

Prestige 792H

G.SHDSL 4-port Security Gateway

User's Guide

Version 3.40(BZ.0)

March 2004



Copyright

Copyright © 2004 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

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

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:

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

Notice 1

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

Certifications

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

Information for Canadian Users

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

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

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

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

Caution

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

Note

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

ZyXEL Limited Warranty

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

Note

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

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

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.
2. Do not use this product near water, for example, in a wet basement or near a swimming pool.
3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

Customer Support

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

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

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE 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

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
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
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
Please have the following information ready when you contact customer support.	vi
List of Figures	xix
List of Tables	xxv
Preface	xxix
Introduction to DSL	xxxi
Chapter 1 Getting to Know Your G.SHDSL Router	1-1
1.1 Features of the Prestige	1-1
1.2 Application Scenarios for the Prestige	1-5
1.2.1 Internet Access	1-5
1.2.2 LAN-to-LAN Application	1-5
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 Navigating the Prestige Web Configurator	2-2
2.4 Configuring Password	2-3
2.5 Resetting the Prestige	2-4
2.5.1 Using The Reset Button	2-5
2.5.2 Uploading a Configuration File Via Console Port	2-5
Chapter 3 Wizard Setup	3-1
3.1 Wizard Setup Introduction	3-1
3.2 WAN Setup	3-1
3.2.1 Service Type	3-1
3.2.2 Rate Adaption	3-1
3.2.3 Transfer Rates	3-2
3.2.4 Standard Mode	3-2
3.3 Encapsulation	3-2
3.3.1 ENET ENCAP	3-2
3.3.2 PPP over Ethernet	3-2
3.3.3 PPPoA	3-3
3.3.4 RFC 1483	3-3
3.4 Multiplexing	3-3
3.4.1 VC-based Multiplexing	3-3
3.4.2 LLC-based Multiplexing	3-3
3.5 VPI and VCI	3-4
3.6 Wizard Setup Configuration: First Screen	3-4

3.7	IP Address and Subnet Mask	3-6
3.8	IP Address Assignment.....	3-7
3.8.1	IP Assignment with PPPoA or PPPoE Encapsulation	3-7
3.8.2	IP Assignment with RFC 1483 Encapsulation	3-7
3.8.3	IP Assignment with ENET ENCAP Encapsulation	3-8
3.8.4	Private IP Addresses	3-8
3.9	Nailed-Up Connection (PPP).....	3-8
3.10	NAT	3-9
3.11	Wizard Setup Configuration: ISP Parameters.....	3-9
3.11.1	PPPoA.....	3-9
3.11.2	RFC 1483.....	3-12
3.11.3	ENET ENCAP	3-12
3.11.4	PPPoE	3-14
3.12	DHCP Setup.....	3-15
3.12.1	IP Pool Setup.....	3-16
3.13	Wizard Setup Configuration: LAN Configuration.....	3-16
3.14	Wizard Setup Configuration: Connection Tests.....	3-18
3.15	Test Your Internet Connection.....	3-19
Chapter 4	LAN Setup	4-1
4.1	LAN Overview.....	4-1
4.1.1	LANs, WANs and the Prestige	4-1
4.2	DNS Server Address.....	4-1
4.3	DNS Server Address Assignment.....	4-2
4.4	LAN TCP/IP	4-2
4.4.1	Factory LAN Defaults.....	4-3
4.4.2	IP Address and Subnet Mask	4-3
4.4.3	RIP Setup	4-3
4.4.4	Multicast	4-3
4.5	Configuring LAN.....	4-4
Chapter 5	WAN Setup	5-1
5.1	WAN Overview	5-1
5.2	Metric.....	5-1
5.3	PPPoE Encapsulation.....	5-2
5.4	Traffic Shaping	5-3
5.5	Configuring WAN Setup	5-4
5.6	Traffic Redirect.....	5-8
5.7	Configuring WAN Backup	5-9
5.8	Outgoing Authentication Protocol	5-12
5.9	Configuring Advanced WAN Backup	5-13
5.10	AT Command Strings	5-17
5.11	DTR Signal.....	5-18
5.12	Response Strings.....	5-18

5.13 Configuring Advanced Modem Setup	5-18
Chapter 6 Network Address Translation (NAT)	6-1
6.1 NAT Overview	6-1
6.1.1 NAT Definitions	6-1
6.1.2 What NAT Does	6-1
6.1.3 How NAT Works	6-2
6.1.4 NAT Application	6-2
6.1.5 NAT Mapping Types	6-3
6.2 SUA (Single User Account) Versus NAT	6-4
6.3 SUA Server	6-5
6.3.1 Port Forwarding: Services and Port Numbers	6-5
6.3.2 Configuring Servers Behind SUA (Example)	6-6
6.4 Selecting the NAT Mode	6-7
6.5 Configuring SUA Server	6-8
6.6 Configuring Address Mapping	6-10
6.7 Editing an Address Mapping Rule	6-12
Chapter 7 Dynamic DNS Setup	7-1
7.1 Dynamic DNS	7-1
7.1.1 DynDNS Wildcard	7-1
7.2 Configuring Dynamic DNS	7-1
Chapter 8 Firewall	8-1
8.1 Firewall Overview	8-1
8.2 Types of Firewalls	8-1
8.2.1 Packet Filtering Firewalls	8-1
8.2.2 Application-level Firewalls	8-1
8.2.3 Stateful Inspection Firewalls	8-2
8.3 Introduction to ZyXEL's Firewall	8-2
8.4 Denial of Service	8-3
8.4.1 Basics	8-3
8.4.2 Types of DoS Attacks	8-4
8.5 Stateful Inspection	8-7
8.5.1 Stateful Inspection Process	8-8
8.5.2 Stateful Inspection and the Prestige	8-9
8.5.3 TCP Security	8-10
8.5.4 UDP/ICMP Security	8-10
8.5.5 Upper Layer Protocols	8-11
8.6 Guidelines for Enhancing Security with Your Firewall	8-11
8.6.1 Security In General	8-11
8.7 Packet Filtering Vs Firewall	8-12
8.7.1 Packet Filtering:	8-13
8.7.2 Firewall	8-13
Chapter 9 Firewall Configuration	9-1

9.1 Remote Management and the Firewall	9-1
9.2 Enabling the Firewall	9-1
9.3 Configuring E-mail Alerts	9-2
9.4 Attack Alert.....	9-3
9.4.1 Alerts.....	9-4
9.4.2 Threshold Values	9-4
9.4.3 Half-Open Sessions.....	9-4
Chapter 10 Creating Custom Rules.....	10-1
10.1 Rules Overview.....	10-1
10.2 Rule Logic Overview	10-1
10.2.1 Rule Checklist.....	10-1
10.2.2 Security Ramifications.....	10-2
10.2.3 Key Fields For Configuring Rules	10-2
10.3 Connection Direction	10-3
10.3.1 LAN to WAN Rules.....	10-3
10.3.2 WAN to LAN Rules	10-4
10.4 Logs	10-4
10.5 Rule Summary	10-6
10.6 Predefined Services.....	10-8
10.7 Creating/Editing Firewall Rules.....	10-11
10.7.1 Source and Destination Addresses	10-13
10.8 Timeout.....	10-14
10.8.1 Factors Influencing Choices for Timeout Values.....	10-15
Chapter 11 Customized Services.....	11-1
11.1 Introduction to Customized Services	11-1
11.2 Creating/Editing A Customized Service	11-2
11.3 Example Custom Service Firewall Rule	11-3
Chapter 12 Content Filtering.....	12-1
12.1 Content Filtering Overview	12-1
12.2 Configuring Keyword Blocking.....	12-1
12.3 Configuring the Schedule.....	12-3
12.4 Configuring Trusted Computers	12-4
12.5 Configuring Logs	12-5
Chapter 13 Introduction to IPSec.....	13-1
13.1 VPN Overview	13-1
13.1.1 IPSec	13-1
13.1.2 Security Association	13-1
13.1.3 Other Terminology.....	13-1
13.1.4 VPN Applications	13-2
13.2 IPSec Architecture	13-3
13.2.1 IPSec Algorithms	13-4
13.2.2 Key Management	13-4

13.3 Encapsulation	13-5
13.3.1 Transport Mode	13-5
13.3.2 Tunnel Mode	13-5
13.4 IPSec and NAT	13-5
Chapter 14 VPN Screens.....	14-1
14.1 VPN/IPSec Overview.....	14-1
14.2 IPSec Algorithms	14-1
14.2.1 AH (Authentication Header) Protocol.....	14-1
14.2.2 ESP (Encapsulating Security Payload) Protocol	14-1
14.3 My IP Address.....	14-2
14.4 Secure Gateway Address.....	14-2
14.4.1 Dynamic Secure Gateway Address	14-2
14.5 VPN Summary Screen	14-3
14.6 Keep Alive	14-5
14.7 ID Type and Content	14-5
14.7.1 ID Type and Content Examples	14-6
14.8 Pre-Shared Key	14-7
14.9 Editing VPN Policies	14-7
14.10 IKE Phases.....	14-13
14.10.1 Negotiation Mode.....	14-14
14.10.2 Diffie-Hellman (DH) Key Groups.....	14-14
14.10.3 Perfect Forward Secrecy (PFS)	14-14
14.11 Configuring Advanced IKE Settings	14-15
14.12 Manual Key Setup	14-18
14.12.1 Security Parameter Index (SPI).....	14-19
14.13 Configuring Manual Key	14-19
14.14 Viewing SA Monitor.....	14-24
14.15 Configuring Global Setting.....	14-26
14.16 Configuring IPSec Logs.....	14-27
14.17 Telecommuter VPN/IPSec Examples	14-31
14.17.1 Telecommuters Sharing One VPN Rule Example.....	14-31
14.17.2 Telecommuters Using Unique VPN Rules Example.....	14-32
14.18 VPN and Remote Management.....	14-34
Chapter 15 Remote Management Configuration	15-1
15.1 Remote Management Overview	15-1
15.1.1 Remote Management Limitations	15-1
15.1.2 Remote Management and NAT.....	15-1
15.1.3 System Timeout.....	15-2
15.2 Telnet	15-2
15.3 FTP	15-2
15.4 Web	15-2
15.5 Configuring Remote Management	15-3

Chapter 16 Universal Plug-and-Play (UPnP)	16-1
16.1 Universal Plug and Play Overview	16-1
16.1.1 How do I know if I'm using UPnP?	16-1
16.1.2 NAT Transversal	16-1
16.1.3 Cautions with UPnP	16-1
16.1.4 UPnP and ZyXEL	16-2
16.2 Accessing the Prestige Web Configurator to Configure UPnP	16-2
16.2.1 Configuring UPnP	16-2
16.3 Installing UPnP in Windows Example	16-3
16.4 Using UPnP in Windows XP Example	16-6
Chapter 17 Maintenance	17-1
17.1 Maintenance Overview	17-1
17.2 System Status Screen	17-1
17.2.1 System Statistics	17-4
17.3 DHCP Table Screen	17-6
17.4 Diagnostic Screens	17-6
17.4.1 Diagnostic General Screen	17-7
17.4.2 Diagnostic DSL Line Screen	17-8
17.5 Firmware Screen	17-9
Chapter 18 Introducing the SMT	18-1
18.1 SMT Introduction	18-1
18.1.1 Procedure for SMT Configuration via Console Port	18-1
18.1.2 Procedure for SMT Configuration via Telnet	18-1
18.1.3 Entering Password	18-1
18.1.4 Prestige SMT Menu Overview	18-2
18.2 Navigating the SMT Interface	18-4
18.2.1 System Management Terminal Interface Summary	18-5
18.3 Changing the System Password	18-6
Chapter 19 General Setup	19-1
19.1 General Setup	19-1
19.2 Configuring Menu 1	19-1
19.2.1 Configuring Dynamic DNS	19-3
Chapter 20 WAN Setup	20-1
20.1 WAN Setup	20-1
20.2 WAN Setup Screen	20-1
Chapter 21 Dial Backup	21-1
21.1 Dial Backup Overview	21-1
21.1.1 Configuring Dial Backup in Menu 2	21-1
21.1.2 Advanced WAN Setup	21-2
21.2 Remote Node Profile (Backup ISP)	21-4
21.2.1 Editing PPP Options	21-7
21.2.2 Editing TCP/IP Options	21-7

21.2.3 Editing Filter Sets.....	21-9
Chapter 22 LAN Setup.....	22-1
22.1 Ethernet Setup	22-1
22.1.1 LAN Port Filter Setup	22-1
22.1.2 IP Alias Setup.....	22-2
22.1.3 Route IP Setup.....	22-3
22.1.4 TCP/IP Ethernet Setup and DHCP	22-4
Chapter 23 Internet Access.....	23-1
23.1 Internet Access Overview	23-1
23.2 Internet Access Setup.....	23-1
Chapter 24 Remote Node Configuration.....	24-1
24.1 Remote Node Overview	24-1
24.2 Remote Node Setup.....	24-1
24.2.1 Encapsulation and Multiplexing Scenarios	24-2
24.3 Remote Node Network Layer Options	24-5
24.3.1 My WAN Addr Sample IP Addresses.....	24-8
24.4 Remote Node Filter	24-8
24.5 Editing ATM Layer Options	24-9
24.5.1 VC-based Multiplexing (non-PPP Encapsulation)	24-10
24.5.2 LLC-based Multiplexing or PPP Encapsulation.....	24-10
Chapter 25 Static Route Setup	25-1
25.1 Static Route Overview	25-1
Chapter 26 Bridging Setup.....	26-1
26.1 Bridging Overview	26-1
26.2 Bridge Ethernet Setup	26-1
26.2.1 Remote Node Bridging Setup.....	26-1
26.2.2 Bridge Static Route Setup	26-2
Chapter 27 Network Address Translation (NAT)	27-1
27.1 SUA (Single User Account) Versus NAT	27-1
27.2 Applying NAT	27-1
27.3 NAT Setup	27-3
27.3.1 Address Mapping Sets.....	27-3
27.3.2 Configuring a Server behind NAT	27-9
27.4 General NAT Examples	27-11
27.4.1 Example 1: Internet Access Only.....	27-11
27.4.2 Example 2: Internet Access with an Inside Server	27-13
27.4.3 Example 3: Multiple Public IP Addresses With Inside Servers	27-14
27.4.4 Example 4: NAT Unfriendly Application Programs	27-18
Chapter 28 Filter Configuration	28-1
28.1 About Filtering	28-1
28.2 Filter Set Configuration.....	28-4
28.2.1 Filter Rules Summary Menus.....	28-8

28.3 Filter Rule Configuration	28-9
28.3.1 TCP/IP Filter Rule	28-10
28.3.2 Generic Filter Rule	28-14
28.4 Filter Types and NAT	28-16
28.5 Example Filter	28-16
28.6 Applying Filters and Factory Defaults	28-20
28.6.1 Ethernet Traffic	28-20
28.6.2 Remote Node Filters	28-21
Chapter 29 SNMP Configuration	29-1
29.1 SNMP Overview	29-1
29.2 Supported MIBs	29-2
29.3 SNMP Configuration	29-2
29.4 SNMP Traps	29-3
Chapter 30 System Maintenance	30-1
30.1 System Maintenance Overview	30-1
30.2 System Status	30-1
30.3 System Information	30-3
30.3.1 System Information	30-3
30.3.2 Console Port Speed	30-5
30.4 Log and Trace	30-5
30.4.1 Viewing Error Log	30-5
30.4.2 Syslog	30-6
30.5 Diagnostic	30-8
Chapter 31 Firmware and Configuration File Maintenance	31-1
31.1 Filename Conventions	31-1
31.2 Backup Configuration	31-2
31.2.1 Backup Configuration	31-3
31.2.2 Using the FTP Command from the Command Line	31-3
31.2.3 Example of FTP Commands from the Command Line	31-3
31.2.4 GUI-based FTP Clients	31-4
31.2.5 TFTP and FTP over WAN Management Limitations	31-4
31.2.6 Backup Configuration Using TFTP	31-5
31.2.7 TFTP Command Example	31-5
31.2.8 GUI-based TFTP Clients	31-5
31.2.9 Backup Via Console Port	31-6
31.3 Restore Configuration	31-7
31.3.1 Restore Using FTP	31-8
31.3.2 Restore Using FTP Session Example	31-9
31.3.3 Restore Via Console Port	31-9
31.4 Uploading Firmware and Configuration Files	31-10
31.4.1 Firmware File Upload	31-10
31.4.2 Configuration File Upload	31-11

31.4.3 FTP File Upload Command from the DOS Prompt Example	31-12
31.4.4 FTP Session Example of Firmware File Upload	31-12
31.4.5 TFTP File Upload.....	31-12
31.4.6 TFTP Upload Command Example	31-13
31.4.7 Uploading Via Console Port.....	31-13
31.4.8 Uploading Firmware File Via Console Port	31-14
31.4.9 Example Xmodem Firmware Upload Using HyperTerminal.....	31-14
31.4.10 Uploading Configuration File Via Console Port	31-15
31.4.11 Example Xmodem Configuration Upload Using HyperTerminal	31-15
Chapter 32 System Maintenance and Information	32-1
32.1 Command Interpreter Mode	32-1
32.2 Call Control Support	32-2
32.2.1 Budget Management.....	32-2
32.3 Time and Date Setting.....	32-4
32.3.1 Resetting the Time	32-5
Chapter 33 IP Policy Routing.....	33-1
33.1 IP Policy Routing Overview	33-1
33.1.1 IP Policy Routing Benefits	33-1
33.1.2 Routing Policy.....	33-1
33.2 IP Routing Policy Setup	33-2
33.3 Applying an IP Policy	33-5
33.3.1 Ethernet IP Policies	33-5
33.4 IP Policy Routing Example	33-7
Chapter 34 Call Scheduling.....	34-1
34.1 Call Scheduling Overview	34-1
34.2 Schedule Setup	34-1
Chapter 35 Remote Management	35-1
35.1 Remote Management Overview	35-1
35.1.1 Remote Management and Telnet Services	35-1
35.1.2 Remote Management and FTP Services.....	35-1
35.1.3 Remote Management and Web Services	35-2
35.1.4 Disabling Remote Management	35-2
35.2 Remote Management Setup	35-2
35.2.1 Remote Management Limitations	35-3
35.3 Remote Management and NAT.....	35-3
35.4 System Timeout	35-3
Chapter 36 VPN/IPSec Setup	36-1
36.1 VPN/IPSec Overview.....	36-1
36.2 IPSec Summary Screen	36-2
36.3 IPSec Setup	36-5
36.4 IKE Setup.....	36-11
36.5 Manual Setup	36-13

- 36.5.1 Active Protocol36-13
- 36.5.2 Security Parameter Index (SPI).....36-13
- Chapter 37 SA Monitor37-1**
 - 37.1 SA Monitor Overview.....37-1
 - 37.2 Using SA Monitor.....37-1
 - 37.3 Viewing IPsec Log.....37-3
 - 37.3.1 VPN Responder IPsec Log.....37-3
- Chapter 38 Internal SPTGEN.....38-1**
 - 38.1 Internal SPTGEN Overview38-1
 - 38.2 The Configuration Text File Format.....38-1
 - 38.2.1 Internal SPTGEN File Modification - Important Points to Remember.....38-2
 - 38.3 Internal SPTGEN FTP Download Example.....38-3
 - 38.4 Internal SPTGEN FTP Upload Example38-4
- Appendix A Troubleshooting.....A-1**
- Appendix B PPPoEB-1**
- Appendix C Virtual Circuit TopologyC-1**
- Appendix D PPTPD-1**
- Appendix E IndexE-1**

List of Figures

Figure 1-1 Internet Access Application	1-5
Figure 1-2 LAN-to-LAN Application	1-5
Figure 2-1 Password Screen	2-2
Figure 2-2 Web Configurator SITE MAP Screen	2-3
Figure 2-3 Password	2-4
Figure 2-4 Example Xmodem Upload	2-5
Figure 3-1 Wizard Screen: WAN Setup	3-4
Figure 3-2 Wizard Screen: Internet Access	3-5
Figure 3-3 Internet Connection with PPPoA	3-10
Figure 3-4 Internet Connection with RFC 1483	3-12
Figure 3-5 Internet Connection with ENET ENCAP	3-13
Figure 3-6 Internet Connection with PPPoE	3-14
Figure 3-7 Wizard Screen: LAN Configuration	3-16
Figure 3-8 Wizard: LAN Configuration	3-17
Figure 3-9 Wizard Screen: Connection Tests	3-19
Figure 4-1 LAN and WAN IP Addresses	4-1
Figure 4-2 LAN	4-4
Figure 5-1 Example of Traffic Shaping	5-4
Figure 5-2 WAN Setup	5-5
Figure 5-3 Traffic Redirect Example	5-8
Figure 5-4 Traffic Redirect LAN Setup	5-9
Figure 5-5 WAN Backup	5-10
Figure 5-6 Advanced WAN Backup	5-14
Figure 5-7 Advanced Modem Setup	5-19
Figure 6-1 How NAT Works	6-2
Figure 6-2 NAT Application With IP Alias	6-3
Figure 6-3 Multiple Servers Behind NAT Example	6-7
Figure 6-4 NAT Mode	6-7
Figure 6-5 Edit SUA/NAT Server Set	6-9
Figure 6-6 Address Mapping Rules	6-11
Figure 6-7 Address Mapping Rule Edit	6-12
Figure 7-1 DDNS	7-2
Figure 8-1 Prestige Firewall Application	8-3
Figure 8-2 Three-Way Handshake	8-5
Figure 8-3 SYN Flood	8-5
Figure 8-4 Smurf Attack	8-6

Figure 8-5 Stateful Inspection	8-8
Figure 9-1 Enabling the Firewall	9-1
Figure 9-2 E-mail	9-2
Figure 9-3 Alert.....	9-6
Figure 10-1 LAN to WAN Traffic	10-3
Figure 10-2 WAN to LAN Traffic	10-4
Figure 10-3 Firewall Logs.....	10-5
Figure 10-4 Firewall Rules Summary: First Screen	10-7
Figure 10-5 Creating/Editing A Firewall Rule	10-12
Figure 10-6 Adding/Editing Source and Destination Addresses	10-14
Figure 10-7 Timeout.....	10-15
Figure 11-1 Customized Services	11-1
Figure 11-2 Creating/Editing A Customized Service	11-2
Figure 11-3 Edit Rule Example.....	11-3
Figure 11-4 Configure Source IP Example	11-4
Figure 11-5 Customized Service for MyService Example	11-4
Figure 11-6 Syslog Rule Configuration Example	11-5
Figure 11-7 Rule Summary Example	11-6
Figure 12-1 Content Filter: Keyword.....	12-2
Figure 12-2 Content Filter: Schedule	12-3
Figure 12-3 Content Filter: Trusted.....	12-4
Figure 12-4 Content Filter Logs.....	12-5
Figure 13-1 Encryption and Decryption.....	13-2
Figure 13-2 VPN Application	13-3
Figure 13-3 IPSec Architecture.....	13-4
Figure 13-4 Transport and Tunnel Mode IPSec Encapsulation.....	13-5
Figure 14-1 IPSec Summary Fields	14-3
Figure 14-2 VPN Summary	14-4
Figure 14-3 VPN IKE	14-8
Figure 14-4 Two Phases to Set Up the IPSec SA	14-13
Figure 14-5 VPN IKE: Advanced	14-15
Figure 14-6 VPN Manual Key	14-20
Figure 14-7 SA Monitor.....	14-25
Figure 14-8 Global Setting.....	14-26
Figure 14-9 VPN Logs.....	14-27
Figure 14-10 Telecommuters Sharing One VPN Rule Example	14-31
Figure 14-11 Telecommuters Using Unique VPN Rules Example	14-33
Figure 15-1 Telnet Configuration on a TCP/IP Network	15-2
Figure 15-2 Remote Management.....	15-3
Figure 16-1 Configuring UPnP	16-3

Figure 17-1 System Status.....	17-2
Figure 17-2 System Status: Show Statistics	17-4
Figure 17-3 DHCP Table.....	17-6
Figure 17-4 Diagnostic.....	17-7
Figure 17-5 Diagnostic General	17-7
Figure 17-6 Diagnostic DSL Line	17-8
Figure 17-7 Firmware Upgrade.....	17-10
Figure 17-8 Network Temporarily Disconnected	17-11
Figure 17-9 Error Message.....	17-11
Figure 18-1 Login Screen.....	18-2
Figure 18-2 Prestige Menu Overview	18-3
Figure 18-3 SMT Main Menu	18-5
Figure 18-4 Menu 23 System Password.....	18-6
Figure 19-1 Menu 1 General Setup	19-2
Figure 19-2 Menu 1.1 Configure Dynamic DNS	19-3
Figure 20-1 WAN Setup.....	20-1
Figure 21-1 Menu 2: Dial Backup Setup.....	21-1
Figure 21-2 Advanced WAN Setup	21-3
Figure 21-3 Remote Node Profile (Backup ISP).....	21-5
Figure 21-4 Menu 11.2 - Remote Node PPP Options.....	21-7
Figure 21-5 Remote Node PPP Options Menu Fields	21-7
Figure 21-6 Remote Node Network Layer Options	21-8
Figure 21-7 Menu 11.5: Remote Node Filter (Ethernet)	21-10
Figure 22-1 TCP/IP Ethernet Setup.....	22-1
Figure 22-2 LAN Port Filter Setup.....	22-1
Figure 22-3 TCP/IP and DHCP Setup	22-2
Figure 22-4 IP Alias Setup	22-3
Figure 22-5 General Setup	22-4
Figure 22-6 TCP/IP and DHCP Ethernet Setup.....	22-4
Figure 23-1 Internet Access Setup.....	23-1
Figure 24-1 Remote Node Setup	24-2
Figure 24-2 Remote Node Profile	24-3
Figure 24-3 Remote Node Network Layer Options	24-6
Figure 24-4 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection	24-8
Figure 24-5 Remote Node Filter (PPPoA or PPPoE Encapsulation).....	24-9
Figure 24-6 Remote Node Filter (RFC1483 or ENET ENCAP Encapsulation).....	24-9
Figure 24-7 Menu 11.6 for VC-based Multiplexing (non-PPP Encapsulation).....	24-10
Figure 24-8 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation.....	24-10
Figure 25-1 Sample Static Routing Topology Configuration	25-1
Figure 25-2 Static Route Setup.....	25-2

Figure 25-3 IP Static Route Setup	25-2
Figure 25-4 Edit IP Static Route	25-3
Figure 26-1 Remote Node Bridging Options	26-2
Figure 26-2 Bridge Static Route Setup	26-3
Figure 26-3 Edit Bridge Static Route	26-3
Figure 27-1 Applying NAT for Internet Access	27-2
Figure 27-2 Applying NAT to the Remote Node.....	27-2
Figure 27-3 NAT Setup	27-3
Figure 27-4 Address Mapping Sets	27-4
Figure 27-5 Address Mapping Rules - SUA	27-4
Figure 27-6 Address Mapping Rules	27-6
Figure 27-7 Editing/Configuring an Individual Rule in a Set	27-8
Figure 27-8 NAT Server Sets	27-9
Figure 27-9 NAT Server Setup.....	27-10
Figure 27-10 Multiple Servers Behind NAT Example	27-11
Figure 27-11 NAT Example 1	27-12
Figure 27-12 Internet Access & NAT Example.....	27-12
Figure 27-13 NAT Example 2	27-13
Figure 27-14 NAT Example 2 - Menu 15.2.1	27-14
Figure 27-15 NAT Example 3	27-15
Figure 27-16 Example 3 - Menu 11.3	27-15
Figure 27-17 Example 3 - Menu 15.1.1.1	27-16
Figure 27-18 Example 3 - Final Menu 15.1.1	27-16
Figure 27-19 Example 3- Menu 15.2	27-18
Figure 27-20 NAT Example 4	27-18
Figure 27-21 Example 4 - Menu 15.1.1.1	27-19
Figure 27-22 Example 4 - Menu 15.1.1	27-20
Figure 28-1 Outgoing Packet Filtering Process	28-2
Figure 28-2 Filter Rule Process.....	28-3
Figure 28-3 Filter Set Configuration	28-4
Figure 28-4 NetBios WAN Filter Rules Summary	28-5
Figure 28-5 NetBios LAN Filter Rules Summary	28-5
Figure 28-6 Telnet_WAN Filter Rules Summary	28-6
Figure 28-7 PPPoE Filter Rules Summary	28-6
Figure 28-8 FTP_WAN Filter Rules Summary	28-7
Figure 28-9 Web Set1 Filter Rules Summary	28-7
Figure 28-10 Web Set2 Filter Rules Summary	28-8
Figure 28-11 TCP/IP Filter Rule	28-10
Figure 28-12 Executing an IP Filter	28-13
Figure 28-13 Generic Filter Rule	28-14

Figure 28-14 Protocol and Device Filter Sets	28-16
Figure 28-15 Sample Telnet Filter	28-17
Figure 28-16 Sample Filter Rules Summary — Menu 21.1	28-18
Figure 28-17 Sample Filter Rules Summary — Menu 21.3.1	28-19
Figure 28-18 Sample Filter Rules Summary — Applying a Remote Node Filter Set	28-20
Figure 28-19 Filtering Ethernet Traffic	28-21
Figure 28-20 Filtering Remote Node Traffic	28-21
Figure 29-1 SNMP Management Model	29-1
Figure 29-2 SNMP Configuration	29-3
Figure 30-1 System Maintenance	30-1
Figure 30-2 System Maintenance — Status	30-2
Figure 30-3 System Information and Console Port Speed	30-3
Figure 30-4 System Maintenance — Information	30-4
Figure 30-5 System Maintenance – Change Console Port Speed	30-5
Figure 30-6 System Maintenance — Log and Trace	30-5
Figure 30-7 Sample Error and Information Messages	30-6
Figure 30-8 System Maintenance — Syslog and Accounting	30-6
Figure 30-9 System Maintenance — Diagnostic	30-8
Figure 31-1 System Maintenance - Backup Configuration	31-3
Figure 31-2 FTP Session Example	31-4
Figure 31-3 System Maintenance – Backup Configuration	31-6
Figure 31-4 System Maintenance – Starting Xmodem Download Screen	31-6
Figure 31-5 Backup Configuration Example	31-7
Figure 31-6 Successful Backup Confirmation Screen	31-7
Figure 31-7 System Maintenance - Restore Configuration	31-8
Figure 31-8 Restore Using FTP Session Example	31-9
Figure 31-9 System Maintenance – Restore Configuration	31-9
Figure 31-10 System Maintenance – Starting Xmodem Download Screen	31-9
Figure 31-11 Restore Configuration Example	31-10
Figure 31-12 Successful Restoration Confirmation Screen	31-10
Figure 31-13 System Maintenance - Upload System Firmware	31-11
Figure 31-14 Telnet Into Menu 24.7.2 – System Maintenance	31-11
Figure 31-15 FTP Session Example of Firmware File Upload	31-12
Figure 31-16 Menu 24.7.1 as seen using the Console Port	31-14
Figure 31-17 Example Xmodem Upload	31-14
Figure 31-18 Menu 24.7.2 as seen using the Console Port	31-15
Figure 31-19 Example Xmodem Upload	31-16
Figure 32-1 Command Mode in Menu 24	32-1
Figure 32-2 Valid Commands	32-2
Figure 32-3 Call Control	32-2

Figure 32-4 Budget Management.....	32-3
Figure 32-5 System Maintenance.....	32-4
Figure 32-6 System Maintenance — Time and Date Setting.....	32-4
Figure 33-1 IP Routing Policy Setup	33-2
Figure 33-2 Sample IP Routing Policy Setup.....	33-3
Figure 33-3 IP Routing Policy	33-4
Figure 33-4 TCP/IP and DHCP Ethernet Setup	33-6
Figure 33-5 Remote Node Network Layer Options	33-6
Figure 33-6 Example of IP Policy Routing	33-7
Figure 33-7 IP Routing Policy Example	33-8
Figure 33-8 IP Routing Policy	33-9
Figure 33-9 Applying IP Policies	33-9
Figure 34-1 Schedule Setup	34-1
Figure 34-2 Schedule Set Setup	34-2
Figure 34-3 Applying Schedule Set(s) to a Remote Node (PPPoE).....	34-4
Figure 35-1 Telnet Configuration on a TCP/IP Network	35-1
Figure 35-2 Remote Management Control.....	35-2
Figure 36-1 VPN SMT Menu Tree.....	36-1
Figure 36-2 Menu 27 VPN/IPSec Setup	36-2
Figure 36-3 Menu 27.1 IPSec Summary.....	36-2
Figure 36-4 Menu 27.1.1 IPSec Setup	36-6
Figure 36-5 Menu 27.1.1.1 IKE Setup.....	36-11
Figure 36-6 Menu 27.1.1.2 Manual Setup	36-14
Figure 37-1 Menu 27.2 SA Monitor.....	37-1
Figure 37-2 Example VPN Initiator IPSec Log	37-3
Figure 38-1 Configuration Text File Format: Column Descriptions	38-2
Figure 38-2 Invalid Parameter Entered: Command Line Example	38-3
Figure 38-3 Valid Parameter Entered: Command Line Example	38-3
Figure 38-4 Internal SPTGEN FTP Download Example	38-3
Figure 38-5 Internal SPTGEN FTP Upload Example	38-4

List of Tables

Table 2-1 Password	2-4
Table 3-1 Wizard Screen: WAN Setup	3-5
Table 3-2 Wizard Screen: Internet Access	3-6
Table 3-3 Internet Connection with PPPoA	3-10
Table 3-4 Internet Connection with RFC 1483	3-12
Table 3-5 Internet Connection with ENET ENCAP	3-13
Table 3-6 Internet Connection with PPPoE	3-15
Table 3-7 Wizard: LAN Configuration	3-17
Table 4-1 LAN	4-5
Table 5-1 WAN Setup	5-6
Table 5-2 WAN Backup	5-11
Table 5-3 Advanced WAN Backup	5-15
Table 5-4 Advanced Modem Setup	5-19
Table 6-1 NAT Definitions	6-1
Table 6-2 NAT Mapping Types	6-4
Table 6-3 Services and Port Numbers	6-6
Table 6-4 NAT Mode	6-8
Table 6-5 Edit SUA/NAT Server Set	6-9
Table 6-6 Address Mapping Rules	6-11
Table 6-7 Address Mapping Rule Edit	6-13
Table 7-1 DDNS	7-2
Table 8-1 Common IP Ports	8-4
Table 8-2 ICMP Commands That Trigger Alerts	8-6
Table 8-3 Legal NetBIOS Commands	8-7
Table 8-4 Legal SMTP Commands	8-7
Table 9-1 E-mail	9-2
Table 9-2 Alert	9-6
Table 10-1 Firewall Logs	10-5
Table 10-2 Firewall Rules Summary: First Screen	10-8
Table 10-3 Predefined Services	10-9
Table 10-4 Creating/Editing A Firewall Rule	10-12
Table 10-5 Adding/Editing Source and Destination Addresses	10-14
Table 10-6 Timeout	10-15
Table 11-1 Customized Services	11-2
Table 11-2 Creating/Editing A Customized Service	11-3
Table 12-1 Content Filter: Keyword	12-2
Table 12-2 Content Filter: Schedule	12-4

Table 12-3 Content Filter: Trusted	12-4
Table 12-4 Content Filter Logs	12-6
Table 13-1 VPN and NAT	13-6
Table 14-1 AH and ESP	14-2
Table 14-2 VPN Summary	14-4
Table 14-3 Local ID Type and Content Fields	14-6
Table 14-4 Peer ID Type and Content Fields	14-6
Table 14-5 Matching ID Type and Content Configuration Example.....	14-7
Table 14-6 Mismatching ID Type and Content Configuration Example.....	14-7
Table 14-7 VPN IKE	14-9
Table 14-8 VPN IKE: Advanced	14-16
Table 14-9 VPN Manual Key	14-21
Table 14-10 SA Monitor.....	14-25
Table 14-11 Global Setting	14-26
Table 14-12 VPN Logs.....	14-27
Table 14-13 Sample IKE Key Exchange Logs.....	14-28
Table 14-14 Sample IPSec Logs During Packet Transmission	14-29
Table 14-15 RFC-2408 ISAKMP Payload Types.....	14-30
Table 14-16 Telecommuters Sharing One VPN Rule Example.....	14-31
Table 14-17 Telecommuters Using Unique VPN Rules Example.....	14-33
Table 15-1 Remote Management	15-3
Table 16-1 Configuring UPnP.....	16-3
Table 17-1 System Status	17-3
Table 17-2 System Status: Show Statistics.....	17-4
Table 17-3 DHCP Table	17-6
Table 17-4 Diagnostic General.....	17-8
Table 17-5 Diagnostic DSL Line.....	17-9
Table 17-6 Firmware Upgrade	17-10
Table 18-1 Main Menu Commands.....	18-4
Table 18-2 Main Menu Summary	18-5
Table 19-1 Menu 1 General Setup.....	19-2
Table 19-2 Menu 1.1 Configure Dynamic DNS.....	19-3
Table 20-1 WAN Setup	20-2
Table 21-1 Menu 2: Dial Backup Setup	21-2
Table 21-2 Advanced WAN Port Setup: AT Commands Fields	21-3
Table 21-3 Advanced WAN Port Setup: Call Control Parameters	21-4
Table 21-4 Remote Node Profile (Backup ISP)	21-5
Table 21-5 Remote Node Network Layer Options.....	21-8
Table 22-1 IP Alias Setup.....	22-3
Table 22-2 TCP/IP and DHCP Ethernet Setup	22-5

Table 23-1 Internet Access Setup	23-2
Table 24-1 Remote Node Profile	24-3
Table 24-2 Remote Node Network Layer Options	24-6
Table 25-1 Edit IP Static Route	25-3
Table 26-1 Remote Node Bridging Options	26-2
Table 26-2 Edit Bridge Static Route	26-3
Table 27-1 Applying NAT to the Remote Node	27-3
Table 27-2 Address Mapping Rules - SUA	27-4
Table 27-3 Address Mapping Rules	27-6
Table 27-4 Editing/Configuring an Individual Rule in a Set	27-8
Table 28-1 Abbreviations Used in the Filter Rules Summary Menu	28-8
Table 28-2 Rule Abbreviations Used	28-9
Table 28-3 TCP/IP Filter Rule	28-10
Table 28-4 Generic Filter Rule Menu Fields	28-15
Table 28-5 Filter Sets Table	28-20
Table 29-1 SNMP Configuration	29-3
Table 29-2 SNMP Traps	29-3
Table 30-1 System Maintenance — Status	30-2
Table 30-2 System Maintenance — Information	30-4
Table 30-3 System Maintenance Menu — Syslog Parameters	30-7
Table 30-4 System Maintenance Menu — Diagnostic	30-9
Table 31-1 Filename Conventions	31-2
Table 31-2 General Commands for GUI-based FTP Clients	31-4
Table 31-3 General Commands for GUI-based TFTP Clients	31-6
Table 32-1 Budget Management	32-3
Table 32-2 Time and Date Setting Fields	32-5
Table 33-1 IP Routing Policy Setup Abbreviations	33-3
Table 33-2 IP Routing Policy	33-4
Table 34-1 Schedule Set Setup	34-2
Table 35-1 Remote Management Control	35-2
Table 36-1 Menu 27.1 IPSec Summary	36-2
Table 36-2 Menu 27.1.1 IPSec Setup	36-6
Table 36-3 Menu 27.1.1.1 IKE Setup	36-11
Table 36-4 Active Protocol: Encapsulation and Security Protocol	36-13
Table 36-5 Menu 27.1.1.2 Manual Setup	36-14
Table 37-1 Menu 27.2 SA Monitor	37-2
Table A-1 Troubleshooting the Start-Up of Your Prestige	A-1
Table A-2 Troubleshooting the LAN Interface	A-1
Table A-3 Troubleshooting the WAN Interface	A-2
Table A-4 Troubleshooting Internet Access	A-2

Table A-5 Troubleshooting the Password..... A-3

Table A-6 Troubleshooting Telnet..... A-3

Diagram C-1 Virtual Circuit Topology..... C-1

Preface

Congratulations on your purchase of the Prestige 792H G.SHDSL Router.

