21.



```
                    Menu 21 - Filter and Firewall Setup

                 1. Filter Setup
                 2. Firewall Setup




                                 Enter Menu Selection Number:
```

Figure 30-4 Menu 21: Filter and Firewall Setup

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



```
                       Menu 21.1 - Filter Set Configuration

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


                      Enter Filter Set Number to Configure= 0

                      Edit Comments= N/A

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

Figure 30-5 Menu 21.1: Filter Set Configuration

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

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

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

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

Table 30-1 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 30-2 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

30.2.1 Configuring a Filter Rule

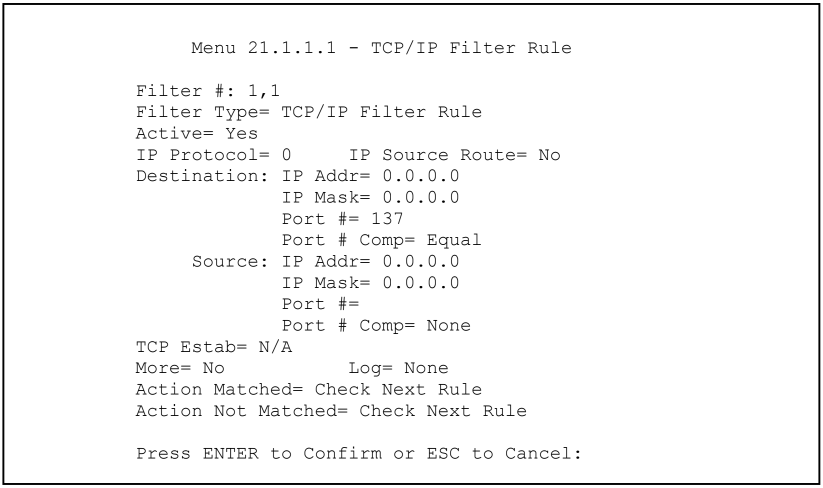
To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

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.

30.2.2 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.



```
          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:
```

Figure 30-6 Menu 21.1.1.1 TCP/IP Filter Rule

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

Table 30-3 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

Table 30-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	OPTIONS
IP Mask	Enter the IP mask to apply to the **Destination: IP Addr**.	0.0.0.0
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given **in Destination: Port #**.	**None** **Less** **Greater** **Equal** **Not Equal**
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Source: IP Addr**.	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**.	**None** **Less** **Greater** **Equal** **Not Equal**
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored.	**Yes** **No**
More	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	**Yes** **No**

Table 30-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	OPTIONS
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
When you have **Menu 21.1.1.1 - TCP/IP Filter Rule** configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.		

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

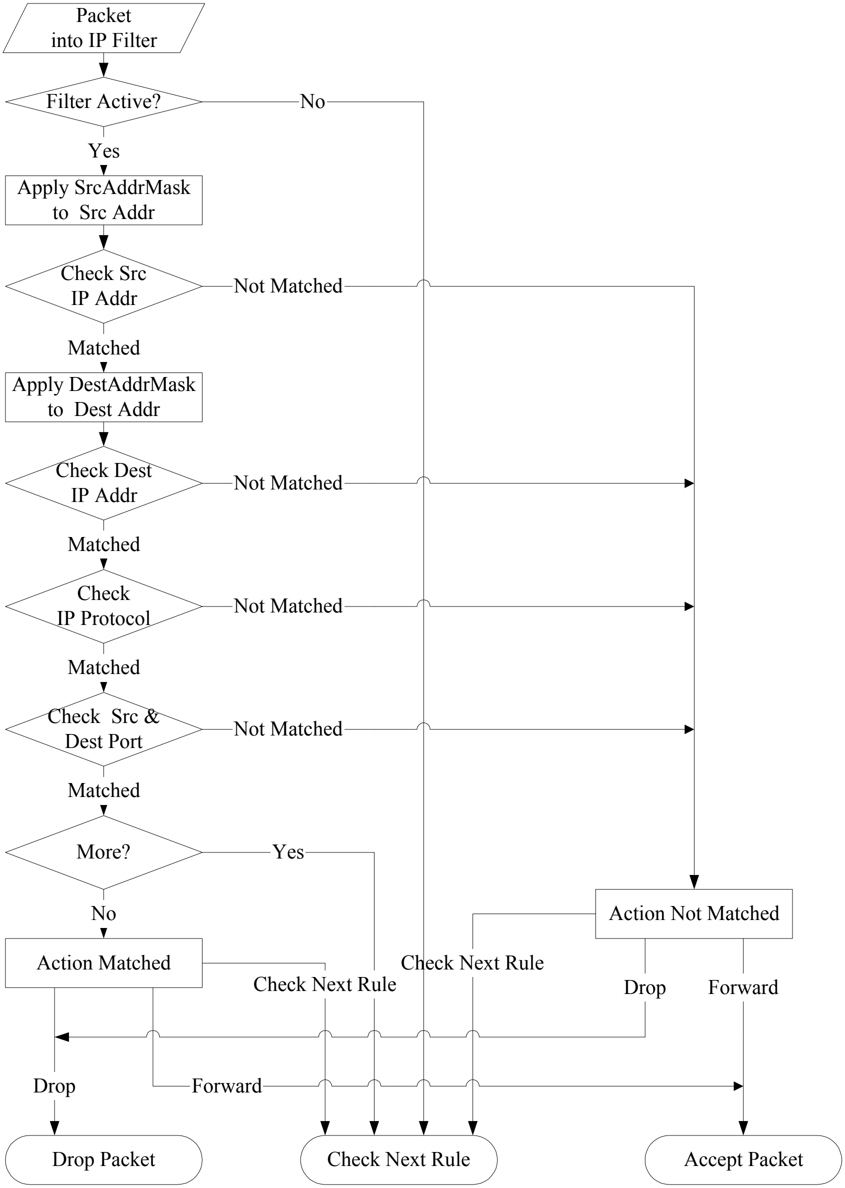


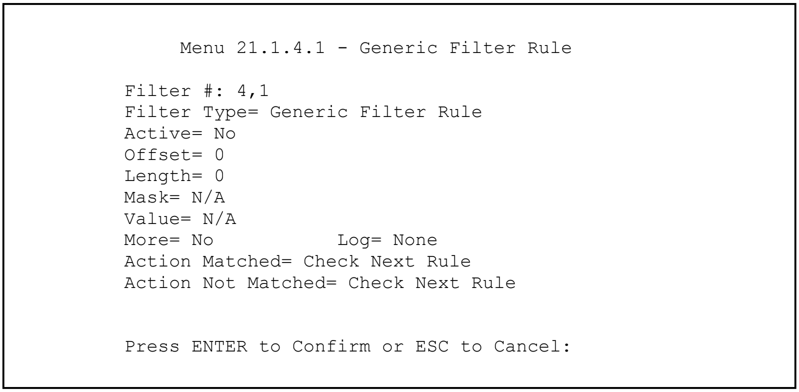
Figure 30-7 Executing an IP Filter

30.2.3 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.



```
                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:
```

Figure 30-8 Menu 21.1.4.1 Generic Filter Rule

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

Table 30-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	

Table 30-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	**Generic Filter Rule** **TCP/IP Filter Rule**
Active	Select **Yes** to turn on the filter rule or **No** to turn it off.	**Yes / No**
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0-255
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0-8
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**.	**Yes** **No**
Log	Select the logging option from the following: **None** - No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a packet matching the rule.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
Once you have completed filling in **Menu 21.4.1.1 - Generic Filter Rule**, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.		

30.3 Example Filter

Let's look at an example to block outside users from accessing the Prestige via telnet.

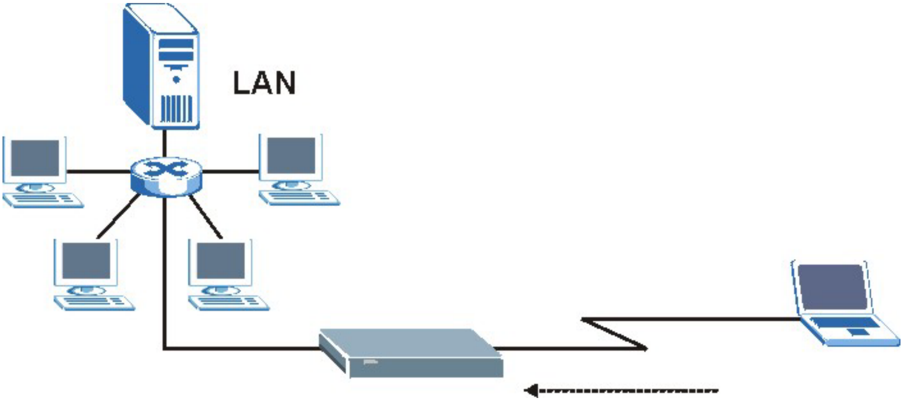


Figure 30-9 Telnet Filter Example

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

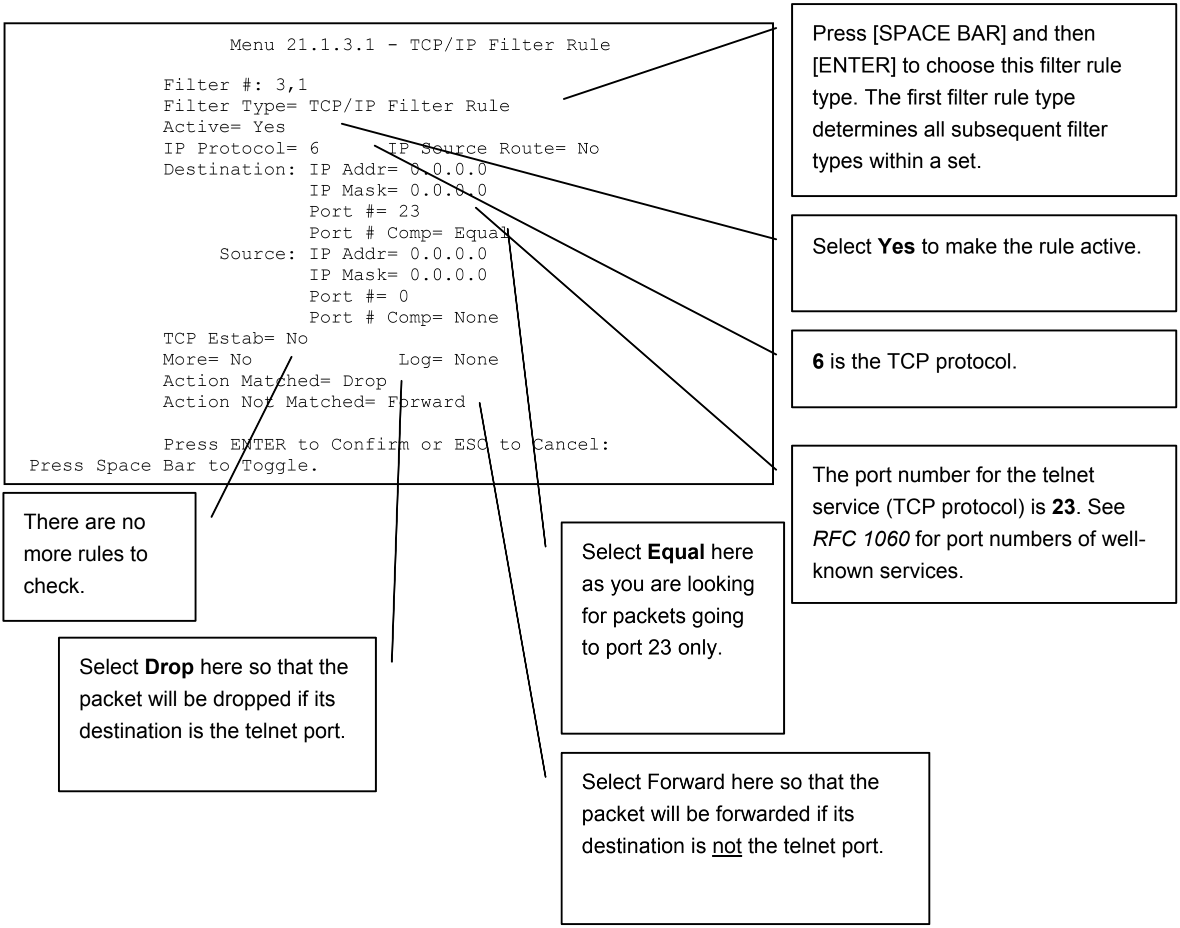
Step 2. Enter 1 to open **Menu 21.1 - Filter Set Configuration**.

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

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

Step 5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.

Step 6. Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.



```
                    Menu 21.1.3.1 - TCP/IP Filter Rule

              Filter #: 3,1
              Filter Type= TCP/IP Filter Rule
              Active= Yes
              IP Protocol= 6      IP Source Route= No
              Destination: IP Addr= 0.0.0.0
                           IP Mask= 0.0.0.0
                           Port #= 23
                           Port # Comp= Equal
                   Source: IP Addr= 0.0.0.0
                           IP Mask= 0.0.0.0
                           Port #= 0
                           Port # Comp= None
              TCP Estab= No
              More= No                 Log= None
              Action Matched= Drop
              Action Not Matched= Forward

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

Press [SPACE BAR] and then [ENTER] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

Select **Yes** to make the rule active.

6 is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

There are no more rules to check.

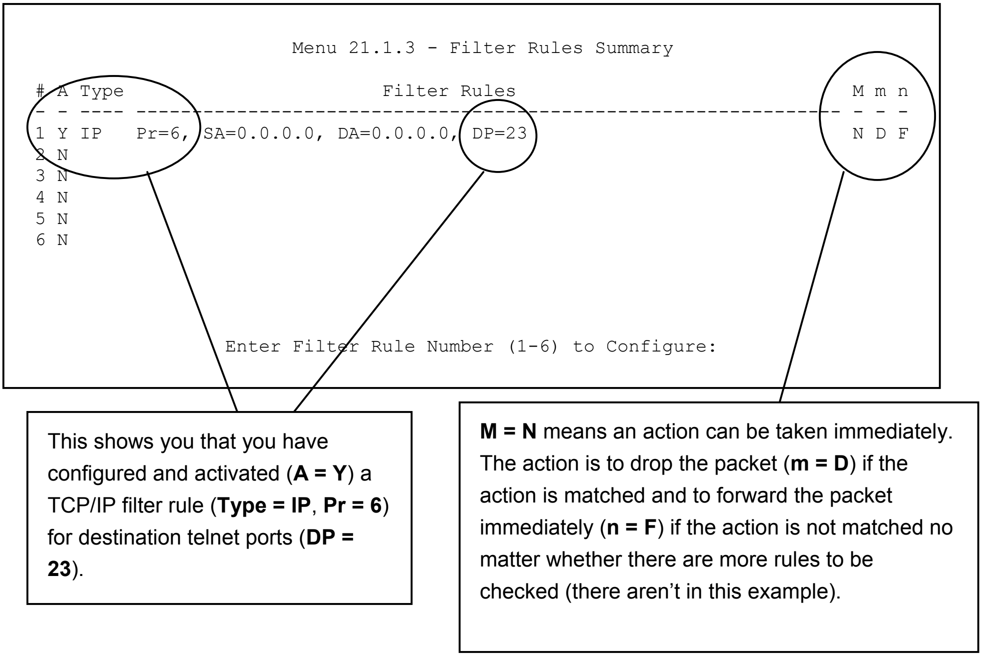
Select **Equal** here as you are looking for packets going to port 23 only.

Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Select Forward here so that the packet will be forwarded if its destination is not the telnet port.