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.

Please visit our web site at www.zyxel.com for the latest release notes and product information.

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

About This User's Guide

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

Related Documentation

- Supporting Disk
Refer to the included CD for support documents.
- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- ZyXEL Web Site
The ZyXEL download library at www.zyxel.com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms.

Syntax Conventions

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

- 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.
- The Prestige 792H may be referred to as the Prestige in this user's guide.
- Images of Prestige 792H are used throughout this document unless otherwise specified.

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

Introduction to DSL

DSL (Digital Subscriber Line) technology enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000 Hz to filter noise off the voice line, but now everybody is searching for ways to get more bandwidth to improve access to the Web - hence DSL technologies.

There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). Asymmetrical services (ADSL) are suitable for Internet users because more information is usually downloaded than uploaded. For example, a simple button click in a web browser can start an extended download that includes graphics and text.

As data rates increase, the carrying distance decreases. That means that users who are beyond a certain distance from the telephone company's central office may not be able to obtain the higher speeds.

A DSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is no dialing required.

Introduction to G.SHDSL

G.SHDSL (Single-pair High-speed Digital Subscriber Line) is a symmetrical, bi-directional DSL service that operates on one twisted-pair wire and provides data rates up to 2.3 Mbits/sec. (The "G." in "G.SHDSL" is defined by the G.991.2 ITU (International Telecommunication Union) state-of-the-art industry standard).

Part I:

Getting Started

This part covers Getting to Know Your Prestige, Hardware Installation, Initial Setup, WAN, LAN and Internet Access.

Chapter 1

Getting to Know Your G.SHDSL Router

This chapter covers the key features and main applications of your Prestige.

The Prestige 792H is high-performance G.SHDSL Router with four port switch for Internet/LAN access via a telephone line. Your Prestige supports multi-protocol routing for TCP/IP, as well as transparent bridging for other protocols.

The Prestige supports symmetrical multi-rate data transmission speeds 72 Kbps up to 2312 Kbps. The actual rate depends on the copper category of your telephone wires, distance from the central office and the type of DSL service you subscribe to. Its 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

The Prestige is also a complete security solution with a robust stateful inspection firewall and multiple session VPN capability.

Should the Internet connection to the Prestige fail; there is a Traffic Redirect service that forwards WAN traffic to a backup gateway.

The Prestige uses TC-PAM line code with echo cancellation for high data rate transmissions over a single-twisted telephone wire pair without being affected by bridge taps or mixed cable links. It also provides high immunity from background noise.

1.1 Features of the Prestige

The following features make the Prestige a complete and the flexible networking solution for most users.

Scalability

One of the best features of G.SHDSL service is its scalability. Your Prestige G.SHDSL router supports symmetrical multi-rate data transmission speeds from 72 Kbps up to 2312 Kbps. You can increase the capacity of the Internet connection (within certain distance limitations) without changing your ISP or purchasing new equipment. G.SHDSL's high symmetrical speeds are ideal for applications like web hosting and videoconferencing as well as the two-way data traffic needs of businesses.

Symmetrical High Speed Internet Access

The Prestige 792H can support symmetrical transmission up to 2.3 Mbps, 40 times faster than a 56K analog modem. For NSP's (Network Service Provider) convenience, the Prestige also supports rate management depending on distance and service charges.

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's 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.

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.

Traffic Redirect

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

Auxiliary Port

The auxiliary port (or dial backup port) can be used in reserve as a traditional dial-up connection when/if ever the broadband connection to the WAN port fails. The P792H/HW uses the same port (labeled **CON/AUX**) for console management and for an auxiliary WAN backup (push the **CON/AUX** switch to **CON** or **AUX**).

SNMP (Simple Network Management Protocol – versions 1 and 2)

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

SNMP is only available if TCP/IP is configured on your Prestige.

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 interface with the Prestige itself as the gateway for each LAN network.

IP Policy Routing

IP Policy Routing provides a mechanism to override the default routing behavior and alter packet forwarding based on the policies defined by the network administrator.

10/100MB Auto-negotiation Ethernet/Fast Ethernet Interface

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately, providing a faster data transfer on the Ethernet network as required. It enables fast data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Protocols Supported

- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- PPP (Point-to-Point Protocol) link layer protocol.
- SUA™ (Single User Account) and NAT (Network Address Translation).

PAP and CHAP Security

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

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (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 other systems that support the DHCP client. The Prestige can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

Encapsulation

The Prestige supports PPPoE, PPP over ATM (RFC-2364), Multiple Protocol over ATM (RFC-1483) and ENET ENCAP.

SUA for Single-IP Address Internet Access

The Prestige's SUA (Single User Account, equivalent to NAT) feature allows multiple users Internet access for the cost of a single ISP account and allows multiple users on the LAN (Local Area Network) to access the Internet concurrently. SUA supports popular Internet applications such as MS traceroute, CuSeeMe,

IRC, ICQ, RealAudio, VDOLive, Quake and PPTP. No extra configuration is needed to support these applications. SUA address mapping can also be used for other LAN-to-LAN connections.

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.

Full Network Management

- Menu driven SMT (System Management Terminal) management
- SNMP manageable
- Web Configurator

Upgrade Firmware via LAN

In addition to the direct console port connection, the Prestige supports the up/downloading of firmware and configuration file over the LAN.

Packet Filtering

Packet filtering blocks unwanted traffic from entering/leaving your network.

Ease of Installation

Your Prestige is designed for quick, easy and intuitive installation. Its compact size and lightweight make it easy to position anywhere in your busy office.

Multiple PVC (Permanent Virtual Circuits) Support

Your Prestige supports up to 12 PVC's.

Session Initiation Protocol (SIP) Pass-Through

The Session Initiation Protocol (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. Sending compressed voice signals over the Internet is called Voice over IP or VoIP. The Prestige is a Session Initiated Protocol (SIP) - based wireless VoIP telephone. SIP is an internationally recognized standard for implementing VoIP.

1.2 Application Scenarios for the Prestige

This section provides examples on how your Prestige can be used.

1.2.1 Internet Access

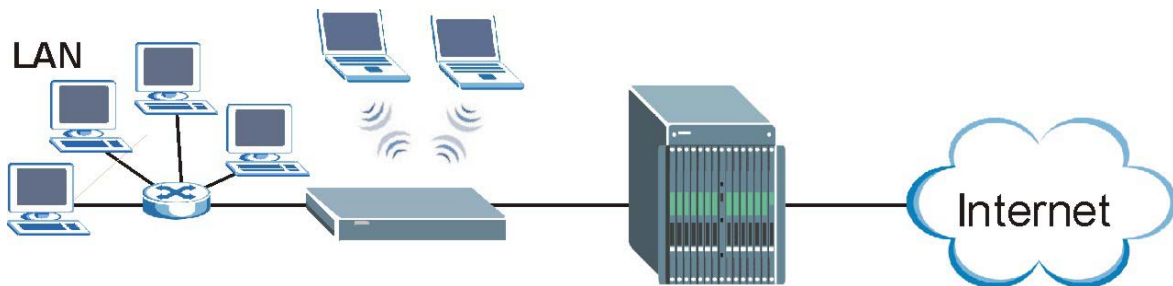


Figure 1-1 Internet Access Application

Your Prestige can act as either of the following:

- A bridge for multi-computer/MAC bridging (RFC-1483, bridged Ethernet/802.3).

1.2.2 LAN-to-LAN Application

You can use the Prestige to connect two geographically dispersed networks over the DSL line. A typical LAN-to-LAN application is shown next.

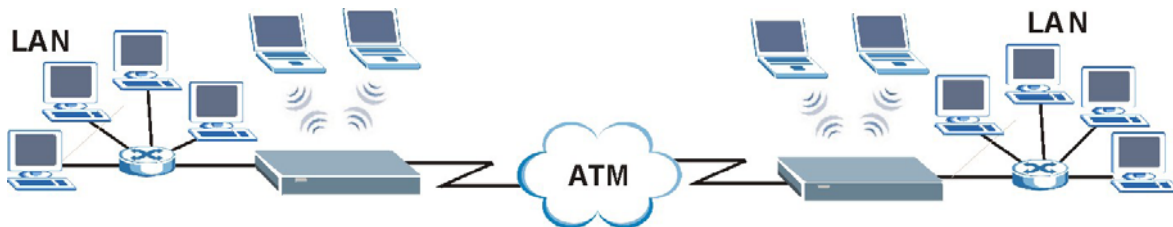


Figure 1-2 LAN-to-LAN Application

Chapter 2

Introducing the Web Configurator

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

2.1 Web Configurator Overview

The embedded web configurator (ewc) 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

2.2 Accessing the Prestige Web Configurator

- Step 1.** Make sure your Prestige hardware is properly connected (refer the *Quick Start Guide*).
- Step 2.** Prepare your computer/computer network to connect to the Prestige (refer the *Quick Start Guide*).
- Step 3.** Launch your web browser.
- Step 4.** Type "192.168.1.1" as the URL.
- Step 5.** An **Enter Network Password** window displays. Enter the user name ("admin" is the default), password ("1234" is the default) and click **OK**.



Figure 2-1 Password Screen

Step 6. You should now see the **Site Map** screen.

The Prestige automatically times out after five minutes of inactivity. Simply log back into the Prestige if this happens to you.

2.3 Navigating the Prestige Web Configurator

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

- Select a language from the **Language** drop-down list box.
- Click **Wizard Setup** to begin a series of screens to configure your Prestige for the first time.
- Click a link under **Advanced Setup** to configure advanced Prestige features.
- Click a link under **Maintenance** to see Prestige performance statistics, upload firmware and back up, restore or upload a configuration file.
- Click **SITE MAP** to go to the **Site Map** screen.
- Click **Logout** in the navigation panel when you have finished a Prestige management session.

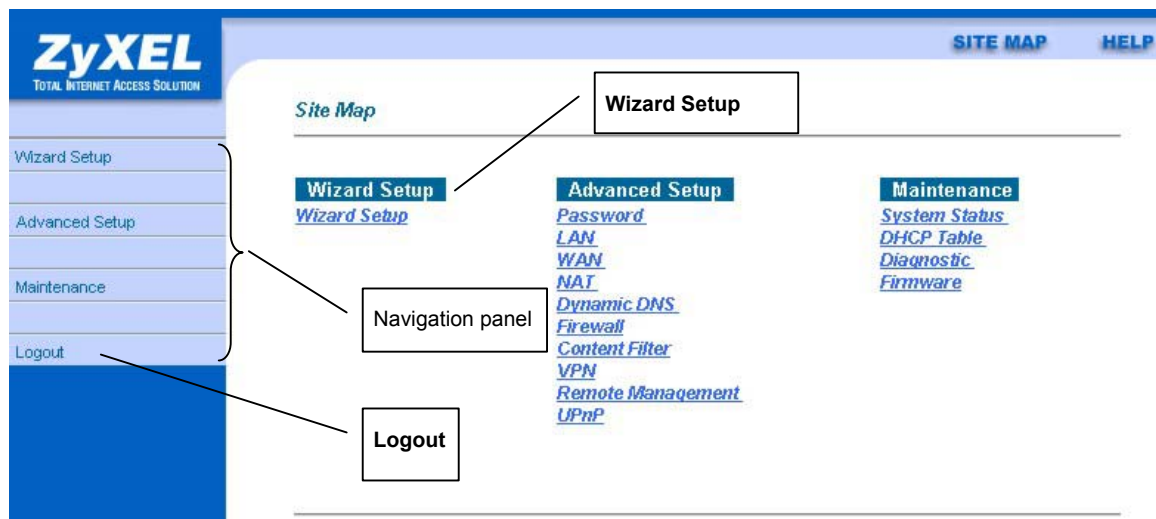


Figure 2-2 Web Configurator SITE MAP Screen

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

2.4 Configuring Password

It is highly recommended that you change the password for accessing the Prestige.

To change your Prestige's password, click **Advanced Setup** and then **Password**. The screen appears as shown.

Password

Old Password

New Password

Retype to confirm

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

Apply

Cancel

Figure 2-3 Password

The following table describes the labels in this screen.

Table 2-1 Password

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

2.5 Resetting the Prestige

If you forget your password or cannot access the Prestige, you will need to reload the factory-default configuration file or use the **RESET** button on the back of the Prestige. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default

of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to "1234", also.

2.5.1 Using The Reset Button

- Step 1.** Make sure the **SYS** LED is on (not blinking).
- Step 2.** Press the **RESET** button for five seconds, and then release it. When the **SYS** LED begins to blink, the defaults have been restored and the Prestige restarts.

2.5.2 Uploading a Configuration File Via Console Port

- Step 1.** Download the default configuration file from the ZyXEL FTP site, unzip it and save it in a folder.
- Step 3.** Turn off the Prestige, begin a terminal emulation software session and turn on the Prestige again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.
- Step 4.** Enter "atlc" after "Enter Debug Mode" message.
- Step 5.** Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.
- Step 6.** Click **Transfer**, then **Send File** to display the following screen.

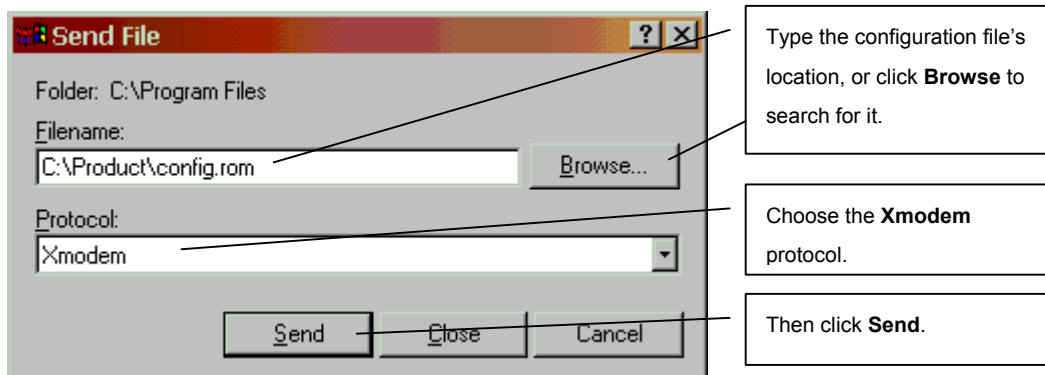


Figure 2-4 Example Xmodem Upload

- Step 7.** After successful firmware upload, enter "atgo" to restart the router.

Chapter 3

Wizard Setup

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

3.1 Wizard Setup Introduction

Use the Wizard Setup screens to configure your system for Internet access settings and fill in the fields with the information in the *Internet Account Information* table of the *Quick Start Guide* or *Read Me First*. Your ISP may have already configured some of the fields in the wizard screens for you.

3.2 WAN Setup

Use the first wizard screen to configure G.SHDSL settings for your WAN line. Different telephone companies deploy different types of G.SHDSL service. If you are unsure of any of this information, please check with your telephone company.

3.2.1 Service Type

Is your Prestige acting as a Server or Client?

1. The Prestige is a server if it is acting as a COE (Central Office Equipment). It will determine transfer rate and mode.
2. The Prestige is a client if it is acting as a CPE (Customer Premise Equipment).

3.2.2 Rate Adaption

Both the Prestige and the peer must have the same transmission rate. Rate Adaption allows the Prestige to auto-detect the peer transfer rate.

3.2.3 Transfer Rates

The Prestige supports the following symmetrical multi-rate data transmission speeds:

72, 136, 200, 264, 392, 520, 776, 1032, 1160, 1544, 1736, 2056 and 2312Kbps.

You can increase the capacity of the Internet connection (within certain limitations) without changing your ISP or buying new equipment.

For back-to-back applications make sure that your Prestige and its peer have the same **Transfer Max Rate** and the same **Transfer Min Rate**. Two (maximum and minimum) transfer rates are used to accommodate fluctuations in line speed. This is known as Dynamic Bandwidth Allocation.

3.2.4 Standard Mode

If your Prestige is a server, then select the mode that applies to your region: ANSI (American National Standards Institute) and ETSI (European Telecommunications Standards Institute). If your Prestige is a client, select the same **Standard Mode** that the server side selects. ANSI and ETSI create recommendations and standards for the telecommunications industry.

3.3 Encapsulation

Be sure to use the encapsulation method required by your ISP. The Prestige supports the following methods.

3.3.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **Ethernet Encapsulation Gateway** field in the second wizard screen. You can get this information from your ISP.

3.3.2 PPP over Ethernet

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The Prestige bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an

ATM PVC (Permanent Virtual Circuit), which connects to ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the appendix.

3.3.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP. The Prestige encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

3.3.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

3.4 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

3.4.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

3.4.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it

is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

3.5 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

3.6 Wizard Setup Configuration: First Screen

In the **SITE MAP** screen click **Wizard Setup** to display the first wizard screen.

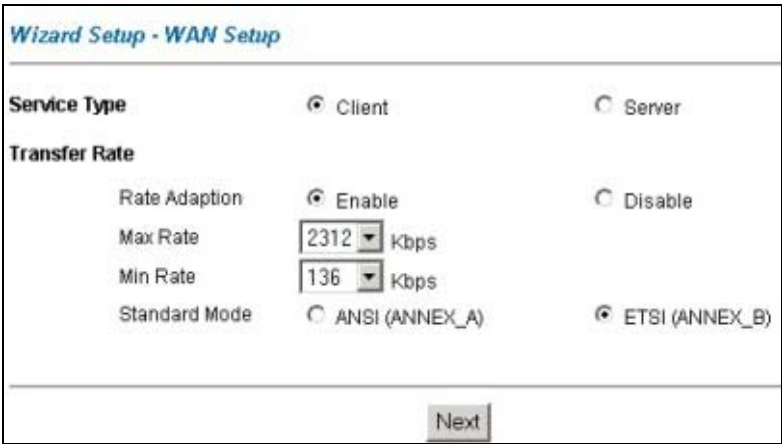


Figure 3-1 Wizard Screen: WAN Setup

The following table describes the labels in this screen.

Table 3-1 Wizard Screen: WAN Setup

LABEL	DESCRIPTION
Service Type	Select Client if your Prestige will act as a client device or Server if your Prestige will act as a server (<i>see Service Type</i>).
Transfer Rate	
Rate Adaption	If you enable Rate Adaption , the Prestige connects at the optimal transfer rate between the min and max rates below. If you disable Rate Adaption , the Prestige attempts to connect at the maximum transfer rate configured. If that rate can't be attained, the connection does not succeed.
Max Rate Min Rate	Select transfer rates from the Max Rate and Min Rate drop-down list boxes. For back-to-back applications make sure that your Prestige and its peer have the same Transfer Max Rate and the same Transfer Min Rate .
Standard Mode	If your Prestige is a server, then select the mode that applies to your region: ANSI American National Standards Institute) and ETSI (European Telecommunications Standards Institute). If your Prestige is a client, select the same Standard Mode that the server side selects.
Next	Click this button to go to the next wizard screen.

Wizard Setup - ISP Parameters for Internet Access

Mode

Routing

Encapsulation

PPPoE

Multiplex

LLC

Virtual Circuit ID

VPI

8

VCI

35

Next

Figure 3-2 Wizard Screen: Internet Access

The following table describes the labels in this screen.

Table 3-2 Wizard Screen: Internet Access

LABEL	DESCRIPTION
Mode	From the Mode drop-down list box, select Routing (default) if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge .
Encapsulation	Select the encapsulation type your ISP uses from the Encapsulation drop-down list box. Choices vary depending on what you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
Multiplex	Select the multiplexing method used by your ISP from the Multiplex drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Next	Click this button to go to the next wizard screen. The next wizard screen you see depends on what protocol you chose above. Click on the protocol link to see the next wizard screen for that protocol.
Back	Click Back to go to the previous Wizard screen.

3.7 IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is

recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Prestige. 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.

3.8 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP Gateway.

3.8.1 IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the IP Address and ENET ENCAP Gateway fields are not applicable (N/A). If you have a static IP, then you *only* need to fill in the IP Address field and *not* the ENET ENCAP Gateway field.

3.8.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the IP Address and ENET ENCAP Gateway fields as stated above.

3.8.3 IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the IP Address and ENET ENCAP Gateway fields as supplied by your ISP. However for a dynamic IP, the Prestige acts as a DHCP client on the WAN port and so the IP Address and ENET ENCAP Gateway fields are not applicable (N/A) as the DHCP server assigns them to the Prestige.

3.8.4 Private IP Addresses

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

10.0.0.0 — 10.255.255.255

172.16.0.0 — 172.31.255.255

192.168.0.0 — 192.168.255.255

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

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*.

3.9 Nailed-Up Connection (PPP)

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

3.10 NAT

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

3.11 Wizard Setup Configuration: ISP Parameters

The second wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

3.11.1 PPPoA

Select **PPPoA** from the **Encapsulation** drop-down list box in the first wizard screen to display the screen as shown.

Wizard Setup - ISP Parameters for Internet Access

User Name

Password

IP Address

☒ Obtain an IP Address Automatically

☐ Static IP Address

0.0.0.0

Connection

☒ Connect on Demand: Max Idle Timeout

0

Secs

☐ Nailed-Up Connection

Network Address Translation

SUA Only

Back

Next

Figure 3-3 Internet Connection with PPPoA

The following table describes the labels in this screen.

Table 3-3 Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.

Table 3-3 Internet Connection with PPPoA

LABEL	DESCRIPTION
IP Address	<p>This option is available if you select Routing in the Mode field.</p> <p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address.</p> <p>Click Obtain an IP Address Automatically if you have a dynamic IP address; otherwise click Static IP Address and type your ISP assigned IP address in the IP Address text box below.</p>
Connection	<p>Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out (in seconds) in the Max. Idle Timeout field. The default setting selects Connection on Demand with 0 as the idle time-out, which means the Internet session will not timeout.</p> <p>Select Nailed-Up Connection when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.</p> <p>The schedule rule(s) in SMT menu 26 has priority over your Connection settings.</p>
Network Address Translation	<p>This option is available if you select Routing in the Mode field.</p> <p>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).</p> <p>Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that maps one public IP address to many private IP addresses.</p> <p>Choose Full Feature if you have multiple public IP addresses. When you select Full Feature, you must use the NAT address mapping rules screen to configure at least one address mapping set. Full Feature mapping types include: One-to-One, Many-to-One (SUA), Many-to-Many Overload, Many-to-Many No Overload and Server.</p> <p>Choose None to disable NAT. Refer to the NAT chapter for more details.</p>
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

3.11.2 RFC 1483

Select **RFC 1483** from the **Encapsulation** drop-down list box in the first wizard screen to display the screen as shown.

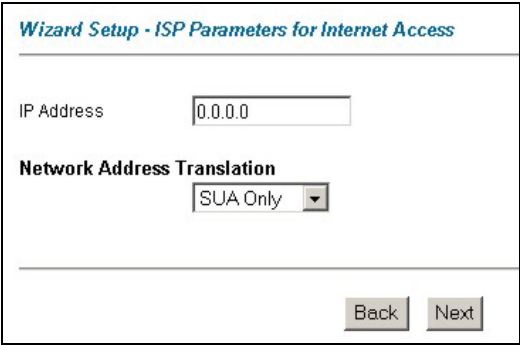


Figure 3-4 Internet Connection with RFC 1483

The following table describes the labels in this screen.

Table 3-4 Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select Routing in the Mode field. Type your ISP assigned IP address in this field.
Network Address Translation	Select None , SUA Only or Full Feature from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

3.11.3 ENET ENCAP

Select **ENET ENCAP** from the **Encapsulation** drop-down list box in the first wizard screen to display the screen as shown.

Wizard Setup - ISP Parameters for Internet Access

IP Address

☒ Obtain an IP Address Automatically

☐ Static IP Address

IP Address

0.0.0.0

Subnet Mask

0.0.0.0

ENET ENCAP Gateway

0.0.0.0

Network Address Translation

SUA Only

Back

Next

Figure 3-5 Internet Connection with ENET ENCAP

The following table describes the labels in this screen.

Table 3-5 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
IP Address	<p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address.</p> <p>Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address text box below.</p>
Subnet Mask	Enter a subnet mask in dotted decimal notation.
ENET ENCAP Gateway	You must specify a gateway IP address (supplied by your ISP) when you use ENET ENCAP in the Encapsulation field in the previous screen.

Table 3-5 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
Network Address Translation	Select None , SUA Only or Full Feature from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

3.11.4 PPPoE

Select **PPPoE** from the **Encapsulation** drop-down list box in the first wizard screen to display the screen as shown.

Wizard Setup - ISP Parameters for Internet Access

Service Name

User Name

Password

IP Address

☒ Obtain an IP Address Automatically

☐ Static IP Address

0.0.0.0

Connection

☒ Connect on Demand: Max Idle Timeout

0

Secs

☐ Nailed-Up Connection

Network Address Translation

SUA Only

Back

Next

Figure 3-6 Internet Connection with PPPoE

The following table describes the labels in this screen.

Table 3-6 Internet Connection with PPPoE

LABEL	DESCRIPTION
Service Name	Type the name of your PPPoE service here.
User Name	Configure User Name and Password fields for PPPoA and PPPoE encapsulation only. Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	<p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address.</p> <p>Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address text box below.</p>
Connection	<p>Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out (in seconds) in the Max. Idle Timeout field. The default setting selects Connection on Demand with 0 as the idle time-out, which means the Internet session will not timeout.</p> <p>Select Nailed-Up Connection when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.</p> <p>The schedule rule(s) in SMT menu 26 has priority over your Connection settings.</p>
Network Address Translation	Select None , SUA Only or Full Feature from the drop-down list box. Refer to the NAT chapter for more details.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

3.12 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 you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

3.12.1 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 for the client machines. This leaves 31 IP addresses, 192.168.1.2 to 192.168.1.32 (excluding the Prestige itself which has a default IP of 192.168.1.1) for other server machines, for example, server for mail, FTP, telnet, web, etc., that you may have.

3.13 Wizard Setup Configuration: LAN Configuration

Verify the settings in the screen shown next. To change the LAN information on the Prestige, click **Change LAN Configurations**. Otherwise click **Save Settings** to save the configuration and skip to section 3.13.

Wizard Setup - ISP Parameters for Internet Access

WAN Information:
Mode: **Routing**
Encapsulation: **PPPoE**
Multiplexing: **LLC**
VPI/VCI: **8/35**
Service Name :
User Name : **user@isp.ch**
Password : *********
IP Address : **Obtain an IP Address Automatically**
Network Address Translation: **SUA Only**
Connect on Demand: **Max Idle Timeout 1500 sec.**

LAN Information:
IP Address: **192.168.1.1**
IP Mask: **255.255.255.0**
DHCP: **ON**
Client IP Pool Starting Address: **192.168.1.33**
Size of Client IP Pool: **32**

Change LAN Configuration

Save Settings

Figure 3-7 Wizard Screen: LAN Configuration

If you want to change your Prestige LAN settings, click **Change LAN Configuration** to display the screen as shown next.

Wizard Setup - ISP Parameters for Internet Access

LAN IP Address

192.168.1.1

LAN Subnet Mask

255.255.255.0

DHCP

DHCP Server

ON

Client IP Pool Starting Address

192.168.1.33

Size of Client IP Pool

32

Primary DNS Server

0.0.0.0

Secondary DNS Server

0.0.0.0

Back

Finish

Figure 3-8 Wizard: LAN Configuration

The following table describes the labels in this screen.

Table 3-7 Wizard: LAN Configuration

LABEL	DESCRIPTION
LAN IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default). If you changed the Prestige's LAN IP address, you must use the new IP address if you want to access the web configurator again.
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.

Table 3-7 Wizard: LAN Configuration

LABEL	DESCRIPTION
DHCP	
DHCP Server	From the DHCP Server drop-down list box, select On to allow your Prestige to assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client. Select Off to disable DHCP server. When DHCP server is used, set the following items:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Back	Click Back to go back to the previous screen.
Finish	Click Finish to save the settings and proceed to the next wizard screen.

3.14 Wizard Setup Configuration: Connection Tests

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

Wizard Setup - ISP Parameters for Internet Access

LAN connections

Test your Ethernet Connection	PASS
-------------------------------	-------------

WAN connections

Test ADSL synchronization	PASS
Test ADSL(ATM OAM) loopback test	PASS
Test PPP/PPPoE server connection	PASS
Ping default gateway	PASS

Figure 3-9 Wizard Screen: Connection Tests

3.15 Test Your Internet Connection

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

Chapter 4

LAN Setup

This chapter describes how to configure LAN settings.

4.1 LAN Overview

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

4.1.1 LANs, WANs and the Prestige

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

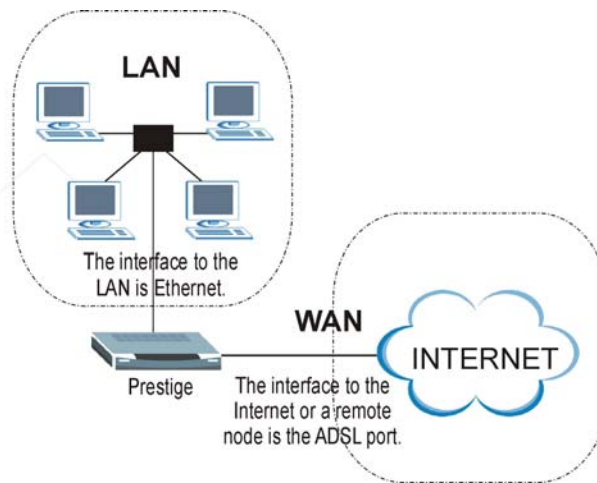


Figure 4-1 LAN and WAN IP Addresses

4.2 DNS Server Address

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 DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Prestige supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in **DHCP Setup** are not specified, for instance, left as 0.0.0.0, the Prestige tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the Prestige, the Prestige forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** menu. This way, the Prestige can pass the DNS servers to the computers and the computers can query the DNS server directly without the Prestige's intervention.

4.3 DNS Server Address Assignment

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

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

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. Leave the DNS Server fields in DHCP Setup blank (for example 0.0.0.0). The Prestige acts as a DNS proxy when this field is blank.

4.4 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.

4.4.1 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.

4.4.2 IP Address and Subnet Mask

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

4.4.3 RIP Setup

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. When set to:

1. **Both** - the Prestige will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only** - the Prestige will not send any RIP packets but will accept all RIP packets received.
3. **Out Only** - the Prestige will send out RIP packets but will not accept any RIP packets received.
4. **None** - the Prestige will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the 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.

4.4.4 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.

4.5 Configuring LAN

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

LAN - Setup

DHCP

DHCP

Server

Client IP Pool Starting Address

192.168.1.33

Size of Client IP Pool

32

Primary DNS Server

0.0.0.0

Secondary DNS Server

0.0.0.0

Remote DHCP Server

N/A

TCP/IP

IP Address

192.168.1.1

IP Subnet Mask

255.255.255.0

RIP Direction

None

RIP Version

N/A

Multicast

None

Apply

Cancel

Figure 4-2 LAN

The following table describes the labels in this screen.

Table 4-1 LAN

LABEL	DESCRIPTION
DHCP	
DHCP	<p>If set to Server, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.</p> <p>If set to None, the DHCP server will be disabled.</p> <p>If set to Relay, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.</p> <p>When DHCP is used, the following items need to be set:</p>
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Remote DHCP Server	If Relay is selected in the DHCP field above then enter the IP address of the actual remote DHCP server here.
TCP/IP	
IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from None , Both , In Only and Out Only .
RIP Version	Select the RIP version from RIP-1 , RIP-2B and RIP-2M .
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 IGMP-v2 . Select None to disable it.

Table 4-1 LAN

LABEL	DESCRIPTION
Apply	Click this button to save these settings back to the Prestige.
Cancel	Click this button to reset the fields in this screen.

Chapter 5

WAN Setup

This chapter describes how to configure WAN settings.

5.1 WAN Overview

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

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

5.2 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 any two of the default routes have the same metric, the Prestige uses the following pre-defined priorities:

1. Normal route: designated by the ISP (see *section 5.5*)
2. Traffic-redirect route (see *section 5.6*)
3. WAN-backup route, also called dial-backup (see *section 5.6*)

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

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

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above (see the *IP Policy Routing* chapter).

5.3 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 **PPPoE** option is for a dial-up connection using PPPoE.

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

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

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

By implementing PPPoE directly on the 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.

5.4 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of “0”, the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

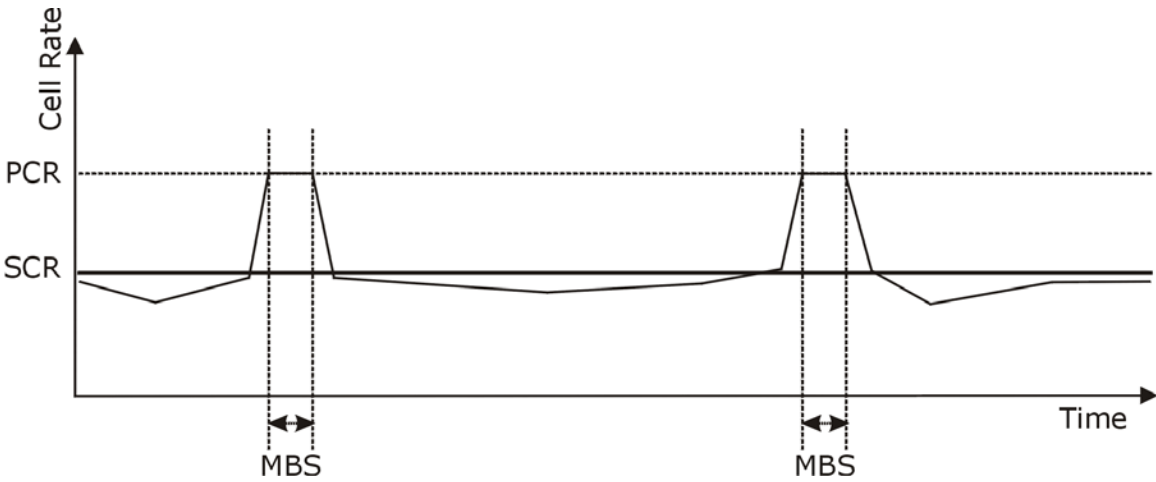


Figure 5-1 Example of Traffic Shaping

5.5 Configuring WAN Setup

To change your Prestige's WAN remote node settings, click **WAN**, **WAN Setup**. The screen differs by the encapsulation.

WAN - WAN Setup

Name

Mode

Encapsulation

Multiplex

Virtual Circuit ID

VPI

VCI

ATM QoS Type

Cell Rate

Peak Cell Rate cell/sec

Sustain Cell Rate cell/sec

Maximum Burst Size

Login Information

Service Name

User Name

Password

IP Address

☐ Obtain an IP Address Automatically

☒ Static IP Address

IP Address

Connection

☐ Nailed-Up Connection

☒ Connect on Demand

Max Idle Timeout Secs

Figure 5-2 WAN Setup

The following table describes the labels in this screen.

Table 5-1 WAN Setup

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select Routing (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge .
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications. VBR is not available on all models.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR.

Table 5-1 WAN Setup

LABEL	DESCRIPTION
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
Service Name	(PPPoE only) Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	<p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address.</p> <p>Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address field below.</p>
IP Address	<p>Enter the static IP address provided.</p> <hr/> <p style="text-align: center;">For remote node setup, enter the IP address in the same subnet as the remote node.</p> <hr/>
Connection (PPPoA and PPPoE encapsulation only)	The schedule rule(s) in SMT menu 26 have priority over your Connection settings.
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session will not timeout.

Table 5-1 WAN Setup

LABEL	DESCRIPTION
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to the <i>Subnetting</i> appendix to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select ENET ENCAP in the Encapsulation field.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

5.6 Traffic Redirect

Traffic redirect forwards traffic to a backup gateway when the Prestige cannot connect to the Internet. An example is shown in the figure below.

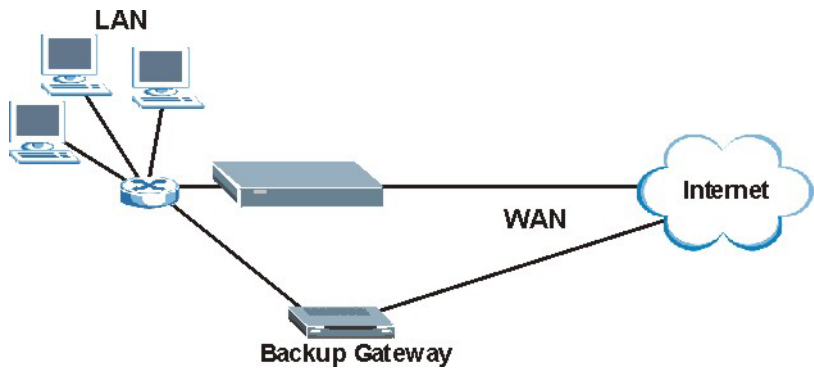


Figure 5-3 Traffic Redirect Example

The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the 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 filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

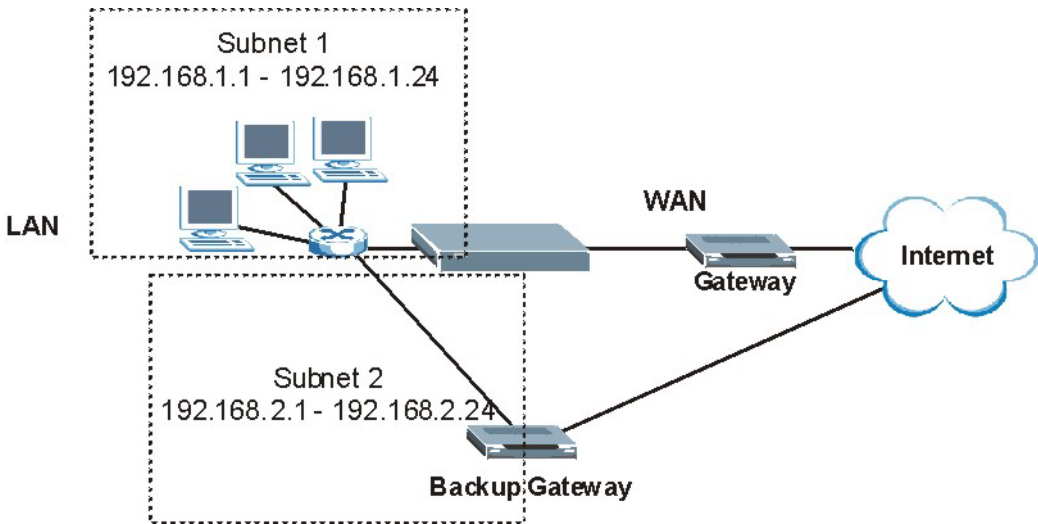


Figure 5-4 Traffic Redirect LAN Setup

5.7 Configuring WAN Backup

The WAN Backup port or CON/AUX port can be used in reserve, if the broadband connection to the WAN port fails. To set up the auxiliary port (WAN Backup or CON/AUX) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the *Quick Start Guide for Hardware Installation*), then configure:

1. WAN Setup (*see section 5.5*)
2. WAN Backup Setup (*see below*)
3. Advanced WAN Setup (*see section 5.8*)

To change your Prestige’s WAN backup settings, click **WAN**, then **WAN Backup**. The screen appears as shown.

WAN - WAN Backup Setup

Backup Type

DSL Link

Check WAN IP Address1

1.2.3.4

Check WAN IP Address2

0.0.0.0

Check WAN IP Address3

0.0.0.0

Fail Tolerance

0

Recovery Interval

0

sec

Timeout

0

sec

Traffic Redirect

☐ Active

Metric

15

Backup Gateway

0.0.0.0

Dial Backup

☒ Active

Metric

15

Port Speed

115200

User Name

Password

Pri Phone #

Advanced Setup

Back

Apply

Cancel

Figure 5-5 WAN Backup

The following table describes the fields in this screen.

Table 5-2 WAN Backup

LABEL	DESCRIPTION
Backup Type	<p>Select the method that the Prestige uses to check the DSL connection. Select DSL Link to have the Prestige check the DSL connection's physical layer. Select ICMP to have the Prestige periodically ping the IP addresses configured in the Check WAN IP Address fields.</p>
Check WAN IP Address1-3	<p>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).</p> <p>When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.</p>
Fail Tolerance	<p>Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the Check WAN IP Address field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).</p>
Recovery Interval	<p>When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection.</p> <p>Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic.</p>
Timeout	<p>Type the number of seconds (3 recommended) for your Prestige to wait for a ping response from one of the IP addresses in the Check WAN IP Address field before timing out the request. 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.</p>
Traffic Redirect	
Active	<p>Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down.</p>
Metric	<p>This field sets this route's priority among the routes the Prestige uses.</p> <p>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".</p>

Table 5-2 WAN Backup

LABEL	DESCRIPTION
Backup Gateway	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.
Dial Backup	
Active	Select this check box to turn on dial backup.
Metric	<p>This field sets this route's priority among the three routes the Prestige uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority.</p> <p>If the three routes have the same metrics, the priority of the routes is as follows: WAN, Traffic Redirect, Dial Backup.</p>
Port Speed	Use the drop-down list box to select the speed of the connection between the dial backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.
User Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Pri Phone #	Type the first (primary) phone number from the ISP for this remote node. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Advanced Setup	Click this button to display the Advanced Setup screen and edit more details of your WAN backup setup.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

5.8 Outgoing Authentication Protocol

You should employ the strongest authentication protocol possible. However, some vendor's implementation includes 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 the

peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

5.9 Configuring Advanced WAN Backup

To edit your Prestige's advanced WAN backup settings, click **WAN**, **WAN Backup** and then the **Advanced Setup** button. The screen appears as shown.

WAN - WAN Backup Setup- WAN Backup Advanced

Basic

Login Name

Password

Retype to Confirm

Authentication Type

CHAP/PAP

Primary Phone Number

Secondary Phone Number

Dial Backup Port Speed

115200

AT Command Initial String

at&fs0=0

Advanced Modem Setup

Edit

TCP/IP Options

Metric

15

☒ Enable SUA

☐ Enable RIP

RIP Version

RIP-1

RIP Direction

BOTH

☐ Enable Multicast

Multicast

IGMP-v2

PPP Options

Encapsulation

Standard PPP

☐ Compression

Connection

☐ Nailed-Up Connection

☒ Connect on Demand

Max Idle Timeout

100

sec

Budget

Allocated Budget

0

min

Period

0

hr

Back

OK

Cancel

Figure 5-6 Advanced WAN Backup

The following table describes the fields in this screen.

Table 5-3 Advanced WAN Backup

LABEL	DESCRIPTION
Basic	
Login Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Authentication Type	<p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p>CHAP/PAP - Your Prestige accepts either CHAP or PAP when requested by this remote node.</p> <p>CHAP - Your Prestige accepts CHAP only.</p> <p>PAP - Your Prestige accept PAP only.</p>
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the primary phone number is busy or does not answer, your Prestige dials the secondary phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Dial Backup Port Speed	Use the drop-down list box to select the speed of the connection between the dial backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your dial backup port for specific AT commands.
Advanced Modem Setup	Click the Edit button to display the Advanced Modem Setup screen and edit the details of your dial backup setup.
TCP/IP Options	
Metric	<p>This field sets this route's priority among the three routes the Prestige uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority.</p> <p>If the three routes have the same metrics, the priority of the routes is as follows: WAN, Traffic Redirect, Dial Backup.</p>

Table 5-3 Advanced WAN Backup

LABEL	DESCRIPTION
Enable SUA	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network.</p> <p>SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the Prestige will use Address Mapping Set 255 in the SMT (see the section on menu 15.1 for more information).</p>
Enable RIP	<p>Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.</p>
RIP Version	<p>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.</p> <p>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.</p>
RIP Direction	<p>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.</p> <p>Choose Both, In Only or Out Only.</p> <p>When set to Both or Out Only, the Prestige will broadcast its routing table periodically.</p> <p>When set to Both or In Only, the Prestige will incorporate RIP information that it receives.</p>
Enable Multicast	<p>Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.</p>
Multicast	<p>Select IGMP-v1 or IGMP-v2. 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 <i>sections 4 and 5 of RFC 2236</i>.</p>

Table 5-3 Advanced WAN Backup

LABEL	DESCRIPTION
PPP Options	
Encapsulation	Select CISCO PPP from the drop-down list box if your backup WAN device uses Cisco PPP encapsulation; otherwise select Standard PPP .
Compression	Select this check box to enable stac compression.
Connection	
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session won't timeout.
Budget	The configuration in the Budget fields has priority over your Connection settings.
Allocate Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the Period field. Set an amount that is less than the time period configured in the Period field. If you set the Allocated Budget to 0, you will not be able to use the dial backup connection.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the Allocated Budget to 10 (minutes) and the Period to 1 (hour). If you set the Period to 0, there is no budget control and the Prestige uses the Connection settings.
Back	Click Back to return to the previous screen.
OK	Click OK to return to the previous screen, then click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

5.10 AT Command Strings

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

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

5.11 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the “Drop DTR When Hang Up” check box is selected, the Prestige uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command “ATH”.

5.12 Response Strings

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

5.13 Configuring Advanced Modem Setup

To configure settings for your backup WAN modem, click **WAN**, **WAN Backup** and then the **Advanced Setup** button. The **Advanced Setup** screen displays, click the **Edit** button to open the **Advanced Modem Setup** screen as shown next.

Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

WAN - WAN Backup Setup- Advanced Modem Setup

AT Command Strings

Dial

Drop

Answer

☒ Drop DTR When Hang Up

AT Response Strings

CLID

Called ID

Speed

Call Control

Dial Timeout sec

Retry Count

Retry Interval sec

Drop Timeout sec

Call Back Delay sec

Figure 5-7 Advanced Modem Setup

The following table describes the fields in this screen.

Table 5-4 Advanced Modem Setup

LABEL	DESCRIPTION
AT Command Strings	
Dial	Type the AT Command string to make a call. Example: atdt
Drop	Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~++++~ath" can be used if your modem has a slow response time.
Answer	Type the AT Command string to answer a call. Example: ata

Table 5-4 Advanced Modem Setup

LABEL	DESCRIPTION
Drop DTR When Hang Up	Select this check box to have the Prestige drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out.
AT Response Strings	
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the Prestige capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication. Example: NMBR
Called ID	Type the keyword preceding the dialed number.
Speed	Type the keyword preceding the connection speed. Example: CONNECT
Call Control	
Dial Timeout	Type a number of seconds for the Prestige to try to set up an outgoing call before timing out (stopping). Example: 60
Retry Count	Type a number of times for the Prestige to retry a busy or no-answer phone number before blacklisting the number. Example: 0
Retry Interval	Type a number of seconds for the Prestige to wait before trying another call after a call has failed. This applies before a phone number is blacklisted. Example: 10
Drop Timeout	Type the number of seconds for the Prestige to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation. Example: 20
Call Back Delay	Type a number of seconds for the Prestige to wait between dropping a callback request call and dialing the corresponding callback call. Example: 15
Back	Click Back to return to the previous screen.
OK	Click OK to return to the previous screen, then click OK to return to the next previous screen and click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

Part II:

NAT and Dynamic DNS

This part covers NAT (Network Address Translation) and dynamic DNS (Domain Name Server)

Chapter 6

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

6.1 NAT Overview

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

6.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the 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 6-1 NAT Definitions

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

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

6.1.2 What NAT Does

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

local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. 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)*.

6.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The 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.

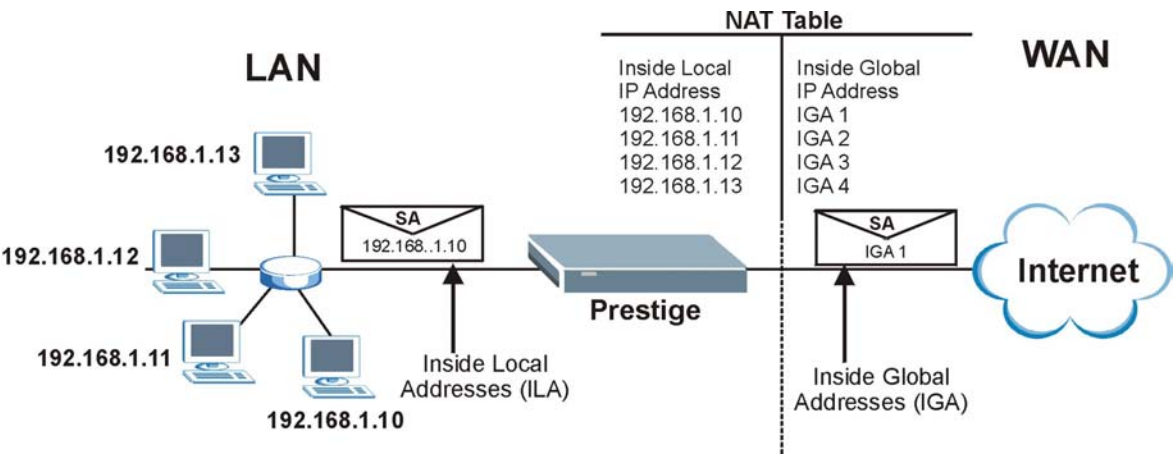


Figure 6-1 How NAT Works

6.1.4 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.

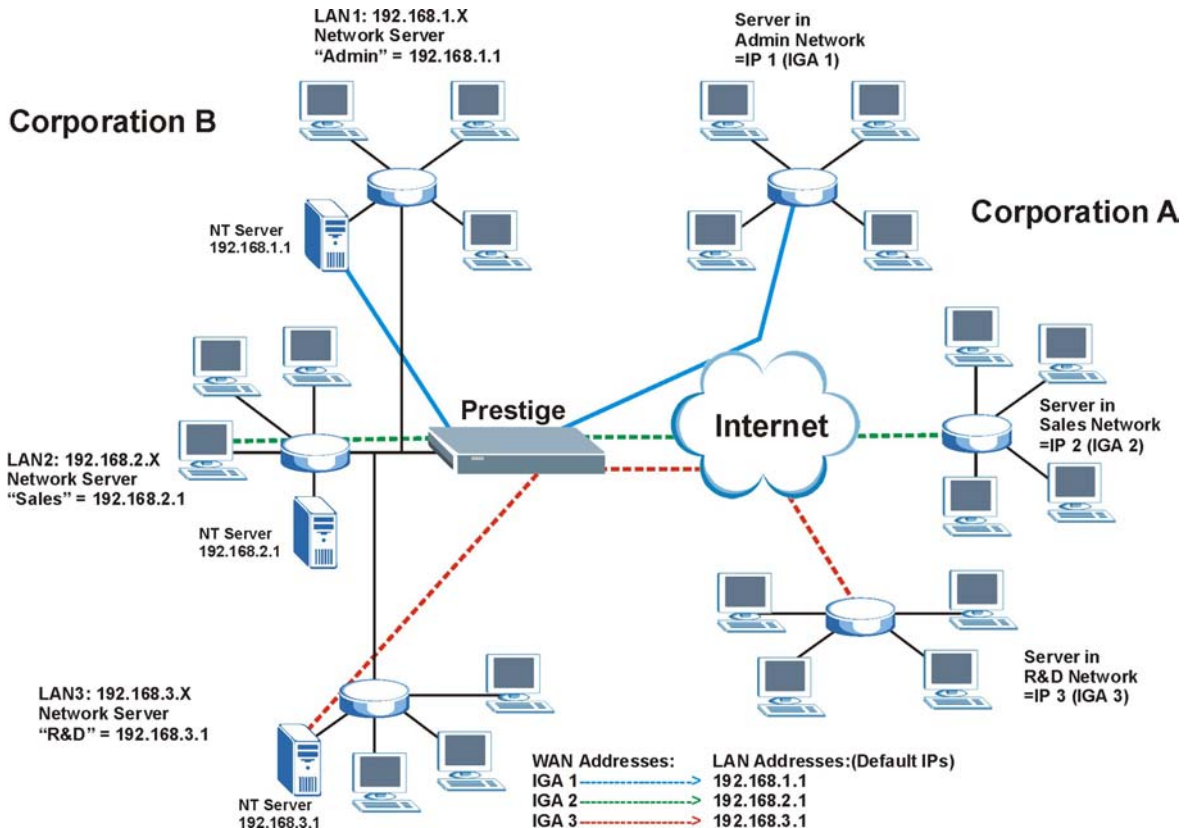


Figure 6-2 NAT Application With IP Alias

6.1.5 NAT Mapping Types

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

1. **One to One:** In One-to-One mode, the Prestige maps one local IP address to one global IP address.
2. **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 (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
3. **Many to Many Overload:** In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.
4. **Many-to-Many No Overload:** In Many-to-Many No Overload mode, the Prestige maps each local IP address to a unique global IP address.

5. **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do not change for One-to-One and Many-to-Many No Overload NAT mapping types.

The following table summarizes these types.

Table 6-2 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-to-Many No Overload	ILA1↔ IGA1 ILA2↔ IGA2 ILA3↔ IGA3 ...	M:M No OV
Server	Server 1 IP↔ IGA1 Server 2 IP↔ IGA1 Server 3 IP↔ IGA1	Server

6.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a Zynos implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The 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 as outlined in *Table 6-2*.

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

6.3 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 an IP address in Server Set 1 (default server), the Prestige discards all packets received for ports that are not specified here or in the remote management setup.

6.3.1 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.

Table 6-3 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

6.3.2 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35 as shown in the next figure.

Private Network IP
address assigned by user

The NAT network appears as
a single host on the Internet

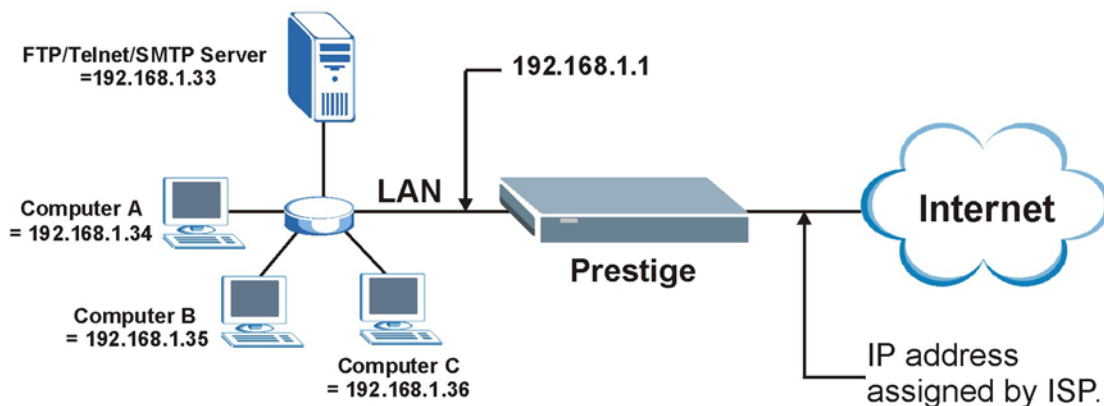


Figure 6-3 Multiple Servers Behind NAT Example

6.4 Selecting the NAT Mode

Click NAT to open the following screen.

NAT - Mode

Network Address Translation

☐ None
 ☒ SUA Only [Edit Details](#)
☐ Full Feature [Edit Details](#)

Figure 6-4 NAT Mode

The following table describes the labels in this screen.

Table 6-4 NAT Mode

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

6.5 Configuring SUA Server

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

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

NAT - Edit SUA/NAT Server Set

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

Save Cancel

Figure 6-5 Edit SUA/NAT Server Set

The following table describes the labels in this screen.

Table 6-5 Edit SUA/NAT Server Set

LABEL	DESCRIPTION
Start Port No.	<p>Enter a port number in this field.</p> <p>To forward only one port, enter the port number again in the End Port No. field.</p> <p>To forward a series of ports, enter the start port number here and the end port number in the End Port No. field.</p>

Table 6-5 Edit SUA/NAT Server Set

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

6.6 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 **NAT**, select **Full Feature** and click **Edit Details** to open the following screen.

NAT - Address Mapping Rules

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

Back

Figure 6-6 Address Mapping Rules

The following table describes the labels in this screen.

Table 6-6 Address Mapping Rules

LABEL	DESCRIPTION
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If 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. You can only do this for Many-to-One and Server mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is N/A for One-to-one , Many-to-One and Server mapping types.

Table 6-6 Address Mapping Rules

LABEL	DESCRIPTION
Type	<p>1-1: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</p> <p>M-1: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</p> <p>M-M Ov (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p>MM No (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</p> <p>Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
Back	Click Back to return to the NAT Mode screen.

6.7 Editing an Address Mapping Rule

To edit an address-mapping rule, click the rule’s link in the **NAT Address Mapping Rules** screen to display the screen shown next.

NAT - Edit Address Mapping Rule 1

Type

One-to-One

Local Start IP

0.0.0.0

Local End IP

N/A

Global Start IP

0.0.0.0

Global End IP

N/A

Server Mapping Set

N/A

[Edit Details](#)

Apply

Cancel

Delete

Figure 6-7 Address Mapping Rule Edit

The following table describes the labels in this screen.

Table 6-7 Address Mapping Rule Edit

LABEL	DESCRIPTION
Type	<p>Choose the port mapping type from one of the following.</p> <ol style="list-style-type: none"> 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 that previous ZyXEL routers supported only. 3. Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. Many-to-Many No Overload: Many-to-Many No Overload 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 local IP address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	<p>This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address.</p> <p>This field is N/A for One-to-One and Server mapping types.</p>
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.
Server Mapping Set	<p>Only available when Type is set to Server.</p> <p>Select a number from the drop-down menu to choose a server set from the NAT - Address Mapping Rules screen.</p>
Edit Details	Click this link to go to the NAT - Edit SUA/NAT Server Set screen to edit a server set that you have selected in the Server Mapping Set field.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to return to the previously saved settings.
Delete	Click Delete to exit this screen without saving

Chapter 7

Dynamic DNS Setup

This chapter discusses how to configure your Prestige to use Dynamic DNS.

7.1 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.

7.1.1 DynDNS Wildcard

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

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

7.2 Configuring Dynamic DNS

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

Dynamic DNS

☐ Active

Service Provider

WWW.DynDNS.ORG

Host Name

E-mail Address

User

Password

☐ Enable Wildcard

Apply

Cancel

Figure 7-1 DDNS

The following table describes the labels in this screen.

Table 7-1 DDNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your Prestige by your Dynamic DNS provider.
E-mail Address	Type your e-mail address.
User	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard	Select this check box to enable DynDNS Wildcard.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to return to the previously saved settings.

Part III:

Firewall and Content Filter

This part introduces firewalls in general and the Prestige firewall. It also explains customized services and logs and gives example firewall rules and an overview of content filtering.

Chapter 8

Firewall

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

8.1 Firewall Overview

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

8.2 Types of Firewalls

There are three main types of firewalls:

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

8.2.1 Packet Filtering Firewalls

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

8.2.2 Application-level Firewalls

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

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

8.2.3 Stateful Inspection Firewalls

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

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

8.3 Introduction to ZyXEL's Firewall

The Prestige firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The 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 also has packet filtering capabilities.

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

The Prestige has one ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

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

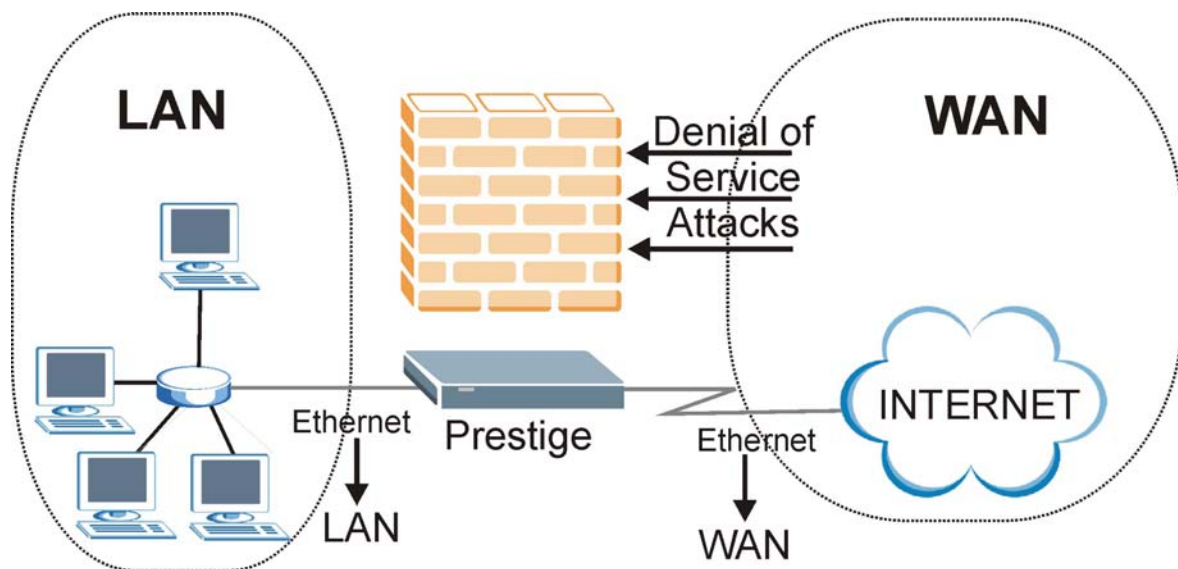


Figure 8-1 Prestige Firewall Application

8.4 Denial of Service

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

8.4.1 Basics

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

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

Some of the most common IP ports are:

Table 8-1 Common IP Ports

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

8.4.2 Types of DoS Attacks

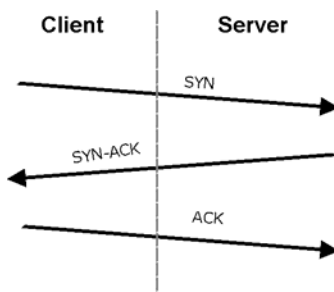
There are four types of DoS attacks:

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

1-a Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

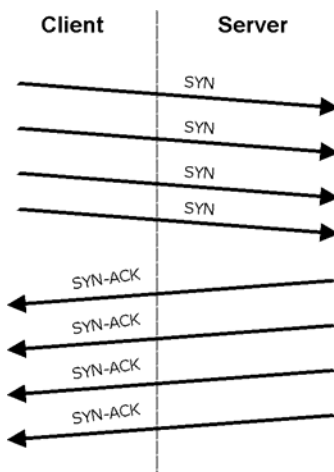
1-b Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

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

**Figure 8-2 Three-Way Handshake**

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

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

**Figure 8-3 SYN Flood**

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

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

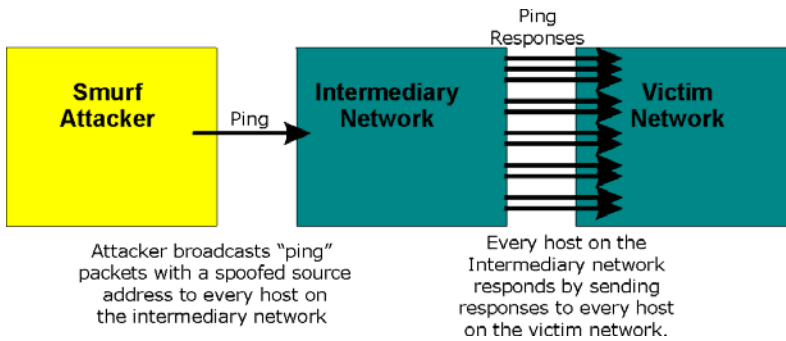


Figure 8-4 Smurf Attack

➤ ICMP Vulnerability

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

Table 8-2 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

➤ Illegal Commands (NetBIOS and SMTP)

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

Table 8-3 Legal NetBIOS Commands

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

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

Table 8-4 Legal SMTP Commands

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

➤ Traceroute

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

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

8.5 Stateful Inspection

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

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

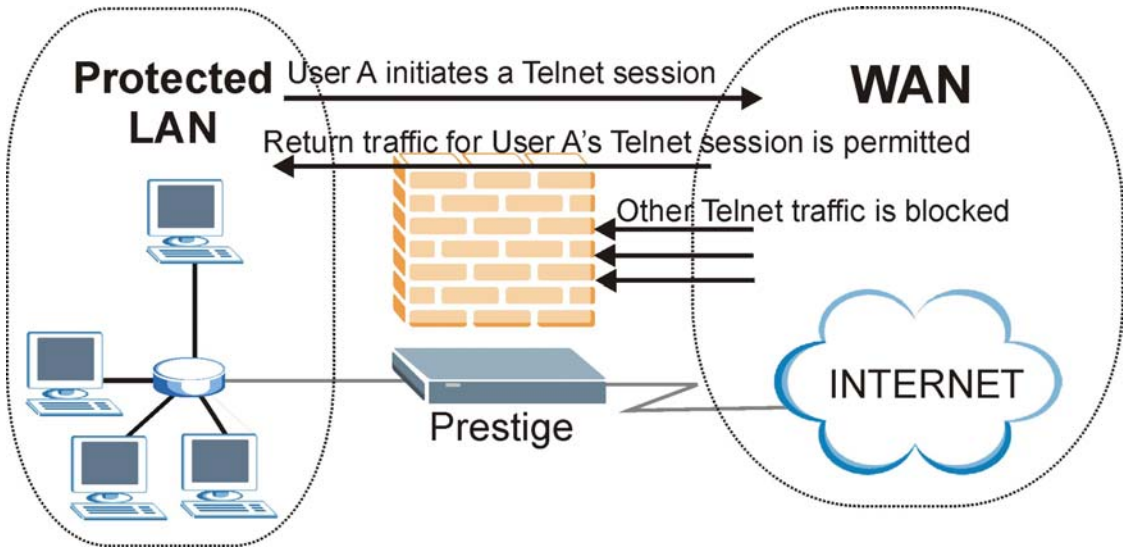


Figure 8-5 Stateful Inspection

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

8.5.1 Stateful Inspection Process

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

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **The default action for packets not matching following rules** field (see *Figure 10-4*) determines the action for this packet.

4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

8.5.2 Stateful Inspection and the Prestige

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

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

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

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

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

8.5.3 TCP Security

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

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

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

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

8.5.4 UDP/ICMP Security

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

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

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

8.5.5 Upper Layer Protocols

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

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

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

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

8.6 Guidelines for Enhancing Security with Your Firewall

1. Change the default password via SMT or web configurator.
2. Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.
3. Limit who can telnet into your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

8.6.1 Security In General

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

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

8.7 Packet Filtering Vs Firewall

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

8.7.1 Packet Filtering:

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

When To Use Filtering

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

8.7.2 Firewall

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

When To Use The Firewall

- To prevent DoS attacks and prevent hackers cracking your network.
- A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.

- To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- The firewall performs better than filtering if you need to check many rules.
- Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
- The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

Chapter 9

Firewall Configuration

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

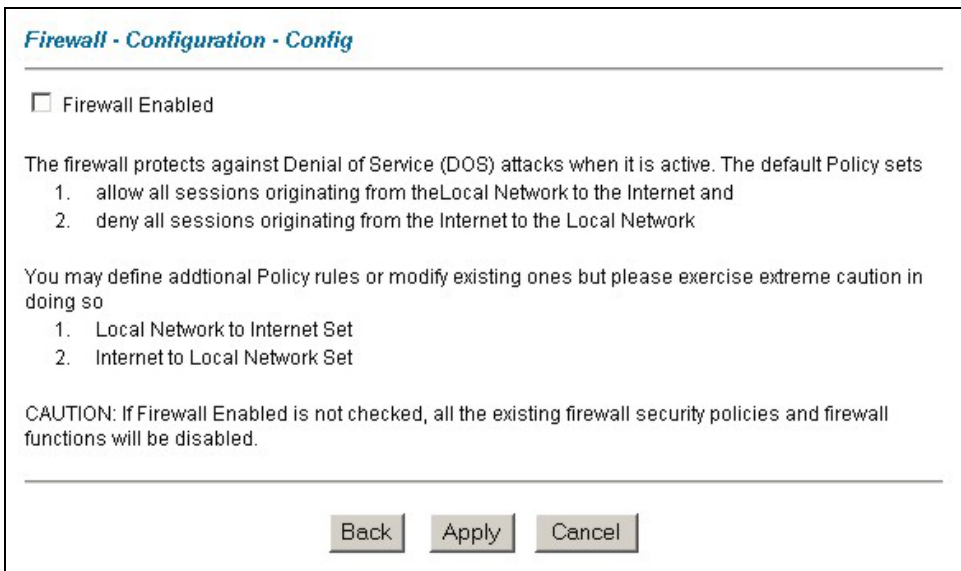
9.1 Remote Management and the Firewall

When remote management 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.

9.2 Enabling the Firewall

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



Firewall - Configuration - Config

☐ Firewall Enabled

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

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

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

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

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

Back Apply Cancel

Figure 9-1 Enabling the Firewall

9.3 Configuring E-mail Alerts

To change your Prestige’s E-mail log settings, click **Advanced Setup**, **Firewall**, and then **E-mail**. The screen appears as shown. This screen is not available on all models.

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

Firewall - Email

Address Info

Mail Server:

0.0.0.0

Subject:

E-mail Alerts To:

(Email)

Return Address:

(Email)

Log Timer

Log Schedule:

When Log is Full

Day for Sending Alerts:

Sunday

Time for Sending Alerts:

0 (hour) : 0 (minute)

Back

Apply

Cancel

Figure 9-2 E-mail

The following table describes the labels in this screen.

Table 9-1 E-mail

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Subject	Type a title that you want to be in the subject line of the log e-mail message that the Prestige sends.