Figure 30-10 Example Filter: Menu 21.1.3.1

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.



```
                    Menu 21.1.3 - Filter Rules Summary

 # A Type                     Filter Rules                                      M m n
 - - ---- -------------------------------------------------------------------- - - -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                                   N D F
 2 N
 3 N
 4 N
 5 N
 6 N



                 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).

Figure 30-11 Example Filter Rules Summary: Menu 21.1.3

After you've created the filter set, you must apply it.

Step 1. Enter 11 from the main menu to go to menu 11.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].

Step 3. This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in *Figure 30-14*.

Step 4. Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

30.4 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.

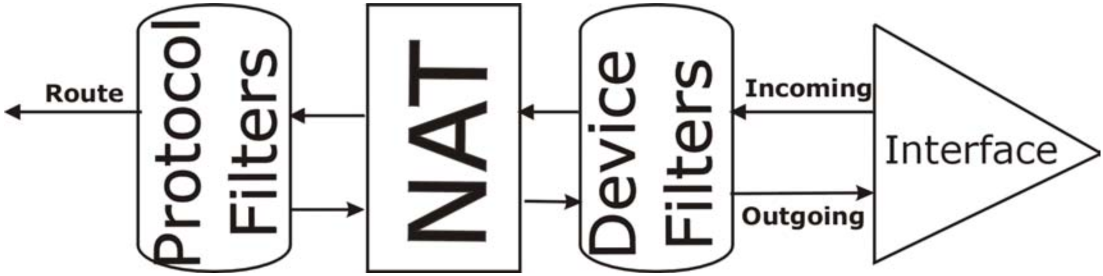


Figure 30-12 Protocol and Device Filter Sets

30.5 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.

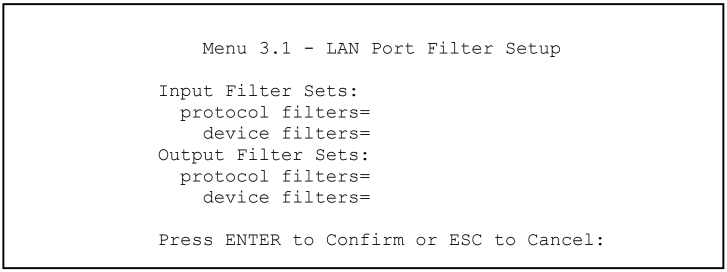
30.6 Applying a Filter

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.

If you do not activate the firewall, it is advisable to apply filters.

30.6.1 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.

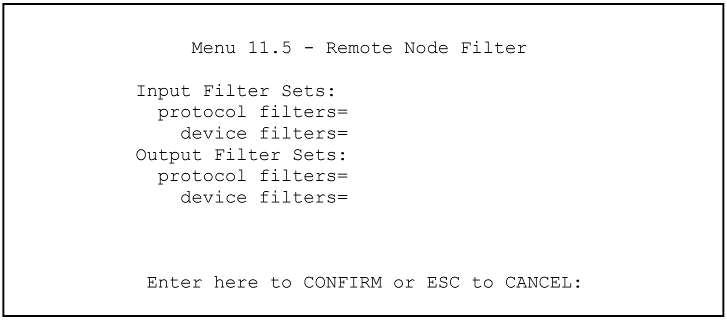


```
    Menu 3.1 - LAN Port Filter Setup

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

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

Figure 30-13 Filtering LAN Traffic

30.6.2 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, and block incoming telnet, FTP and HTTP connections.



```
                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 30-14 Filtering Remote Node Traffic

Chapter 31
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

31.1 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.

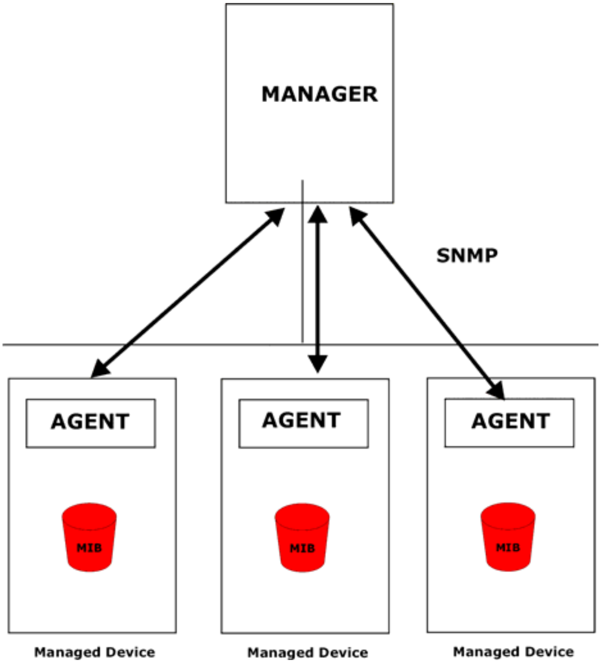


Figure 31-1 SNMP Management Model

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:

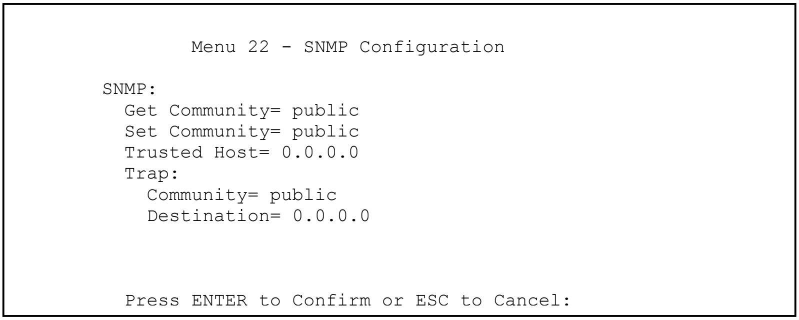
- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed 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.

31.2 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.

31.3 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.



```
                Menu 22 - SNMP Configuration

        SNMP:
          Get Community= public
          Set Community= public
          Trusted Host= 0.0.0.0
          Trap:
            Community= public
            Destination= 0.0.0.0



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

Figure 31-2 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 31-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the **Set** community, which is the password for incoming Set requests from the management station.	public
Trusted Host	If you enter a trusted host, your 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.	0.0.0.0
Trap:		
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	public
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

31.4 SNMP Traps

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

Table 31-2 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.
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 31-3 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
…	…
13	12
14	xDSL

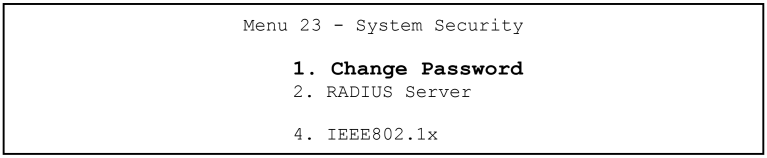
Chapter 32 System Security

This chapter describes how to configure the system security on the Prestige.

32.1 System Security

You can configure the system password, an external RADIUS server and 802.1x in this menu.

32.1.1 System Password



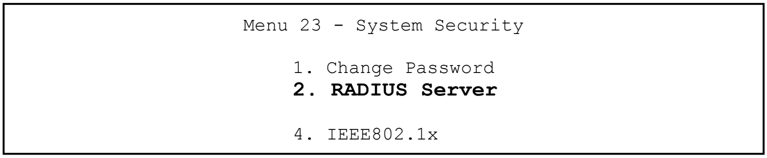
```
                    Menu 23 - System Security

                          1. Change Password
                          2. RADIUS Server

                          4. IEEE802.1x
```

Figure 32-1 Menu 23 System Security

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.

32.1.2 Configuring External RADIUS Server

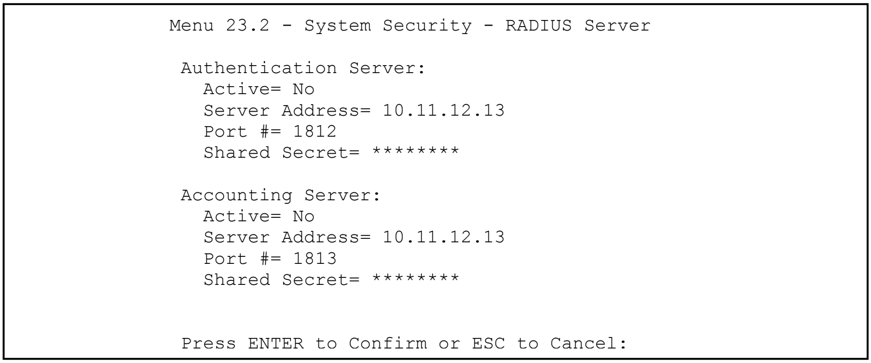
Enter 23 in the main menu to display **Menu 23 – System Security**.



```
                    Menu 23 - System Security

                          1. Change Password
                          2. RADIUS Server

                          4. IEEE802.1x
```

Figure 32-2 Menu 23 System Security

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 - System Security-RADIUS Server** as shown next.



```
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:
```

Figure 32-3 Menu 23.2 System Security : RADIUS Server

The following table describes the fields in this screen.

Table 32-1 Menu 23.2 System Security : RADIUS Server

FIELD	DESCRIPTION	EXAMPLE
Authentication Server		
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server.	**No**
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.	10.11.12.13
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.	**1812**
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.	**No**

Table 32-1 Menu 23.2 System Security : RADIUS Server

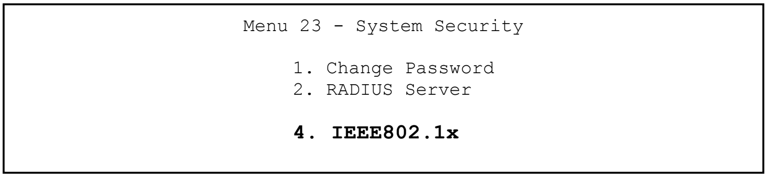
FIELD	DESCRIPTION	EXAMPLE
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.	10.11.12.13
Port	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.	**1813**
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.		

32.1.3 802.1x

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.

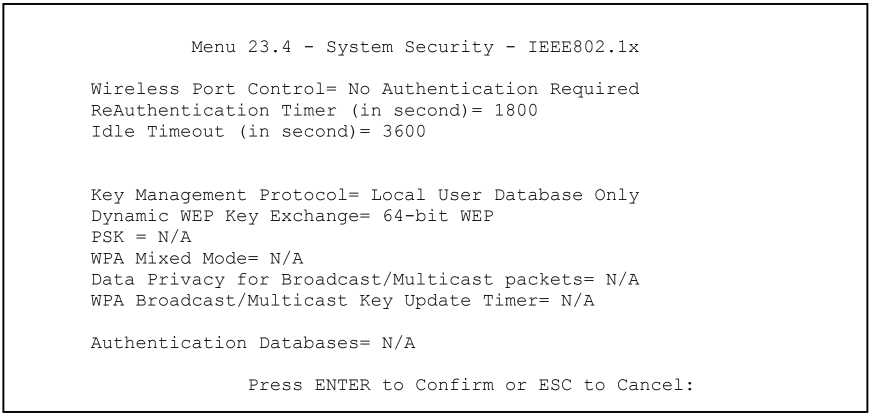
Step 1. From the main menu, enter 23 to display **Menu23 – System Security**.



```
                    Menu 23 - System Security

                        1. Change Password
                        2. RADIUS Server

                        4. IEEE802.1x
```

Figure 32-4 Menu 23 System Security

Step 2. Enter 4 to display **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= Local User Database Only
 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:
```

Figure 32-5 Menu 23.4 System Security : IEEE802.1x

The following table describes the fields in this menu.

Table 32-2 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).

Table 32-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Idle Timeout (in second)	The ZyAIR 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].
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**. Local user database may not be used. 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 ZyAIR 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 ZyAIR default is 1800 seconds (30 minutes).

Table 32-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this field to decide which database the ZyAIR should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database** with **802.1x Key Management Protocol**. Select **Local User Database Only** to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password. Select **RADIUS Only** to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.
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.	

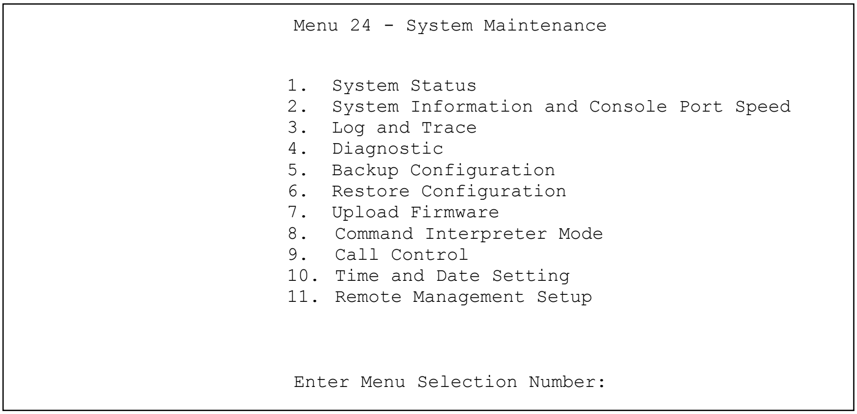
Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the Prestige for authentication.

Chapter 33
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.



```
                    Menu 24 - System Maintenance


                    1.  System Status
                    2.  System Information and Console Port Speed
                    3.  Log and Trace
                    4.  Diagnostic
                    5.  Backup Configuration
                    6.  Restore Configuration
                    7.  Upload Firmware
                    8.   Command Interpreter Mode
                    9.   Call Control
                    10.  Time and Date Setting
                    11.  Remote Management Setup



                    Enter Menu Selection Number:
```

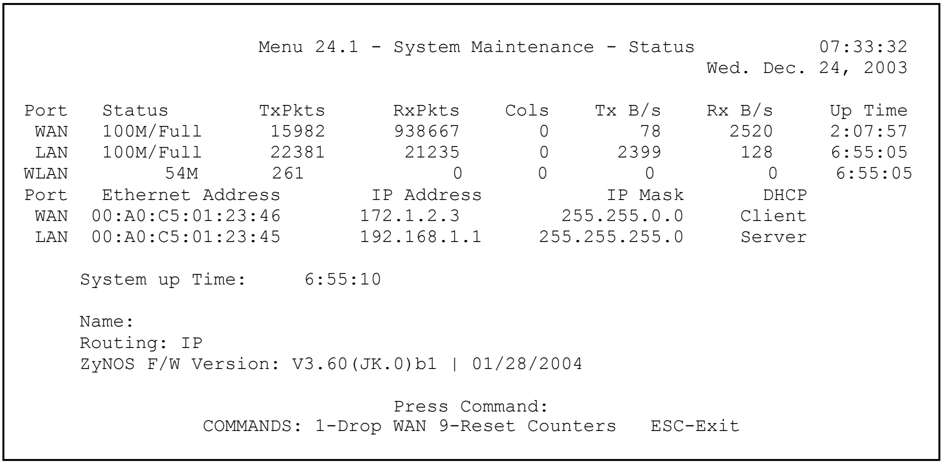
Figure 33-1 Menu 24 System Maintenance

33.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next *Figure 33-2*. 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.



```
                       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.0)b1 | 01/28/2004

                            Press Command:
                  COMMANDS: 1-Drop WAN 9-Reset Counters   ESC-Exit
```

Figure 33-2 Menu 24.1 System Maintenance : Status

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 33-1 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.

Table 33-1 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
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.	

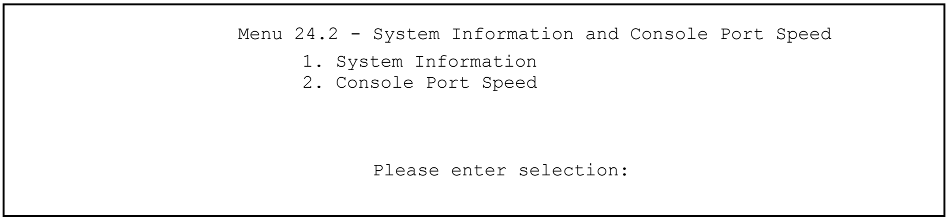
33.2 System Information

To get to the System Information:

Step 2. Enter 24 to display **Menu 24** — **System Information and Console Port Speed**.

Step 3. Enter 2 to display **Menu 24.2** — **System Information**.

Step 4. From this menu you have two choices as shown in the next figure:

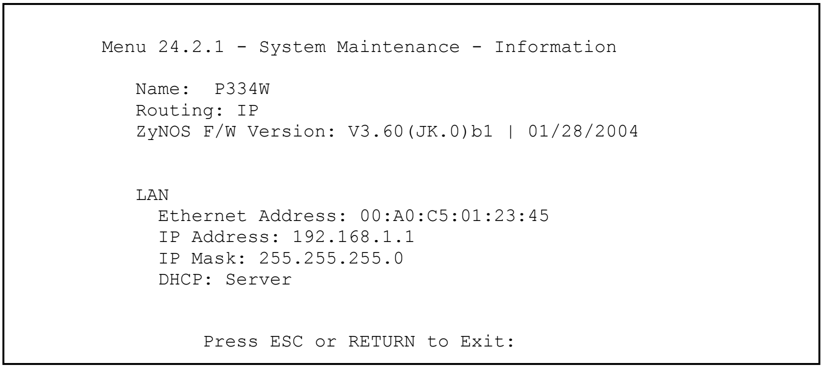


```
              Menu 24.2 - System Information and Console Port Speed
                    1. System Information
                    2. Console Port Speed



                          Please enter selection:
```

Figure 33-3 Menu 24.2 System Information and Console Port Speed

33.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.



```
        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
             IP Address: 192.168.1.1
             IP Mask: 255.255.255.0
             DHCP: Server


                 Press ESC or RETURN to Exit:
```

Figure 33-4 Menu 24.2.1 System Maintenance : Information

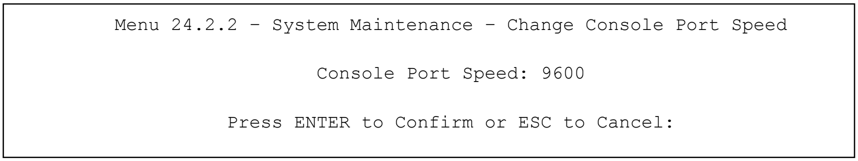
The following table describes the fields in this menu.

Table 33-2 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.

33.2.2 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.



```
          Menu 24.2.2 – System Maintenance – Change Console Port Speed

                           Console Port Speed: 9600

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

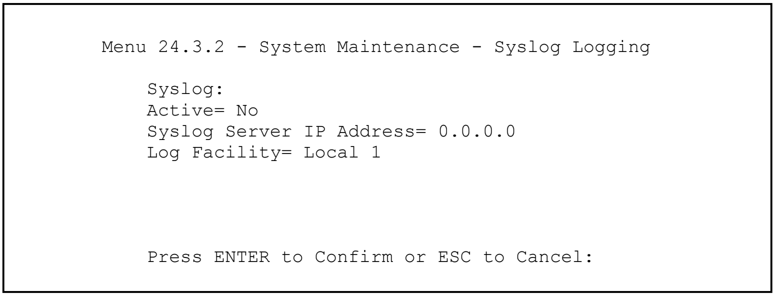
Figure 33-5 Menu 24.2.2 System Maintenance : Change Console Port Speed

33.3 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.

33.3.1 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.



```
        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:
```

Figure 33-6 Menu 24.3.2 System Maintenance : Syslog Logging

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 33-3 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.