Table 9-1 E-mail

LABEL	DESCRIPTION
E-mail Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
Return Address	Type an E-mail address to identify the Prestige as the sender of the e-mail messages i.e., a "return-to-sender" address for backup purposes.
Log Timer	
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <p>Step 4. Daily</p> <p>Step 5. Weekly</p> <p>Step 6. Hourly</p> <p>Step 7. When Log is Full</p> <p>Step 8. None.</p> <p>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</p>
Day for Sending Alerts	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Alerts	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to return to the previously saved settings.

9.4 Attack Alert

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

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

9.4.1 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Alert** screen (*Figure 9-3* - select the **Generate alert when attack detected** checkbox) or when a rule is matched in the **Edit Rule** screen (see *Figure 10-5*). When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **Log Settings** screen (see the chapter on logs).

9.4.2 Threshold Values

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

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

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

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

9.4.3 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see *Figure 8-2*). For UDP, "half-open" means that the firewall has detected no return traffic.

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

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

When the rate of new connection attempts rises above a threshold (**one-minute high**), the Prestige starts deleting half-open sessions as required to accommodate new connection requests. The Prestige continues to

delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

TCP Maximum Incomplete and Blocking Time

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

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

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

The Prestige also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click **Advanced Setup**, **Firewall**, and **Alert** to bring up the next screen.

Firewall - Configuration - Alert

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

☐ Generate alert when attack detected

Denial of Service Thresholds

One Minute Low :

80

One Minute High :

100

Maximum Incomplete Low :

80

Maximum Incomplete High :

100

TCP Maximum Incomplete :

10

☐ Blocking Time

10

(minute)

Back

Apply

Cancel

Figure 9-3 Alert

The following table describes the labels in this screen.

Table 9-2 Alert

LABEL	DESCRIPTION
Generate alert when attack detected	Select this check box to generate an alert whenever an attack is detected.
Denial of Services Thresholds	
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number. "80" is the default.

Table 9-2 Alert

LABEL	DESCRIPTION
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. The default is "100". When the rate of new connection attempts rises above this number, the Prestige deletes half-open sessions as required to accommodate new connection attempts. The Prestige stops deleting half-open sessions when the number is less than the One Minute Low .
Maximum Incomplete Low	This is the number of existing half-open sessions (default "80") that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions (default "100") that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the Prestige deletes half-open sessions as required to accommodate new connection requests. The Prestige stops deleting half-open sessions when the number is less than the Max Incomplete Low . Do not set Maximum Incomplete High to lower than the current Max Incomplete Low number.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions (default "10") with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256 . As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.
Blocking Time	When TCP Maximum Incomplete is reached you can choose if the next session should be allowed or blocked. If you select Blocking Time , any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.
(min)	Type the length of Blocking Time in minutes (1-256). The default is "0".
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to return to the previously saved settings.

Chapter 10

Creating Custom Rules

This chapter contains instructions for defining both Local Network and Internet rules.

10.1 Rules Overview

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

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

For example, you may create rules to:

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

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

10.2 Rule Logic Overview

Study these points carefully before configuring rules.

10.2.1 Rule Checklist

1. State the intent of the rule. For example, “This restricts all IRC access from the LAN to the Internet.” Or, “This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.”
2. Is the intent of the rule to forward or block traffic?

3. What is the direction connection: from the LAN to the Internet, or from the Internet to the LAN?
4. What IP services will be affected?
5. What computers on the LAN are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

10.2.2 Security Ramifications

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

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the **Rules** screen in the web configurator.

10.2.3 Key Fields For Configuring Rules

Action

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

“Block” means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See *section 10.6* for more information on predefined services.

Source Address

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

Destination Address

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

10.3 Connection Direction

This section talks about configuring firewall rules for connections going from LAN to WAN and WAN to LAN in your firewall.

10.3.1 LAN to WAN Rules

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

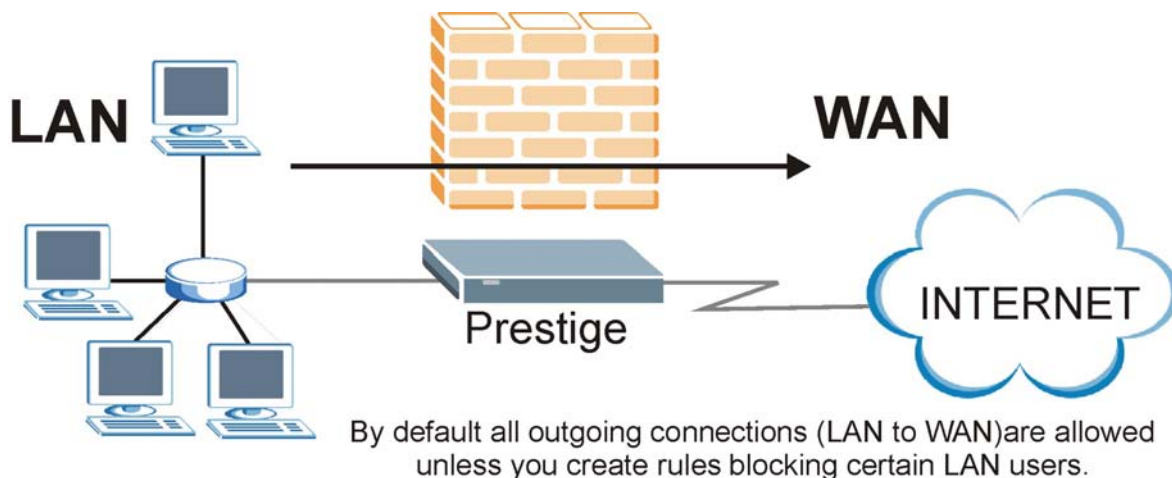


Figure 10-1 LAN to WAN Traffic

10.3.2 WAN to LAN Rules

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

See the following figure.

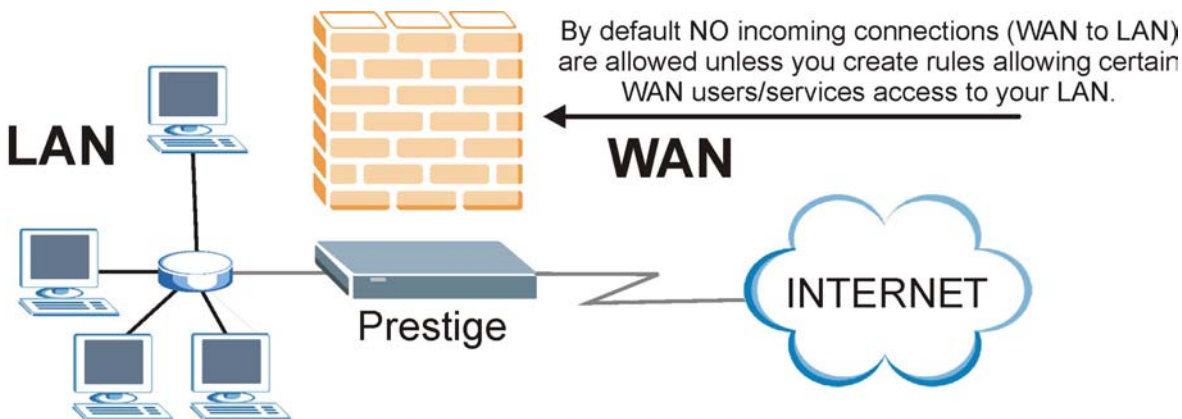


Figure 10-2 WAN to LAN Traffic

10.4 Logs

A log is a detailed record that you create for packets that either match a rule, don't match a rule or both when you are creating/editing a firewall rule (see *Figure 10-5*). You can also choose not to create a log for a rule in this screen. An attack automatically generates a log. Logs can be sent to an e-mail account or syslog server that you specify in the **E-mail** screen (see the section on E-mail logs).

Use this screen to view your firewall and content filtering logs. This screen is not available on all models.

Click **Advanced Setup**, **Firewall**, and then **Logs** to open the **Logs** screen.

Firewall Logs				
(Page 1/1)				
No.	Time	Packet Information		Action
127	Jan 01 00:04:28	From:192.168.1.1	To:192.168.1.33	default policy
		ICMP	type:00003 code:00001	forward
<div> Back Previous Page Refresh Clear Next Page </div>				

Figure 10-3 Firewall Logs

The following table describes the labels in this screen.

Table 10-1 Firewall Logs

LABEL	DESCRIPTION	EXAMPLE
No.	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	
Time	This is the time the log was recorded in this format. You must configure menu 24.10 to have the logs display the correct time.	dd:mm:yy e.g., Jan 01 0 hh:mm:ss e.g., 00:04:28
Packet Information	This field lists packet information such as: From and To IP addresses, protocol and port numbers.	

Table 10-1 Firewall Logs

LABEL	DESCRIPTION	EXAMPLE
Reason	This field states the reason for the log; i.e., was the rule matched, not matched, or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol.
	This is a log for a DoS attack.	attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop, or syn flood. <i>Chapter 8</i> has more detailed discussion of what these attacks mean.
Action	This field displays whether the packet was blocked (i.e., silently discarded), forwarded or neither (Block , Forward or None). "None" means that no action is dictated by this rule.	Block , Forward or None
Back	Click Back to return to the previous screen.	
Previous Page	Click Previous Page to view more logs.	
Refresh	Click Refresh to update the report display. The report also refreshes automatically when you close and reopen the screen.	
Clear	Click Clear to delete all the logs.	
Next Page	Click Next Page to view more logs.	

10.5 Rule Summary

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

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

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

Firewall - LAN to WAN - Rule Summary

The default action for packets not matching following rules:

☒ Default Permit Log

No.	Source IP	Destination IP	Service	Action	Log
1	<input type="text" value="Any"/>	<input type="text" value="Any"/>	<input type="text" value="Any(UDP)"/>	Forward	None
2	<input type="text"/>	<input type="text"/>	<input type="text"/>		
3	<input type="text"/>	<input type="text"/>	<input type="text"/>		
4	<input type="text"/>	<input type="text"/>	<input type="text"/>		
5	<input type="text"/>	<input type="text"/>	<input type="text"/>		
6	<input type="text"/>	<input type="text"/>	<input type="text"/>		
7	<input type="text"/>	<input type="text"/>	<input type="text"/>		
8	<input type="text"/>	<input type="text"/>	<input type="text"/>		
9	<input type="text"/>	<input type="text"/>	<input type="text"/>		
10	<input type="text"/>	<input type="text"/>	<input type="text"/>		

Rules Reorder: Move rule number to rule number

Figure 10-4 Firewall Rules Summary: First Screen

The following table describes the labels in this screen.

Table 10-2 Firewall Rules Summary: First Screen

LABEL	DESCRIPTION
The default action for packets not matching following rules	Use the drop-down list box to select whether to Block (silently discard) or Forward (allow the passage of) packets that do not match the following rules.
Default Permit Log	Select this check box to log all matched rules in the default set.
The following fields summarize the rules you have created. Note that these fields are read only. Click the tab at the top of the box to order the rules according to that tab.	
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The Move field below allows you to reorder your rules. Click a rule's number to edit the rule.
Source IP	This is the source address of the packet. Please note that a blank source or destination address is equivalent to Any .
Destination IP	This is the destination address of the packet. Please note that a blank source or destination address is equivalent to Any .
Service	This is the service to which the rule applies. See <i>Table 10-3</i> for more information.
Action	This is the specified action for that rule, whether to Block (discard) or Forward (allow the passage of) packets.
Log	This field shows you if a log is created for packets that match the rule (Match), don't match the rule (Not Match), both (Both) or no log is created (None).
Rules Reorder	You may reorder your rules using this function. Use the drop-down list box to select the number of the rule you want to move. The ordering of your rules is important as rules are applied in turn.
To Rule Number	Use the drop-down list box to select to where you want to move the rule.
Move	Click Move to move the rule.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to return to the previously saved settings.

10.6 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see *Figure 10-5*) displays all predefined services that the Prestige already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that

defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled “**(DNS)**”. **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom services may also be configured using the **Custom Ports** function discussed later.

Table 10-3 Predefined Services

SERVICE	DESCRIPTION
AIM/NEW_ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20,21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	Net Meeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IPSEC_TRANSPORT/TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.

Table 10-3 Predefined Services

SERVICE	DESCRIPTION
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
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.

Table 10-3 Predefined Services

SERVICE	DESCRIPTION
SSDP(UDP:1900)	Simple Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using UDP port 1900.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRMWORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

10.7 Creating/Editing Firewall Rules

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

Firewall - LAN to WAN - Edit Rule 1

Source Address:

Source IP Address #####
Any

SrcAdd

SrcEdit

SrcDelete

Destination Address:

Destination IP Address ####
Any

DestAdd

DestEdit

DestDelete

Service:

Available Services:

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

<<

>>

Selected Services:

Any(UDP)
Any(TCP)

[Edit Available Service](#)

Action for Matched Packets:

Forward

Log:

None

☐ Alert

Apply

Cancel

Delete

Figure 10-5 Creating/Editing A Firewall Rule

The following table describes the labels in this screen.

Table 10-4 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Source Address	Click SrcAdd to add a new address, SrcEdit to edit an existing one or SrcDelete to delete one.

10-12

Creating Custom Rules

Table 10-4 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Destination Address	Click DestAdd to add a new address, DestEdit to edit an existing one or DestDelete to delete one.
Services	Select a service in the Available Services box on the left, then click >> to select. The selected service shows up on the Selected Services box on the right. To remove a service, click on it in the Selected Services box on the right, then click << .
Edit Available Service	Click this button to go to the Customized Services screen. Refer to <i>Chapter 14</i> for more information.
Action for Matched Packets	Use the drop down list box to select whether to Block (silently discard) or Forward (allow the passage of) packets that match this rule.
Log	This field determines if a log is created for packets that match the rule (Match), don't match the rule (Not Match), match either rule (Both) or no log is created (None).
Alert	Select the Alert check box to determine that this rule generates an alert when the rule is matched.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to exit this screen without saving.
Delete	Click Delete to remove the current rule.

10.7.1 Source and Destination Addresses

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

Firewall - LAN to WAN - Rule IP Config

Address Type:

Subnet Address

Start IP Address:

0.0.0.0

End IP Address:

0.0.0.0

Subnet Mask:

0.0.0.0

Apply

Cancel

Figure 10-6 Adding/Editing Source and Destination Addresses

The following table describes the labels in this screen.

Table 10-5 Adding/Editing Source and Destination Addresses

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

10.8 Timeout

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

10.8.1 Factors Influencing Choices for Timeout Values

The factors influencing choices for timeout values are the same as the factors influencing choices for threshold values – see *section 9.4.2*. Click **Timeout** for either **Local Network** or **Internet**.

Firewall - LAN to WAN - Timeout

TCP Timeout Values

Connection Timeout: (sec)

FIN-Wait Timeout: (sec)

Idle Timeout: (sec)

UDP Idle Timeout: (sec)

ICMP Timeout: (sec)

Figure 10-7 Timeout

The following table describes the labels in this screen.

Table 10-6 Timeout

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

Table 10-6 Timeout

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to return to the previous configuration.

Chapter 11

Customized Services

This chapter covers creating, viewing and editing custom services.

11.1 Introduction to Customized Services

Configure customized services and port numbers not predefined by the Prestige (see *Figure 10-5*). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read *section 10.6*. To configure a custom service, click **Edit Available Service** in an edit rule screen to bring up the following screen.

Firewall - Customized Services

No.	Name	Protocol	Port
1	MyService	TCP/UDP	123
2			
3			
4			
5			
6			
7			
8			
9			
10			

[Back](#)

Figure 11-1 Customized Services

The next table describes the labels in this screen.

Table 11-1 Customized Services

LABEL	DESCRIPTION
Customized Services	
No.	This is the number of your customized port. Click a rule’s number of a service to go to the Firewall Customized Services Config screen to configure or edit a customized service.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (TCP , UDP or Both) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click Back to return the Firewall Edit Rule screen.

11.2 Creating/Editing A Customized Service

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

Firewall - Customized Services - Config

Service Name:

Service Type:

TCP/UDP

Port Configuration

Type:

☒ Single

☐ Range

Port Number:

0

-

0

Back

Apply

Cancel

Delete

Figure 11-2 Creating/Editing A Customized Service

The next table describes the labels in this screen.

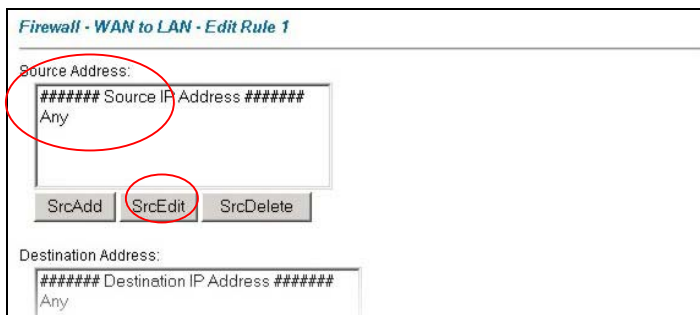
Table 11-2 Creating/Editing A Customized Service

LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (TCP , UDP or TCP/UDP) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click Single to specify one port only or Range to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Back	Click Back to return to the Firewall Customized Services screen.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to return to the previously saved settings.
Delete	Click Delete to delete the current rule.

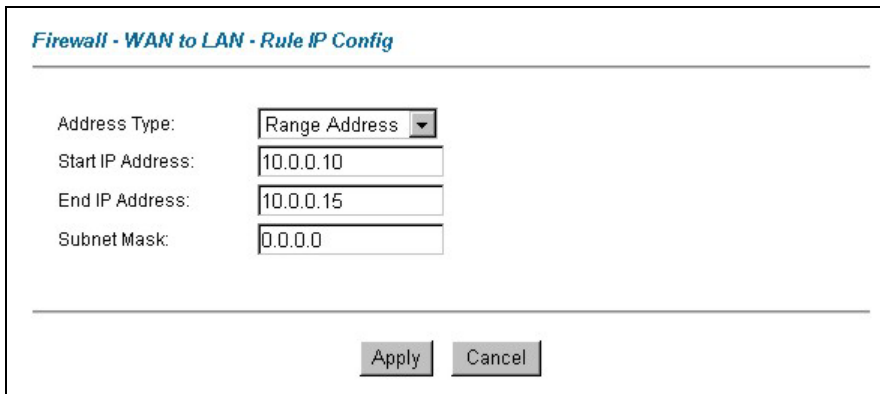
11.3 Example Custom Service Firewall Rule

The following Internet firewall rule example allows a hypothetical “My Service” connection from the Internet.

- Step 1.** Click **Rule Summary** under **Internet to Local Network Set**.
- Step 2.** Click a rule number to open the edit rule screen.
- Step 3.** Click **Any** in the **Source Address** box and then click **SrcDelete**.

**Figure 11-3 Edit Rule Example**

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



Firewall - WAN to LAN - Rule IP Config

Address Type:

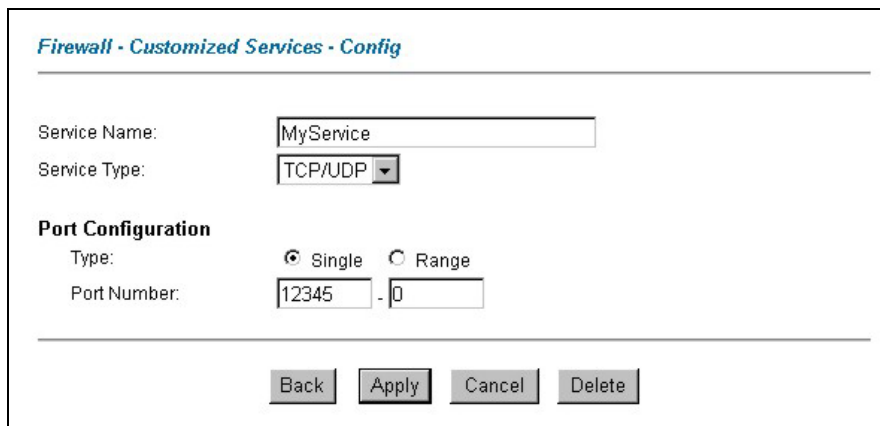
Start IP Address:

End IP Address:

Subnet Mask:

Figure 11-4 Configure Source IP Example

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



Firewall - Customized Services - Config

Service Name:

Service Type:

Port Configuration

Type: ☒ Single ☐ Range

Port Number: -

Figure 11-5 Customized Service for MyService Example

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

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

Firewall - WAN to LAN - Edit Rule 1

Source Address:

Source IP Address #####
10.0.0.10 - 10.0.0.15

SrcAdd SrcEdit SrcDelete

Destination Address:

Destination IP Address ####
Any

DestAdd DestEdit DestDelete

Service:

Available Services:

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

[Edit Available Service](#)

Selected Services:

*MyService(TCP/UDP:12345)

Action for Matched Packets: Forward

Log: None

☐ Alert

Click **Apply** when finished.

Apply Cancel Delete

This is the address range of the MyService computers.

This is your MyService custom port.

Figure 11-6 Syslog Rule Configuration Example

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

This rule allows a MyService connection from the WAN.

Firewall - WAN to LAN - Rule Summary

The default action for packets not matching following rules:

Block

☒ Default Permit Log

No.	Source IP	Destination IP	Service	Action	Log
1	<div>10.0.0.10 - 10.0.0.15</div>	<div>Any</div>	<div>*MyService(TCP/UDP:12345)</div>	Forward	None
2	<div></div>	<div></div>	<div></div>		
3	<div></div>	<div></div>	<div></div>		
4	<div></div>	<div></div>	<div></div>		
5	<div></div>	<div></div>	<div></div>		
6	<div></div>	<div></div>	<div></div>		
7	<div></div>	<div></div>	<div></div>		
8	<div></div>	<div></div>	<div></div>		
9	<div></div>	<div></div>	<div></div>		
10	<div></div>	<div></div>	<div></div>		

Rules Reorder: Move rule number

1

 to rule number

1

Move

Back

Apply

Cancel

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

Figure 11-7 Rule Summary Example

Chapter 12

Content Filtering

This chapter covers how to configure content filtering.

12.1 Content Filtering Overview

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering gives you the ability to block web sites that contain key words (that you specify) in the URL. You can set a schedule for when the Prestige performs content filtering. You can also specify trusted IP addresses on the LAN for which the Prestige will not perform content filtering.

12.2 Configuring Keyword Blocking

Use this screen to block sites containing certain keywords in the URL. For example, if you enable the keyword "bad", the Prestige blocks all sites containing this keyword including the URL <http://www.website.com/bad.html>, even if it is not included in the Filter List.

To have your Prestige block Web sites containing keywords in their URLs, click **Content Filter** and **Keyword**. The screen appears as shown.

Content Filter- Keyword

☒ Enable Keyword Blocking

Block Websites that contain these keywords in the URL :

bad

Delete

Clear All

Keyword

Add Keyword

Back

Apply

Cancel

Figure 12-1 Content Filter: Keyword

The following table describes the labels in this screen.

Table 12-1 Content Filter: Keyword

LABEL	DESCRIPTION
Enable Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the Prestige to block.
Delete	Highlight a keyword in the box and click Delete to remove it.
Clear All	Click Clear All to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.

Table 12-1 Content Filter: Keyword

LABEL	DESCRIPTION
Add Keyword	Click Add Keyword after you have typed a keyword. Repeat this procedure to add other keywords. Up to 127 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to return to the previously saved settings.

12.3 Configuring the Schedule

To set the days and times for the Prestige to perform content filtering, click **Content Filter** and **Schedule**. The screen appears as shown.

Content Filter - Schedule

Days to Block:

☒ Everyday

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Time of Day to Block: (24 Hour Format)

☐ All day

Start: (hour) (minute) End: (hour) (minute)

Figure 12-2 Content Filter: Schedule

The following table describes the labels in this screen.

Table 12-2 Content Filter: Schedule

LABEL	DESCRIPTION
Days 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:	Use the 24 hour format to configure which time of the day (or select the All day check box) you want the content filtering to be active.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to return to the previously saved settings.

12.4 Configuring Trusted Computers

To exclude a range of users on the LAN from content filtering on your Prestige, click **Content Filter** and **Trusted**. The screen appears as shown.

Content Filter - Trusted

Trusted User IP Range

From : (IP address)

To : (IP address)

Figure 12-3 Content Filter: Trusted

The following table describes the labels in this screen.

Table 12-3 Content Filter: Trusted

LABEL	DESCRIPTION
Trusted User IP Range	
From	Type the IP address of a computer (or the beginning IP address of a specific range of computers) on the LAN that you want to exclude from content filtering.

Table 12-3 Content Filter: Trusted

LABEL	DESCRIPTION
To	Type the ending IP address of a specific range of users on your LAN that you want to exclude from content filtering. Leave this field blank if you want to exclude an individual computer.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to return to the previously saved settings.

12.5 Configuring Logs

This screen records the results of your content filter policies. Click **Content Filter** and **Logs**. The screen appears as shown

Content Filter - Logs

Page

No.	Time	Source IP	Reason	Action
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Figure 12-4 Content Filter Logs

The following table describes the labels in this screen.

Table 12-4 Content Filter Logs

LABEL	DESCRIPTION
Page	Choose a page of logs from the drop-down list box to display.
No.	This is the index number of the content filter log.
Time	This field displays the time of the log.
Source IP	This field displays the IP address of the computer accessing the web site.
Reason	This field shows what type of configuration in content filtering caused the event. For example: (BLOCK_EXCEPT_TRUSTED_DOMAINS), (BLOCK_UNTRUST_DOMAIN), (BLOCK_KEYWORD), (BLOCK_ACTIVEX), (BLOCK_JAVA_APPLET), (BLOCK_COOKIE), (BLOCK_PROXY), (BLOCK_CYBERNOT).
Action	This field shows if access was allowed (FORWARD) or blocked (BLOCK).
Back	Click Back to return to the previous screen.
Refresh	Click Refresh to update the report display. The report also refreshes automatically when you close and reopen the screen.
Clear	Click Clear to delete all the logs.

Part IV:

VPN/IPSec

This part provides information about configuring VPN/IPSec for secure communications.

Chapter 13

Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

13.1 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.

13.1.1 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.

13.1.2 Security Association

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

13.1.3 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.

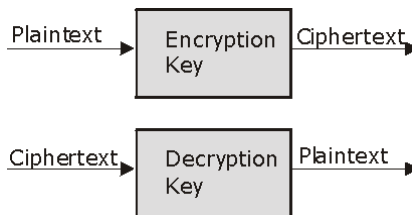


Figure 13-1 Encryption and Decryption

➤ **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.

13.1.4 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.

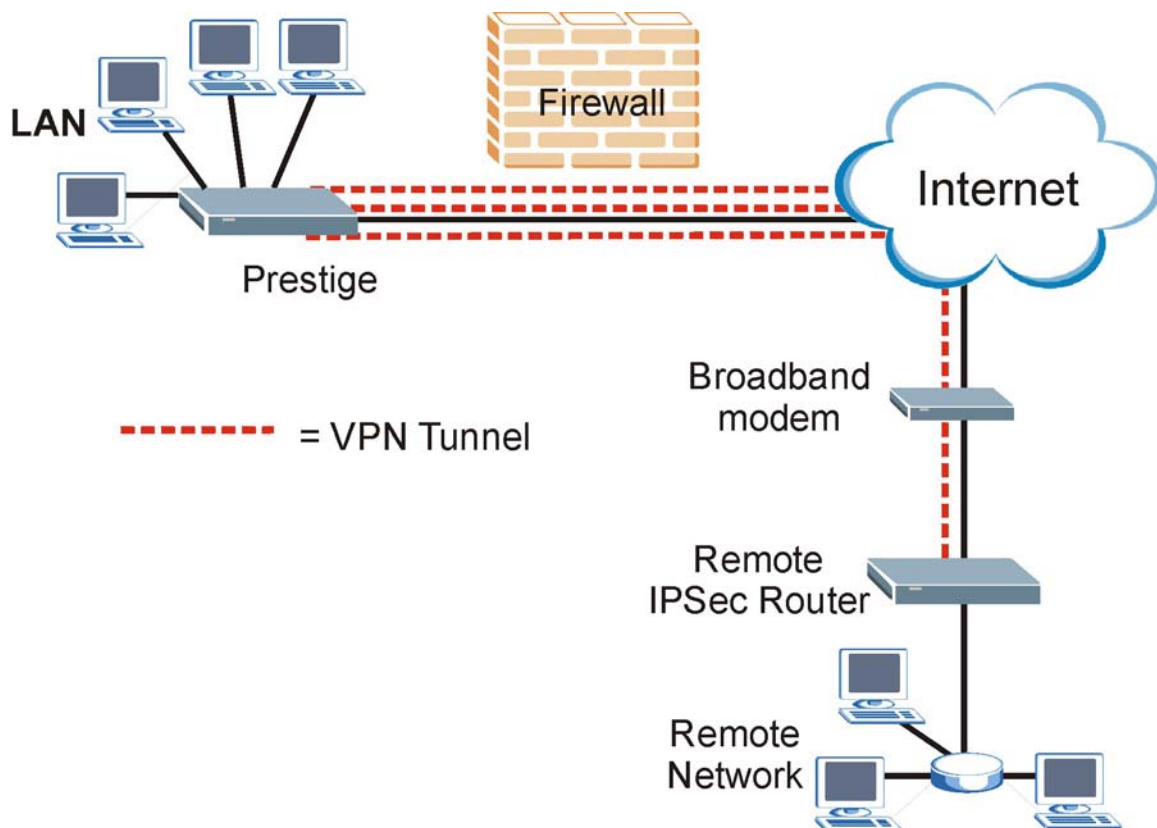
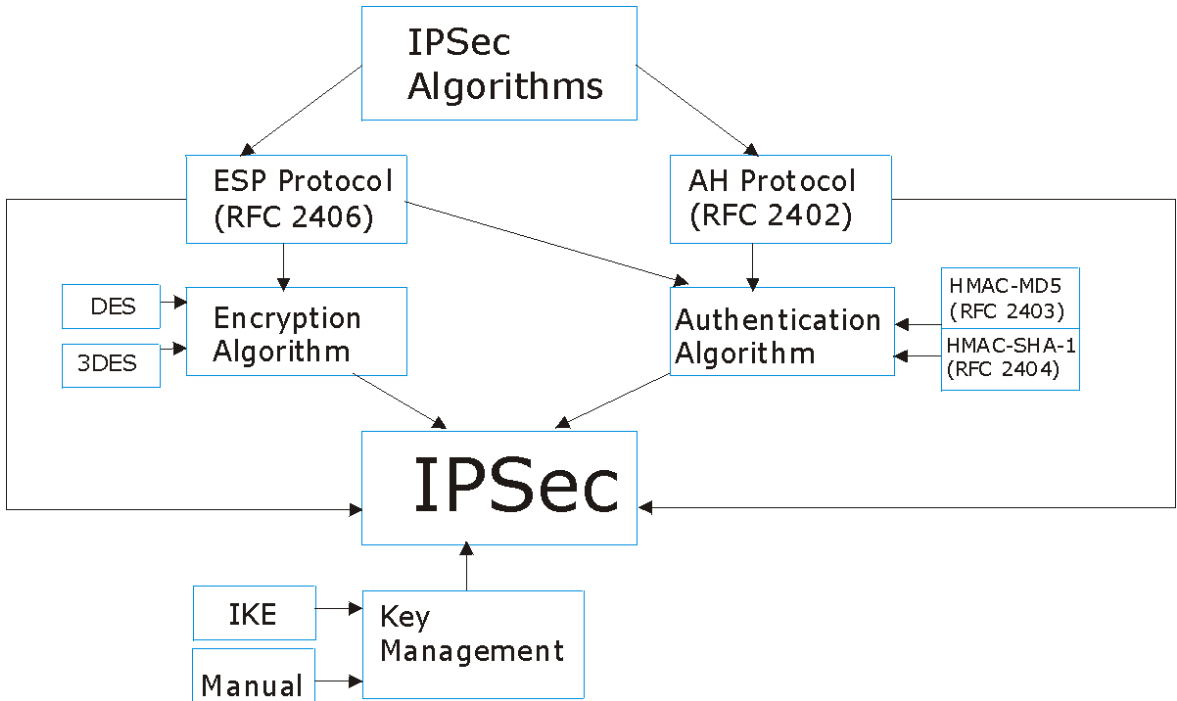


Figure 13-2 VPN Application

13.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

**Figure 13-3 IPsec Architecture**

13.2.1 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 14.2* for more information.

13.2.2 Key Management

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

13.3 Encapsulation

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

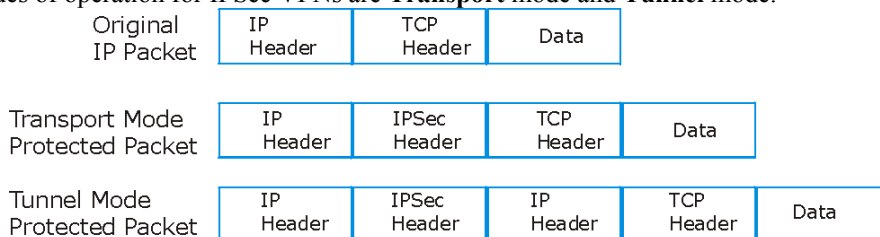


Figure 13-4 Transport and Tunnel Mode IPSec Encapsulation

13.3.1 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.

13.3.2 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.

13.4 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.

Table 13-1 VPN and NAT

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

Chapter 14

VPN Screens

This chapter introduces the VPN screens. See the Logs chapter for information on viewing logs and the Reference Guide for IPSec log description

14.1 VPN/IPSec Overview

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

14.2 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.

14.2.1 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.

14.2.2 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 14-1 AH and ESP

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

14.3 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.

14.4 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).

14.4.1 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 14.16* 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.

14.5 VPN Summary Screen

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

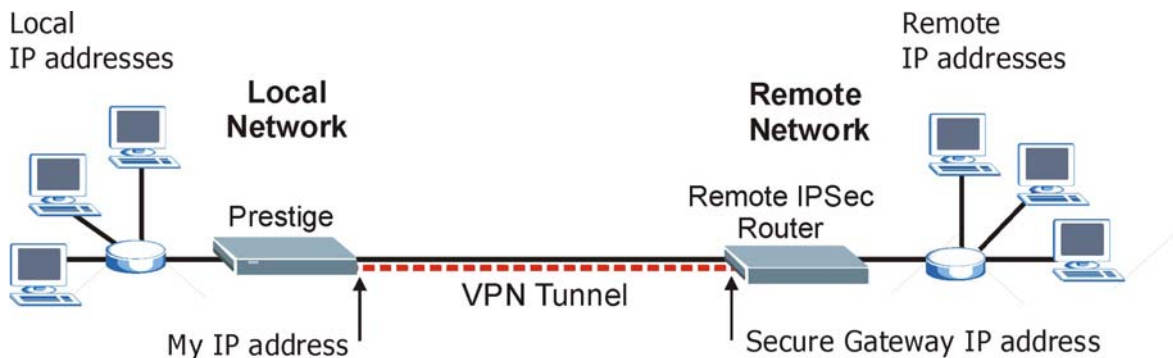


Figure 14-1 IPSec Summary Fields

Local and remote IP addresses must be static.

Click **VPN** and **Setup** to open the **VPN Summary** screen. This is a read-only menu of your IPSec rules (tunnels). The IPSec summary menu is read-only. Edit a VPN by selecting an index number and then configuring its associated submenus.

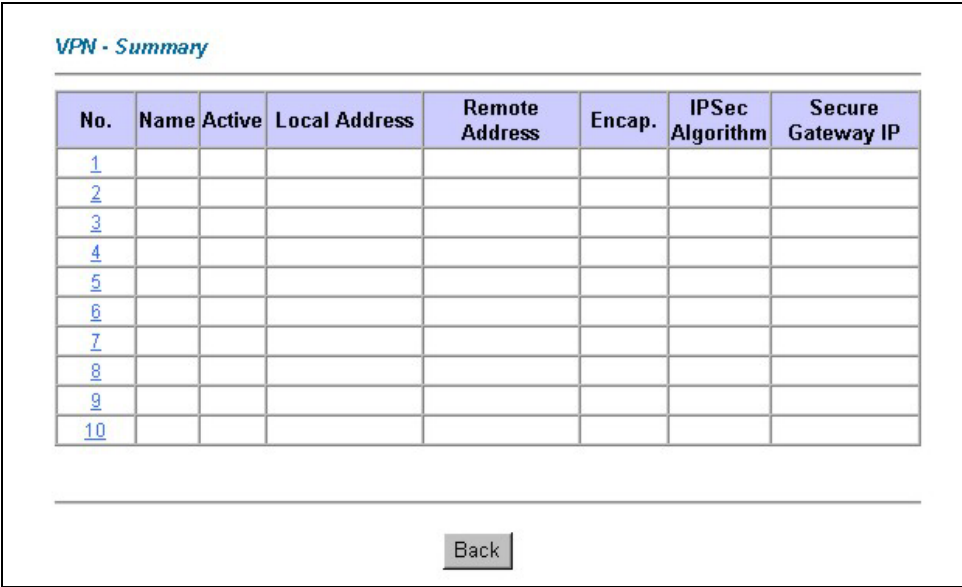


Figure 14-2 VPN Summary

The following table describes the labels in this screen.

Table 14-2 VPN Summary

LABEL	DESCRIPTION
No.	This is the VPN policy index number. Click a number to edit VPN policies.
Name	This field displays the identification name for this VPN policy.
Active	This field displays whether the VPN policy is active or not. A "Y" signifies that this VPN policy is active.
Local Address	This is the IP address(es) of computers on your local network behind your Prestige.
Remote Address	This is the IP address(es) of computers on the remote network behind the remote IPSec router.
Encap.	This field displays Tunnel or Transport mode.

Table 14-2 VPN Summary

LABEL	DESCRIPTION
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase Prestige processing requirements and communications latency (delay).
Secure Gateway IP	This is the IP address of the remote IPSec router. This must be a fixed, public IP address for traffic going through the Internet.
Back	Click Back to return to the previous screen.

14.6 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 14.10* 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. Check *Table 1-1 Model Specific Features* in *chapter 1* to see how many simultaneous IPSec SAs your Prestige model can support.

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

14.7 ID Type and Content

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 aggressive negotiation mode (see *section 14.10.1*), 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 14.17.2* for a telecommuter configuration example).

With main mode (see *section 14.10.1*), 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 two 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 14.11*). 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 14-3 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 14-4 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.	

14.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel. The two Prestiges in this example can complete negotiation and establish a VPN tunnel.

Table 14-5 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 14-6 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
Peer ID content: aa@yahoo.com	Peer ID content: N/A

14.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see *section 14.10* 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.

14.9 Editing VPN Policies

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

VPN - IKE

IPSec Setup

☐ Active

☐ Keep Alive

Name

IPSec Key Mode

IKE

Negotiation Mode

Main

Encapsulation Mode

Tunnel

DNS Server (for IPSec VPN)

0.0.0.0

Local

Local Address Type

Single

IP Address Start

0.0.0.0

End / Subnet Mask

0.0.0.0

Remote

Remote Address Type

Single

IP Address Start

0.0.0.0

End / Subnet Mask

0.0.0.0

Address Information

Local ID Type

IP

Content

My IP Address

0.0.0.0

Peer ID Type

IP

Content

Secure Gateway Address

0.0.0.0

Security Protocol

VPN Protocol

ESP

Pre-Shared Key

Encryption Algorithm

DES

Authentication Algorithm

SHA1

Advanced

Back

Apply

Cancel

Delete

Figure 14-3 VPN IKE

The following table describes the labels in this screen.

Table 14-7 VPN IKE

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy.
Keep Alive	<p>Select either Yes or No from the drop-down list box.</p> <p>Select Yes 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.</p>
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the Prestige drops trailing spaces.
IPSec Key Mode	Select IKE or Manual from the drop-down list box. Manual is a useful option for troubleshooting if you have problems using IKE key management.
Negotiation Mode	Select Main or Aggressive from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encapsulation Mode	Select Tunnel mode or Transport mode from the drop-down list box.
DNS Server (for IPSec VPN)	<p>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.</p> <p>A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.</p>
Local	<p>Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.</p> <p>Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p> <p>In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0.</p>

Table 14-7 VPN IKE

LABEL	DESCRIPTION
Local Address Type	Use the drop-down menu to choose Single , Range , or Subnet . Select Single for a single IP address. Select Range for a specific range of IP addresses. Select Subnet to specify IP addresses on a network by their subnet mask.
IP Address Start	When the Local Address Type field is configured to Single , enter a (static) IP address on the LAN behind your Prestige. When the Local Address Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige. When the Local Address Type field is configured to Subnet , this is a (static) IP address on the LAN behind your Prestige.
End / Subnet Mask	When the Local Address Type field is configured to Single , enter the IP address in the IP Address Start field again here. When the Local Address Type field is configured to Range , enter the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the Local Address Type field is configured to Subnet , this is a subnet mask on the LAN behind your Prestige.
Remote	<p>Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the Secure Gateway Address field is configured to 0.0.0.0. In this case only the remote IPSec router can initiate the VPN.</p> <p>Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>
Remote Address Type	Use the drop-down menu to choose Single , Range , or Subnet . Select Single with a single IP address. Select Range for a specific range of IP addresses. Select Subnet to specify IP addresses on a network by their subnet mask.
IP Address Start	When the Remote Address Type field is configured to Single , enter a (static) IP address on the network behind the remote IPSec router. When the Remote Address Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Remote Address Type field is configured to Subnet , enter a (static) IP address on the network behind the remote IPSec router.

Table 14-7 VPN IKE

LABEL	DESCRIPTION
End / Subnet Mask	When the Remote Address Type field is configured to Single , enter the IP address in the IP Address Start field again here. When the Remote Address Type field is configured to Range , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Remote Address Type field is configured to Subnet , enter a subnet mask on the network behind the remote IPSec router.
Address Information	
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.
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 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.
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 14-7 VPN IKE

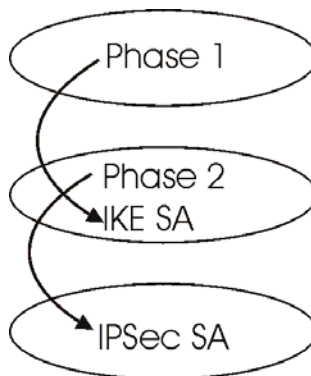
LABEL	DESCRIPTION
Content	<p>When you select IP in the Peer ID Type field, type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Prestige automatically use the address in the Secure Gateway Address field.</p> <p>When you select DNS in the Peer ID Type field, type a domain name (up to 31 characters) by which to identify the remote IPSec router.</p> <p>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.</p> <p>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.</p>
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 Key Mode field must be set to IKE).
Security Protocol	
VPN Protocol	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH . If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described next).
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. Multiple SAs connecting through a secure gateway must have the same pre-shared key.
Encryption Algorithm	<p>Select DES, 3DES or NULL from the drop-down list box.</p> <p>When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. Select NULL to set up a tunnel without encryption. When you select NULL, you do not enter an encryption key.</p>

Table 14-7 VPN IKE

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.
Advanced	Click Advanced to configure more detailed settings of your IKE key management.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to begin configuring this screen afresh.
Delete	Click Delete to delete the current rule.

14.10 IKE Phases

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

**Figure 14-4 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 14.10.3*. 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.

14.10.1 Negotiation Mode

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

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

14.10.2 Diffie-Hellman (DH) Key Groups

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

14.10.3 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised,

previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security. This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the 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).

14.11 Configuring Advanced IKE Settings

Click **Advanced** in the **VPN IKE** screen. This is the **VPN IKE- Advanced** screen as shown next.

VPN - IKE - Advanced Setup

VPN - IKE

Protocol

0

Enable Replay Detection

NO

LocalStart Port

0

End

0

RemoteStart Port

0

End

0

Phase1

Negotiation Mode

Main

Pre-Shared Key

123456789001234567890

Encryption Algorithm

DES

Authentication Algorithm

MD5

SA Life Time (Seconds)

28800

Key Group

DH1

Phase2

Active Protocol

ESP

Encryption Algorithm

DES

Authentication Algorithm

SHA1

SA Life Time (Seconds)

28800

Encapsulation

Tunnel

Perfect Forward Secrecy(PFS)

NONE

Apply

Cancel

Figure 14-5 VPN IKE: Advanced

The following table describes the labels in this screen.

Table 14-8 VPN IKE: Advanced

LABEL	DESCRIPTION
VPN - IKE	
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Protection	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.
Local Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If Local Start Port is left at 0, End will also remain at 0.
Remote Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
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 Start Port is left at 0, End will also remain at 0.
Phase 1	
Negotiation Mode	Select Main or Aggressive from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

Table 14-8 VPN IKE: Advanced

LABEL	DESCRIPTION
Pre-Shared Key	<p>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.</p> <p>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.</p> <p>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.</p>
Encryption Algorithm	<p>Select DES or 3DES from the drop-down list box.</p> <p>When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.</p>
Authentication Algorithm	<p>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.</p>
SA Life Time (Seconds)	<p>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).</p> <p>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.</p>
Key Group	<p>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.</p>
Phase 2	
Active Protocol	<p>Use the drop-down list box to choose from ESP or AH.</p>

Table 14-8 VPN IKE: Advanced

LABEL	DESCRIPTION
Encryption Algorithm	<p>Select DES, 3DES or NULL from the drop-down list box.</p> <p>When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. Select NULL to set up a tunnel without encryption. When you select NULL, you do not enter an encryption key.</p>
Authentication Algorithm	<p>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.</p>
SA Life Time (Seconds)	<p>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).</p> <p>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.</p>
Encapsulation	<p>Select Tunnel mode or Transport mode from the drop-down list box.</p>
Perfect Forward Secrecy (PFS)	<p>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 DH1 or DH2 from the drop-down list box 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).</p>
Apply	<p>Click Apply to save your changes back to the Prestige and return to the VPN IKE screen.</p>
Cancel	<p>Click Cancel to return to the VPN IKE screen without saving your changes.</p>

14.12Manual Key Setup

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

14.12.1 Security Parameter Index (SPI)

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

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

14.13 Configuring Manual Key

You only configure **VPN Manual Key** when you select **Manual** in the **Key Management** field on the **VPN IKE** screen. This is the **VPN Manual Key** screen as shown next.

VPN - Manual Key

IPSec Setup

☐ Active

Name

IPSec Key Mode

Manual

SPI

0

Encapsulation Mode

Transport

DNS Server (for IPSec VPN)

0.0.0.0

Local

Local Address Type

Single

IP Address Start

0.0.0.0

End / Subnet Mask

0.0.0.0

Remote

Remote Address Type

Single

IP Address Start

0.0.0.0

End / Subnet Mask

0.0.0.0

Address Information

My IP Address

0.0.0.0

Secure Gateway Address

0.0.0.0

Security Protocol

IPSec Protocol

ESP

Encryption Algorithm

DES

Encapsulation Key

Authentication Algorithm

SHA1

Authentication Key

Back

Apply

Cancel

Delete

Figure 14-6 VPN Manual Key

The following table describes the labels in this screen.

14-20

VPN Screens

Table 14-9 VPN Manual Key

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the Prestige drops trailing spaces.
IPSec Key Mode	Select IKE or Manual from the drop-down list box. Manual is a useful option for troubleshooting if you have problems using IKE key management.
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.
DNS Server (for IPSec VPN)	<p>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.</p> <p>A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.</p>
Local	<p>Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.</p> <p>Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p> <p>In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0.</p>
Local Address Type	Use the drop-down menu to choose Single , Range , or Subnet . Select Single for a single IP address. Select Range for a specific range of IP addresses. Select Subnet to specify IP addresses on a network by their subnet mask.

Table 14-9 VPN Manual Key

LABEL	DESCRIPTION
IP Address Start	When the Local Address Type field is configured to Single , enter a (static) IP address on the LAN behind your Prestige. When the Local Address Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige. When the Local Address Type field is configured to Subnet , this is a (static) IP address on the LAN behind your Prestige.
End / Subnet Mask	When the Local Address Type field is configured to Single , enter the IP address in the IP Address Start field again here. When the Local Address Type field is configured to Range , enter the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the Local Address Type field is configured to Subnet , this is a subnet mask on the LAN behind your Prestige.
Remote	<p>Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the Secure Gateway Address field is configured to 0.0.0.0. In this case only the remote IPSec router can initiate the VPN.</p> <p>Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>
Remote Address Type	Use the drop-down menu to choose Single , Range , or Subnet . Select Single with a single IP address. Select Range for a specific range of IP addresses. Select Subnet to specify IP addresses on a network by their subnet mask.
IP Address Start	When the Remote Address Type field is configured to Single , enter a (static) IP address on the network behind the remote IPSec router. When the Remote Address Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Remote Address Type field is configured to Subnet , enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the Remote Address Type field is configured to Single , enter the IP address in the IP Address Start field again here. When the Remote Address Type field is configured to Range , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Remote Address Type field is configured to Subnet , enter a subnet mask on the network behind the remote IPSec router.

Table 14-9 VPN Manual Key

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

Table 14-9 VPN Manual Key

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to begin configuring this screen afresh.
Delete	Click Delete to remove the current rule.

14.14Viewing SA Monitor

Click **VPN** and **Monitor** to open the **SA Monitor** screen as shown. 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 fields 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 14.6* on keep alive to have the Prestige renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

VPN - SA Monitor

No.	Name	Encapsulation	IP Sec Algorithm	Disconnect
1	-	-	-	<input type="radio"/>
2	-	-	-	<input type="radio"/>
3	-	-	-	<input type="radio"/>
4	-	-	-	<input type="radio"/>
5	-	-	-	<input type="radio"/>
6	-	-	-	<input type="radio"/>
7	-	-	-	<input type="radio"/>
8	-	-	-	<input type="radio"/>
9	-	-	-	<input type="radio"/>
10	-	-	-	<input type="radio"/>

Figure 14-7 SA Monitor

The following table describes the labels in this screen.

Table 14-10 SA Monitor

LABEL	DESCRIPTION
No	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays Tunnel or Transport mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase Prestige processing requirements and communications latency (delay).
Disconnect	Select Disconnect next to a security association and then click Apply to stop that security association.

Table 14-10 SA Monitor

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the Prestige.
Refresh	Click Refresh to display the current active VPN connection(s).

14.15Configuring Global Setting

To change your Prestige’s global settings, click **VPN** and then **Global Setting**. The screen appears as shown.

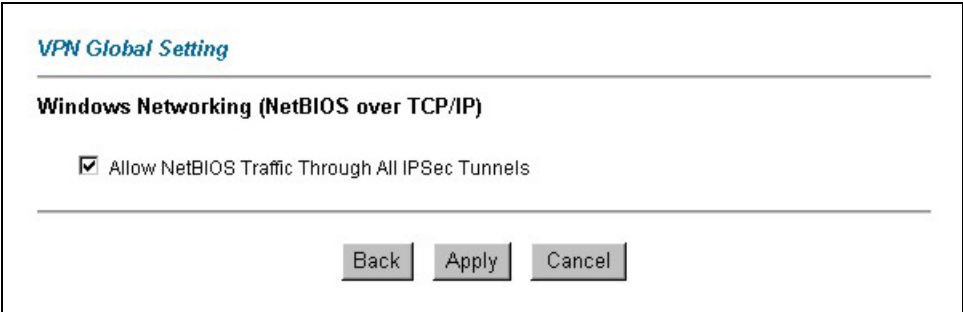


Figure 14-8 Global Setting

The following table describes the labels in this screen.

Table 14-11 Global Setting

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

Table 14-11 Global Setting

LABEL	DESCRIPTION
Cancel	Click Cancel to begin configuring this screen afresh.

14.16 Configuring IPSec Logs

To view IPSec logs in this screen, click **Advanced Setup**, **VPN**, and then **Logs** to open the screen shown next.

**Figure 14-9 VPN Logs**

The following table describes the labels in this screen.

Table 14-12 VPN Logs

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen.
Previous Page	Click Previous Page to view more logs.
Refresh	Click Refresh to update the report display. The report also refreshes automatically when you close and reopen the screen.
Clear	Click Clear to delete all the logs.
Next Page	Click Next Page to view more logs.

This screen is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.

Double exclamation marks (!!) denote an error or warning message.

The following table shows sample log messages during IKE key exchange.

Table 14-13 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
Cannot find outbound SA for rule <#d>	The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.
Send Main Mode request to <IP> Send Aggressive Mode request to <IP>	The Prestige has started negotiation with the peer.
Recv Main Mode request from <IP> Recv Aggressive Mode request from <IP>	The Prestige has received an IKE negotiation request from the peer.
Send:<Symbol><Symbol> Recv:<Symbol><Symbol>	IKE uses the ISAKMP protocol (refer to RFC2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log - see <i>Table 14-15</i> .
Phase 1 IKE SA process done	Phase 1 negotiation is finished.
Start Phase 2: Quick Mode	Phase 2 negotiation is beginning using Quick Mode.
!! IKE Negotiation is in process	The Prestige has begun negotiation with the peer for the connection already, but the IKE key exchange has not finished yet.
!! Duplicate requests with the same cookie	The Prestige has received multiple requests from the same peer but it is still processing the first IKE packet from that peer.
!! No proposal chosen	The parameters configured for Phase 1 or Phase 2 negotiations don't match. Please check all protocols and settings for these phases. For example, one party may be using 3DES encryption, but the other party is using DES encryption, so the connection will fail.
!! Verifying Local ID failed !! Verifying Remote ID failed	During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, then the connection fails.

Table 14-13 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
!! Local / remote IPs of incoming request conflict with rule <#d>	If the security gateway is "0.0.0.0", the Prestige will use the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule then the connection is not allowed.
!! Invalid IP <IP start>/<IP end>	The peer's "Local IP Addr" range is invalid.
!! Remote IP <IP start> / <IP end> conflicts	If the security gateway is "0.0.0.0", the Prestige will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the Prestige will not accept VPN connection requests from this peer.
!! Active connection allowed exceeded	The Prestige limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
!! IKE Packet Retransmit	The Prestige did not receive a response from the peer and so retransmits the last packet sent.
!! Failed to send IKE Packet	The Prestige cannot send IKE packets due to a network error.
!! Too many errors! Deleting SA	The Prestige deletes an SA when too many errors occur.

The following table shows sample log messages during packet transmission.

Table 14-14 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
!! WAN IP changed to <IP>	If the Prestige's WAN IP changes, all configured "My IP Addr" are changed to b "0.0.0.0".. If this field is configured as 0.0.0.0, then the Prestige will use the current Prestige WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find Phase 2 SA	The Prestige cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
!! Discard REPLAY packet	If the Prestige receives a packet with the wrong sequence number it will discard it.

Table 14-14 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
!! Inbound packet authentication failed	The authentication configuration settings are incorrect. Please check them.
!! Inbound packet decryption failed	The decryption configuration settings are incorrect. Please check them.
Rule <#d> idle time out, disconnect	If an SA has no packets transmitted for a period of time (configurable via CI command), the Prestige drops the connection.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 14-15 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

14.17 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single Prestige at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The Prestige at headquarters has a static public IP address.

14.17.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (A, B and C in the figure) to use one VPN rule to simultaneously access a Prestige at headquarters (HQ in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

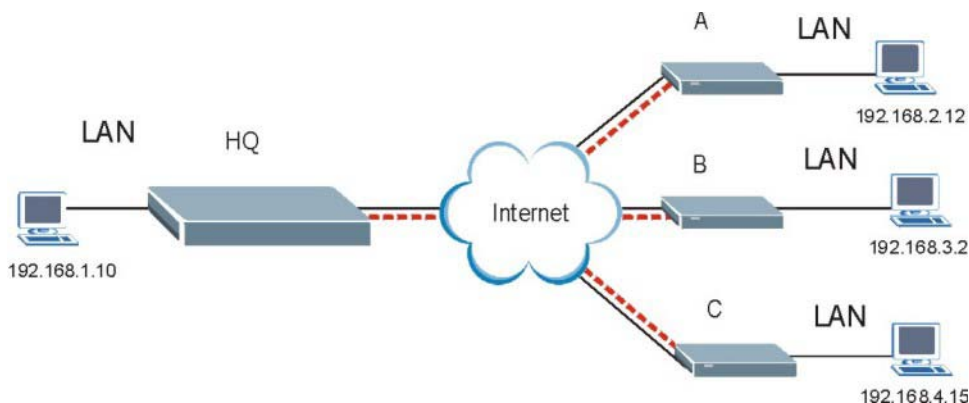


Figure 14-10 Telecommuters Sharing One VPN Rule Example

Table 14-16 Telecommuters Sharing One VPN Rule Example

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

Table 14-16 Telecommuters Sharing One VPN Rule Example

	HEADQUARTERS	TELECOMMUTERS
Local IP Address:	192.168.1.10	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15
Remote IP Address:	0.0.0.0 (N/A)	192.168.1.10

14.17.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see *section 14.10.1*), 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. The local IP addresses (or ranges of addresses) of the rules configured on the Prestige at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters’ IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a Prestige located at headquarters. The Prestige at headquarters (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The Prestige at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

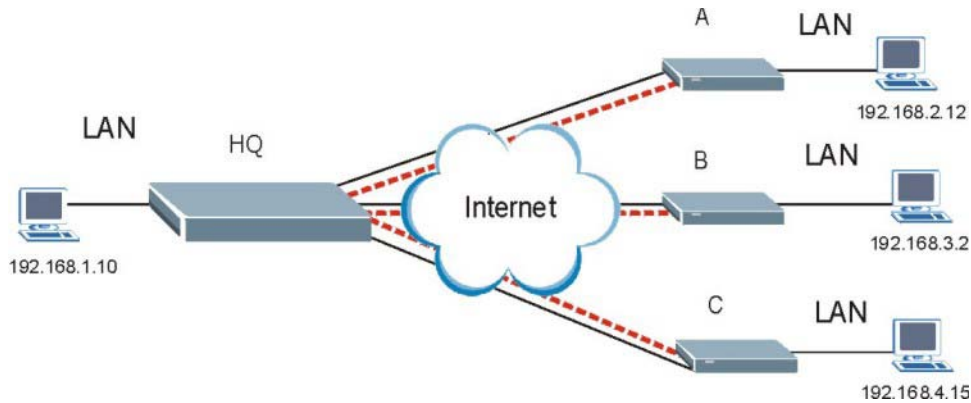


Figure 14-11 Telecommuters Using Unique VPN Rules Example**Table 14-17 Telecommuters Using Unique VPN Rules Example**

HEADQUARTERS	TELECOMMUTERS
All Headquarters Rules:	All Telecommuter Rules:
My IP Address: bigcompanyhq.com	My IP Address 0.0.0.0
Local IP Address: 192.168.1.10	Secure Gateway Address: bigcompanyhq.com
Local ID Type: E-mail	Remote IP Address: 192.168.1.10
Local ID Content: bob@bigcompanyhq.com	Peer ID Type: E-mail
	Peer ID Content: bob@bigcompanyhq.com
Headquarters Prestige Rule 1:	Telecommuter A (telecommutera.dydns.org)
Peer ID Type: IP	Local ID Type: IP
Peer ID Content: 192.168.2.12	Local ID Content: 192.168.2.12
Secure Gateway Address: telecommuter1.com	Local IP Address: 192.168.2.12
Remote Address 192.168.2.12	
Headquarters Prestige Rule 2:	Telecommuter B (telecommuterb.dydns.org)
Peer ID Type: DNS	Local ID Type: DNS
Peer ID Content: telecommuterb.com	Local ID Content: telecommuterb.com
Secure Gateway Address: telecommuterb.com	Local IP Address: 192.168.3.2
Remote Address 192.168.3.2	
Headquarters Prestige Rule 3:	Telecommuter C (telecommuterc.dydns.org)
Peer ID Type: E-mail	Local ID Type: E-mail
Peer ID Content: myVPN@myplace.com	Local ID Content: myVPN@myplace.com
Secure Gateway Address: telecommuterc.com	Local IP Address: 192.168.4.15
Remote Address 192.168.4.15	

14.18VPN and Remote Management

If a VPN tunnel uses Telnet, FTP, WWW, SNMP, DNS or ICMP, then you should configure remote management (**REMOTE MGNT**) to allow access for that service.

Part V:

Remote Management and UPnP

This part contains Remote Management and UPnP

Chapter 15

Remote Management Configuration

This chapter provides information on configuring remote management

15.1 Remote Management Overview

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

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

15.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in one of the remote management screens.
3. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
6. There is a web remote management session running with a Telnet session. A web session will be disconnected if you begin a Telnet session; it will not begin if there already is a Telnet session.
7. There is a firewall rule that blocks it.

15.1.2 Remote Management and NAT

When NAT is enabled:

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

15.1.3 System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or telnet/web/FTP connections. Your Prestige automatically logs you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys_stdio` has been changed on the command line.

15.2 Telnet

You can configure your Prestige for remote Telnet access as shown next.

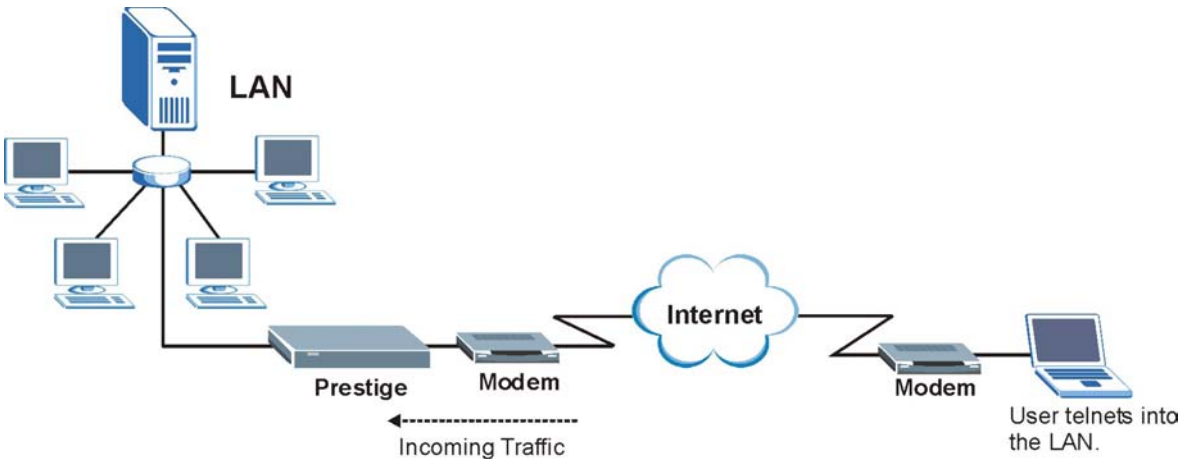


Figure 15-1 Telnet Configuration on a TCP/IP Network

15.3 FTP

You can upload and download Prestige firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

15.4 Web

You can use the Prestige's embedded web configurator for configuration and file management. See the online help for details.

15.5 Configuring Remote Management

Click **Remote Management** to open the following screen.

Remote Management Control

Server Type	Access Status	Port	Secured Client IP
Telnet	All	23	0.0.0.0
FTP	All	21	0.0.0.0
Web	All	80	0.0.0.0

Apply Cancel

Figure 15-2 Remote Management

The following table describes the labels in this screen.

Table 15-1 Remote Management

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

Chapter 16

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

16.1 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.

16.1.1 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.

16.1.2 NAT Transversal

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 Transversal and UPnP.

See the Network Address Translation (NAT) chapter in your User's Guide for further information about NAT.

16.1.3 Cautions with UPnP

The automated nature of NAT Transversal 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.

16.1.4 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.

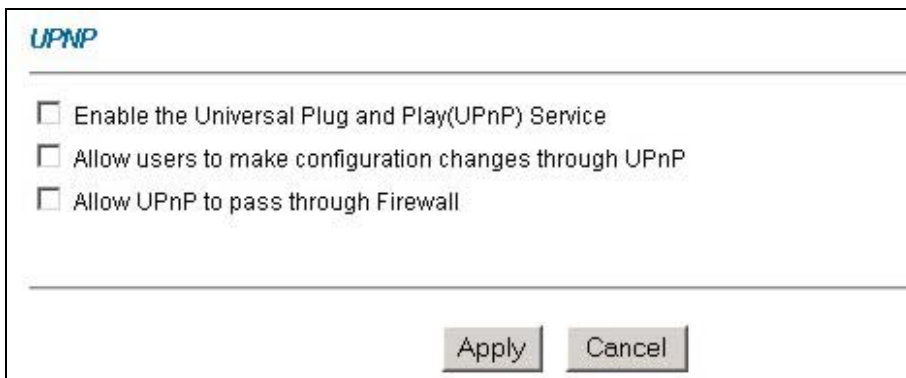
See later sections for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

16.2 Accessing the Prestige Web Configurator to Configure UPnP

- Step 1.** Make sure your Prestige hardware is properly connected (refer to instructions in *Chapter 2*).
- Step 2.** Prepare your computer/computer network to connect to the Internet (refer to the *Preparing Your Network* portion of the *Quick Start Guide*).
- Step 3.** Launch your web browser.
- Step 4.** Type "192.168.1.1" as the URL.
- Step 5.** Type "admin" as the user name and "1234" (default) as the password and click **OK**. The main menu screen displays.

16.2.1 Configuring UPnP

From the navigation panel in the main menu, click **UPnP** under **Advanced Setup** to display the screen shown next.



UPNP

☐ Enable the Universal Plug and Play(UPnP) Service

☐ Allow users to make configuration changes through UPnP

☐ Allow UPnP to pass through Firewall

Apply Cancel

Figure 16-1 Configuring UPnP**Table 16-1 Configuring UPnP**

FIELD	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Service	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 Transversal, 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 the setting to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

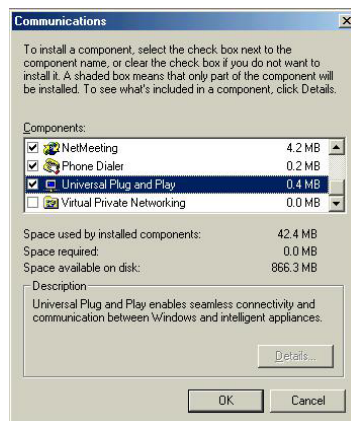
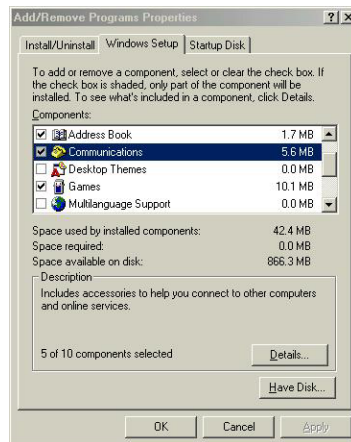
16.3 Installing UPnP in Windows Example

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

Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

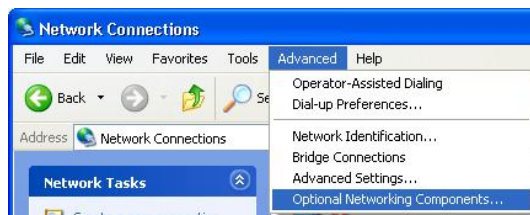
- Step 1.** Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- Step 2.** Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.
- Step 3.** In the **Communications** window, select the **Universal Plug and Play** 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.



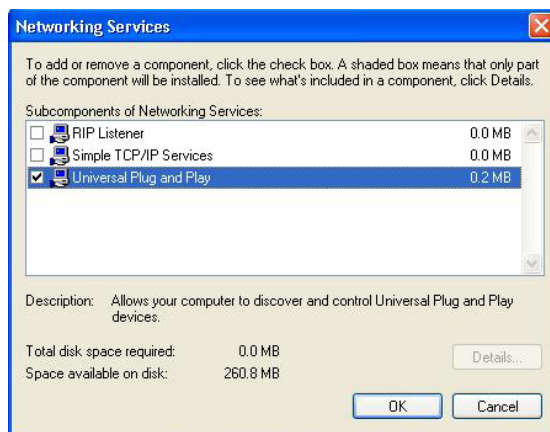
Installing UPnP in Windows XP

Follow the steps below to install the 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**.



- 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**.



16.4 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 Prestige.

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

Auto-discover Your UPnP-enabled Network Device

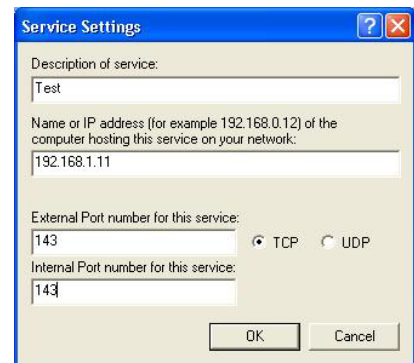
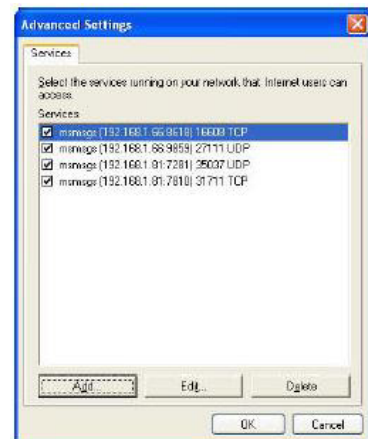
- Step 1.** Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- Step 2.** Right-click the icon and select **Properties**.



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

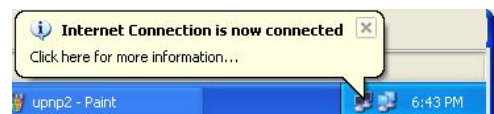


- Step 4.** You may edit or delete the port mappings or click **Add** to manually add port mappings.



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

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



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

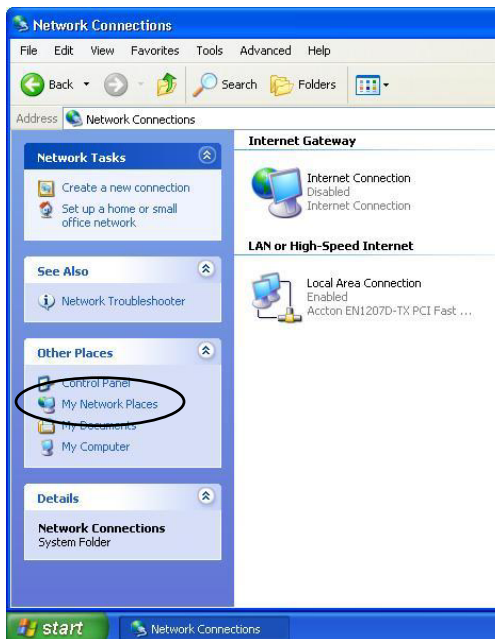


Web Configurator Easy Access Example

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

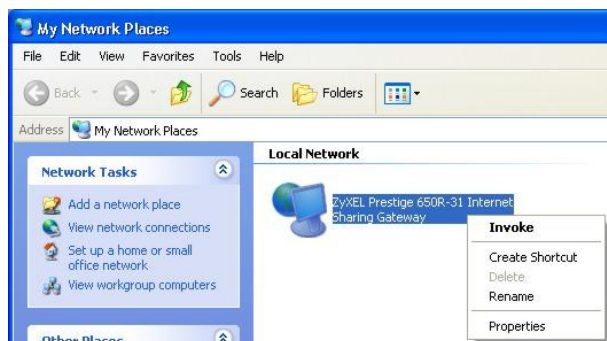
Follow the steps below to access the web configurator.

- 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 on the icon for your Prestige and select **Invoke**. The web configurator login screen displays.



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



Part VI:

Maintenance

This part covers the maintenance screens.

Chapter 17

Maintenance

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

17.1 Maintenance Overview

Use the maintenance screens to view system information, upload new firmware, manage configuration and restart your Prestige.