Table 33-3 Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
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.
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:

1. CDR

```
CDR Message Format
            SdcmdSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String );
            String = board xx line xx channel xx, call xx, str
            board = the hardware board ID
            line = the WAN ID in a board
            Channel = channel ID within the WAN
            call = the call reference number which starts from 1 and increments by 1 for each new call
            str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
                        L02         Tunnel Connected(L2TP)
                        C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)

                        L02 Call Terminated
                        C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
```

2. Packet triggered

```
Packet triggered Message Format
SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
        String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
        Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
        Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f707172
7374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

3. Filter log

Filter log Message Format

```
        SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD

IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop
(D).
        Src: Source Address
        Dst: Destination Address
        prot: Protocol ("TCP","UDP","ICMP")
spo: Source port
dpo: Destination port
Mar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[ffffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[ffffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170  dpo=00021]}S04>R01mF
```

4. PPP log

PPP Log Message Format

```
SdcmdSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing
```

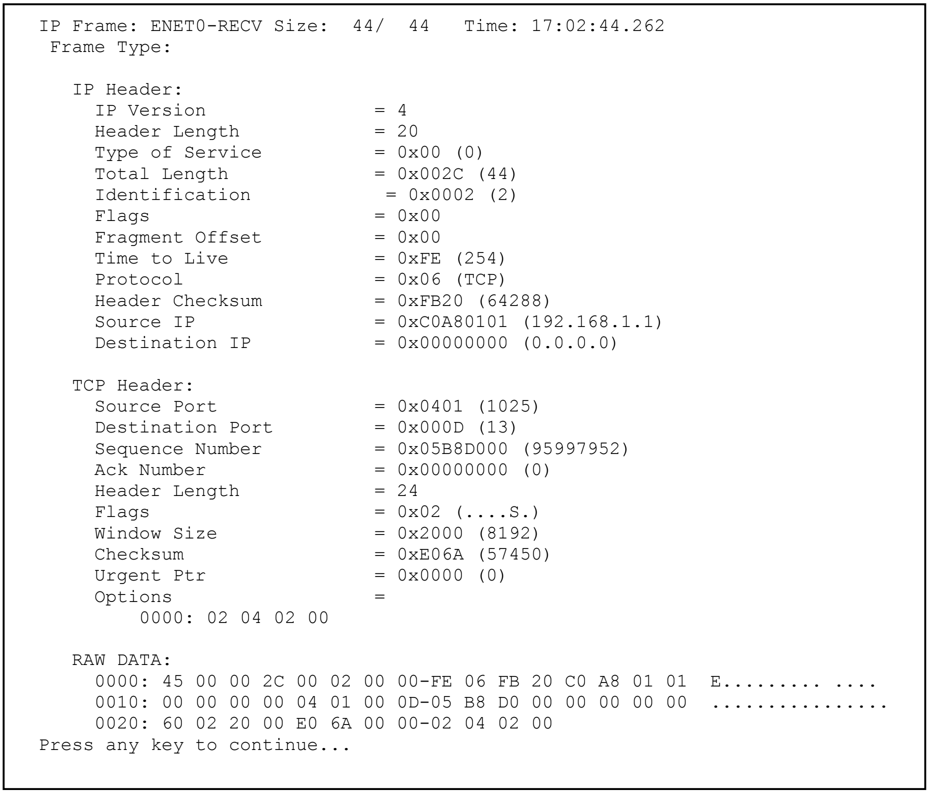
5. Firewall log

Firewall Log Message Format

```
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol ("TCP","UDP","ICMP", "IGMP", "GRE", "ESP")
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-2000       11:48:41 Local1.Notice    192.168.10.10    RAS: FW 172.21.1.80     :137  -
>172.21.1.80     :137  |UDP|default permit:<2,0>|B
08-01-2000       11:48:41 Local1.Notice    192.168.10.10    RAS: FW 192.168.77.88   :520  -
>192.168.77.88   :520  |UDP|default permit:<2,0>|B
08-01-2000       11:48:39 Local1.Notice    192.168.10.10    RAS: FW 172.21.1.50     ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-2000       11:48:39 Local1.Notice    192.168.10.10    RAS: FW 172.21.1.25     ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
```

33.3.2 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.



```
IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
 Frame Type:

   IP Header:
     IP Version                = 4
     Header Length             = 20
     Type of Service           = 0x00 (0)
     Total Length              = 0x002C (44)
     Identification             = 0x0002 (2)
     Flags                     = 0x00
     Fragment Offset           = 0x00
     Time to Live              = 0xFE (254)
     Protocol                  = 0x06 (TCP)
     Header Checksum           = 0xFB20 (64288)
     Source IP                 = 0xC0A80101 (192.168.1.1)
     Destination IP            = 0x00000000 (0.0.0.0)

   TCP Header:
     Source Port               = 0x0401 (1025)
     Destination Port          = 0x000D (13)
     Sequence Number           = 0x05B8D000 (95997952)
     Ack Number                = 0x00000000 (0)
     Header Length             = 24
     Flags                     = 0x02 (....S.)
     Window Size               = 0x2000 (8192)
     Checksum                  = 0xE06A (57450)
     Urgent Ptr                = 0x0000 (0)
     Options                   =
         0000: 02 04 02 00

   RAW DATA:
     0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E......... ....
     0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00  ................
     0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...
```

Figure 33-7 Call-Triggering Packet Example

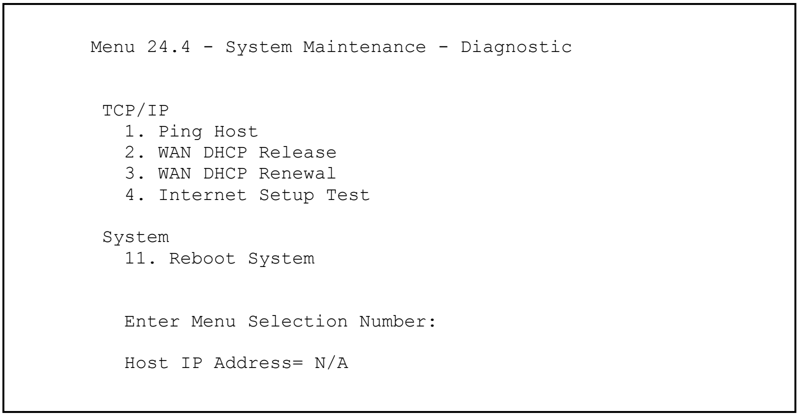
33.4 Diagnostic

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:

Step 1. From the main menu, type 24 to open **Menu 24 – System Maintenance**.

Step 2. From this menu, type 4 to open **Menu 24.4** – **System Maintenance** – **Diagnostic**.



```
      Menu 24.4 - System Maintenance - Diagnostic


       TCP/IP
         1. Ping Host
         2. WAN DHCP Release
         3. WAN DHCP Renewal
         4. Internet Setup Test

       System
         11. Reboot System


         Enter Menu Selection Number:

         Host IP Address= N/A
```

Figure 33-8 Menu 24.4 System Maintenance : Diagnostic

33.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 33-9*. 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.

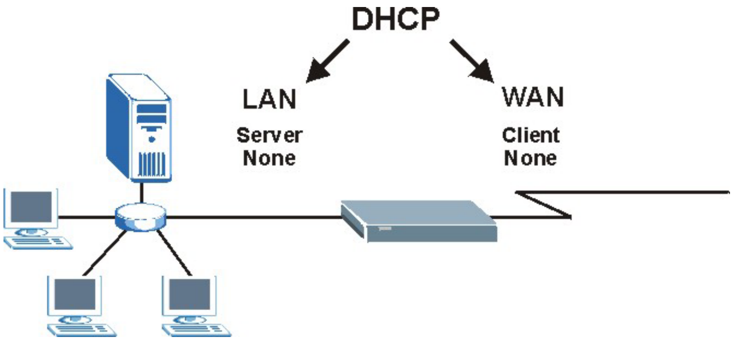


Figure 33-9 LAN & WAN DHCP

The following table describes the diagnostic tests available in menu 24.4 for your Prestige and associated connections.

Table 33-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the **Host IP Address** field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.
Internet Setup Test	Enter 4 to test the Internet setup. You can also test the Internet setup in **Menu 4 - Internet Access**. Please refer to the *Internet Access* chapter for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation.
Reboot System	Enter 11 to reboot the 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 34 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.

34.1 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.

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 not 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 34-1 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

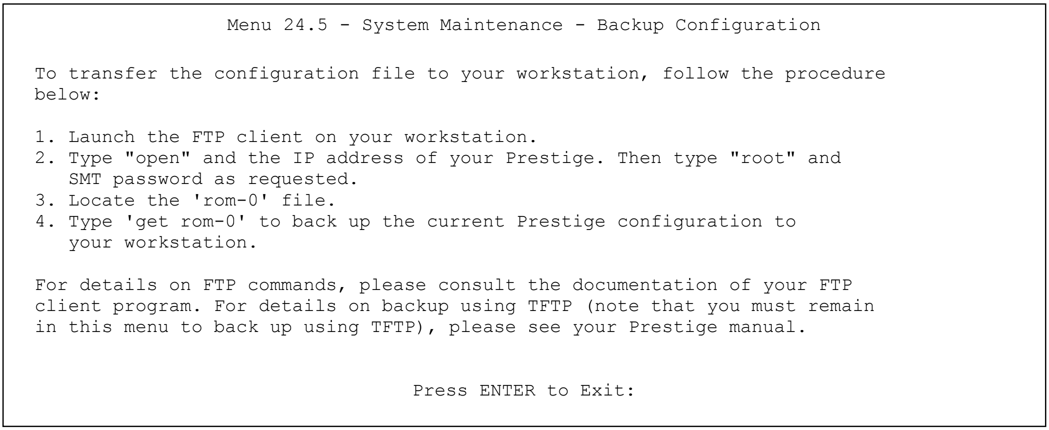
34.2 Backup Configuration

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.

34.2.1 Backup Configuration

Follow the instructions as shown in the next screen.



```
                    Menu 24.5 - System Maintenance - Backup Configuration

  To transfer the configuration file to your workstation, follow the procedure
  below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your 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:
```

Figure 34-1 Telnet in Menu 24.5

34.2.2 Using the FTP Command from the Command Line

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "get" to transfer files from the 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.

Step 7. Enter "quit" to exit the ftp prompt.

34.2.3 Example of FTP Commands from the Command Line

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 34-2 FTP Session Example

34.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 34-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. 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).

34.2.5 TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

1. You have disabled Telnet service in menu 24.11.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.

3. 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.
4. You have an SMT console session running.

34.2.6 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.

Step 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.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24** – **System Maintenance**.

Step 3. Enter command "sys stdio 0" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the 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.

34.2.7 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.

34.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 34-3 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.

Refer to *section 34.2.5* to read about configurations that disallow TFTP and FTP over WAN.

34.3 Restore Configuration

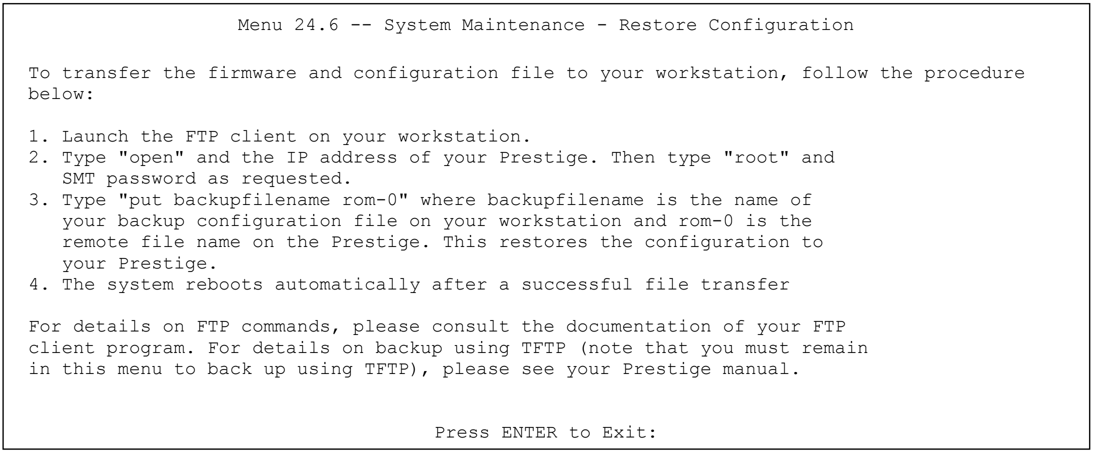
This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

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.

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE.

34.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.



```
                    Menu 24.6 -- System Maintenance - Restore Configuration

  To transfer the firmware and configuration file to your workstation, follow the procedure
  below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your 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:
```

Figure 34-3 Telnet into Menu 24.6

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

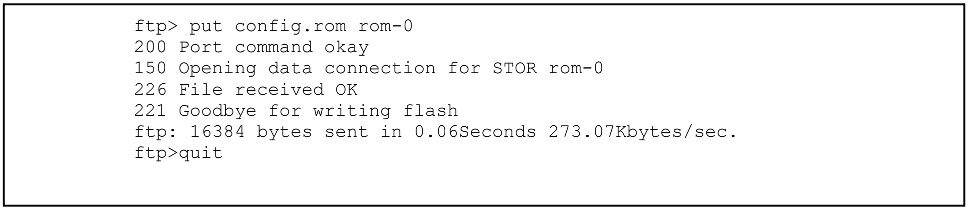
Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Find the "rom" file (on your computer) that you want to restore to your Prestige.

Step 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.

Step 8. Enter "quit" to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

34.3.2 Restore Using FTP Session Example



```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Figure 34-4 Restore Using FTP Session Example

Refer to *section 34.2.5* to read about configurations that disallow TFTP and FTP over WAN.

34.4 Uploading Firmware and Configuration Files

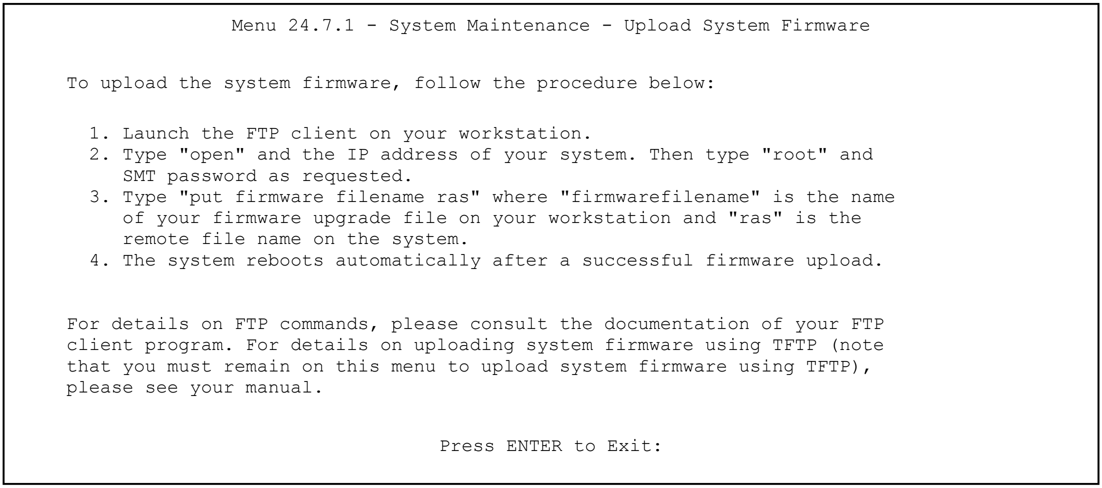
This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File**.

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE.

34.4.1 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.

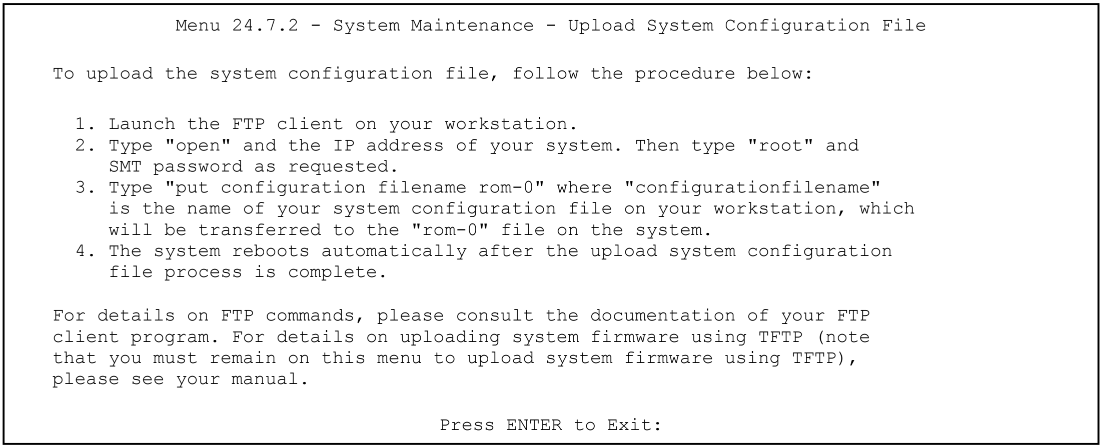


```
                    Menu 24.7.1 - System Maintenance - Upload System Firmware

     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:
```

Figure 34-5 Telnet Into Menu 24.7.1 Upload System Firmware

34.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.



```
               Menu 24.7.2 - System Maintenance - Upload System Configuration File

    To upload the system configuration file, follow the procedure below:

      1. Launch the FTP client on your workstation.
      2. Type "open" and the IP address of your system. Then type "root" and
         SMT password as requested.
      3. Type "put 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:
```

Figure 34-6 Telnet Into Menu 24.7.2 System Maintenance

To upload the firmware and the configuration file, follow these examples

34.4.3 FTP File Upload Command from the DOS Prompt Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

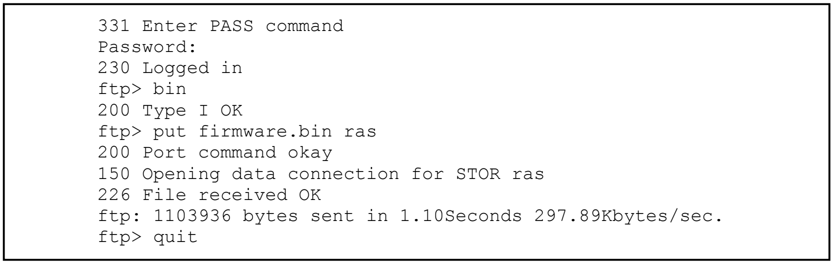
Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "put" to transfer files from the computer to the 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.

Step 7. Enter "quit" to exit the ftp prompt.

The Prestige automatically restarts after a successful file upload.

34.4.4 FTP Session Example of Firmware File Upload



```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 34-7 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 34.2.5* to read about configurations that disallow TFTP and FTP over WAN.

34.4.5 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.

Step 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.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter the command "sys stdio 0" to disable the console timeout, so the TFTP transfer will not be interrupted. Enter "command sys stdio 5" to restore the five-minute console timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the 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.

34.4.6 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).

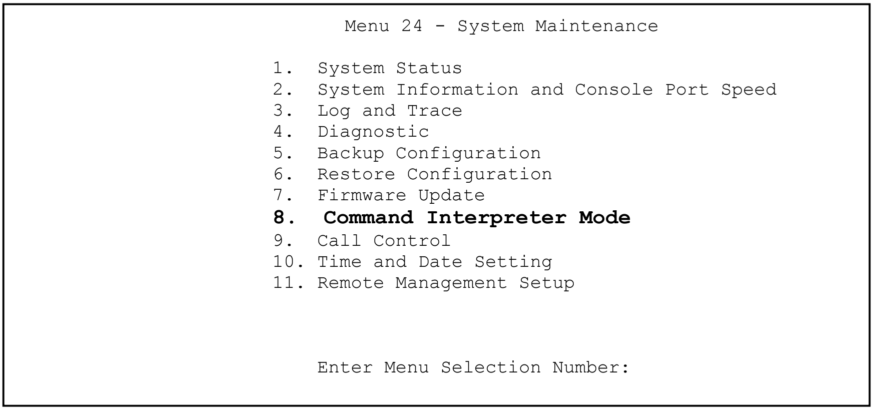
Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Chapter 35
System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

35.1 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.



```
                              Menu 24 - System Maintenance

                         1.  System Status
                         2.  System Information and Console Port Speed
                         3.  Log and Trace
                         4.  Diagnostic
                         5.  Backup Configuration
                         6.  Restore Configuration
                         7.  Firmware Update
                         8.  Command Interpreter Mode
                         9.  Call Control
                         10. Time and Date Setting
                         11. Remote Management Setup



                         Enter Menu Selection Number:
```

Figure 35-1 Command Mode in Menu 24

35.1.1 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".

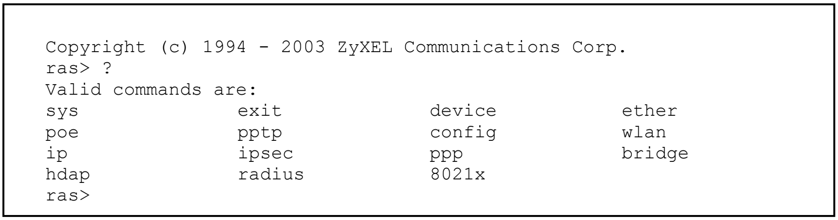
For example,

```
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.

35.1.2 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.



```
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>
```

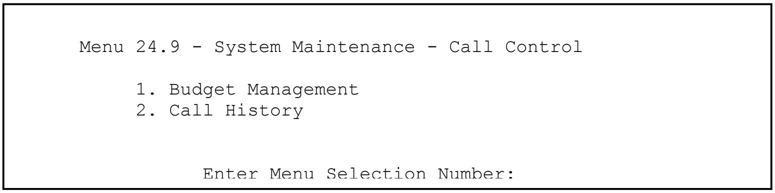
Figure 35-2 Valid Commands

35.2 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.

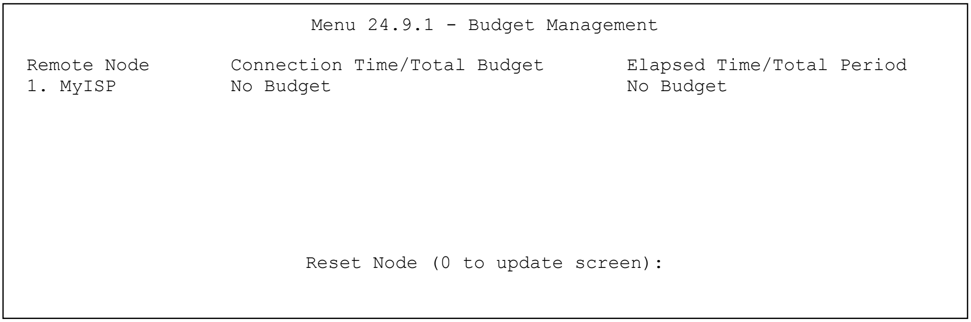


```
        Menu 24.9 - System Maintenance - Call Control

              1. Budget Management
              2. Call History


                     Enter Menu Selection Number:
```

Figure 35-3 Menu 24.9 System Maintenance : Call Control

35.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.



```
                        Menu 24.9.1 - Budget Management

Remote Node       Connection Time/Total Budget       Elapsed Time/Total Period
1. MyISP          No Budget                          No Budget









                       Reset Node (0 to update screen):
```

Figure 35-4 Budget Management

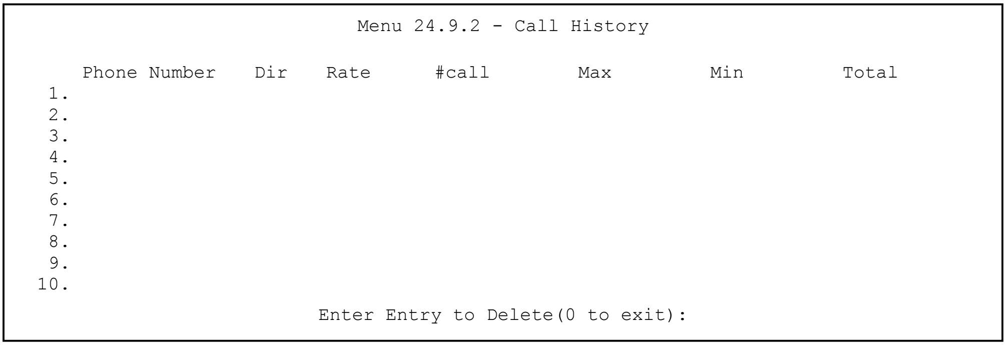
The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 35-1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1-hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

35.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.



```
                              Menu 24.9.2 - Call History

      Phone Number    Dir    Rate      #call        Max         Min         Total
   1.
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
  10.
                           Enter Entry to Delete(0 to exit):
```

Figure 35-5 Call History

The following table describes the fields in this screen.

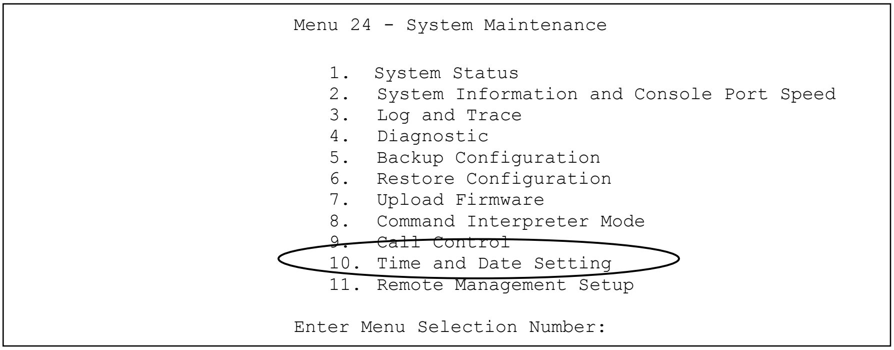
Table 35-2 Call History Fields

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or ‘”0” to exit.	

35.3 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.

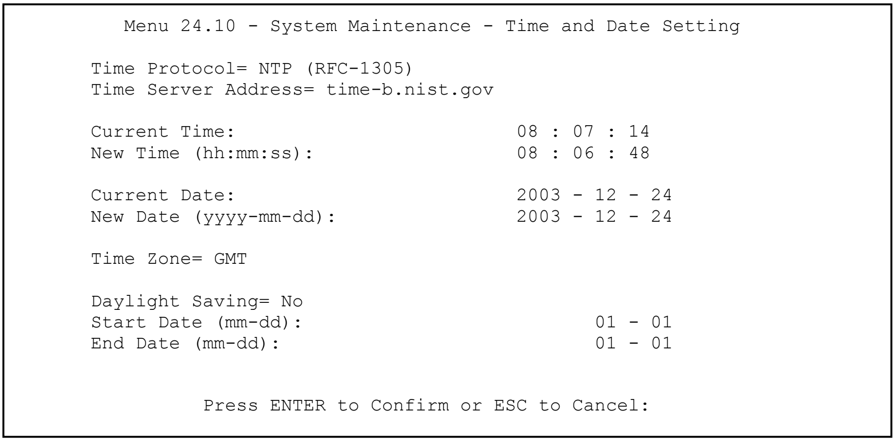
Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.



```
                         Menu 24 - System Maintenance

                            1.  System Status
                            2.  System Information and Console Port Speed
                            3.  Log and Trace
                            4.  Diagnostic
                            5.  Backup Configuration
                            6.  Restore Configuration
                            7.  Upload Firmware
                            8.  Command Interpreter Mode
                            9.  Call Control
                            10. Time and Date Setting
                            11. Remote Management Setup

                         Enter Menu Selection Number:
```

Figure 35-6 Menu 24: System Maintenance

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.



```
          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:
```

Figure 35-7 Menu 24.10 System Maintenance: Time and Date Setting

The following table describes the fields in this screen.

Table 35-3 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 (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** the default, is similar to **Time (RFC-868)**. **None** enter the time manually.
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose **Yes**.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Yes** in the **Daylight Saving** field.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Yes** in the **Daylight Saving** field.
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

35.3.1 Resetting the Time

The Prestige resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the Prestige starts up, if there is a timeserver configured in menu 24.10.

iii. 24-hour intervals after starting.

Chapter 36
Remote Management

This chapter covers remote management (SMT menu 24.11).

36.1 Remote Management

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

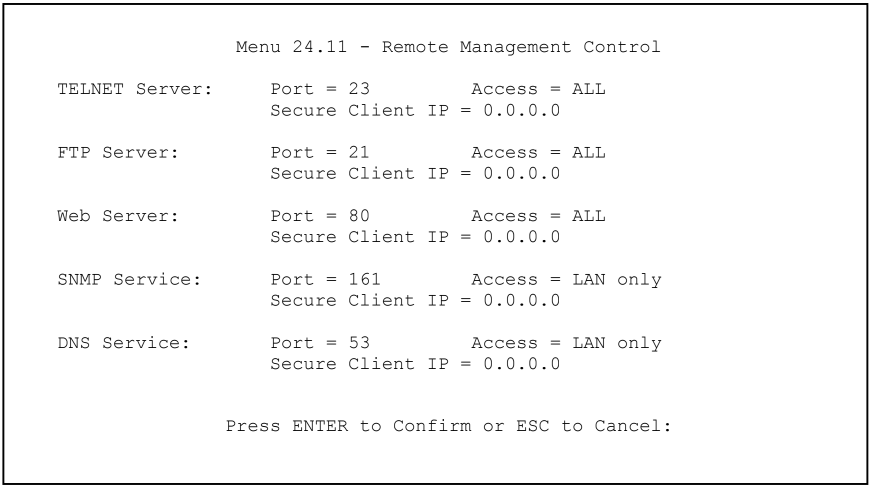
You may manage your Prestige from a remote location via:

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

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

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

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.



```
                 Menu 24.11 - Remote Management Control

TELNET Server:     Port = 23         Access = 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:
```

Figure 36-1 Menu 24.11 – Remote Management Control

The following table describes the fields in this screen.

Table 36-1 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a service 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.	23
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.	**LAN Only** (default)
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.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

36.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

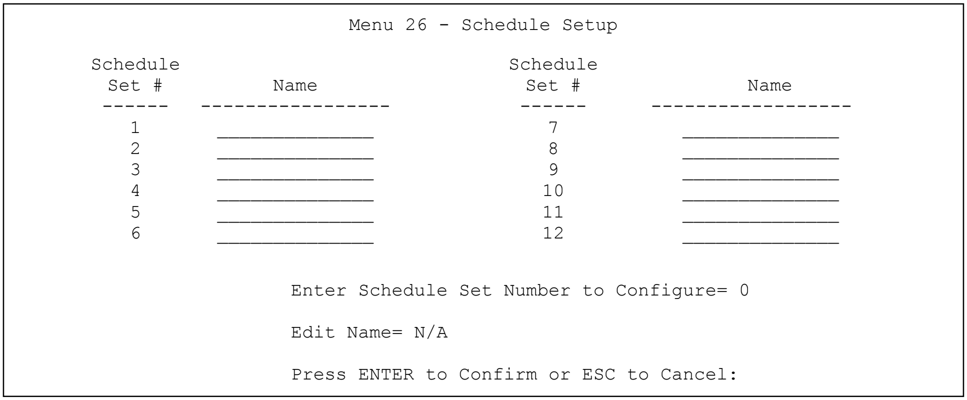
1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
6. There is a firewall rule that blocks it.

Chapter 37
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.

37.1 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.



```
                          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:
```

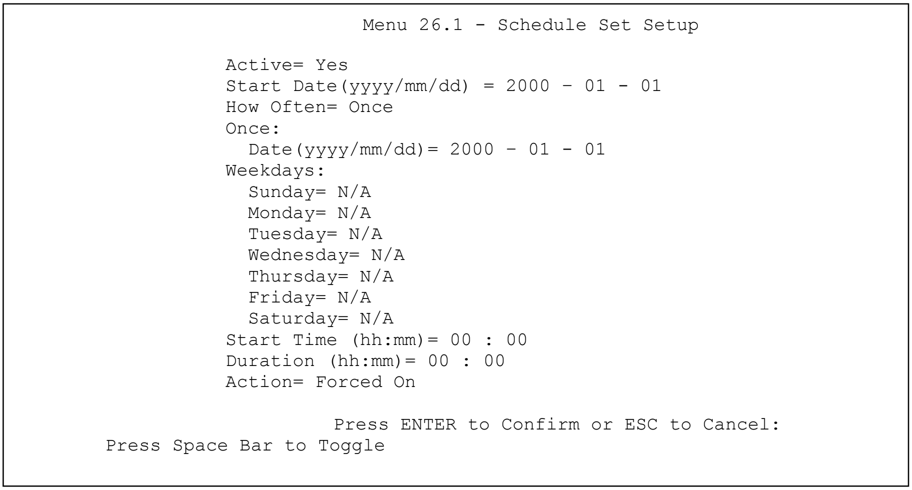
Figure 37-1 Menu 26 Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2 ,3 and 4 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.

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.



```
                       Menu 26.1 - Schedule Set Setup

           Active= Yes
           Start Date(yyyy/mm/dd) = 2000 - 01 - 01
           How Often= Once
           Once:
             Date(yyyy/mm/dd)= 2000 - 01 - 01
           Weekdays:
             Sunday= N/A
             Monday= N/A
             Tuesday= N/A
             Wednesday= N/A
             Thursday= N/A
             Friday= N/A
             Saturday= N/A
           Start Time (hh:mm)= 00 : 00
           Duration (hh:mm)= 00 : 00
           Action= Forced On

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

Figure 37-2 Menu 26.1 Schedule Set Setup

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**.

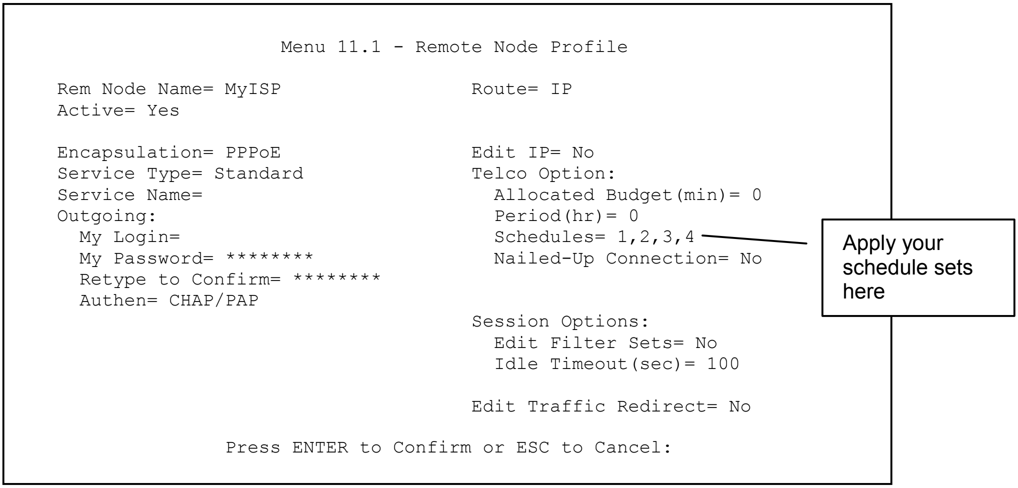
Table 37-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.	**Yes**
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.	2000-01-01
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**
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.	2000-01-01

Table 37-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	**Yes** **No** **N/A**
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	09:00
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	08:00
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On**
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.