17.2 System Status Screen

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

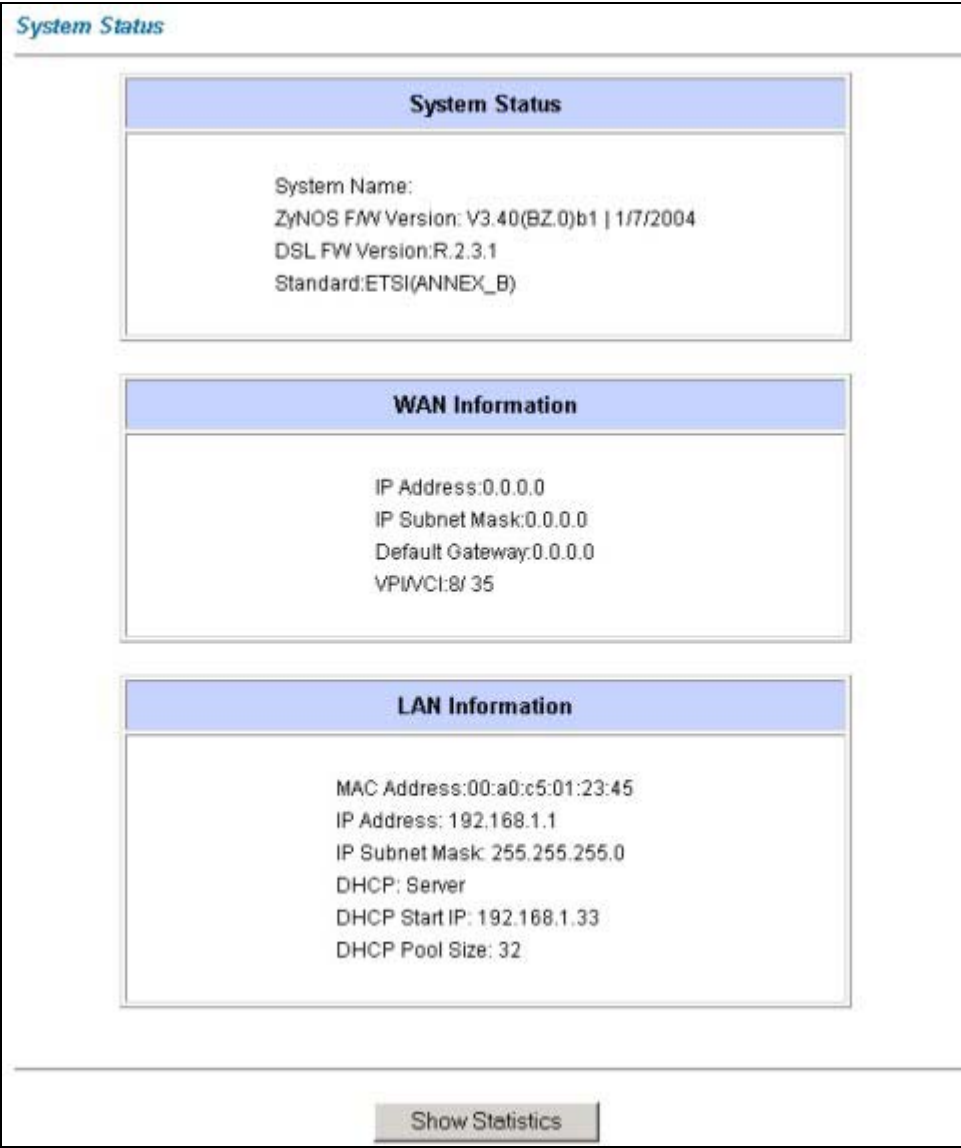


Figure 17-1 System Status

The following table describes the labels in this screen.

Table 17-1 System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your Prestige. It is for identification purposes.
ZyNOS F/W Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL FW Version	This is the DSL firmware version associated with your Prestige.
Standard	This is the standard that your Prestige is using.
WAN Information	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Prestige.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - Server , Relay or None .
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
Show Statistics	Click Show Statistics to see router performance statistics such as number of packets sent and number of packets received for each port.

17.2.1 System Statistics

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

System up Time: 217:56:15

WAN Port Statistics:

Link Status: Down

Transfer Rate: 0 kbps

Node-Link	Status	TxPkts	RxPkts	Errors	Tx B/s	Rx B/s	Up Time
1-1483	N/A	0	0	0	0	0	0:00:00

LAN Port Statistics:

Status	TxPkts	RxPkts	Collisions	CPU Load:
10M/Half Duplex	33929	7560	0	0.56%

Poll Interval(s) :

5

Set Interval

Stop

Figure 17-2 System Status: Show Statistics

The following table describes the labels in this screen.

Table 17-2 System Status: Show Statistics

LABEL	DESCRIPTION
System up Time	This is the elapsed time the system has been up.

Table 17-2 System Status: Show Statistics

LABEL	DESCRIPTION
WAN Port Statistics	This is the WAN port.
Link Status	This is the status of your WAN link.
Transfer Rate	This is the transfer rate in kbps.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
LAN Port Statistics	This is the LAN port.
Status	For the WAN port, 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. For a LAN port, this shows the port speed and duplex setting.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
CPU Load	This field specifies the percentage of CPU utilization.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval field above.
Stop	Click this button to halt the refreshing of the system statistics.

17.3 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.

DHCP Table

Host Name	IP Address	MAC Address
TWer-4	192.168.1.33	00-02-DD-32-91-6A
oemcomputer	192.168.1.35	00-A0-C5-41-A7-96

Figure 17-3 DHCP Table

The following table describes the labels in this screen.

Table 17-3 DHCP Table

LABEL	DESCRIPTION
Host Name	This is the name of the host computer.
IP Address	This field displays the IP address relative to the Host Name field.
MAC Address	<p>This field displays the MAC (Media Access Control) address of the computer with the displayed host name.</p> <p>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.</p>

17.4 Diagnostic Screens

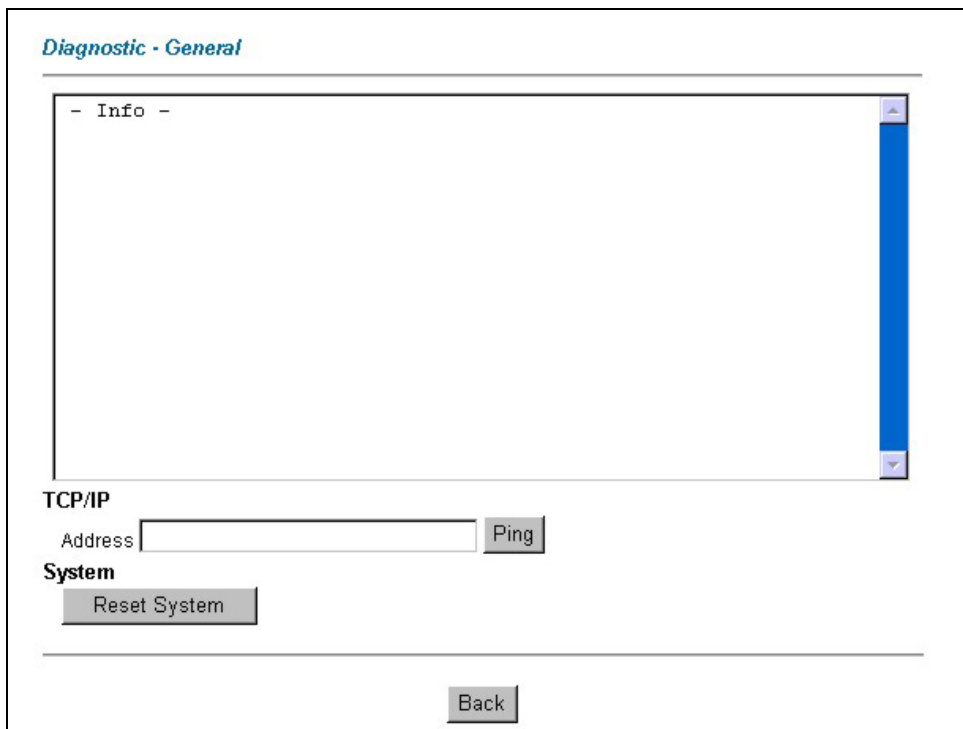
These read-only screens display information to help you identify problems with the Prestige.

Click **Diagnostic** to display the following screen.

**Figure 17-4 Diagnostic**

17.4.1 Diagnostic General Screen

Click **Diagnostic** and then **General** to open the screen shown next.

**Figure 17-5 Diagnostic General**

The following table describes the labels in this screen.

Table 17-4 Diagnostic General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.
Reset System	Click this button to reboot the Prestige. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click OK to proceed.
Back	Click this button to go back to the main Diagnostic screen.

17.4.2 Diagnostic DSL Line Screen

Click **Diagnostic** and then **DSL Line** to open the screen shown next.



Figure 17-6 Diagnostic DSL Line

The following table describes the labels in this screen.

Table 17-5 Diagnostic DSL Line

LABEL	DESCRIPTION
Reset xDSL Line	Click this button to reinitialize the xDSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset xDSL... Reset xDSL Line Successfully!"
Back	Click this button to go back to the main Diagnostic screen.

17.5 Firmware 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 in the parts that document the SMT for upgrading firmware using FTP/TFTP commands.

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

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

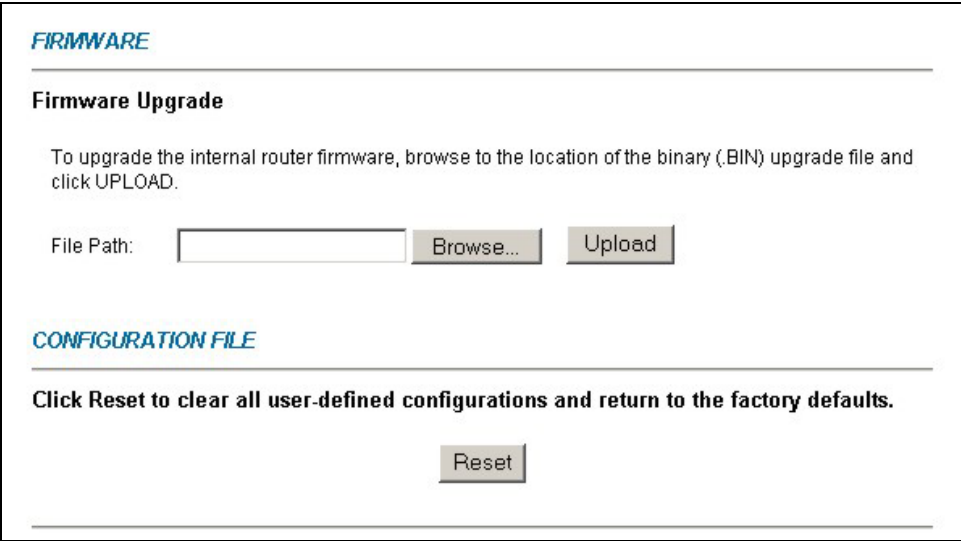


Figure 17-7 Firmware Upgrade

The following table describes the labels in this screen.

Table 17-6 Firmware Upgrade

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.
Reset	Click this button to clear all user-entered configuration information and return the Prestige to its factory defaults. Refer to the <i>Resetting the Prestige</i> section.

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.

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

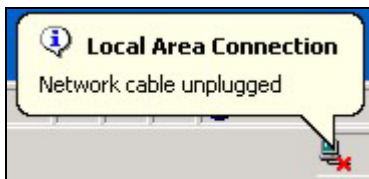


Figure 17-8 Network Temporarily Disconnected

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 **Back** to go back to the **Firmware** screen.

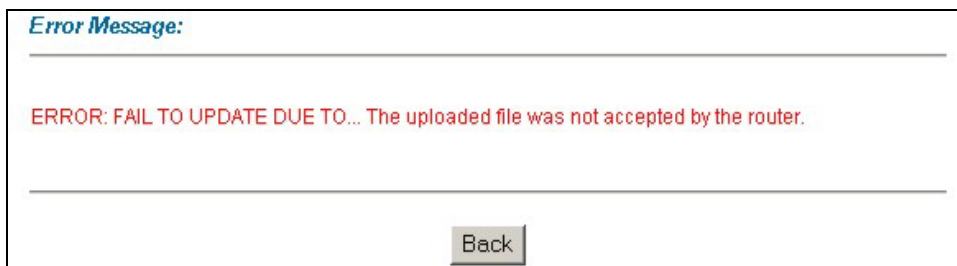


Figure 17-9 Error Message

Part VII:

SMT General Configuration

This part covers System Management Terminal configuration for general setup, LAN setup, wireless LAN setup, Internet access, remote nodes, remote node TCP/IP, static routing and NAT.

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

Chapter 18

Introducing the SMT

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

18.1 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.

18.1.1 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".

18.1.2 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.

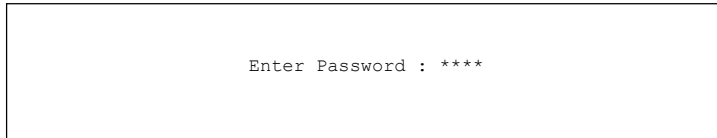
Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again.

18.1.3 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 18-1 Login Screen

18.1.4 Prestige SMT Menu Overview

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

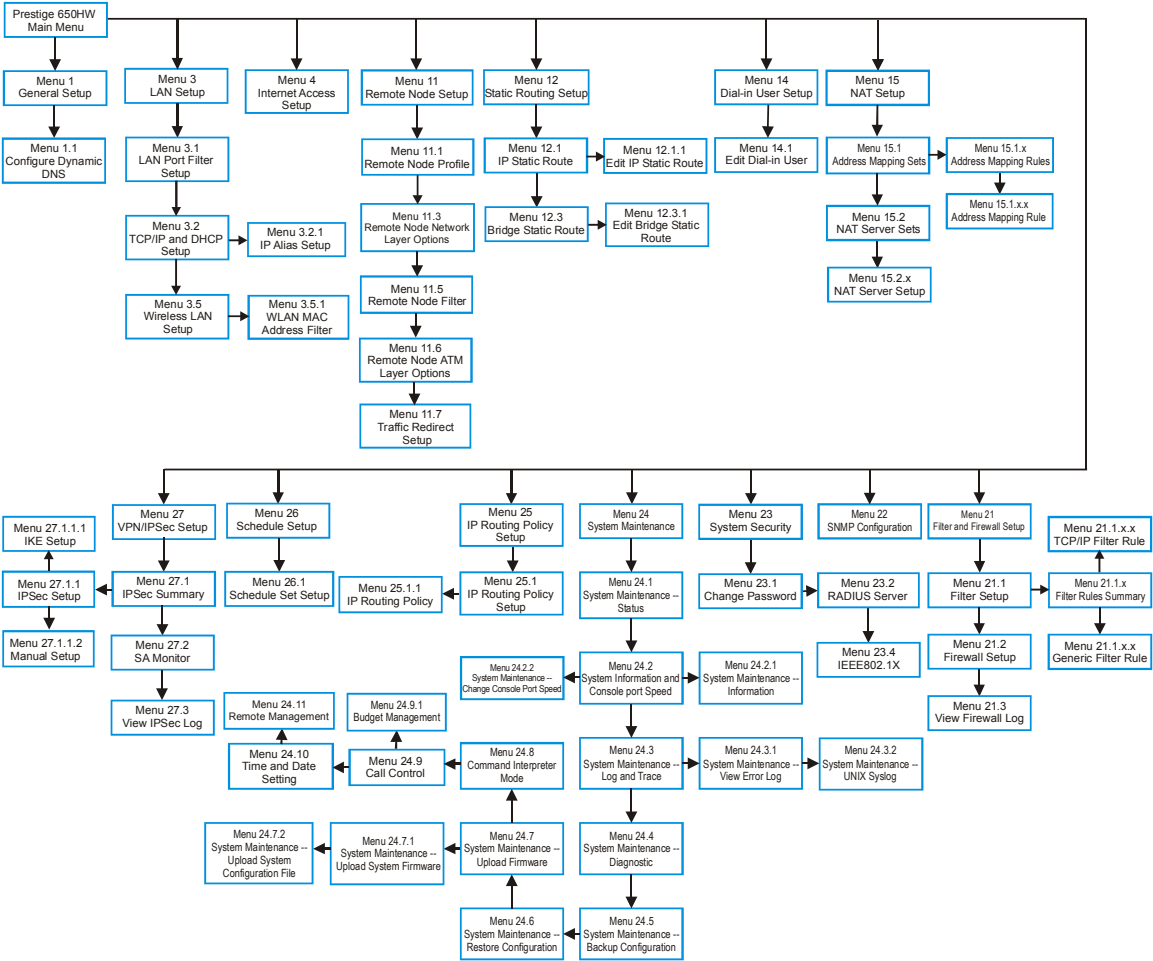


Figure 18-2 Prestige Menu Overview

18.2 Navigating the SMT Interface

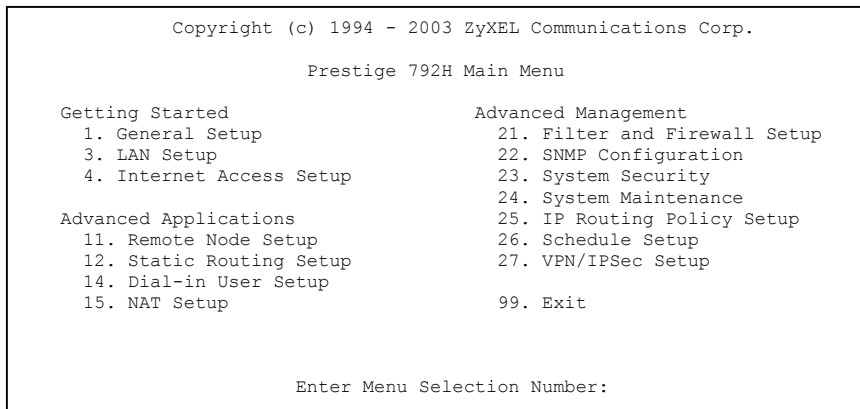
The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

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

Table 18-1 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 , then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? > or ChangeMe	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with ChangeMe must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

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

**Figure 18-3 SMT Main Menu**

18.2.1 System Management Terminal Interface Summary

Table 18-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
3	LAN Setup	Use this menu to set up your wireless LAN (Prestige 650H/HW only) and LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
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	Configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	Use this menu to configure your IP routing policy.

Table 18-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN/IPSec Setup	Use this menu to configure VPN connections on the Prestige 650H/HW.
99	Exit	Use this to exit from SMT and return to a blank screen.

18.3 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**.
- Step 2.** Enter 1 to display **Menu 23.1 - System Security - Change Password** as shown next.
- Step 3.** Type your existing system password in the **Old Password** field, for example “1234”, and press [ENTER].

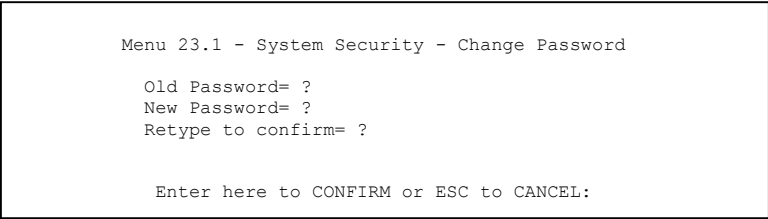


Figure 18-4 Menu 23 System Password

- 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 19

General Setup

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

19.1 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.

19.2 Configuring Menu 1

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

```
Menu 1 - General Setup

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

Route IP= Yes
Bridge= No

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

Figure 19-1 Menu 1 General Setup

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

Table 19-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
System Name	Enter a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.	JohnDoe
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway. If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.	zyxel.com.tw
Edit Dynamic DNS	Press the [SPACE BAR] to select Yes or No (default). Select Yes to configure Menu 1.1 — Configure Dynamic DNS (discussed next).	No
Route IP	Set this field to Yes to enable or No to disable IP routing. You must enable IP routing for Internet access.	Yes
Bridge	Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous Route IP field. Select Yes to turn bridging on; select No to turn bridging off.	No

19.2.1 Configuring Dynamic DNS

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

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

```

Menu 1.1 - Configure Dynamic DNS

Service Provider = WWW.DynDNS.ORG
Active= Yes
Host= me.ddns.org
EMAIL= mail@mailserver
USER= username
Password= *****
Enable Wildcard= No

Press ENTER to confirm or ESC to cancel:

```

Figure 19-2 Menu 1.1 Configure Dynamic DNS

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

Table 19-2 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
Host	Enter the domain name assigned to your Prestige by your Dynamic DNS provider.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
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
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 20

WAN Setup

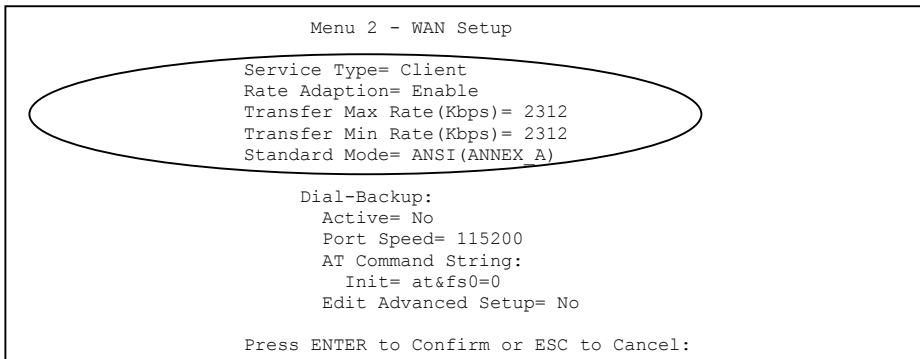
This chapter shows you how to configure the WAN settings of your Prestige.

20.1 WAN Setup

Use **Menu 2 – WAN Setup** to configure G.SHDSL settings for your WAN line. Different telephone companies deploy different types of G.SHDSL service. If you are unsure of any of this information, please check with your telephone company.

20.2 WAN Setup Screen

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



```
Menu 2 - WAN Setup

Service Type= Client
Rate Adaption= Enable
Transfer Max Rate(Kbps)= 2312
Transfer Min Rate(Kbps)= 2312
Standard Mode= ANSI (ANNEX A)

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

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

Figure 20-1 WAN Setup

Table 20-1 WAN Setup

FIELD	DESCRIPTION
Service Type	Press [SPACE BAR] to select Server (COE) or Client (CPE).
Rate Adaption	Press [SPACE BAR] to select Enable (activate) or Disable (deactivate).
Transfer Max Rate (2312 Kbps)	Press [SPACE BAR] to select a Transfer Max Rate greater than or equal to the Transfer Min Rate and press [ENTER] to continue.
Transfer Min Rate (2312 Kbps)	Press [SPACE BAR] to select a Transfer Min Rate less than or equal to the Transfer Max Rate and press [ENTER] to continue.
Standard Mode	Press [SPACE BAR] to select ANSI (ANNEX A) or ETSI (ANNEX B) and press [ENTER] to continue. The Client side must match the Server side.

Chapter 21

Dial Backup

This chapter shows you how to configure Dial Backup for your Prestige.

21.1 Dial Backup Overview

To set up the auxiliary port (Dial Backup or CON/AUX) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the *Quick Start Guide* for the *Hardware Installation* chapter), then configure:

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

21.1.1 Configuring Dial Backup in Menu 2

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

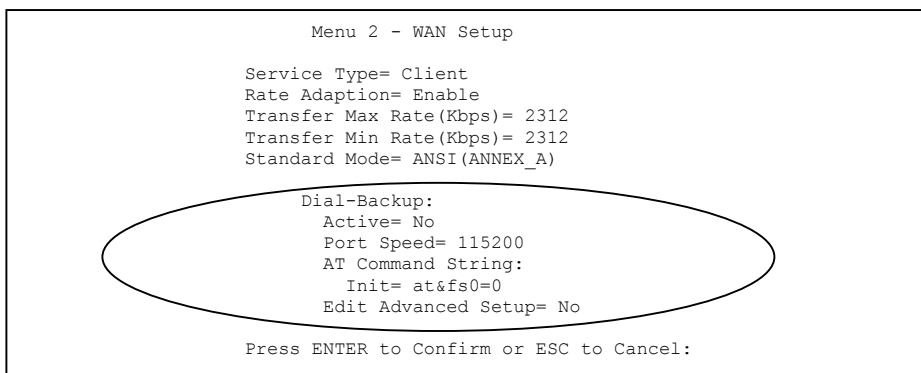


Figure 21-1 Menu 2: Dial Backup Setup

Table 21-1 Menu 2: Dial Backup Setup

FIELD	DESCRIPTION	EXAMPLE
Dial-Backup:		
Active	Use this field to turn the dial-backup feature on (Yes) or off (No).	No
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.	115200
AT Command String:		
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.	at&fs0=0
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select Yes and then press [ENTER] to go to Menu 2.1: Advanced Setup .	Yes
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.		

21.1.2 Advanced WAN Setup

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

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

Menu 2.1 - Advanced WAN Setup

AT Command Strings:

Dial= atdt

Drop= ~++~ath

Answer= ata

Drop DTR When Hang Up= Yes

AT Response Strings:

CLID= NMBR =

Called Id=

Speed= CONNECT

Call Control:

Dial Timeout(sec)= 60

Retry Count= 0

Retry Interval(sec)= N/A

Drop Timeout(sec)= 20

Call Back Delay(sec)= 15

Press ENTER to Confirm or ESC to Cancel:

Figure 21-2 Advanced WAN Setup

Table 21-2 Advanced WAN Port Setup: AT Commands Fields

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

Table 21-2 Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION	DEFAULT
Speed	Enter the keyword preceding the connection speed.	CONNECT

Table 21-3 Advanced WAN Port Setup: Call Control Parameters

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

21.2 Remote Node Profile (Backup ISP)

Enter **12** in **Menu 11 Remote Node Setup** to open **Menu 11.1 Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection.


```

Menu 11.1 - Remote Node Profile (Backup ISP)

Rem Node Name= ?           Edit PPP Options= No
Active= Yes                Rem IP Addr= 0.0.0.0
                             Edit IP= No

Outgoing:
  My Login=
  My Password= *****
  Authen= CHAP/PAP
  Pri Phone #= ?
  Sec Phone #=

Telco Option:
  Allocated Budget(min)= 0
  Period(hr)= 0
  Nailed-Up Connection= No

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

Press ENTER to Confirm or ESC to Cancel:

```

Figure 21-3 Remote Node Profile (Backup ISP)**Table 21-4 Remote Node Profile (Backup ISP)**

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select Yes to enable the remote node or No to disable the remote node.	Yes
Outgoing		
My Login	Enter the login name assigned by your ISP for this remote node.	jim
My Password	Enter the password assigned by your ISP for this remote node.	*****
Authen	<p>This field sets the authentication protocol used for outgoing calls.</p> <p>Options for this field are:</p> <p>CHAP/PAP - Your Prestige will accept either CHAP or PAP when requested by this remote node.</p> <p>CHAP - accept CHAP only.</p> <p>PAP - accept PAP only.</p>	CHAP/PAP

Table 21-4 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Pri Phone # Sec Phone #	Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your Prestige dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.	
Edit PPP Options	Move the cursor to this field and use the space bar to select [Yes] and press [Enter] to edit the PPP options for this remote node. This brings you to Menu 11.2 - Remote Node PPP Options (see <i>section 21.2.1</i>).	No (default)
Rem IP Addr	Leave the field set to 0.0.0.0 (default) if the remote gateway has a dynamic IP address. Enter the remote gateway's IP address here if it is static.	0.0.0.0 (default)
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select Yes and press [ENTER] to go to Menu 11.3 - Remote Node Network Layer Options . See <i>section 21.2.2</i> for more information.	No (default)
Telco Option		
Allocated Budget	Enter the maximum number of minutes that this remote node may be called within the time period configured in the Period field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node.	0 (default)
Period (hr)	Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the Allocated Budget to 10 (minutes) and the Period to 1 (hour).	0 (default)
Nailed-Up Connection	Press [SPACE BAR] to select Yes to set this connection to always be on, regardless of whether or not there is any traffic. Select No to have this connection act as a dial-up connection.	No (default)
Session Options		
Edit Filter sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select Yes and press [ENTER] to open menu 11.5 to edit the filter sets.	No (default)
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the Prestige to the remote node) that can elapse before the Prestige automatically disconnects the PPP connection. This option only applies when the Prestige initiates the call.	100 seconds (default)

Table 21-4 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
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.		

21.2.1 Editing PPP Options

The Prestige's dial back-up feature uses PPP. To edit the remote node PPP Options, move the cursor to the **Edit PPP Options** field in **Menu 11.1 - Remote Node Profile**, and use the space bar to select **Yes**. Press [Enter] to open menu 11.2 as shown next.

```
Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No
Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figure 21-4 Menu 11.2 - Remote Node PPP Options

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

Figure 21-5 Remote Node PPP Options Menu Fields

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

21.2.2 Editing TCP/IP Options

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

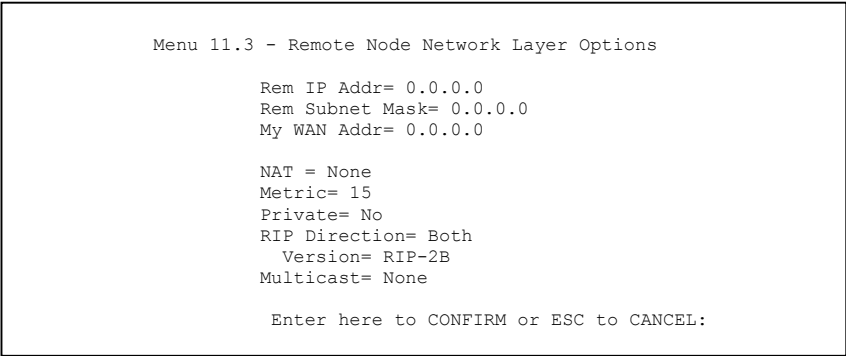


Figure 21-6 Remote Node Network Layer Options

Table 21-5 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
Rem IP Address	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Enter the remote gateway’s IP address here if you know it (static).	0.0.0.0 (default)
Rem IP Subnet Mask	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Enter the remote gateway’s subnet mask here if you know it (static).	0.0.0.0 (default)
My WAN Addr	Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static). This is the address assigned to your local Prestige, not the remote router.	0.0.0.0 (default)
NAT	Press [SPACE BAR] and then [ENTER] to select either Full Feature , None or SUA Only . See the Network Address Translation (NAT) chapter for a full discussion on this feature.	None (default)
Metric	Enter a number from 1 to 15 to set this route’s priority among the Prestige’s routes. The smaller the number, the higher priority the route has.	15 (default)

Table 21-5 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
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 not included in RIP broadcasts. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.	No (default)
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from Both/ None/In Only/Out Only and None .	Both (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from RIP-1/RIP-2B/RIP-2M .	RIP-1
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (IGMP-v1) and version 2 (IGMP-v2). Press the [SPACE BAR] to enable IP Multicasting or select None to disable it. See the LAN Setup chapter for more information on this feature.	None (default)
Once you have completed filling in Menu 11.3 Remote Node Network Layer Options , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

21.2.3 Editing Filter Sets

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 four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to the Filters chapter for more information on defining the filters.

```
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 21-7 Menu 11.5: Remote Node Filter (Ethernet)

Chapter 22

LAN Setup

This chapter shows you how to configure the LAN settings for your Prestige.

22.1 Ethernet Setup

This section describes how to configure the Ethernet using **Menu 3 – Ethernet Setup**. From the main menu, enter 3 to open the menu as follows.

```
Menu 3 - Ethernet Setup

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

Enter Menu Selection Number:
```

Figure 22-1 TCP/IP Ethernet Setup

22.1.1 LAN Port Filter Setup

In this menu type 1 to open **Menu 3.1- LAN Port Filter Setup**. Use this menu to specify filter set(s) that you want to apply to Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful for blocking certain packets, reducing traffic and preventing 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 22-2 LAN Port Filter Setup

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

22.1.2 IP Alias Setup

Use **Menu 3.2** to configure the first network. To edit **Menu 3.2**, enter 3 from the main menu to display **Menu 3 — Ethernet Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup** shown next. Move the cursor to **Edit IP Alias** field and press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

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

DHCP Setup:
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
  Version= N/A
  Multicast= None
  IP Policies=
  Edit IP Alias= No

Press ENTER to confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 22-3 TCP/IP and DHCP Setup

Pressing [ENTER] displays **Menu 3.2.1 — IP Alias Setup**, as shown next.

```
Menu 3.2.1 - IP Alias Setup

IP Alias 1= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
  Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A
IP Alias 2= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
  Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A
Enter here to CONFIRM or ESC to CANCEL:
```


Figure 22-4 IP Alias Setup

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

Table 22-1 IP Alias Setup

FIELD	DESCRIPTION	EXAMPLE
IP Alias	Choose Yes to configure the LAN network for the Prestige.	Yes
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.2.1
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] to select the RIP direction. Choices are None , Both , In Only or Out Only .	None
Version	Press [SPACE BAR] to select the RIP version. Choices 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.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

22.1.3 Route IP Setup

You must enable IP routing for Internet access. You can enable IP routing in **Menu 1 — General Setup**.

To edit menu 1, type in 1 in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR].

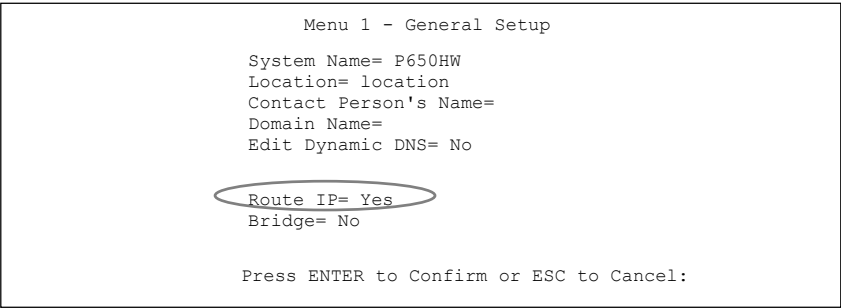


Figure 22-5 General Setup

22.1.4 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 — Ethernet Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup** as shown next:

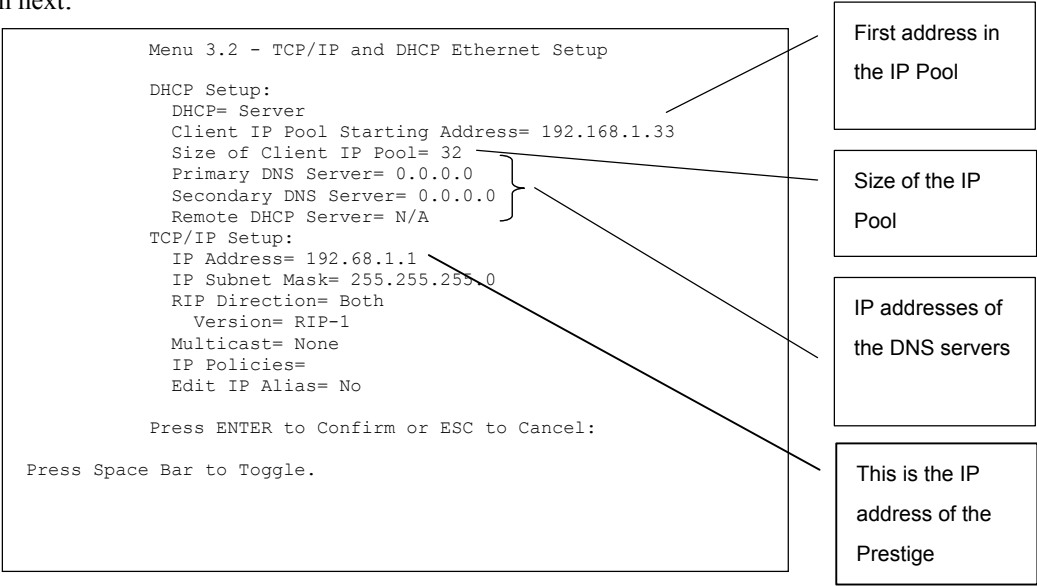


Figure 22-6 TCP/IP and DHCP Ethernet Setup

Table 22-2 TCP/IP and DHCP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
DHCP Setup		
DHCP	<p>If set to Server, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to None, the DHCP server will be disabled. If set to Relay, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case.</p> <p>When DHCP is used, the following items need to be set:</p>	Server (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size or count of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Remote DHCP Server	If Relay is selected in the DHCP field above then enter the IP address of the actual remote DHCP server here.	
TCP/IP Setup		
IP Address	Enter the (LAN) 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] to select the RIP direction. Choices are Both , In Only , Out Only or None .	Both (default)
Version	Press [SPACE BAR] to select the RIP version. Choices are RIP-1 , RIP-2B or RIP-2M .	RIP-1 (default)

Table 22-2 TCP/IP and DHCP Ethernet Setup

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 the [SPACE BAR] to enable IP Multicasting or select None to disable it.	None (default)
IP Policies	Create policies using SMT menu 25 (see the <i>IP Policy Routing chapter</i>) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.	2,4,7,9
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 change No to Yes and press [ENTER] to for menu 3.2.1	No (default)

Chapter 23

Internet Access

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

23.1 Internet Access Overview

This section provides information on configuring your Prestige for Internet access. It includes information on encapsulation types, IP address assignment and ATM networks.

23.2 Internet Access Setup

Menu 4 allows you to enter the Internet Access information in one screen. **Menu 4** is actually a simplified setup for one of the remote nodes that you can access in **Menu 11**.