```
                    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:
```

Apply your schedule sets here

Figure 37-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Part IX:

SMT VPN/IPSec

This part provides information about configuring VPN/IPSec for secure communications.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 38
VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

38.1 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.

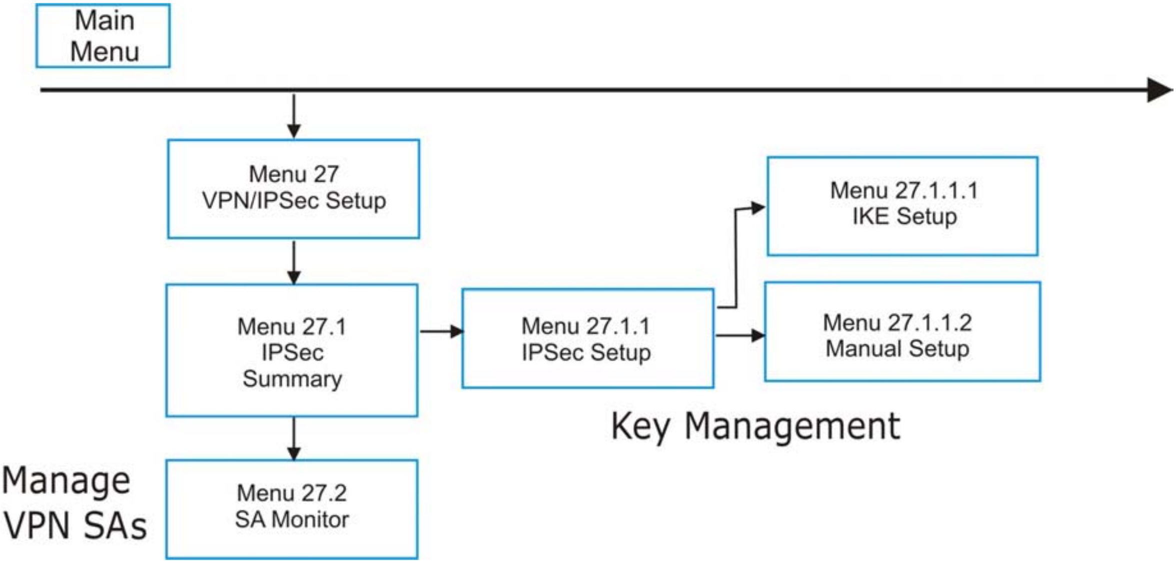
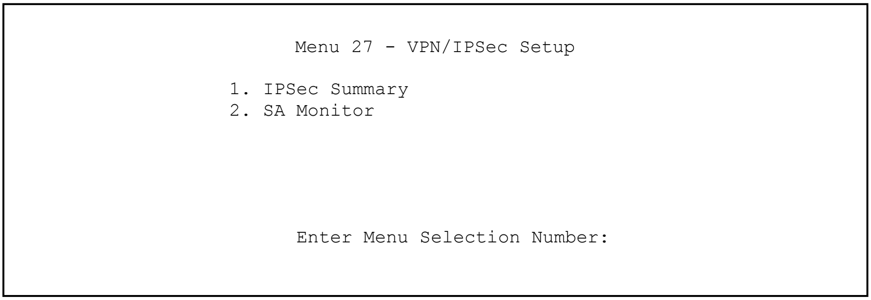


Figure 38-1 VPN SMT Menu Tree

From the main menu, enter 27 to display the first VPN menu (shown next).

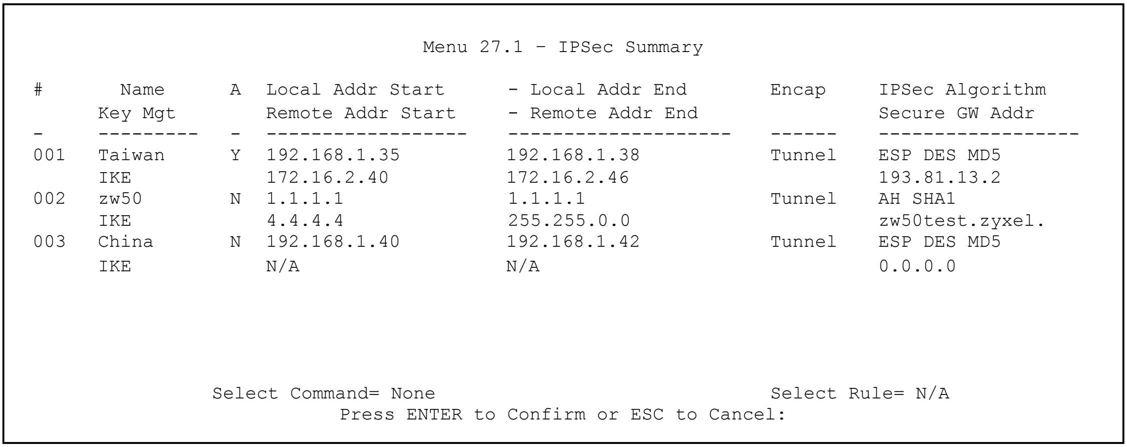


```
                    Menu 27 - VPN/IPSec Setup

              1. IPSec Summary
              2. SA Monitor





                   Enter Menu Selection Number:
```

Figure 38-2 Menu 27 VPN/IPSec Setup

38.2 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.



```
                                    Menu 27.1 - IPSec Summary

 #       Name      A  Local Addr Start      - Local Addr End       Encap    IPSec Algorithm
       Key Mgt        Remote Addr Start     - Remote Addr End               Secure GW Addr
 -     ---------   -  ------------------    --------------------   ------   ------------------
 001   Taiwan      Y  192.168.1.35          192.168.1.38           Tunnel   ESP DES MD5
       IKE            172.16.2.40           172.16.2.46                     193.81.13.2
 002   zw50        N  1.1.1.1               1.1.1.1                Tunnel   AH SHA1
       IKE            4.4.4.4               255.255.0.0                     zw50test.zyxel.
 003   China       N  192.168.1.40          192.168.1.42           Tunnel   ESP DES MD5
       IKE            N/A                   N/A                             0.0.0.0





                   Select Command= None                            Select Rule= N/A
                               Press ENTER to Confirm or ESC to Cancel:
```

Figure 38-3 Menu 27.1 IPSec Summary

Table 38-1 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
#	This is the VPN policy index number.	1

Table 38-1 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.	Taiwan
A	**Y** signifies that this VPN rule is active.	**Y**
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.	192.168.1.35
Local Addr End	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Local Addr Start** field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the LAN behind your 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.	192.168.1.38
Encap	This field displays **Tunnel** mode or **Transport** mode. See earlier for a discussion of these. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.	**Tunnel**
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption. **AH** (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits)**.** Both **AH** and **ESP** increase the 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.	**ESP DES MD5**

Table 38-1 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Key Mgt	This field displays the SA’s type of key management, (**IKE** or **Manual**).	**IKE**
Remote Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.	172.16.2.40
Remote Addr End	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Remote Addr Start** field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.	172.16.2.46
Secure GW Addr	This is the WAN IP address or the domain name (up to the first 15 characters are displayed) of the IPSec router with which you are making the VPN connection. This field displays **0.0.0.0** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.	193.81.13.2

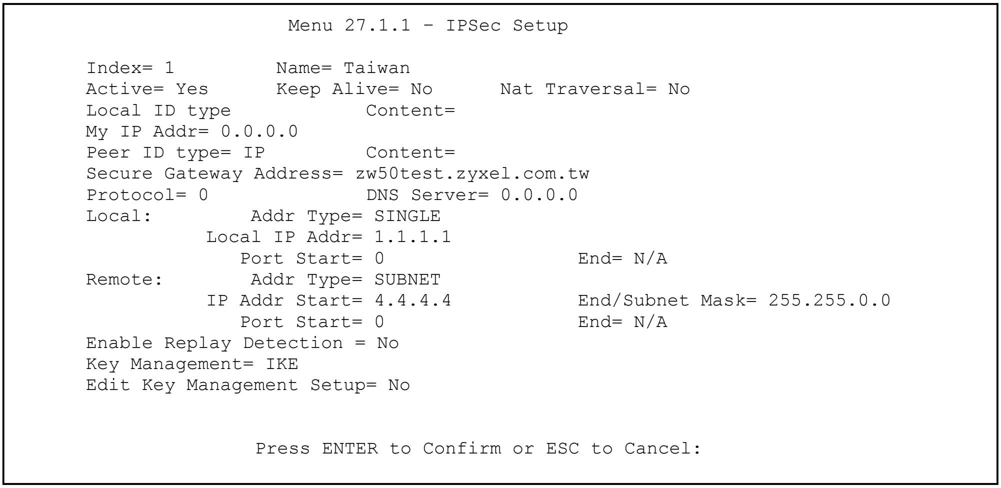
Table 38-1 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, Delete or **Go To** commands. Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt. Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do not move up in the page list. Use **Go To Rule** to view the page where your desired rule is listed. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).	**None**
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].	3
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

38.3 IPSec Setup

Select **Edit** in the **Select Command** field; type the index number of a rule in the **Select Rule** field and press [ENTER] to edit the VPN using the menu shown next.

You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.



```
                      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
               Local IP Addr= 1.1.1.1
                  Port Start= 0                 End= N/A
    Remote:        Addr Type= SUBNET
               IP Addr Start= 4.4.4.4           End/Subnet Mask= 255.255.0.0
                  Port Start= 0                 End= N/A
    Enable Replay Detection = No
    Key Management= IKE
    Edit Key Management Setup= No


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

Figure 38-4 Menu 27.1.1 IPSec Setup

The following table describes the fields in this menu.

Table 38-2 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Index	This is the VPN rule index number you selected in the previous menu.	**1**
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in **Menu 27.1 - IPSec Summary**.	Taiwan
Active	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.	**Yes**
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.	**No**

Table 38-2 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
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.	
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.	0.0.0.0
Peer ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.	

Table 38-2 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
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).	Zw50test.com.tw
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.	0
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.	
Addr Type	This field displays **SINGLE** for a single IP address.	**SINGLE**
Local IP Addr	Enter a static IP address on the LAN behind your Prestige.	192.168.1.35
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. You cannot create a VPN tunnel if you try to connect using a port number that does not match this port number or range of port numbers. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3	0

Table 38-2 Menu 27.1.1 IPSec Setup

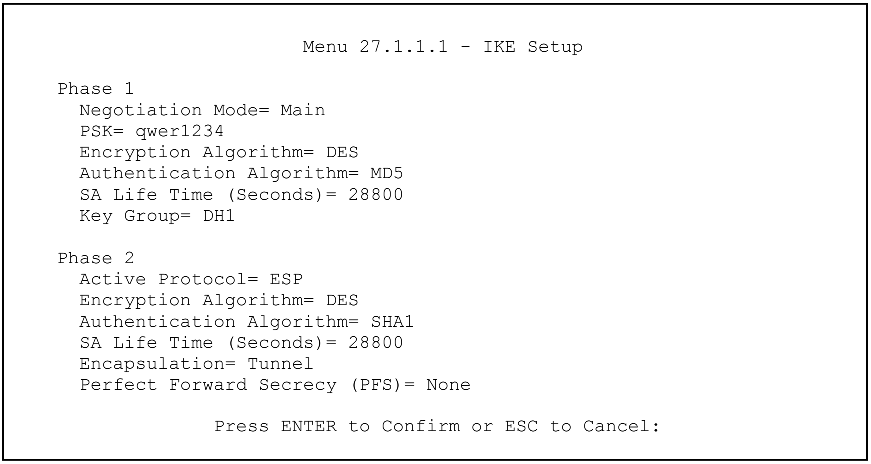
FIELD	DESCRIPTION	EXAMPLE
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.	N/A
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields are **N/A** when the **Secure Gateway 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.	**SUBNET**
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the network behind the remote IPSec router. When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field is configured to **SUBNET**, enter a static IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.	4.4.4.4
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.	255.255.0.0

Table 38-2 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Someone behind the remote IPSec router cannot create a VPN tunnel when attempting to connect using a port number that does not match this port number or range of port numbers. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.	0
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.	
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **Yes**. Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to enable replay detection.	**No**
Key Management	Press [SPACE BAR] to choose either **IKE** or **Manual** and then press [ENTER]. **Manual** is useful for troubleshooting if you have problems using **IKE** key management.	**IKE**
Edit Key Management Setup	Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the **Key Management** field to **IKE**, this will take you to **Menu 27.1.1.1 – IKE Setup**. If you set the **Key Management** field to **Manual**, this will take you to **Menu 27.1.1.2 – Manual Setup**.	**No**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

38.4 IKE Setup

To edit this menu, the **Key Management** field in **Menu 27.1.1 – IPSec Setup** must be set to **IKE**. Move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 – IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 – IKE Setup**.



```
                    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:
```

Figure 38-5 Menu 27.1.1.1 IKE Setup

The following table describes the fields in this menu.

Table 38-3 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Phase 1		
Negotiation Mode	Press [SPACE BAR] to choose from **Main** or **Aggressive** and then press [ENTER]. See earlier for a discussion of these modes. Multiple SAs connecting through a secure gateway must have the same negotiation mode.	**Main**
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.	

Table 38-3 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. 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].	**DES**
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slightly slower. Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].	**SHA1**
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short **SA Life Time** increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.	28800 (default)
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.	**DH1**
Phase 2		
Active Protocol	Press [SPACE BAR] to choose from **ESP** or **AH** and then press [ENTER]. See earlier for a discussion of these protocols.	**ESP**
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Select **NULL** to set up a tunnel without encryption.	**DES**
Authentication Algorithm	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].	**MD5**
SA Life Time (Seconds)	Define the length of time before an IPSec Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).	28800 (default)
Encapsulation	Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these.	**Tunnel**

Table 38-3 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).	**None**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

38.5 Manual Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPSec Setup**. Manual key management is useful if you have problems with **IKE** key management.

38.5.1 Active Protocol

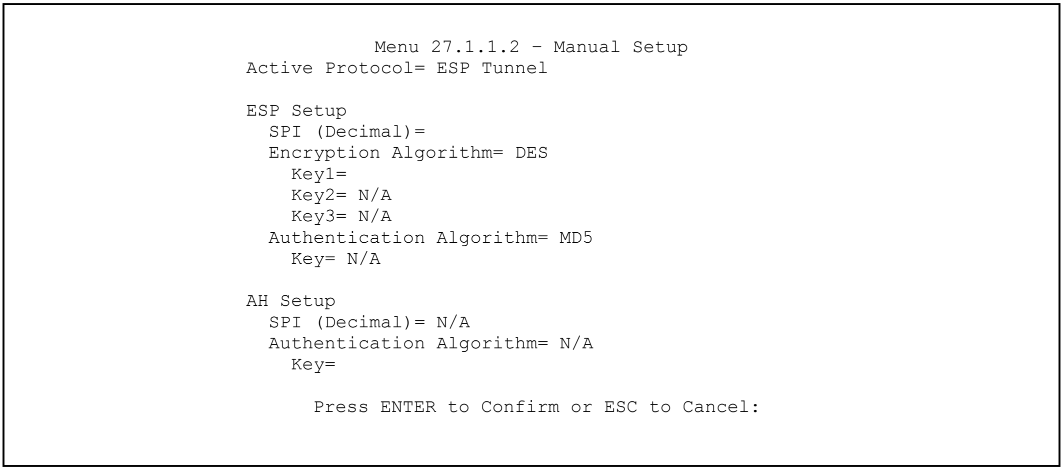
This field is a combination of mode and security protocols used for the VPN. See the Web Configurator part on VPN for more information on these parameters.

Table 38-4 Active Protocol: Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

38.5.2 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**.



```
             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:
```

Figure 38-6 Menu 27.1.1.2 Manual Setup

The following table describes the fields in this menu.

Table 38-5 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Active Protocol	Press [SPACE BAR] to choose from **ESP Tunnel**, **ESP Transport**, **AH Tunnel** or **AH Transport** and then press [ENTER]. Choosing an **ESP** combination causes the **AH Setup** fields to be non-applicable (**N/A**)	**ESP Tunnel**
ESP Setup	The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**.	
SPI (Decimal)	The **SPI** must be unique and from one to four integers ("0" to "9").	1234
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Fill in the **Key1** field below when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter any encryption keys.	**DES**
Key1	Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated. Fill in the **Key1** field when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**.	89abcde
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	

Table 38-5 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].	**MD5**
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.	123456789a bcde
AH Setup	The **AH Setup** fields are **N/A** if you chose an **ESP Active Protocol**.	
SPI (Decimal)	The **SPI** must be from one to four unique decimal characters ("0" to "9") long.	**N/A**
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].	**N/A**
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.	**N/A**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Chapter 39
SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

39.1 SA Monitor Overview

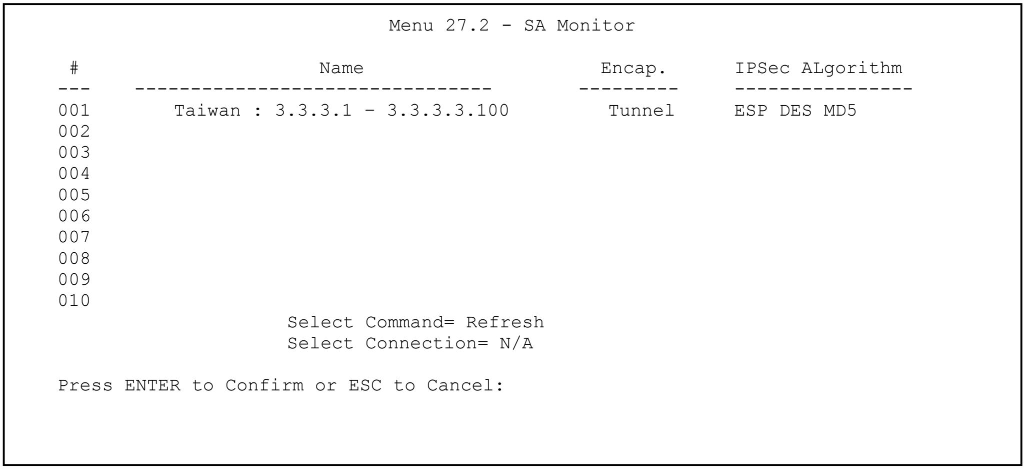
A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

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.

39.2 Using SA Monitor

1. Use the **Refresh** function to display active VPN connections.
2. Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.



```
                                  Menu 27.2 - SA Monitor

    #                     Name                        Encap.      IPSec ALgorithm
   ---    --------------------------------         ---------      ----------------
   001       Taiwan : 3.3.3.1 - 3.3.3.3.100          Tunnel       ESP DES MD5
   002
   003
   004
   005
   006
   007
   008
   009
   010
                        Select Command= Refresh
                        Select Connection= N/A

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

Figure 39-1 Menu 27.2 SA Monitor

The following table describes the fields in this menu.

Table 39-1 Menu 27.2 SA Monitor

FIELD	DESCRIPTION	EXAMPLE
#	This is the security association index number.	
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a public static IP address. When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this same VPN rule. In this case, the name is followed by the remote IP address as configured in **Menu 27.1.1. – IPSec Setup**. Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule.	**Taiwan**
Encap.	This field displays **Tunnel** mode or **Transport** mode. See previous for discussion.	**Tunnel**
IPSec ALgorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption. An incoming SA may have an **AH** in addition to **ESP**. The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits). Both **AH** and **ESP** increase Prestige processing requirements and communications latency (delay).	**ESP DES MD5**
Select Command	Press [SPACE BAR] to choose from **Refresh**, **Disconnect**, **None**, **Next Page**, or **Previous Page** and then press [ENTER]. You must select a connection in the next field when you choose the **Disconnect** command. **Refresh** displays current active VPN connections. **None** allows you to jump to the “Press ENTER to Confirm…” prompt. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).	**Refresh**
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].	**1**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Part X:

Appendices and Index

This section provides some Appendices and an Index.

Appendix A PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) that connects to an xDSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN & ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

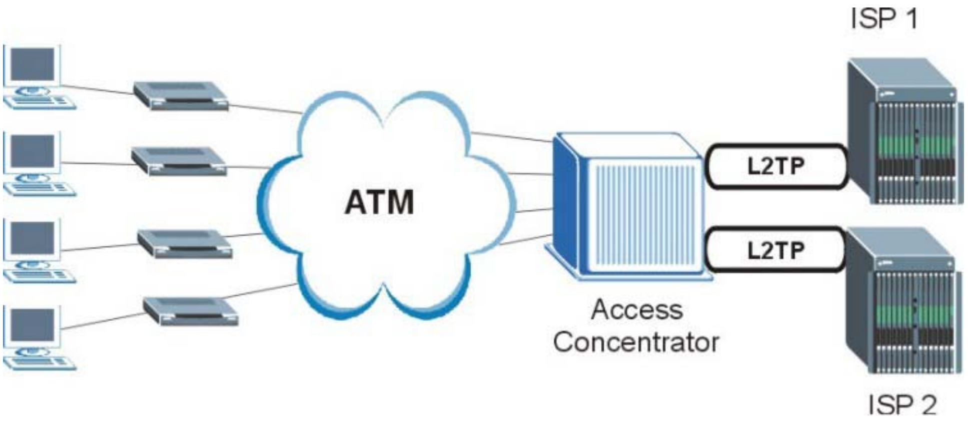


Diagram A-1 Single-PC per Modem Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

The Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

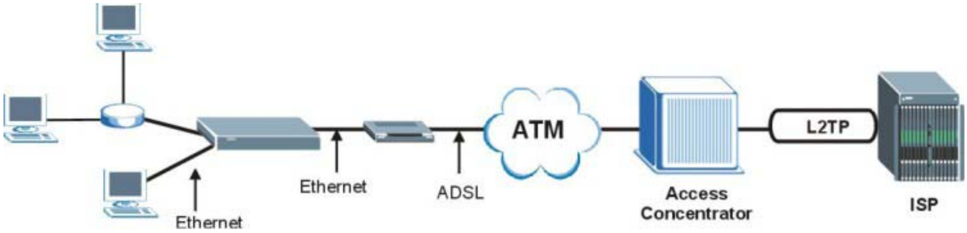


Diagram A-2 The Prestige as a PPPoE Client

Appendix B PPTP

What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

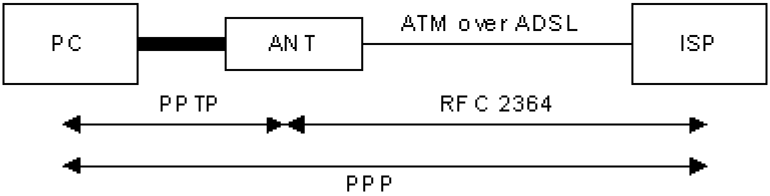


Diagram B-1 Transport PPP frames over Ethernet

PPTP and the Prestige

When the Prestige is deployed in such a setup, it appears as a PC to the ANT (ADSL Network Termination).

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 NAT mode, the Prestige is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. In the case above as the PPTP connection is initialized by the remote PPTP Client, 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.

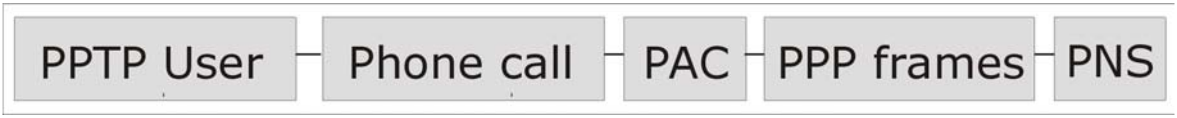


Diagram B-2 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, 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 PC and an ANT.

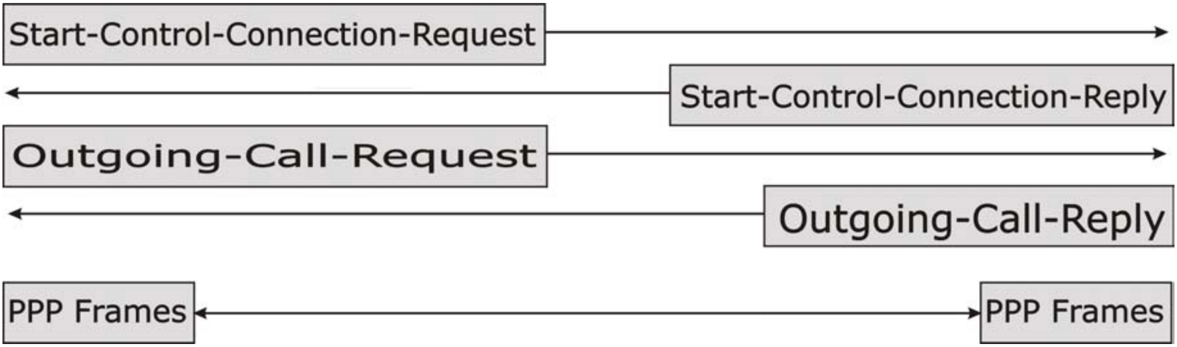

Start-Control-Connection-Request
Start-Control-Connection-Reply
Outgoing-Call-Request
Outgoing-Call-Reply
PPP Frames
PPP Frames

Diagram B-3 Example Message Exchange between PC and an ANT

PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix C
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.

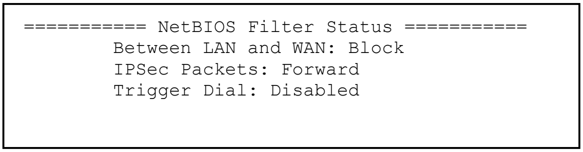
You can configure NetBIOS filters to:

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or deny NetBIOS packets to be sent through VPN connections.
- Block or forward NetBIOS packets from initiating calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command displays the current NetBIOS filter settings.