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

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
    Peak Cell Rate (PCR)= 0
    Sustain Cell Rate (SCR)= 0
    Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Dynamic
    IP Address= N/A
Network Address Translation= SUA Only
    Address Mapping Set= N/A

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

Figure 23-1 Internet Access Setup

Table 23-1 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
ISP's Name	Enter the name of your Internet Service Provider. This information is for identification purposes only.	ChangeMe
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are PPPoE , PPPoA , RFC 1483 or ENET ENCAP .	ENET ENCAP
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are VC-based or LLC-based .	LLC-based
VPI #	Enter the Virtual Path Identifier (VPI) that the telephone company gives you.	8
VCI #	Enter the Virtual Channel Identifier (VCI) that the telephone company gives you.	35
ATM QoS Type	Press [SPACE BAR] and select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.	UBR
Peak Cell Rate (PCR)	This is the maximum rate at which the sender can send cells. Type the PCR.	0
Sustain Cell Rate (SCR)= 0	Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. Type the SCR; it must be less than the PCR, unless both are set to zero.	0
Maximum Burst Size (MBS)= 0	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535.	0
My Login	Configure the My Login and My Password fields for PPPoA and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation, then this field must be of the form user@domain where domain identifies your PPPoE service name.	N/A
My Password	Enter the password associated with the login name above.	N/A
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP when you are using ENET ENCAP encapsulation.	N/A

Table 23-1 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
Idle Timeout	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.	0
IP Address Assignment	Press [SPACE BAR] to select Static or Dynamic address assignment.	Dynamic
IP Address	Enter the IP address supplied by your ISP if applicable.	N/A
Network Address Translation	Press [SPACE BAR] to select None , SUA Only or Full Feature . Please see the <i>NAT Chapter</i> for more details on the SUA (Single User Account) feature.	SUA Only
Address Mapping Set	Type the numbers of mapping sets (1-8) to use with NAT. See the <i>NAT</i> chapter for details.	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.		

If all your settings are correct your Prestige automatically connects to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

Part VIII:

Advanced Applications

This part shows how to configure Remote Nodes, Static Routes, Bridging and NAT.

Chapter 24

Remote Node Configuration

This chapter covers remote node configuration.

24.1 Remote Node Overview

This section describes the protocol-independent parameters for a remote node. A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use Menu 4 to set up Internet access, you are configuring one of the remote nodes.

You first choose a remote node in **Menu 11- Remote Node Setup**. You can then edit that node's profile in menu 11.1, as well as configure specific settings in three submenus: edit IP and bridge options in menu 11.3; edit ATM options in menu 11.6; and edit filter sets in menu 11.5.

24.2 Remote Node Setup

To configure a remote node, follow these steps:

- Step 1.** From the Main Menu, select menu option **11 Remote Node Setup**.
- Step 2.** When Menu 11 appears as shown in the following figure, type the number of the remote node that you want to configure.

Menu 11 - Remote Node Setup

1. MyISP (ISP, SUA)

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

11. _____

12. _____

Enter Node # to Edit:

Figure 24-1 Remote Node Setup

24.2.1 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. For LAN-to-LAN applications, for example, between a branch office and corporate headquarters, prior agreement on methods is necessary because encapsulation and multiplexing cannot be automatically determined. What method(s) you use depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

Scenario 1. One VC, Multiple Protocols

PPPoA (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

Scenario 2. One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPPoA** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

Scenario 3. Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select **RFC-1483** encapsulation and **VC-based** multiplexing.

Menu 11.1 - Remote Node Profile

Rem Node Name= myISP

Active= Yes

Encapsulation= RFC-1483

Multiplexing= VC-based

Incoming:

Rem Login= N/A

Rem Password= N/A

Outgoing:

My Login= N/A

My Password= N/A

Authen= N/A

Route= IP

Bridge= No

Edit IP/Bridge= No

Edit ATM Options= No

Telco Option:

Allocated Budget(min)= N/A

Period(hr)= N/A

Schedule Sets= N/A

Nailed-Up Connection= N/A

Session Options:

Edit Filter Sets= No

Idle Timeout(sec)= N/A

DELETE PROFILE:

Press Space Bar to Toggle.

Edit IP/Bridge Options in menu 11.3.

Edit ATM Options in menu 11.6.

Edit Filter Sets in menu 11.5.

Figure 24-2 Remote Node Profile

Table 24-1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.	myISP
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate or No to deactivate this node. Inactive nodes are displayed with a minus sign “-“ in SMT menu 11.	Yes
Encapsulation	PPPoA refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5). PPPoE refers to RFC 2516 (PPP Encapsulation over Ethernet). If RFC-1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5) or ENET ENCAP are selected, then the Rem Login , Rem Password , My Login , My Password and Authen fields are not applicable (N/A).	ENET ENCAP
Multiplexing	Press [SPACE BAR] and then [ENTER] to select the method of multiplexing that your ISP uses, either VC-based or LLC-based .	LLC-based
Service Name	When using PPPoE encapsulation, type the name of your PPPoE service here.	N/A
Incoming: <div>Rem Login</div>	Type the login name that this remote node will use to call your Prestige. The login name and the Rem Password will be used to authenticate this node.	

Table 24-1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Password	Type the password used when this remote node calls your Prestige.	
Outgoing: My Login	Type the login name assigned by your ISP when the Prestige calls this remote node.	
My Password	Type the password assigned by your ISP when the Prestige calls this remote node.	
Authen	<p>This field sets the authentication protocol used for outgoing calls. Options for this field are:</p> <p>CHAP/PAP – Your Prestige will accept either CHAP or PAP when requested by this remote node.</p> <p>CHAP – accept CHAP (Challenge Handshake Authentication Protocol) only.</p> <p>PAP – accept PAP (Password Authentication Protocol) only.</p>	CHAP
Route	This field determines the protocol used in routing. Options are IP and None .	IP
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select Yes to enable and No to disable.	No
Edit IP/Bridge	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 11.3 – Remote Node Network Layer Options .	No
Edit ATM Options	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 11.6 – Remote Node ATM Layer Options .	No
Telco Option Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	10
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).	1

Table 24-1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Schedule Sets	This field is only applicable for PPPoE and PPPoA encapsulation. You can apply up to four schedule sets here. For more details please refer to the <i>Call Schedule Setup</i> chapter.	
Nailed up Connection	This field is only applicable for PPPoE and PPPoA encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options Edit Filter Sets	Use [SPACE BAR] to choose Yes and press [ENTER] to open menu 11.5 to edit the filter sets. See the <i>Remote Node Filter</i> section for more details.	No (default)
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout.	
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.		

24.3 Remote Node Network Layer Options

Perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

Step 1. In menu 11.1, make sure **IP** is among the protocols in the **Route** field.

Step 2. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes**, then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.

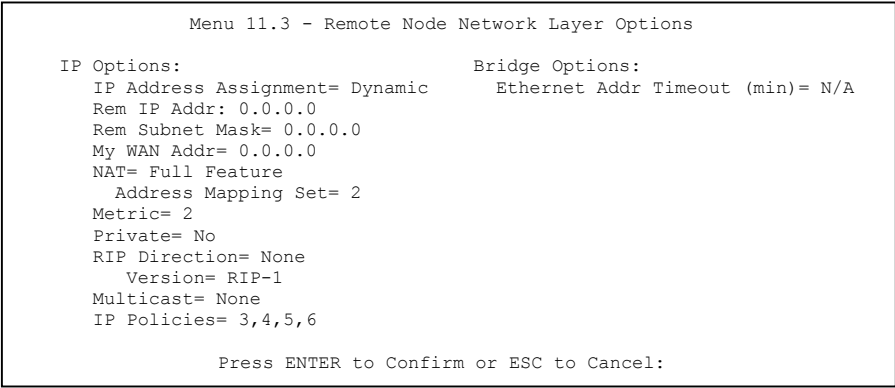


Figure 24-3 Remote Node Network Layer Options

Table 24-2 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
IP Options		
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select Dynamic if the remote node is using a dynamically assigned IP address or Static if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in Menu 4). All other nodes are set to Static .	Dynamic
Rem IP Addr	This is the IP address you entered in the previous menu.	
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. This address refers to the local Prestige address, not the remote router address.	

Table 24-2 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
NAT	<p>Press [SPACE BAR] and then [ENTER] to select Full Feature if you have multiple public WAN IP addresses for your Prestige.</p> <p>Select SUA Only if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (menu 15.1 - see section 27.3.1).</p> <p>Select None to disable NAT.</p>	SUA Only
Address Mapping Set	<p>When Full Feature is selected in the NAT field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see the <i>NAT</i> chapter for details) and type that number here.</p> <p>When SUA Only is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see the <i>NAT</i> chapter for details).</p>	2
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the cost measurement, 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.	2
Private	This 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. 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
Multicast	IGMP-v1 sets IGMP to version 1, IGMP-v2 sets IGMP to version 2 and None disables IGMP.	None
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see the <i>IP Policy Routing</i> chapter) and then apply them here.	3, 4, 5, 6
Bridge Options		
Ethernet Addr Timeout (min)	See the chapter on Bridging Setup for information on bridging.	
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.		

24.3.1 My WAN Addr Sample IP Addresses

The following diagram explains the sample IP addresses to help you understand the field of **My Wan Addr** in Menu 11.3. **My WAN Addr** indicates the local Prestige WAN IP while **Rem IP Addr** indicates the peer WAN IP.

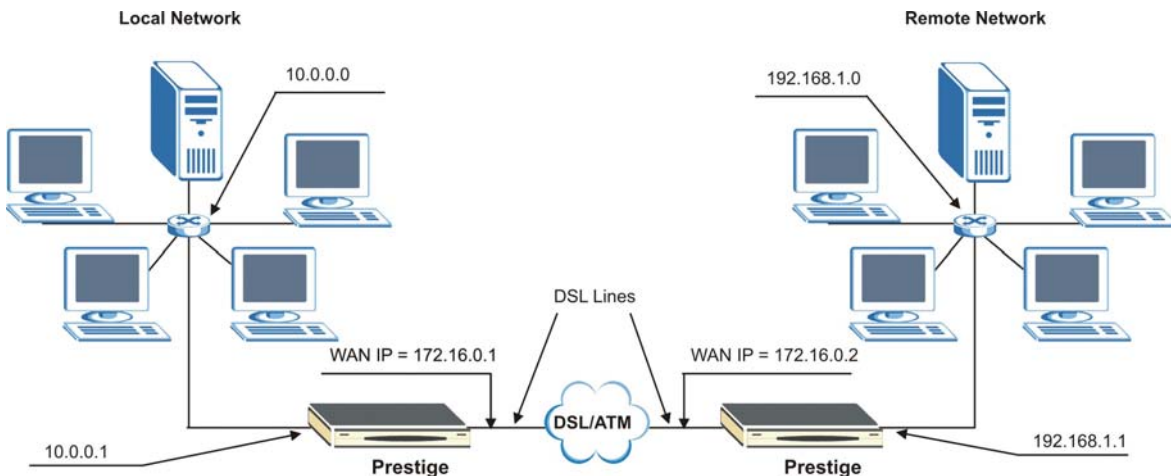


Figure 24-4 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

24.4 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. The Prestige has prepackaged filter sets; refer to the chapter on Filter Configuration for details. Include these in the call filter sets if you want to prevent NetBIOS packets from triggering calls to a remote node.

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters= 12, 11
  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 24-5 Remote Node Filter (PPPoA or PPPoE Encapsulation)

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters= 12, 11
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

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

Figure 24-6 Remote Node Filter (RFC1483 or ENET ENCAP Encapsulation)

24.5 Editing ATM Layer Options

Follow these steps to edit **Menu 11.6 – Remote Node ATM Layer Options**.

Step 1. In Menu 11.1, move the cursor to the **Edit ATM Options** then press [SPACE BAR] to toggle and set the value to **Yes**.

Step 2. Press [ENTER] to open **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of Menu 11.6 for the Prestige, depending on whether you chose **VC-based** or **LLC-based** multiplexing and **PPP** (either PPPoA or PPPoE) encapsulation in menu 11.1.

24.5.1 VC-based Multiplexing (non-PPP Encapsulation)

For **VC-based** multiplexing, by prior agreement, a protocol is assigned a specific virtual circuit, e.g., VC1 will carry IP, VC2 will carry IPX, etc. Separate VPI and VCI numbers must be specified for each protocol.

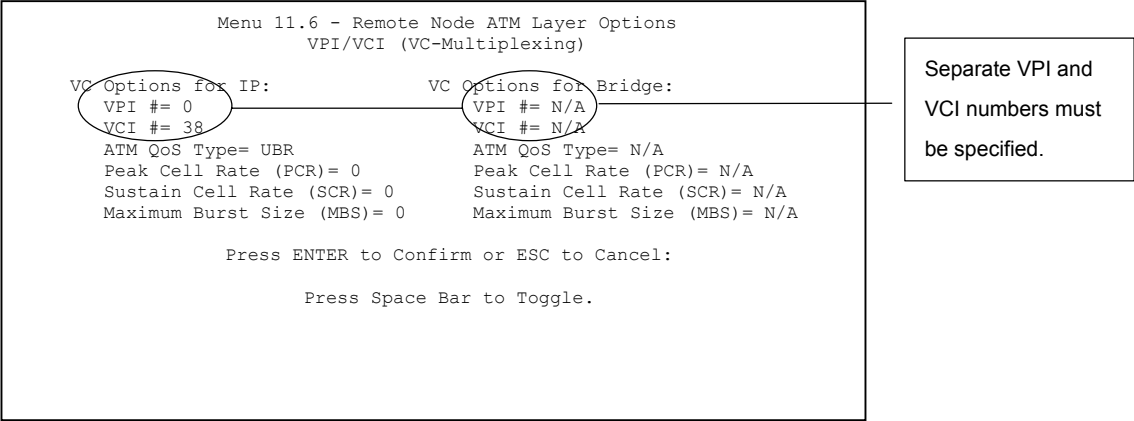


Figure 24-7 Menu 11.6 for VC-based Multiplexing (non-PPP Encapsulation)

24.5.2 LLC-based Multiplexing or PPP Encapsulation

For **LLC-based** multiplexing or **PPP** encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header.

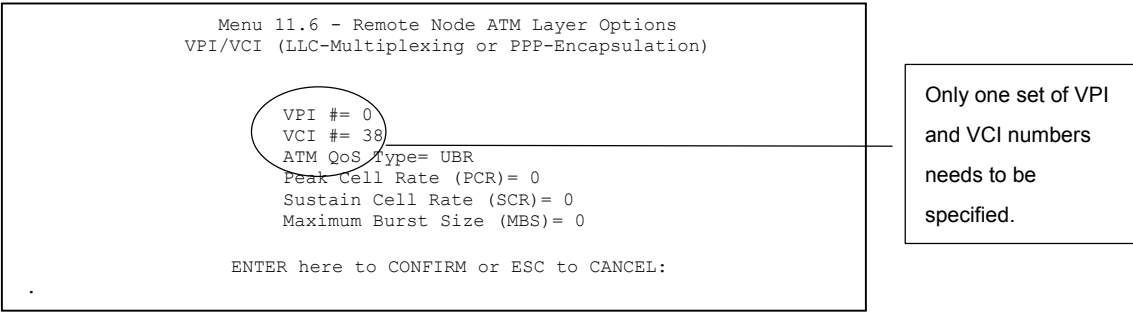


Figure 24-8 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

In this case, only one set of VPI and VCI numbers need be specified for all protocols. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

Chapter 25

Static Route Setup

This chapter shows how to setup IP static routes.

25.1 Static Route Overview

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

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

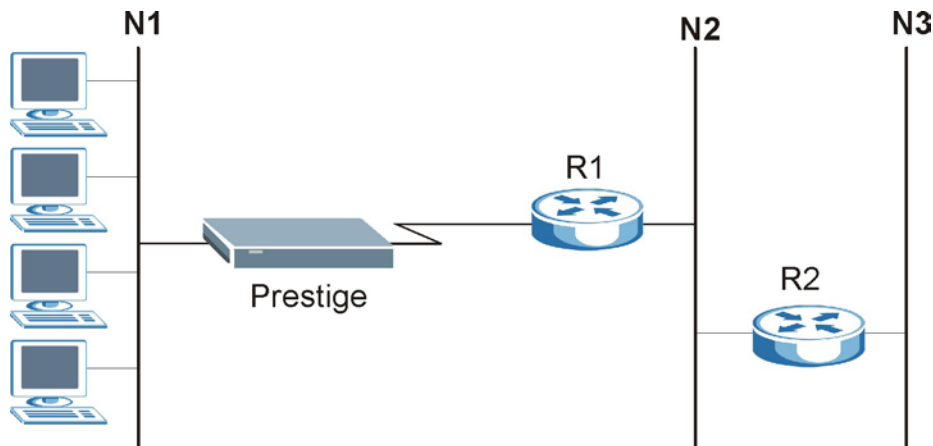


Figure 25-1 Sample Static Routing Topology Configuration

Step 1. To configure an IP static route, use **Menu 12 – Static Route Setup** (shown next). See the bridging chapter for more information on Bridge Static Routes.

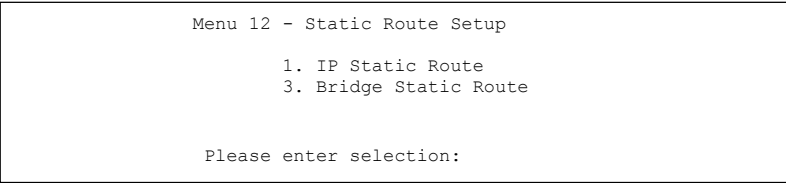


Figure 25-2 Static Route Setup

Step 2. From Menu 12, select **1** to open **Menu 12.1 – IP Static Route Setup**, as shown next.

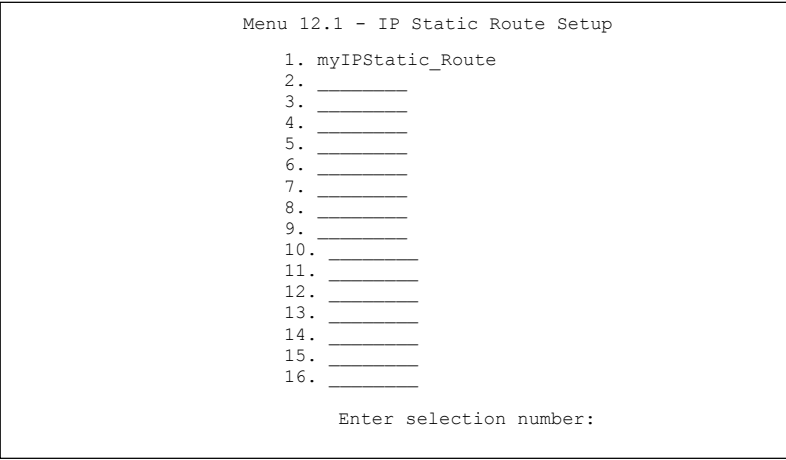


Figure 25-3 IP Static Route Setup

Now, type the index number of one of the static routes you want to configure.


```
Menu 12.1.1 - Edit IP Static Route

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

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

Figure 25-4 Edit IP Static Route

Table 25-1 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 <i>IP Subnet Mask</i> in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and is not included in RIP broadcasts. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 26

Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

26.1 Bridging Overview

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, for example, SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol, and it also demands more CPU cycles and memory.

For efficiency reasons, do *not* turn on bridging unless you need to support protocols other than IP on your network. For IP, enable the routing if you need it; do not bridge what the Prestige can route.

26.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN. Your Prestige does not support IPX.

26.2.1 Remote Node Bridging Setup

Follow the procedure in another section to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related parameters, you need to configure **Menu 11.3 – Remote Node Network Layer Options**.

To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:

- Step 1.** In menu 11.1, make sure the **Bridge** field is set to **Yes**.
- Step 2.** Move the cursor to the **Edit IP/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

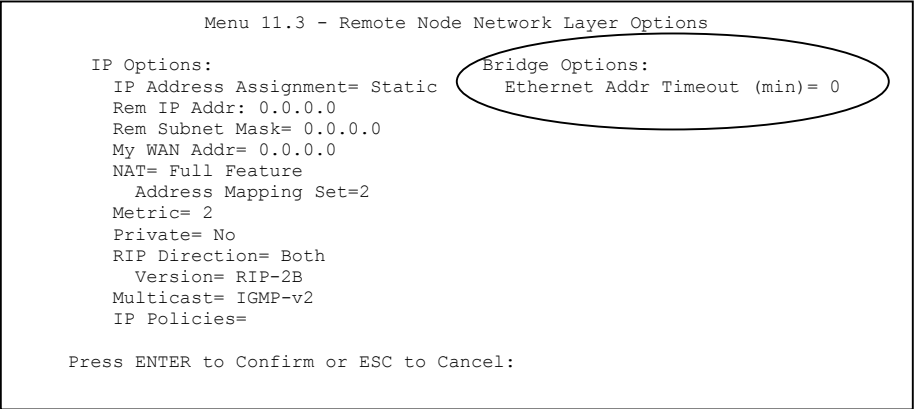


Figure 26-1 Remote Node Bridging Options

Table 26-1 Remote Node Bridging Options

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to Yes .
Edit IP/Bridge (menu 11.1)	Press [SPACE BAR] to select Yes and press [ENTER] to display menu 11.3.
Ethernet Addr Timeout (min.) (menu 11.3)	Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

26.2.2 Bridge Static Route Setup

Similar to IP layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. Go to menu 12, choose option 3 to see menu 12.3 shown next.

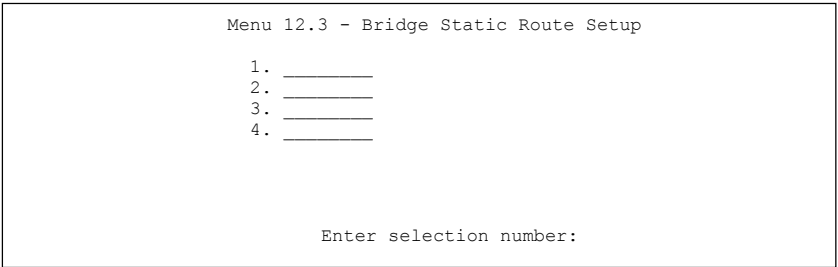


Figure 26-2 Bridge Static Route Setup

Choose a static route to edit in menu 12.3. You configure bridge static routes in menu 12.3.1 as shown next.

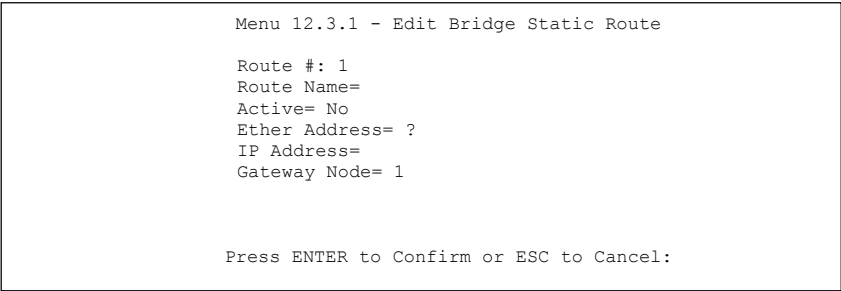


Figure 26-3 Edit Bridge Static Route

Table 26-2 Edit Bridge Static Route

FIELD	DESCRIPTION
Route #	This is the route index number you typed in Menu 12.3 – Bridge Static Route Setup .
Route Name	Type a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active (Yes) or not (No).
Ether Address	Type the MAC address of the destination computer that you want to bridge the packets to.
IP Address	If available, type the IP address of the destination computer that you want to bridge the packets to.
Gateway Node	Press [SPACE BAR] and then [ENTER] to select the number of the remote node (one to eight) that is the gateway of this static route.

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

Chapter 27

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

27.1 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 27.3.1 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.

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

27.2 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**. Use the space bar to toggle through the selections for NAT and choose the option you want.

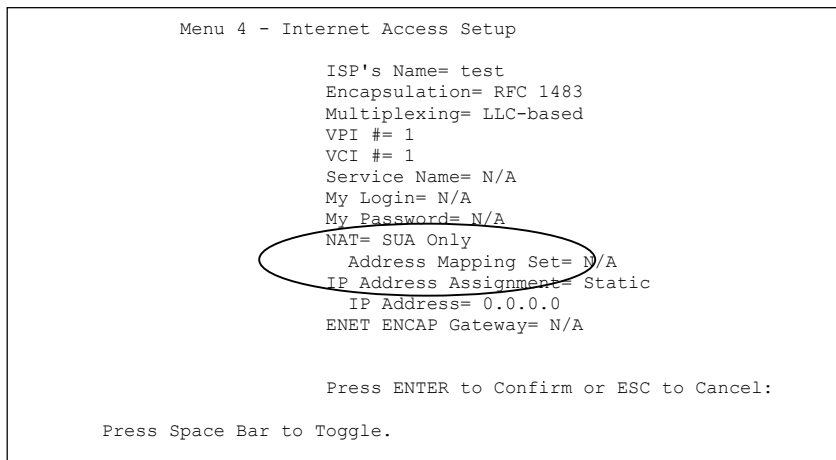


Figure 27-1 Applying NAT for Internet Access

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

- Step 1.** Enter 11 from the main menu and choose a node number.
- Step 2.** Move the cursor to the **Edit IP/IPX/Bridge** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**. Use the space bar to toggle through the selections for NAT and choose the option you want.

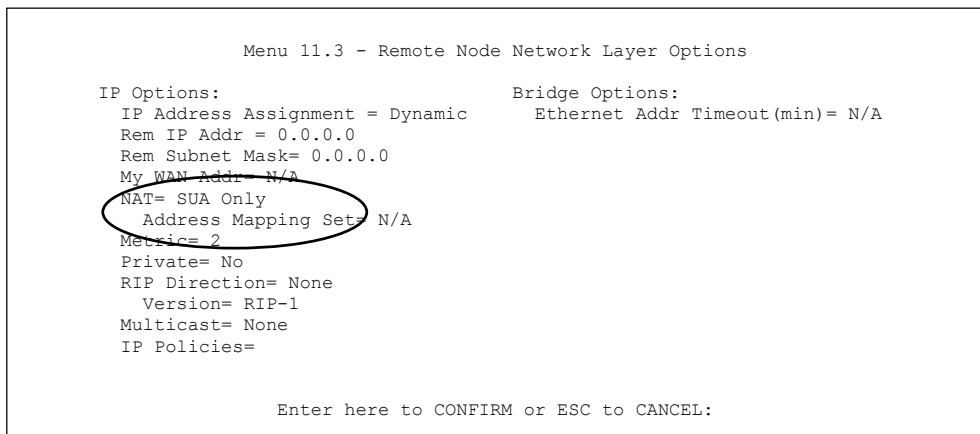


Figure 27-2 Applying NAT to the Remote Node

Table 27-1 Applying NAT to the Remote Node

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 27.3.1).	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 27.3.1). Choose SUA Only if you have just one public WAN IP address for your Prestige.	SUA Only

27.3 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. You can see two NAT Address Mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**, which supports all mapping types. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The Server Set is a list of LAN side servers mapped to external ports. To use this set (one set for the Prestige 10), a server rule must be set up inside the NAT Address Mapping set. To configure NAT, enter 15 from the main menu to bring up the following screen.

```

Menu 15 - NAT Setup

1.   Address Mapping Sets
2.   NAT Server Sets

Enter Menu Selection Number:

```

Figure 27-3 NAT Setup

27.3.1 Address Mapping Sets

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

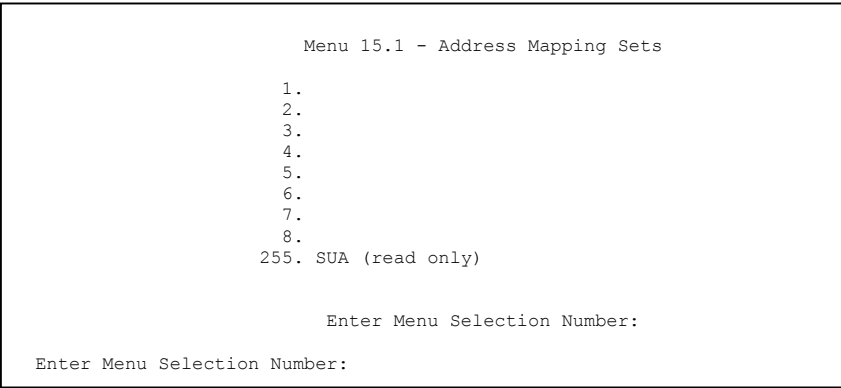


Figure 27-4 Address Mapping Sets

Enter 255 to display the next screen (see also *section 27.1*). The fields in this menu cannot be changed.

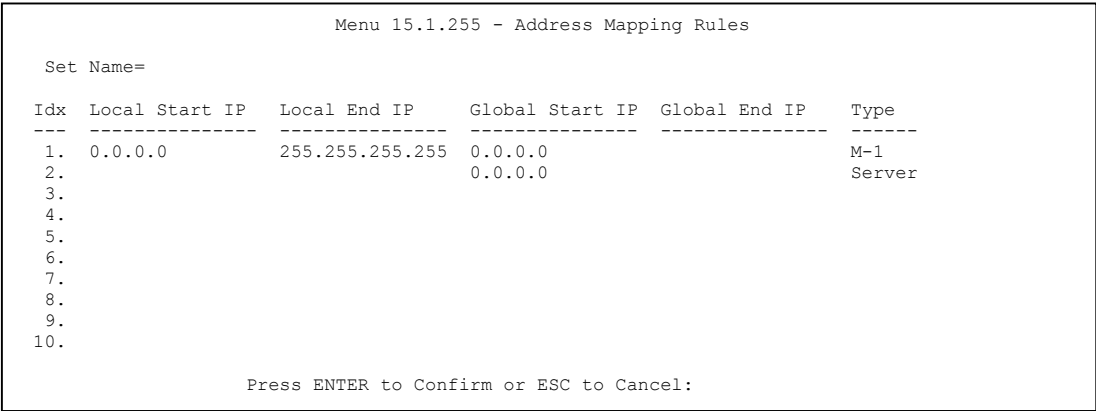


Figure 27-5 Address Mapping Rules - SUA

Table 27-2 Address Mapping Rules - SUA

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

Table 27-2 Address Mapping Rules - SUA

FIELD	DESCRIPTION	EXAMPLE
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 discussed above. Server allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
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= ?

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 27-6 Address Mapping Rules

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 27-3 Address Mapping Rules

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

FIELD	DESCRIPTION	EXAMPLE
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.

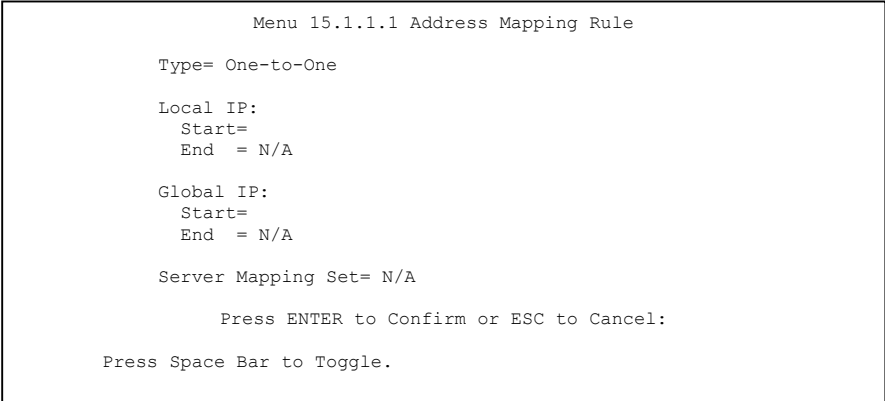


Figure 27-7 Editing/Configuring an Individual Rule in a Set

Table 27-4 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. Server allows you to specify multiple servers of different types behind NAT to this computer. See <i>section 27.4.3</i> 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 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 global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server types .	N/A
Server Mapping Set	Only available when Type is set to Server . Type a number from 1 to 10 to choose a server set from menu 15.2.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

27.3.2 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 Sets** as shown next.

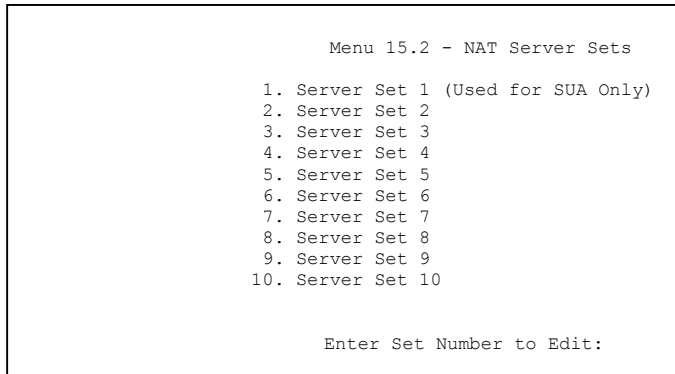


Figure 27-8 NAT Server Sets

Step 3. Enter 1 to go to **Menu 15.2 NAT Server Setup** as follows.

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 27-9 NAT Server Setup

- Step 4.

Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.
- Step 5.

Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
- Step 6.

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

Private Network IP
address assigned by user

The NAT network appears as
a single host on the Internet

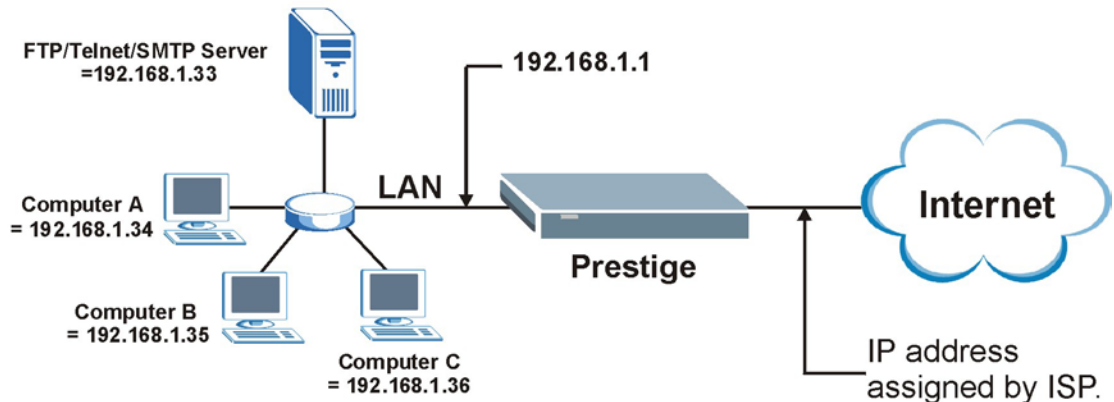


Figure 27-10 Multiple Servers Behind NAT Example

27.4 General NAT Examples

This section provides some examples with Network Address Translation.

27.4.1 Example 1: Internet Access Only

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

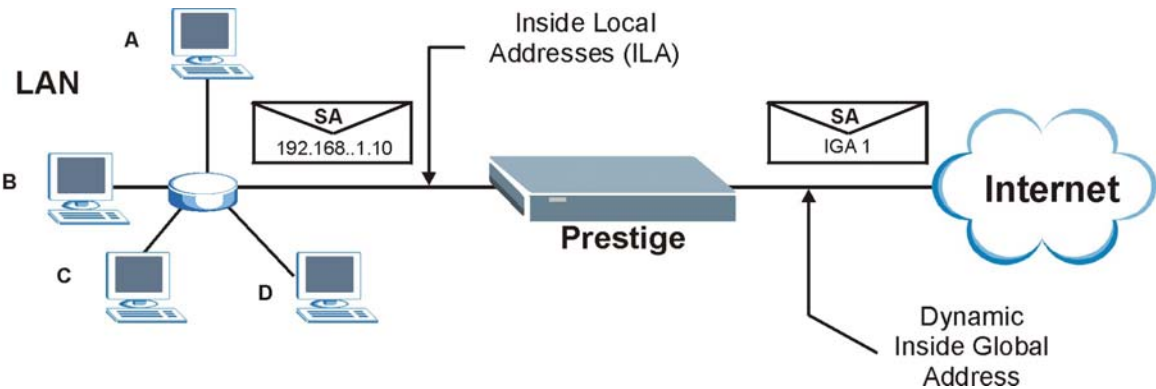


Figure 27-11 NAT Example 1

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= RFC-1483
Multiplexing= LLC-based
VPI #= 1
VCI #= 1
ATM QoS Type= UBR
    Peak Cell Rate (PCR)= 5500
    Sustained Cell Rate (SCR)= 0
    Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
    IP Address= 0.0.0.0
    Network Address Translation= SUA Only
    Address Mapping Set=
```

Figure 27-12 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 27.4*. 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.