```
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Block
        IPSec Packets: Forward
        Trigger Dial: Disabled
```

Diagram C-1 NetBIOS Display Filter Settings Command

The filter types and their default settings are as follows.

Table C-1 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
Between LAN and WAN	This field displays whether NetBIOS packets are blocked or forwarded from the LAN to the WAN or from the WAN to the LAN.	Forward
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

Syntax: `sys filter netbios config <type> <on|off>`

where

`<type> =` Identify which NetBIOS filter (numbered 0-3) to configure.

`0` = LAN to WAN and WAN to LAN

3 = IPSec Packets

4 = Trigger dial

`<on|off> =` For type `0`, 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

Command: `sys filter netbios config 0 on`

This command blocks LAN to WAN and WAN to LAN NetBIOS packets

Command: `sys filter netbios config 3 on`

This command blocks IPSec NetBIOS packets

Command: `sys filter netbios config 4 off`

This command stops NetBIOS commands from initiating calls.

Appendix D
Log Descriptions

Configure centralized logs using the embedded web configurator; see the online help for details. This appendix describes some of the log messages.

Chart 1 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

Chart 2 System Maintenance Logs

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

Chart 2 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`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.

Chart 3 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Chart 4 Content Filtering Logs

CATEGORY	LOG MESSAGE	DESCRIPTION
URLFOR	`IP/Domain Name`	The Prestige allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name.
URLBLK	`IP/Domain Name`	The Prestige blocked access to this IP address or domain name due to a forbidden keyword. All web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list.

Chart 4 Content Filtering Logs

CATEGORY	LOG MESSAGE	DESCRIPTION
JAVBLK	IP/Domain Name	The Prestige blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy.

Chart 5 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

Chart 5 ICMP Type and Code Explanations

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

Appendix E
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.

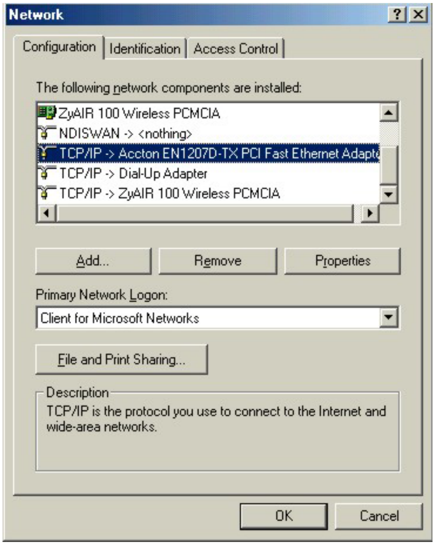
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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 (192.168.1.2 to 192.168.1.254 range with a subnet mask of 255.255.255.0.) as the default Prestige's LAN port IP address (192.168.1.1).

Windows 95/98/Me

1. Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.



The following network components are installed:

- ZyAIR 100 Wireless PCMCIA
- NDISWAN -> <nothing>
- TCP/IP -> Accton EN1207D-TX PCI Fast Ethernet Adapte
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> ZyAIR 100 Wireless PCMCIA

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

2. The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

a. In the **Network** window, click **Add**.

b. Select **Adapter** and then click **Add**.

c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a. In the **Network** window, click **Add**.

b. Select **Protocol** and then click **Add**.

c. Select **Microsoft** from the list of **manufacturers**.

d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

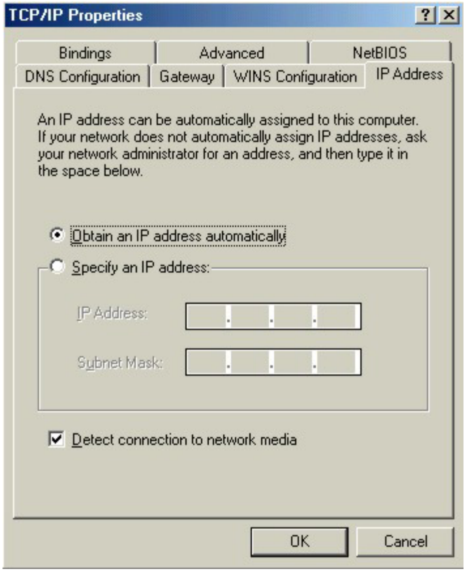
e. Restart your computer so the changes you made take effect.

In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

1. Click the **IP Address** tab.

   -To have your computer assigned a dynamic IP address, select **Obtain an IP address automatically**.

   -To give your computer a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

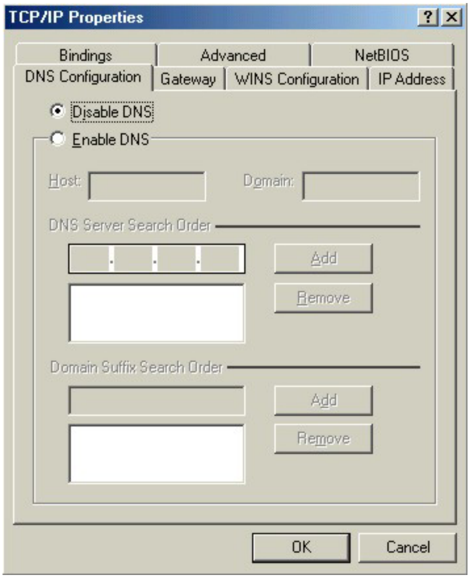
Subnet Mask: . . .

☑ Detect connection to network media

2. Click the **DNS** Configuration tab.

   -If you do not know your DNS information, select **Disable DNS**.

   -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

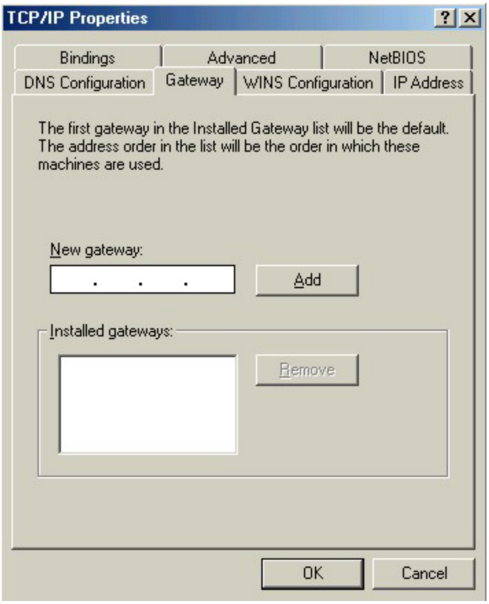


● Disable DNS
○ Enable DNS

3. Click the **Gateway** tab.

   -If you do not know your gateway's IP address, remove previously installed gateways.

   -If you have a gateway IP address, type it in the **New gateway field** and click **Add**.



The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

4. Click **OK** to save and close the **TCP/IP Properties** window.

5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

6. Turn on your Prestige and restart your computer when prompted.

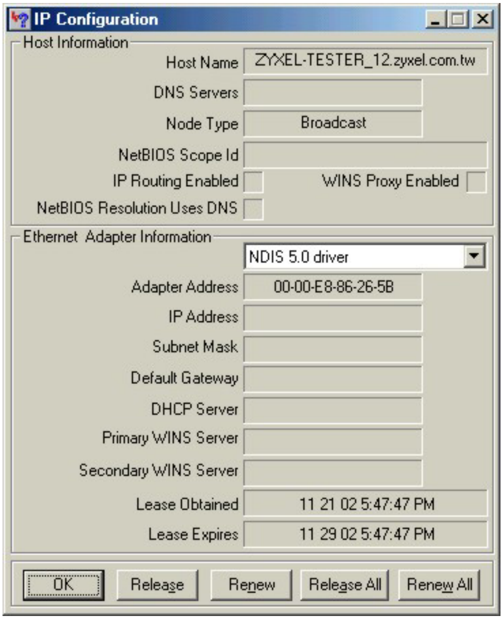
Checking/Modifying Your Computer's IP Address

1. Click **Start** and then **Run**.

2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3. Select your network adapter. You should see your computer's (static) IP address, subnet mask and default gateway in this screen. Verify that your computer's static IP address is in the correct subnet (192.168.1.2 to 192.168.1.254 if using the default Prestige LAN IP address). Alternatively, to have the Prestige assign your computer a new IP address (from the IP pool), make sure your Prestige is turned on and click **Renew** in this screen.

   Your computer can now communicate with the Prestige using the LAN port.



IP Configuration

Host Information

Host Name: ZYXEL-TESTER_12.zyxel.com.tw

DNS Servers:

Node Type: Broadcast

NetBIOS Scope Id:

IP Routing Enabled □ WINS Proxy Enabled □

NetBIOS Resolution Uses DNS □

Ethernet Adapter Information

NDIS 5.0 driver

Adapter Address: 00-00-E8-86-26-5B

IP Address:

Subnet Mask:

Default Gateway:

DHCP Server:

Primary WINS Server:

Secondary WINS Server:

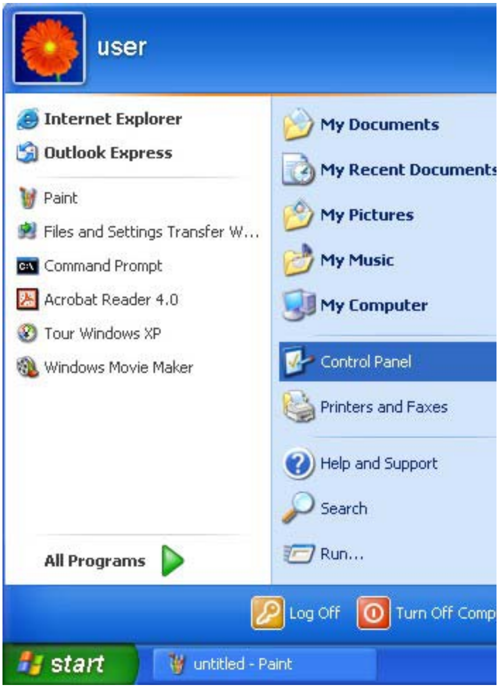
Lease Obtained: 11 21 02 5:47:47 PM

Lease Expires: 11 29 02 5:47:47 PM

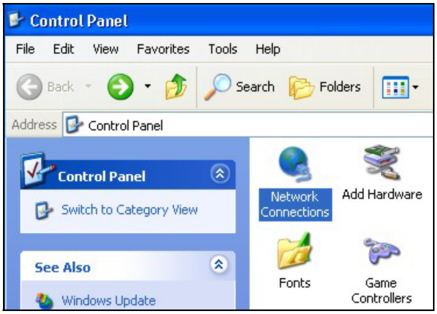
Windows 2000/NT/XP

1. In Windows XP, click **start**, **Control Panel**.

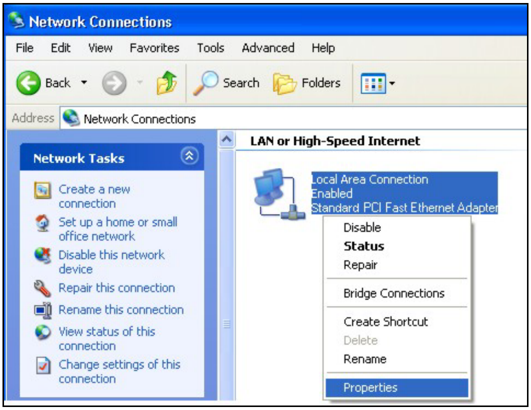
   In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.



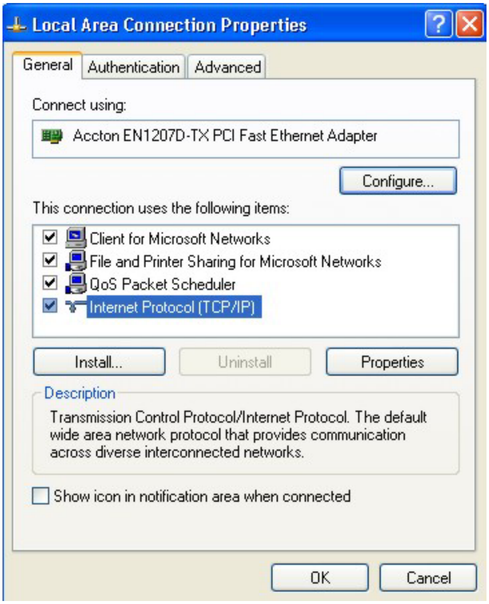
2. In Windows XP, click **Network Connections**. In Windows 2000/NT, click **Network and Dial-up Connections**.



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



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



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

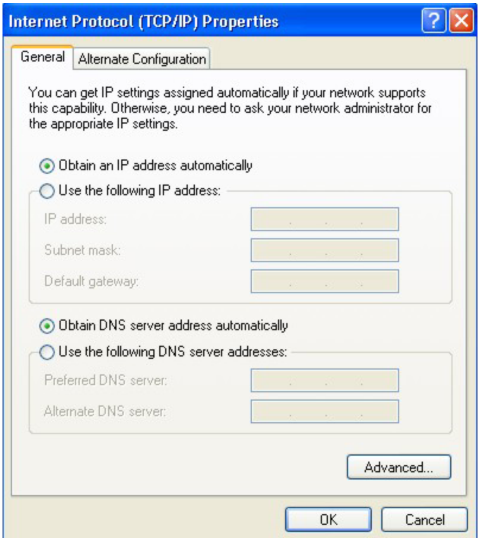
□ Show icon in notification area when connected

5. The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

   - To have your computer assigned 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** to go to the **Advanced TCP/IP Settings** screen shown next.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

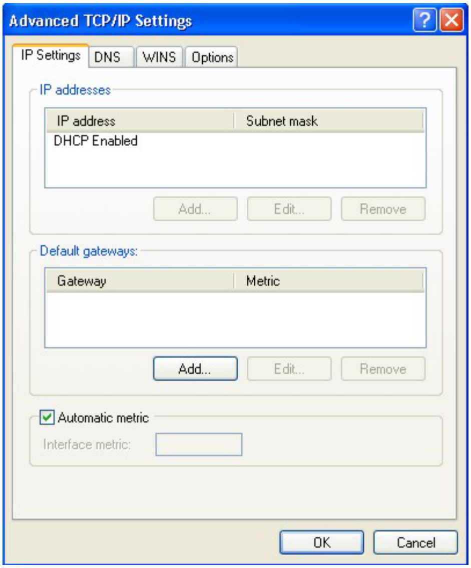
Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .



DHCP Enabled

☑ Automatic metric

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.

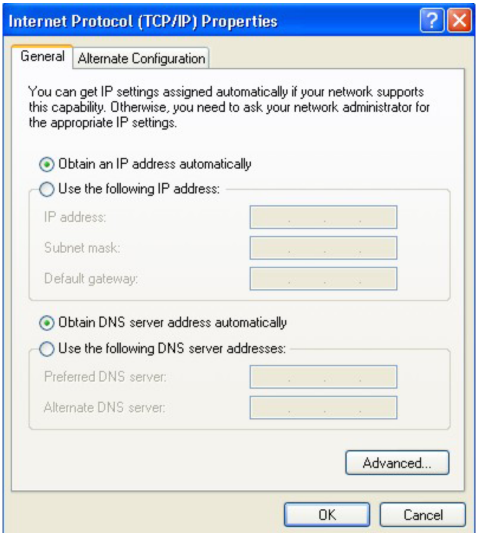
   -Click **OK** when finished.

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 wish to have more than two DNS servers, click **Advanced**, the **DNS** tab and then configure them using **Add**.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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).

Checking/Modifying Your Computer’s IP Address

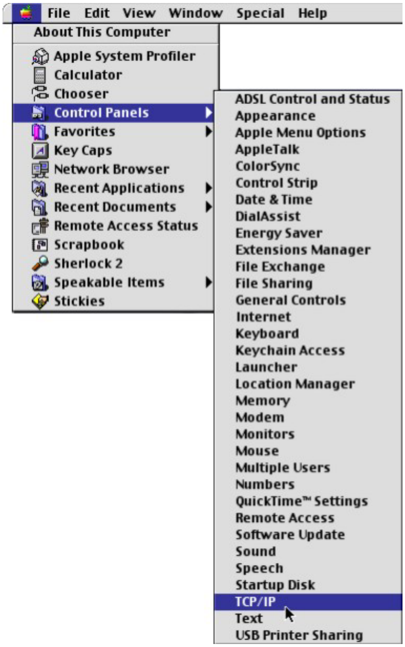
1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2. In the **Command Prompt** window, type "ipconfig" and then press **ENTER** to verify that your computer’s static IP address is in the correct subnet (192.168.1.2 to 192.168.1.254 if using the default Prestige LAN IP address). Alternatively, to have the Prestige assign your computer a new IP address (from the IP pool), make sure your Prestige is turned on, type "ipconfig/renew" and then press **ENTER**.

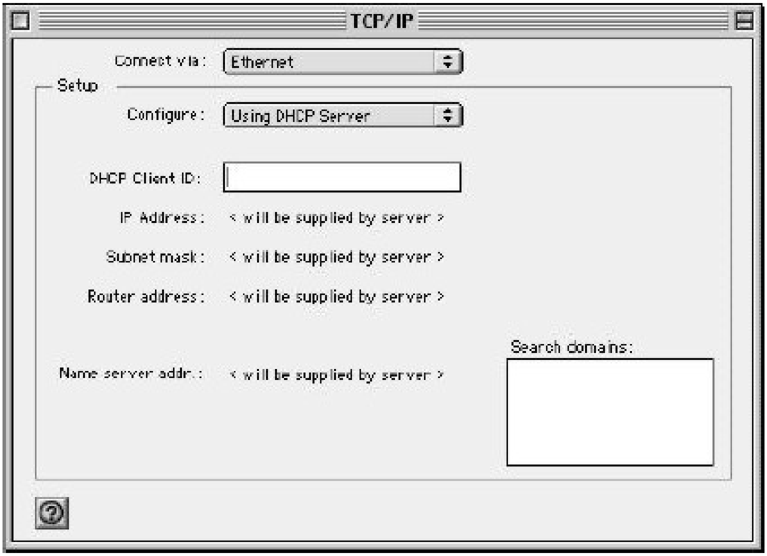
   Your computer can now communicate with the Prestige using the LAN port.

Macintosh OS 8/9

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



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



TCP/IP

Connect via : Ethernet

Setup

Configure : Using DHCP Server

DHCP Client ID:

IP Address : < will be supplied by server >

Subnet mask : < will be supplied by server >

Router address : < will be supplied by server >

Name server addr. : < will be supplied by server >

Search domains:

3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

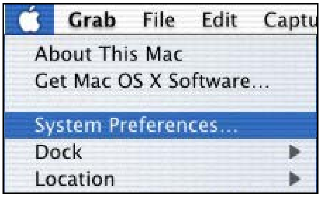
   -Type the IP address of your Prestige in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your Prestige and restart your computer (if prompted).

Verifying Your Computer's IP Address

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1. Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

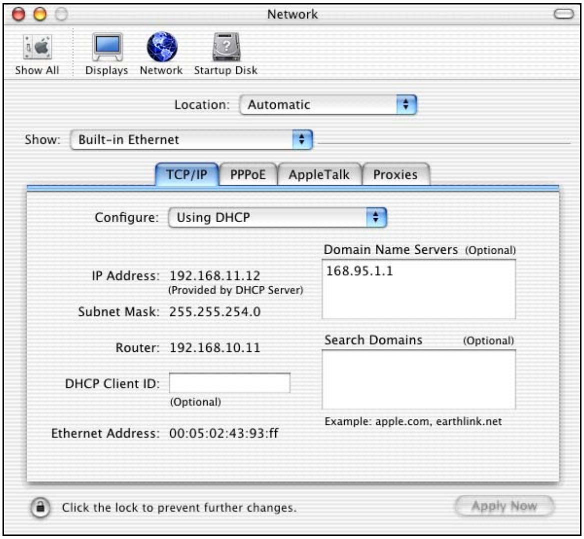


2. Click **Network** in the icon bar.

   - Select **Automatic** from the **Location** list.

   - Select **Built-in Ethernet** from the **Show** list.

   - Click the **TCP/IP** tab.



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

3. For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

   -Type the IP address of your 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 Your Computer's IP Address

Check your TCP/IP properties in the **Network** window.

Appendix F
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area. WLAN is not available on all models.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

1. It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.
4. It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".
5. It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence

Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). See the following diagram of an example of an Ad-hoc wireless LAN.

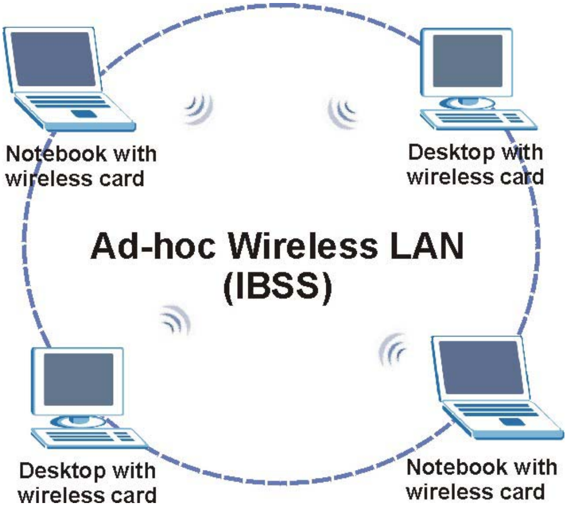

Notebook with wireless card
Desktop with wireless card
Ad-hoc Wireless LAN (IBSS)
Desktop with wireless card
Notebook with wireless card

Diagram F-1 Peer-to-Peer Communication in an Ad-hoc Network

Infrastructure Wireless LAN Configuration

For infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between access points and seamless campus-wide coverage is possible.

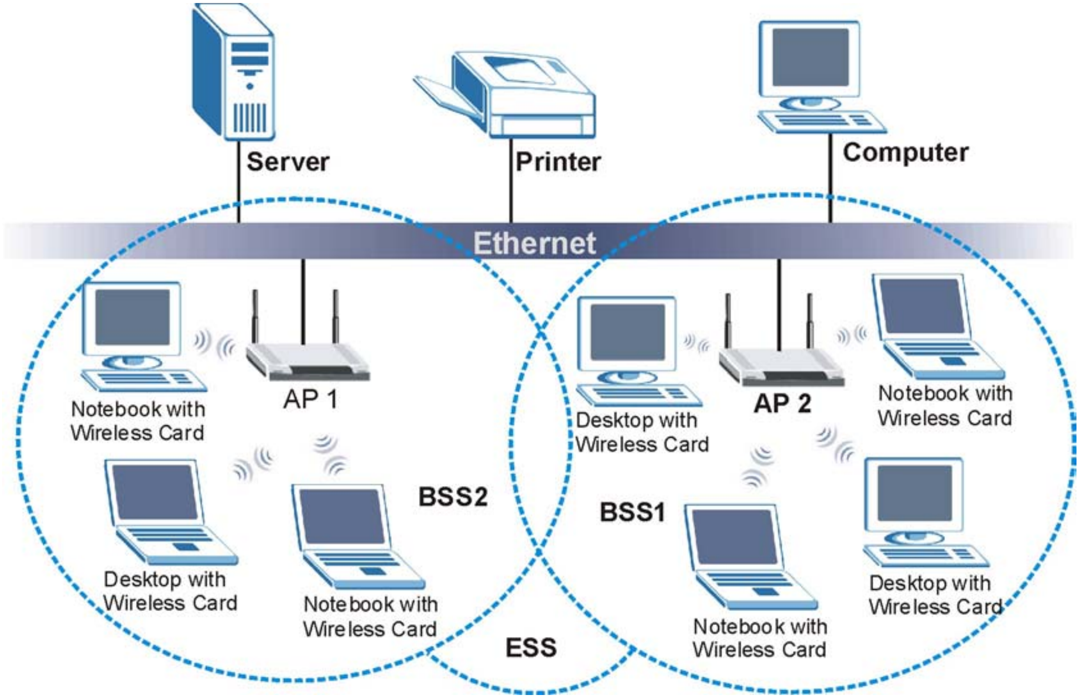

Server
Printer
Computer
Ethernet
Notebook with Wireless Card
AP 1
Desktop with Wireless Card
Notebook with Wireless Card
BSS2
ESS
Desktop with Wireless Card
AP 2
Notebook with Wireless Card
BSS1
Notebook with Wireless Card
Desktop with Wireless Card

Diagram F-2 ESS Provides Campus-Wide Coverage

Appendix G
Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

Advantages of the IEEE 802.1x

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

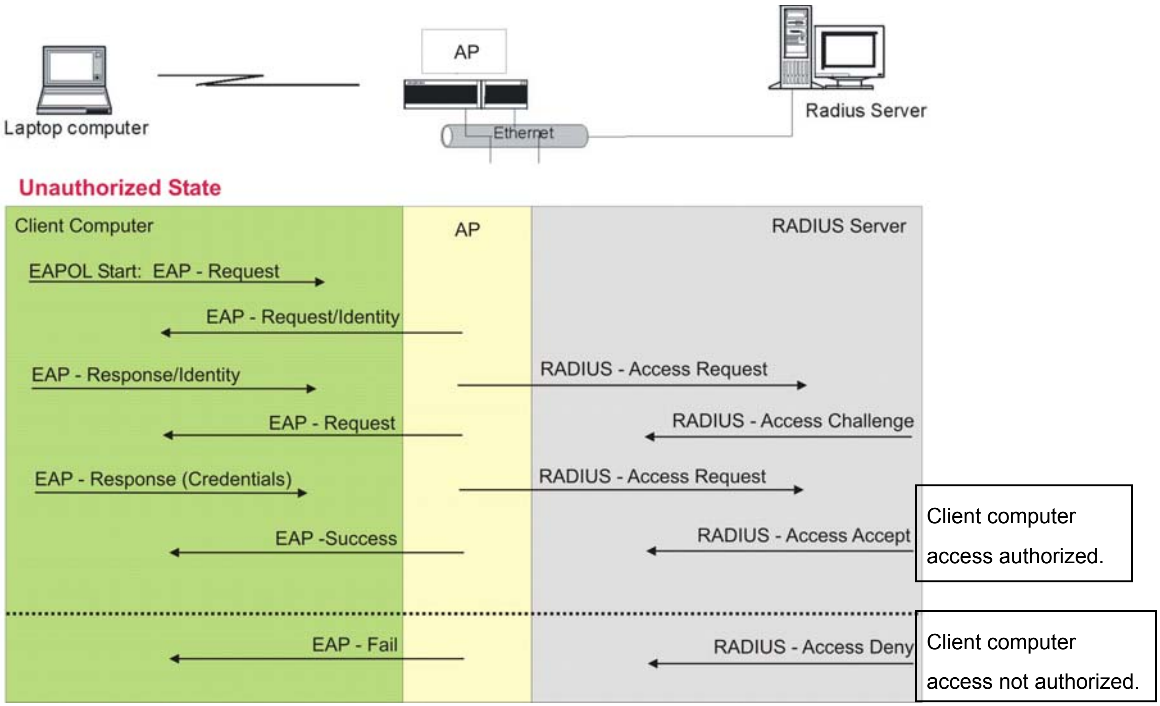


Diagram G-1 Sequences for EAP MD5–Challenge Authentication

Appendix H
Types of EAP Authentication

This appendix discusses the four popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS** and **PEAP**. 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 and EAP-MSCHAPv2, for client authentication.

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, simple user name and password pair is more practical. The following table is a comparison of the features of four authentication types.

Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP
Mutual Authentication	No	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional
Certificate – Server	No	Yes	Yes	Yes
Dynamic Key Exchange	No	Yes	Yes	Yes
Credential Security	None	Strong	Strong	Strong
Deployment Difficulty	Easy	Hard	Moderate	Moderate
Wireless Security	Poor	Best	Good	Good
Client Identity Protection	No	No	Yes	Yes

Appendix I
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 J
Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See other *appendices* for information on the command structure.

Chart 6 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 K
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.

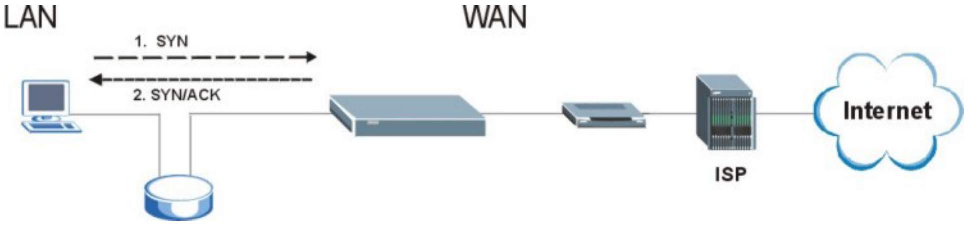


Diagram K-1 Ideal Setup

The "Triangle Route" Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the "triangle route" problem may occur. The steps below describe the "triangle route" problem.

Step 1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

Step 2. The Prestige reroutes the SYN packet through Gateway **B** on the LAN to the WAN.

Step 3. The reply from the WAN goes directly to the computer on the LAN without going through the Prestige.

As a result, the Prestige resets the connection, as the connection has not been acknowledged.

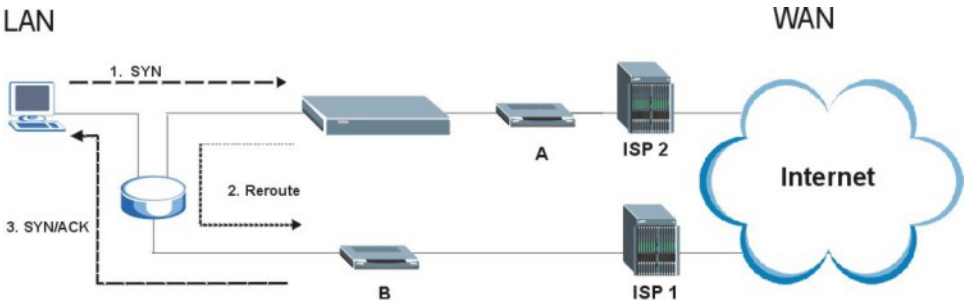


Diagram K-2 "Triangle Route" Problem

The "Triangle Route" Solutions

This section presents you two solutions to the "triangle route" problem.

IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your 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.

Step 1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

Step 2. The Prestige reroutes the packet to Gateway **B** which is in Subnet 2.

Step 3. The reply from WAN goes through the Prestige to the computer on the LAN in Subnet 1.

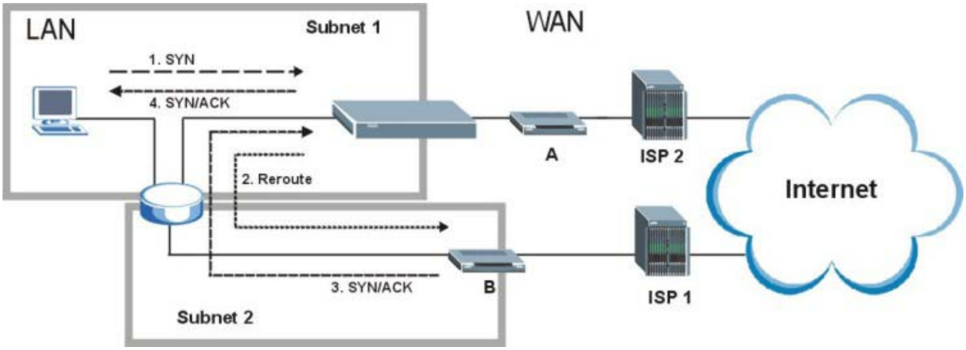


Diagram K-3 IP Alias

Gateways on the WAN Side

A second solution to the "triangle route" problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your Prestige to your LAN. Therefore your LAN is protected.

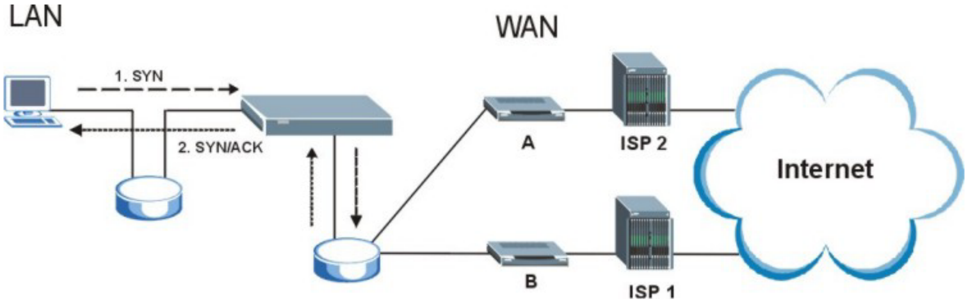


Diagram K-4 Gateways on the WAN Side

How To Configure Triangle Route:

Step 1. From the SMT main menu, enter 24.

Step 2. Enter "8" in menu 24 to enter CI command mode.

Step 3. Use the following commands to allow/disallow triangle route.

`sys firewall ignore triangle all off`	This command allows triangle route.
`sys firewall ignore triangle all on`	This command disallows triangle route.

Index

8

802.1x 8-16

A

Active.. 25-2
Address Assignment 3-10, 3-11
Address Resolution Protocol (ARP) 6-4
Ad-hoc Configuration F-2
Allocated Budget 25-5
Antenna
  Directional I-2
  Omni-directional...I-2
  Types I-2
Antenna gain I-1
Applications 1-5
AT command 34-1
Authen.. 25-5
Authentication...............................8-4, 25-4, 25-5
Authentication Protocol 25-4
auto-negotiation 1-1

B

Backup 19-9, 34-2
Bandwidth Borrowing.................................... 18-7
Bandwidth Services.. 18-2
Basic Service Set...F-2
Bridging 23-2
BSS ....7-1. See Basic Service Set
Budget Management 35-3

C

CA... H-1
Call Control... 35-2
Call History... 35-4
Call Scheduling..................................... 1-3, 37-1
  Maximum Number of Schedule Sets......... 37-1
  PPPoE.. 37-3
  Precedence... 37-1
  Precedence Example................ See precedence
Call-Trigerring Packet 33-8
Canada iv
Caution...iv
CDR (Call Detail Record).............................. 33-5
Certificate Authority .... See CA
Channel ID.. 7-6, 23-7
CHAP 25-5
Command Interpreter Mode........................... 35-1
Community 31-2
Computer Name.. 21-1
Computer's IP Address..................................E-1
Conditions that prevent TFTP and FTP from
  working over WAN 34-4
Configuration... 6-1, 19-4
Connection ID/Name 25-6
Content Filtering 1-2
Copyright..ii
Cost Of Transmission 26-2
Customer Support vi

D

Data Encryption 8-4
DDNS Type 21-4
Default 19-11
Denial of Service 29-1
DHCP 3-1, 3-12, 5-3, 6-1, 6-5, 19-4, 23-2, 33-4
DHCP (Dynamic Host Configuration Protocol) 1-
  4
Diagnostic Tools 33-1
Direct Sequence Spread Spectrum.................. F-2

Disclaimer..ii
Distribution System F-3
DNS 14-11, 23-3
DNS Server
 For VPN Host... 16-7
Domain Name............ 3-1, 3-11, 10-7, 18-3, 33-3
DoS (Denial of Service)................................. 1-2
DS .... See Distribution System
DSL Modem 1-6, 25-4
DSSS.........See Direct Sequence Spread Spectrum
Dynamic DNS...................................... 5-3, 21-3
Dynamic DNS Support 1-4
Dynamic WEP Key Exchange 8-17
DYNDNS Wildcard....................................... 5-3

E

e.g. ....See Syntax Conventions
EAP.. 1-2
EAP Authentication H-1, 8-30
 MD5 ....H-1
 TLS..H-1
 TTLS H-1
ECHO 10-7, 18-3
Edit IP 25-3
eDonkey.. 18-3
E-Mail 18-2
eMule 18-3
Enable Wildcard 21-4
Encapsulation.............................24-2, 25-2, 25-6
 PPP over Ethernet.......................................A-1
Encryption 8-9
Enter ....See Syntax Conventions
ESS 7-2. See Extended Service Set. See Extended Service Set
Ethernet...3-5, 3-7, 13-2
Ethernet Encapsulation 10-6, 24-1, 25-1, 25-2, 25-9
Extended Service Set F-3, 7-2
Extended Service Set IDentification............... 7-6

F

Factory Default...22-1
Factory LAN Defaults 6-1
Fail Tolerance...25-11
FCC iii
FHSS .. See Frequency-Hopping Spread Spectrum
Filename Conventions 34-1
Filter 23-1, 25-9
 Applying...30-16
 Configuring 30-4
 Example 30-13
 Generic Filter Rule....................................30-11
 Generic Rule 30-11
 NAT 30-15
 Remote Node..30-17
 Structure 30-2
 TCP/IP Rule 30-7
Filters
 Executing a Filter Rule..............................30-2
 IP Filter Logic Flow 30-9
Finger 10-7, 18-3
Firewall...................................... 1-2, 13-1, 13-2
 Access Methods 29-1
 Remote Management 29-1
 SMT Menus..29-1
Firmware File
 Maintenance 19-6, 19-8
Fragment Threshold......................................23-7
Fragmentation Threshold.................................7-4
Frequency-Hopping Spread Spectrum............ F-2
FTP ... 5-3, 6-1, 10-6, 10-7, 13-2, 14-2, 14-6, 18-3, 36-2
FTP File Transfer 34-8
FTP Restrictions 14-2, 34-4, 36-2
FTP Server....................................... 1-5, 28-13
Full Network Management..............................1-5

G

Gateway..26-2
Gateway IP Addr 25-7

Gateway IP Address 24-2
General Setup 3-1, 5-1, 21-1
Global 10-1

H

Hidden Menus 20-4
Hop Count 26-2
Host 5-6, 21-4
How PPPoE Works A-2
HTTP 10-7, 18-3, 38-8, 38-10

I

i.e. ....See Syntax Conventions
IBSS .... 7-1. See Independent Basic Service Set
Idle Timeout 25-4, 25-5
IEEE 802.11 .... F-1
    Deployment Issues G-1
    Security Flaws G-1
IEEE 802.1x G-1, 1-2
    Advantages G-1
IGMP 6-2
Incoming Protocol Filters 23-6
Independent Basic Service Set F-2, 7-1
Industry Canada iv
Infrastructure Configuration F-2
Inside 10-1
Inside Global Address 10-1
Inside Local Address 10-1
Internet access 24-1
Internet Access 23-2, 24-1
    ISP's Name 24-2
Internet Access Setup 24-1, 24-2, 28-1
Internet Security Gateway 1-1
Introduction to Filters 30-1
IP Address..3-10, 3-11, 6-2, 6-6, 10-6, 10-8, 10-9,
    19-4, 23-4, 23-6, 24-2, 25-7, 26-2, 33-4
IP Address Assignment 25-7
IP Address Assignment 24-2
IP Alias 1-4, 23-6
IP Alias Setup 23-5
IP Multicast 1-4
Internet Group Management Protocol (IGMP)
    1-4
IP Pool 6-5, 6-6, 23-3
IP Pool Setup 6-1
IP Ports 38-8, 38-10
IP Static Route 26-1
IP Static Route Setup 26-1
IP Subnet Mask 23-6
IPSec standard 1-2
IPSec VPN Capability 1-2
ISP's Name 24-2

L

LAN Setup 6-1, 9-1
LAN TCP/IP 6-1
Local 10-1
Local User Database 8-27
Log Facility 33-6
Logging 1-5
Login Name ....See My Login Name

M

MAC Address 22-1
MAC Address Filter Action 8-27, 23-10
MAC Address Filtering 8-25, 23-9
MAC Filter 8-25
Main Menu 20-4
Management Information Base (MIB).. 14-8, 31-2
Many to Many No Overload ....See NAT
Many to Many Overload ....See NAT
Many to One ....See NAT
MD5 ....H-1
Message Digest Algorithm 5 ....See MD5
Message Logging 33-5
Metric 9-1, 11-3, 25-8, 26-2
Multicast 6-2, 6-7, 23-4, 25-9
My IP Addr 25-6
My Login 25-2
My Login Name 24-2
My Password 24-2, 25-3
My Server IP Addr 25-6

N

Nailed-up Connection 25-4
Nailed-Up Connection 25-5
NAT 3-7, 10-6, 10-7, 10-8, 10-9, 25-8, 30-16
  Applying NAT in the SMT Menus 28-1
  Configuring 28-3
  Definitions 10-1
  Examples 28-10
  How NAT Works 10-2
  Mapping Types 10-4
  Non NAT Friendly Application Programs28-16
  Ordering Rules 28-6
  Server Sets 10-6
  What NAT does 10-2
NAT Traversal 12-1, 12-2, 12-3
Navigation Panel 2-3
Network Address Translation 24-3
Network Address Translation (NAT) 1-4, 28-1
Network Management 10-7, 18-4
Network Topology With RADIUS Server
  Example G-2
NNTP 10-7, 18-4
Notice iii

O

Offline 21-5
One to One ....See NAT
Online Registration v
Outgoing Protocol Filters 23-6
Outside 10-1

P

Packet Filtering 1-3
Packing List Card xxxi
PAP 25-5
Password 5-5, 20-1, 20-6, 31-2. See My Password
Period(hr) 25-5
Ping 33-11
Point-to-Point Tunneling Protocol 3-9, 10-7, 18-4.
  See PPTP
POP3 .... 10-7, 18-4
Port Forwarding 1-4
Port Numbers 10-7, 18-3
PPPoE 1-3, 3-5, 3-7
PPPoE Encapsulation 24-1, 24-5, 25-1, 25-4, 25-5
PPTP 3-5, 3-7, 3-9, 10-7, 18-4
  Client 24-3, 24-4
  Configuring a Client 24-3, 24-4
PPTP and the Prestige B-1
PPTP Encapsulation 1-3, 3-9, 25-6
PPTP Protocol Overview B-2
PPTP, What is it? B-1
Preamble Mode 8-6
Prestige as a PPPoE Client A-3
Priorities 18-2
Priority 18-2
Priority Level 18-2
Private 11-4, 25-8, 26-3
Private IP Address 3-11
Protocol Filters 23-6
  Incoming 23-6
  Outgoing 23-6

Q

Quick Start Guide 2-1

R

RADIUS 1-2, 8-29
RAS 33-4
Related Documentation xxxi
Relay 23-2
Rem Node Name 25-2
Remote Authentication Dial In User Service .. See
  RADIUS
Remote Management
  Firewall 29-1
Remote Management and NAT 14-2
Remote Management Limitations 14-2, 36-2
Remote Node 25-1
Remote Node Filter 25-9
Remote Node Traffic 30-18

Repairs v
Replacement v
Required fields 20-4
Reset Button 1-1
Resetting the Time 35-6
Restore 19-9
Restore Configuration 34-6
Return Material Authorization Number v
RF signals F-1
RIP 6-2, 23-4, 23-6, 25-8
  Direction 23-6
  Version 23-6, 25-8
RoadRunner Support 1-5
Roaming 7-6
  Enable on ZyAIR 23-11
  Example 7-7
  Requirements 7-8
Route 25-3
RTC .... See Real Time Chip
RTS Threshold 7-3, 23-7

S

SA Monitor 39-1
Schedule Sets
  Duration 37-2
Schedules 25-5
Security Association 39-1
Security Parameters 8-3
Select ....See Syntax Conventions
Server 5-8, 10-5, 24-2, 25-3, 28-3, 28-4, 28-5, 28-8, 28-9, 28-11, 28-12, 35-6
Server IP 25-3
Service v
Service Name 25-5
Service Set 7-6
Service Type 24-2, 25-2
Services 10-6, 10-7, 13-8, 18-3
Session Initated Protocol 18-2
setup a schedule 37-2
SIP 18-2
SMT Menu Overview 20-2
SMTP 10-7, 18-3
SNMP 10-7, 13-2, 14-7, 18-4
  Community 31-3
  Configuration 31-2
  Get 14-9, 31-2
  Manager 14-8, 31-2
  MIBs 14-9, 31-2
  Trap 14-9, 31-2
  Trusted Host 31-3
SNMP (Simple Network Management Protocol) 1-4
Stateful Inspection 1-2, 13-1
Static Route 11-1
SUA 10-6, 10-7, 10-9
SUA (Single User Account) .. See NAT. See NAT
Subnet Mask . 3-11, 6-2, 6-6, 23-4, 24-2, 25-7, 26-2, 33-4
Support Disk xxxi
Syntax Conventions xxxi
Syslog 33-5
Syslog IP Address 33-6
Syslog Server 33-5
System
  Console Port Speed 33-4
  Diagnostic 33-9
  Log and Trace 33-5
  Syslog and Accounting 33-5
  System Information 33-3
  System Status 33-1
System Information 33-3
System Information & Diagnosis 33-1
System Maintenance ... 17-2, 33-1, 33-2, 33-3, 33-11, 34-2, 34-5, 34-11, 35-1, 35-2, 35-3, 35-4, 35-5
System Management Terminal 20-3
System Name 5-2, 21-2
System Status 33-2
System Timeout 14-2

T

TCP/IP 6-6, 14-4, 23-3, 23-4, 25-7, 30-6, 30-7, 30-9, 30-12, 30-15
  Setup 23-4
TCP/IP filter rule 30-6
Telnet 14-4
Telnet Configuration 14-4
TFTP and FTP over WAN Management
  Limitations 34-4
TFTP and FTP Over WAN} 14-2, 36-2
TFTP File Transfer 34-10
TFTP Restrictions 14-2, 34-4, 36-2
Time and Date 1-1
Time and Date Setting 35-5, 35-6
Time Zone 5-6, 35-6
Timeout 24-4, 24-5, 25-5
TLS H-1
Trace Records 33-5
Tracing 1-5
Trademarks ii
Traffic Redirect 1-4, 9-12
  Setup 25-10
Transport Layer Security .... See TLS
Triangle K-1
Triangle Route\ Solutions K-2
Trigger Port Forwarding 28-18
  Process 10-14
TTLS H-1
Tunneled Transport Layer Service .... See TTLS

U

Universal Plug and Play 1-3
Universal Plug and Play (UPnP) 12-1, 12-3
UNIX Syslog 33-5
UNIX syslog parameters 33-5
Upload Firmware 34-8
UPnP 1-3
UPnP Examples 12-4
Use Server Detected IP 21-5
User Authentication 8-9
User Name 5-5, 21-4
User Profiles 8-27, 27-1
User Specified IP Addr 21-5

V

Virtual Private Network 1-2
VoIP 18-2
VPN 9-6
VPN Application 1-6

W

WAN DHCP 33-10, 33-11
WAN Setup 3-12, 22-1
Warranty v
Web 14-2
Web Configurator 2-1, 29-2
WEP 8-4
WEP Encryption 8-7, 8-11, 23-7
What is PPTP? B-1
Wireless Client WPA Supplicants 8-13
Wireless LAN F-1, 23-6
  Benefits F-1
Wireless LAN Setup 23-6
Wireless Security 8-1
Wizard Setup 3-1, 3-2, 3-3, 3-10, 4-1, 4-2
WLAN .... See Wireless LAN
WPA 8-8
WPA with RADIUS Application 8-13
WPA-PSK Application 8-9
WWW 18-3
www.dyndns.org 21-5

X

XBox Live 18-2

Z

ZyNOS 33-3, 34-1, 34-2
ZyNOS F/W Version 33-3, 34-1
ZyXEL Limited Warranty
  Note v