27.4.2 Example 2: Internet Access with an Inside Server

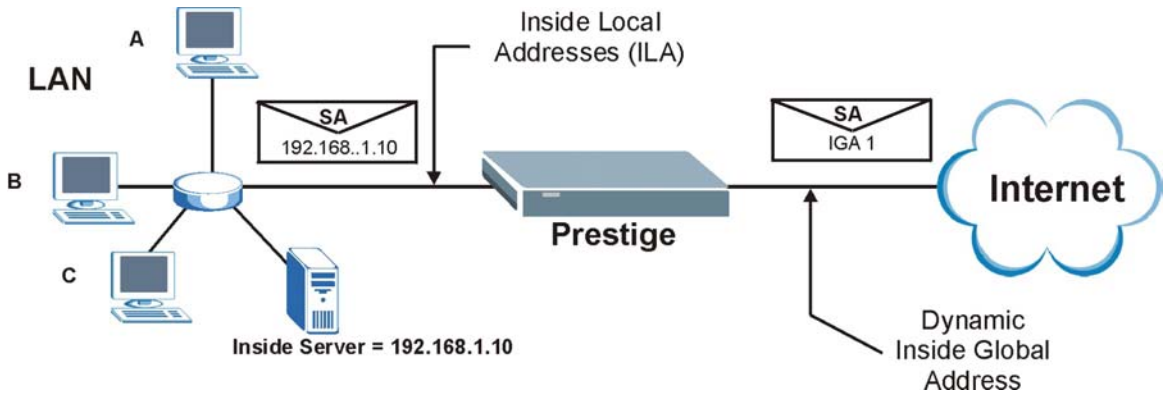
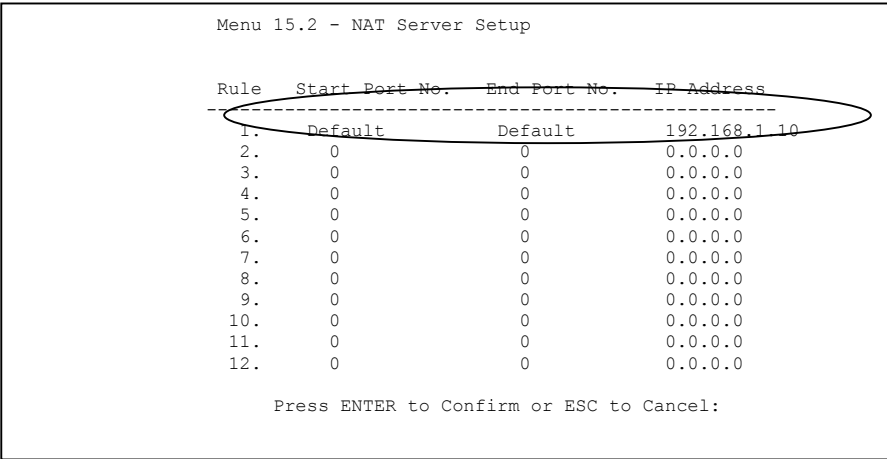


Figure 27-13 NAT Example 2

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



Menu 15.2 - NAT Server Setup

Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	192.168.1.10
2.	0	0	0.0.0.0
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Figure 27-14 NAT Example 2 - Menu 15.2.1

27.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

- Rule 1.** Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 2.** Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 3.** Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
- Rule 4.** You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

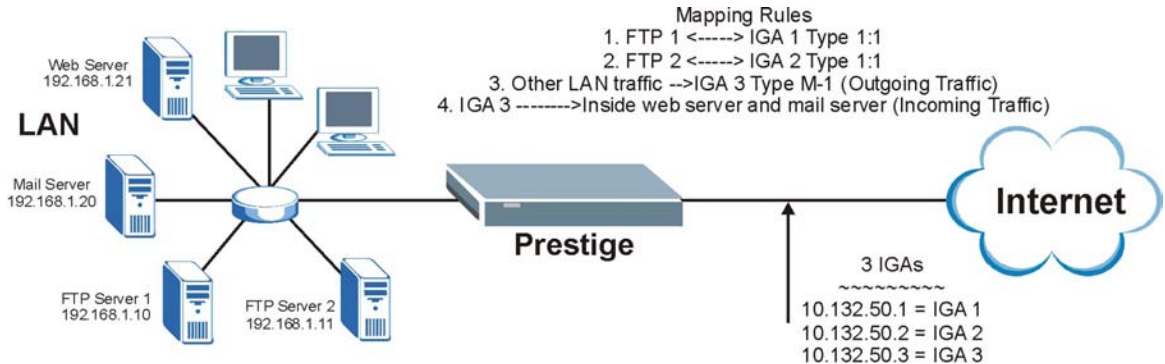


Figure 27-15 NAT Example 3

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). See the figure below.

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:                               Bridge Options:
IP Address Assignment= Static              Ethernet Addr Timeout (min)= 0
Rem IP Addr: 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0
NAT= Full Feature
Address Mapping Set= 2
Metric= 2
Private= No
RIP Direction= Both
Version= RIP-2B
Multicast= IGMP-v2
IP Policies=

Press ENTER to Confirm or ESC to Cancel:

```

Figure 27-16 Example 3 - Menu 11.3

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. In menu 15.1.1.1, select **Type** as **One-to-One** (direct mapping for packets going both ways), and set the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1) and the global **Start IP** as 10.132.50.1 (our first IGA). See the figure below.

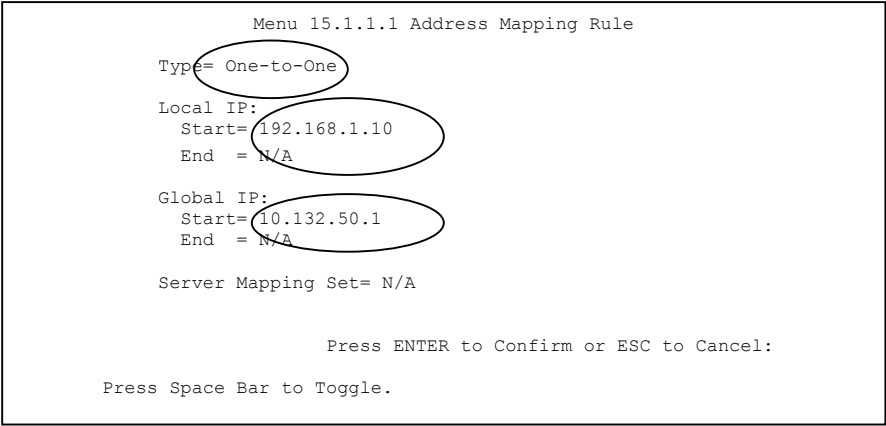


Figure 27-17 Example 3 - Menu 15.1.1.1

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

Step 7. When finished, menu 15.1.1 should look as follows.

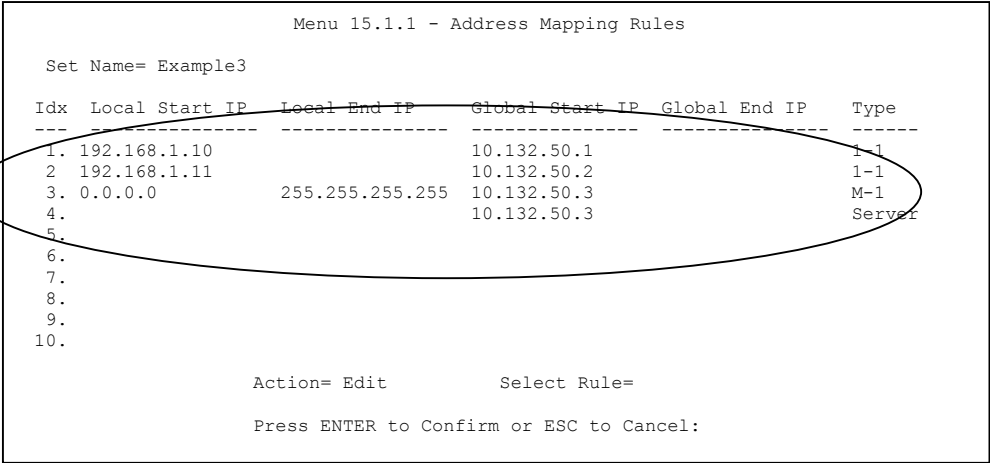


Figure 27-18 Example 3 - Final Menu 15.1.1

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 Sets** and enter 1 again 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:

Figure 27-19 Example 3- Menu 15.2

27.4.4 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.

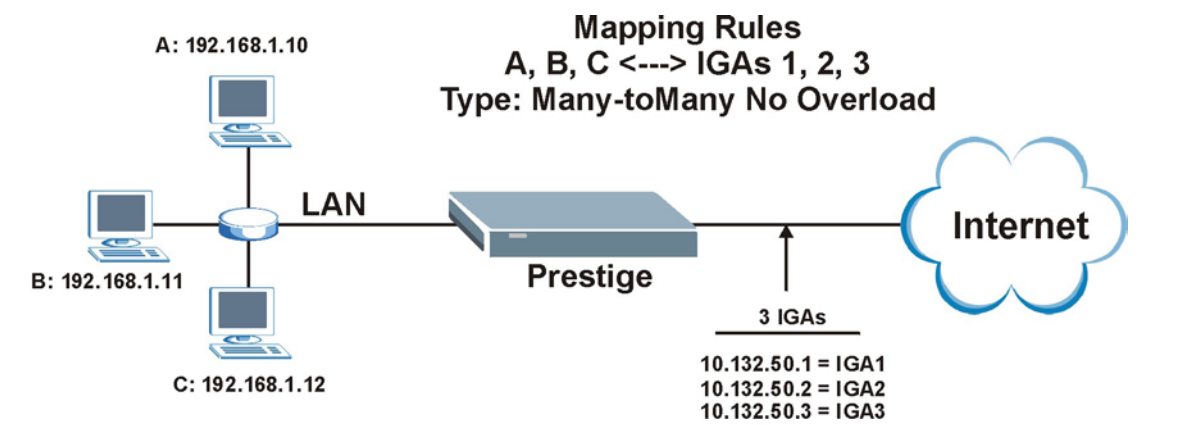


Figure 27-20 NAT Example 4

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-to-Many No Overload

Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Server Mapping Set= N/A

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

Figure 27-21 Example 4 - Menu 15.1.1.1

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 27-22 Example 4 - Menu 15.1.1

Part IX:

Advanced Management

This part discusses Filter Configuration, SNMP, System Maintenance and IP Policy Routing, Call Scheduling and Remote Management.

Chapter 28

Filter Configuration

This chapter shows you how to create and apply filters.

28.1 About Filtering

Your Prestige uses filters to decide whether or not 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 Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, e.g., RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

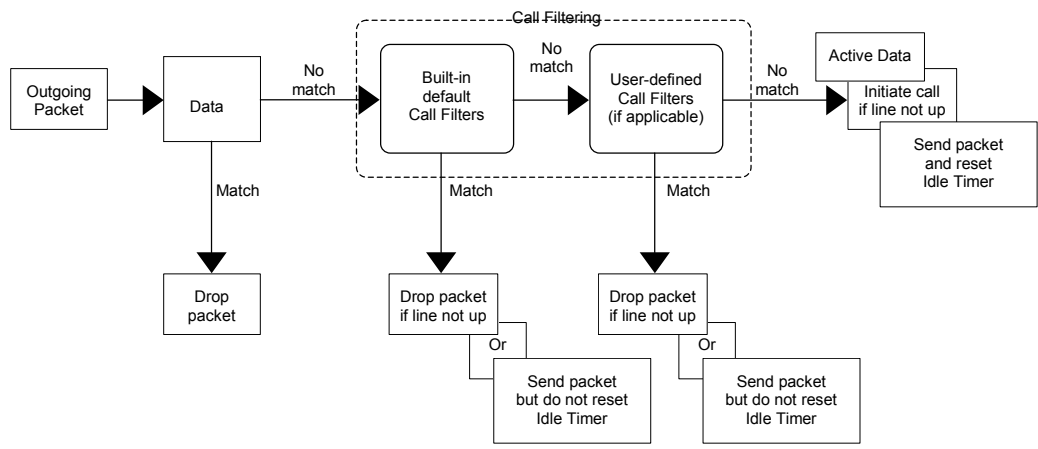
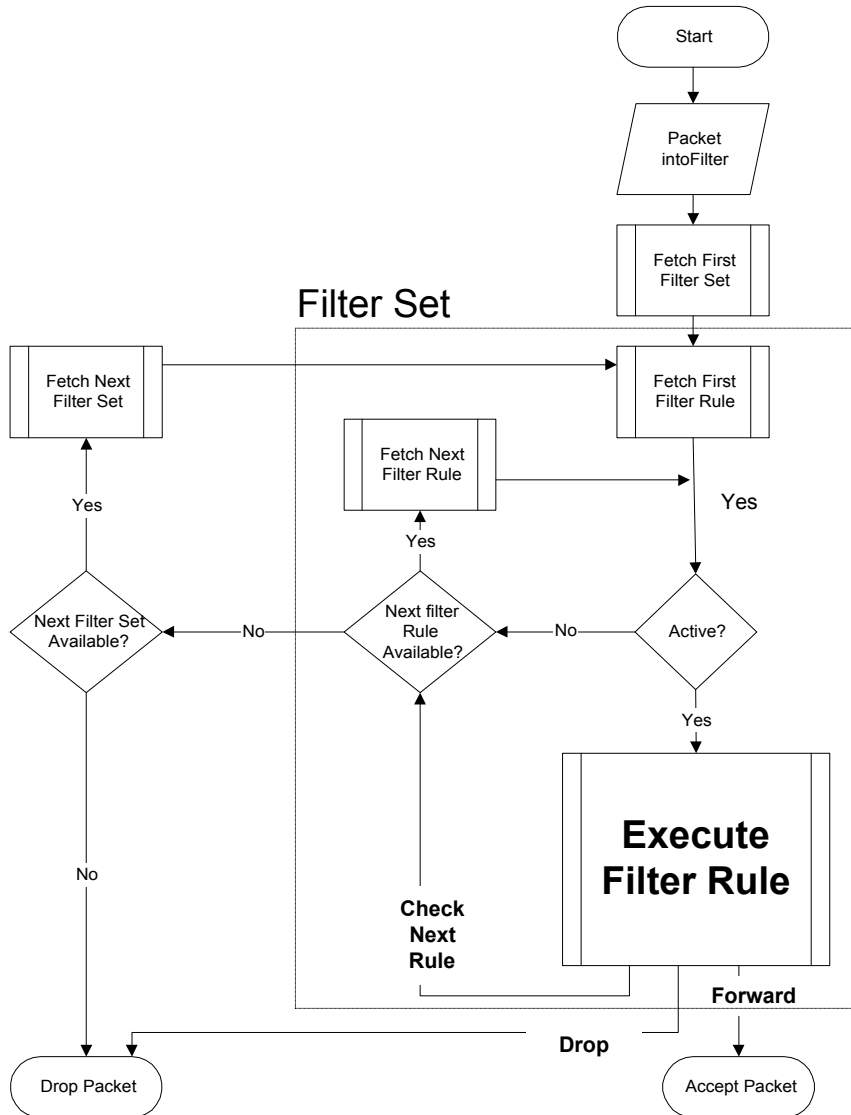


Figure 28-1 Outgoing Packet Filtering Process

Two sets of factory filter rules have been configured in Menu 21 to prevent NetBIOS traffic from triggering calls. 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.

**Figure 28-2 Filter Rule Process**

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

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

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. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

You can apply up to 4 filter sets to a particular port to block multiple types of packets. Because each filter set can have up to 6 rules, you can have a maximum of 24 rules active for a single port.

28.2 Filter Set Configuration

To configure a filter set, follow the procedures indicated:

Step 1. Type 21 in the main menu and then enter 1 to configure filter sets.

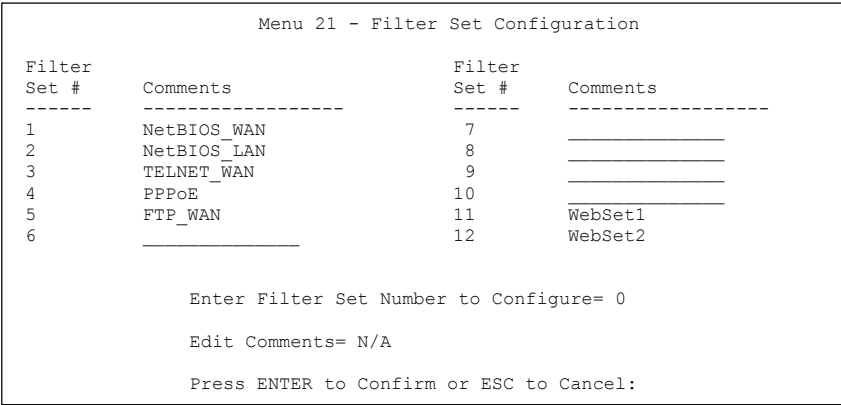


Figure 28-3 Filter Set Configuration

Step 2. Type the filter set to configure (no. 1 to 12) and press [ENTER].

Filter rule sets 11 and 12 are used by the web configurator. Your custom configurator may be lost if you use rule 11 or 12.

Step 3. Type a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 4. Press [ENTER] at the message “Press ENTER to confirm...” to display **Menu 21.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21).

Menu 21.1 - Filter Rules Summary									
#	A	Type	Filter Rules						M m n
1	Y	IP	Pr=6,	SA=0.0.0.0,	DA=0.0.0.0,	DP=137			N D N
2	Y	IP	Pr=6,	SA=0.0.0.0,	DA=0.0.0.0,	DP=138			N D N
3	Y	IP	Pr=6,	SA=0.0.0.0,	DA=0.0.0.0,	DP=139			N D N
4	Y	IP	Pr=17,	SA=0.0.0.0,	DA=0.0.0.0,	DP=137			N D N
5	Y	IP	Pr=17,	SA=0.0.0.0,	DA=0.0.0.0,	DP=138			N D N
6	Y	IP	Pr=17,	SA=0.0.0.0,	DA=0.0.0.0,	DP=139			N D F
Enter Filter Rule Number (1-6) to Configure: 1									

Figure 28-4 NetBios WAN Filter Rules Summary

Menu 21.2 - Filter Rules Summary									
#	A	Type	Filter Rules						M m n
1	Y	IP	Pr=17,	SA=0.0.0.0,	SP=137,	DA=0.0.0.0,	DP=53		N D F
2	Y								
3	Y								
4	Y								
5	Y								
6	Y								
Enter Filter Rule Number (1-6) to Configure: 1									

Figure 28-5 NetBios LAN Filter Rules Summary

Menu 21.3 - Filter Rules Summary									
#	A	Type	Filter Rules					M	m n
-	-	-	-----					-	- -
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23					N	D F
2	N								
3	N								
4	N								
5	N								
6	N								
Enter Filter Rule Number (1-6) to Configure:									

Figure 28-6 Telnet_WAN Filter Rules Summary

Menu 21.4 - Filter Rules Summary									
#	A	Type	Filter Rules					M	m n
-	-	-	-----					-	- -
1	Y	Gen	Off=12, Len=2, Mask=ffff, Value=8863					N	F N
2	Y	Gen	Off=12, Len=2, Mask=ffff, Value=8864					N	F D
3	N								
4	N								
5	N								
6	N								
Enter Filter Rule Number (1-6) to Configure:									

Figure 28-7 PPPoE Filter Rules Summary

Menu 21.5 - Filter Rules Summary				
#	A	Type	Filter Rules	M m n
1	Y	IP	PR=6, SA=0.0.0.0, DA=0.0.0.0, DP=21	N D F
2	N			
3	N			
4	N			
5	N			
6	N			
Enter Filter Rule Number (1-6) to Configure:				

Figure 28-8 FTP_WAN Filter Rules Summary

Menu 21.11 - Filter Rules Summary				
#	A	Type	Filter Rules	M m n
1	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=161	N D N
2	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=162	N D F
3	N			
4	N			
5	N			
6	N			
Enter Filter Rule Number (1-6) to Configure: 1				

Figure 28-9 Web Set1 Filter Rules Summary

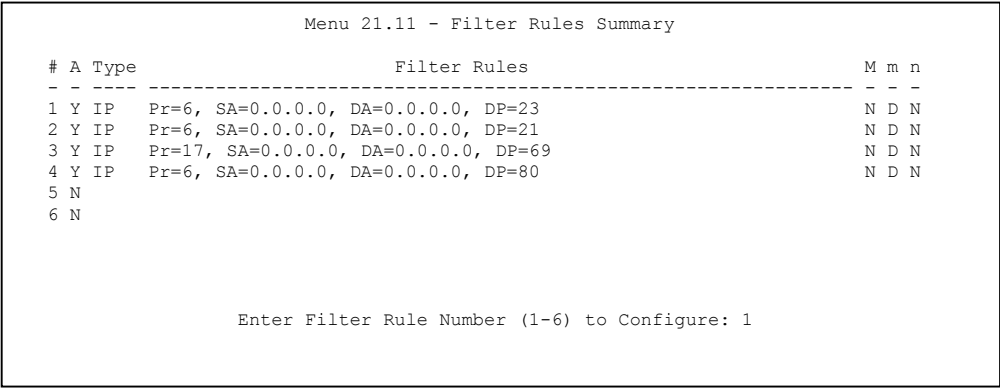


Figure 28-10 Web Set2 Filter Rules Summary

28.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menus 21.1 and 21.2.

Table 28-1 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 for instance, 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.

FIELD	DESCRIPTION
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 28-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number
GEN	
Off	Offset
Len	Length

28.3 Filter Rule Configuration

To configure a filter rule, type its number in **Menu 21.1 – Filter Rules Summary** and press [ENTER] to open menu 21.1.1 for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, for instance, 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 filters field or vice versa, the Prestige will warn you and will not allow you to save.

28.3.1 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 – TCP/IP Filter Rule**, as shown next.

```
Menu 21.1.1 - TCP/IP Filter Rule
Filter #: 1,1
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 #= 137
               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= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 28-11 TCP/IP Filter Rule

Table 28-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	1,1
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are TCP/IP Filter Rule or Generic Filter Rule .	TCP/IP Filter Rule
Active	Select Yes to activate or No to deactivate the filter rule.	No (default)

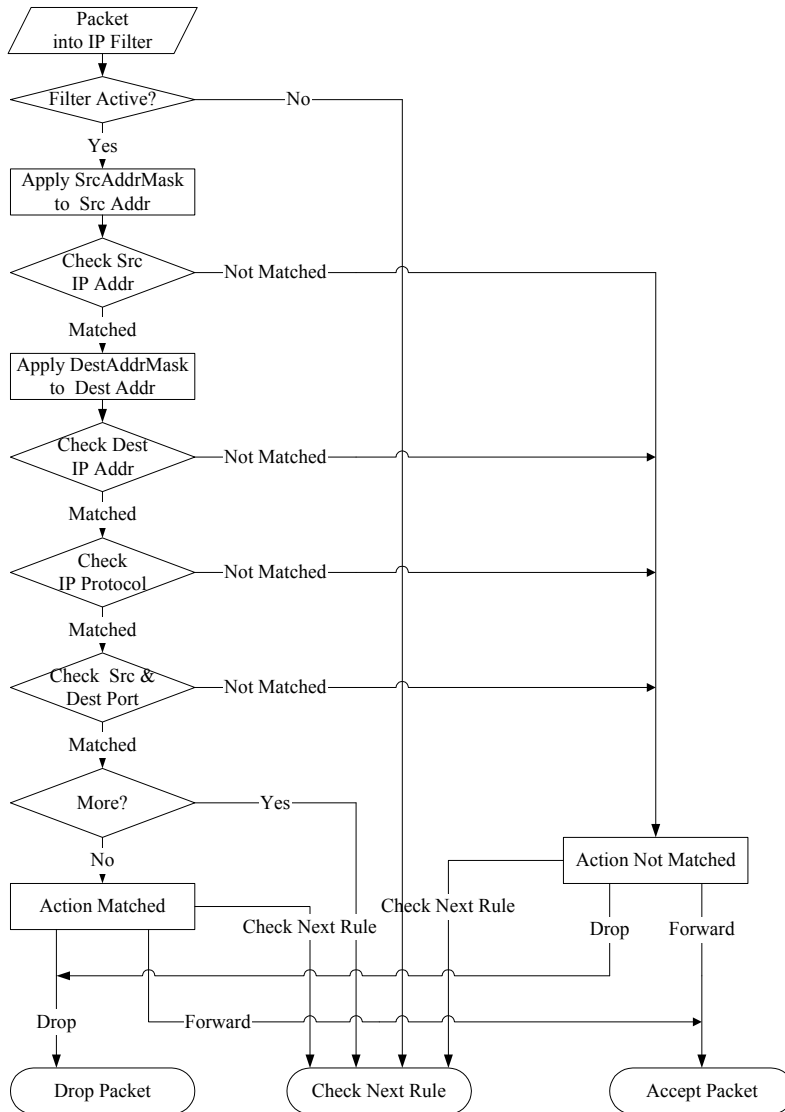
Table 28-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of 0 matches ANY protocol.	0 to 255
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If Yes , the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	No (default)
Destination: IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	IP address
IP Mask	Type the IP mask to apply to the Destination: IP Addr field.	IP mask
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port # . Choices are None , Less , Greater , Equal or Not Equal .	None
Source: IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	IP address
IP Mask	Type the IP mask to apply to the Source: IP Addr field.	IP mask
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port # field. Choices are None , Less , Greater , Equal or Not Equal .	None
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If Yes , the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	No (default)
More	If Yes , a matching packet is passed to the next filter rule before an action is taken or else 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.	No (default)

Table 28-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
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	Select the action for a matching packet. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
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.		

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

**Figure 28-12 Executing an IP Filter**

28.3.2 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 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** fields 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 an empty filter set in menu 21, for example 7. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.5.1 – Generic Filter Rule**, as shown in the following figure.

```
Menu 21.7.1 - Generic Filter Rule

Filter #: 7,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 28-13 Generic Filter Rule

Table 28-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.	5,1
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are Generic Filter Rule or TCP/IP Filter Rule .	Generic Filter Rule
Active	Select Yes to turn on or No to turn off the filter rule.	No (default)
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in Hexadecimal) to compare with the data portion.	
More	If Yes , a matching packet is passed to the next filter rule before an action is taken or else 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 .	No (default)
Log	Select the logging option from the following: None – No packets will be logged. Action Matched – Only matching packets and rules 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	Select the action for a matching packet. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
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 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 IP packets.

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 where the Prestige is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

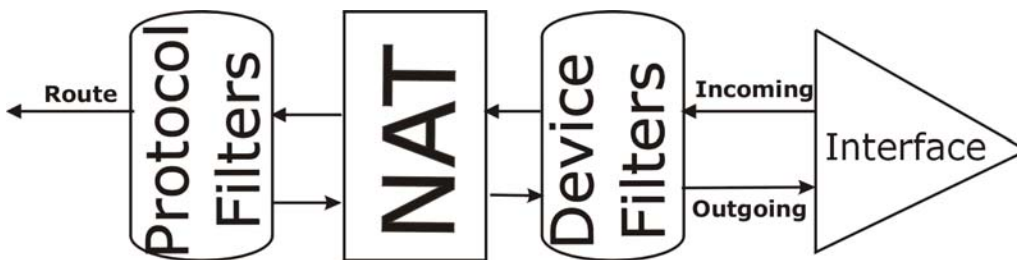


Figure 28-14 Protocol and Device Filter Sets

28.5 Example Filter

Let's look at an example to block outside users from Telnetting into the Prestige.

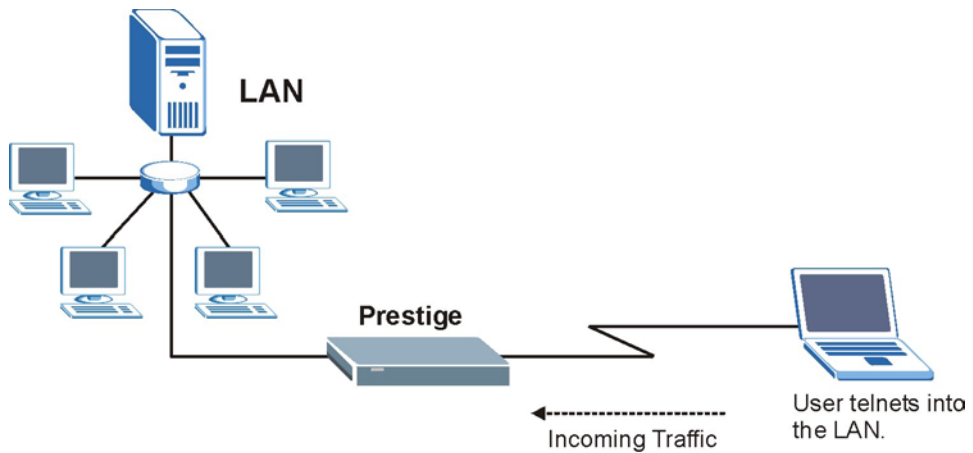


Figure 28-15 Sample Telnet Filter

- Step 1.** Enter 21 from the main menu to open **Menu 21 — Filter Set Configuration**.
- Step 2.** Enter the index number of the filter set you want to configure (in this case 3).
- Step 3.** Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].
- Step 4.** Press [ENTER] at the message “Press [ENTER] to confirm or [ESC] to cancel” to open **Menu 21.3 — Filter Rules Summary**.

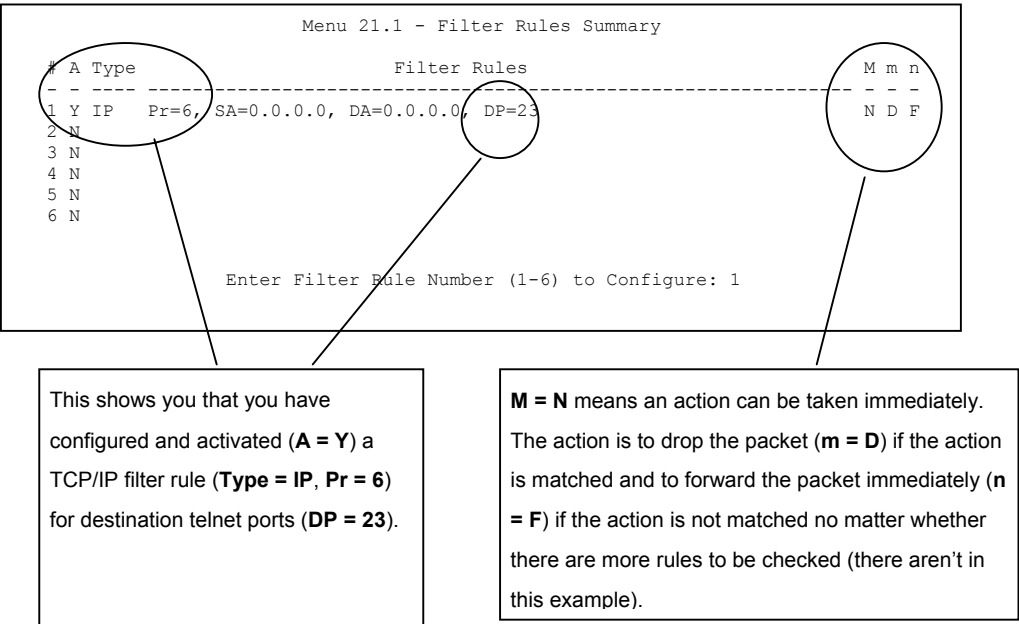


Figure 28-16 Sample Filter Rules Summary — Menu 21.1

Step 5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next. When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

Menu 21.3.1 - TCP/IP Filter Rule

```

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6
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 # =
         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 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 **Drop** here so that the packet will be dropped if its destination is the telnet port.

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

Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port and there are no more rules in this filter set to check. Select **Next** if there are more rules to check.

Figure 28-17 Sample Filter Rules Summary — Menu 21.3.1

After you have created the filter set, you must apply it.

Step 1. Enter 11 in the main menu to display menu 11 and type the remote node number to edit it.

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

Step 3. This brings you to menu 11.5. Enter the example filter set number in this menu as shown in the following figure.

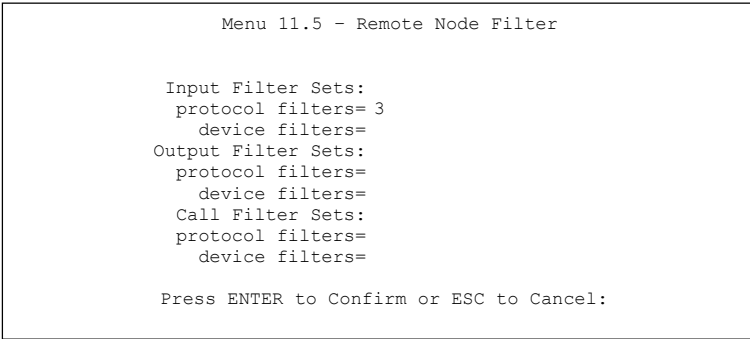


Figure 28-18 Sample Filter Rules Summary — Applying a Remote Node Filter Set

28.6 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

Table 28-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

28.6.1 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. Go to menu 3.1 (shown next) and type 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 typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

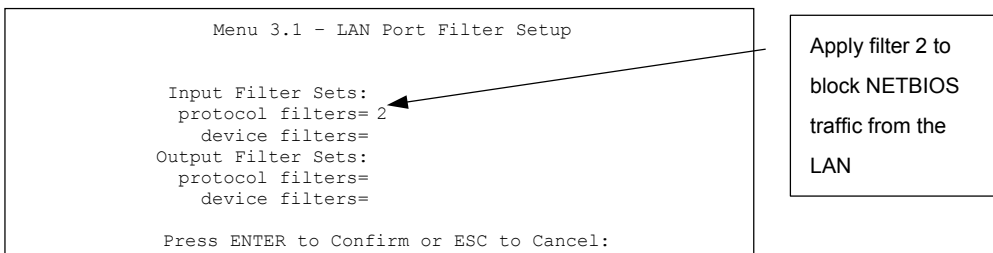


Figure 28-19 Filtering Ethernet Traffic

28.6.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, NetBIOS_WAN, is inserted in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

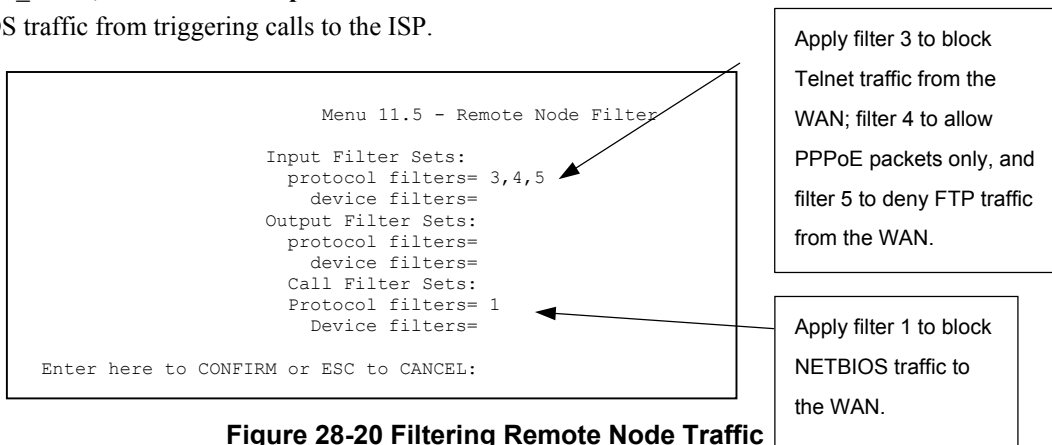


Figure 28-20 Filtering Remote Node Traffic

Note that call filter sets are visible when you select PPPoA or PPPoE encapsulation.

Chapter 29

SNMP Configuration

This chapter explains SNMP Configuration.

SNMP is only available if TCP/IP is configured.

29.1 SNMP Overview

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of 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). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

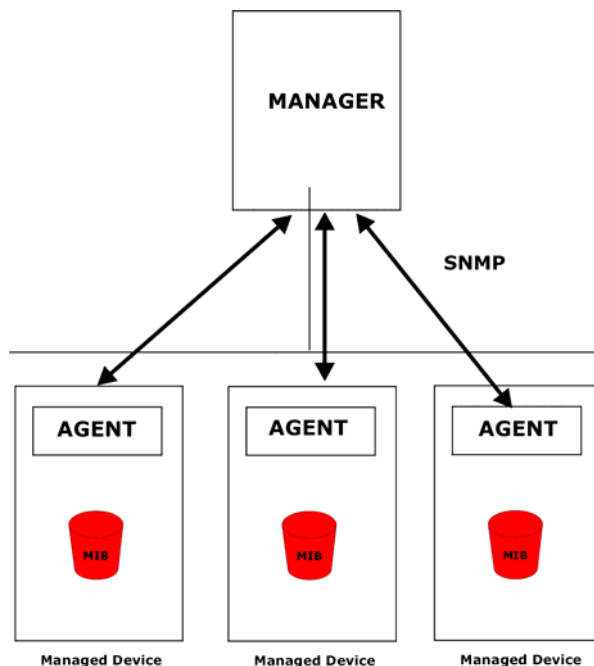


Figure 29-1 SNMP Management Model

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 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.

29.2 Supported MIBs

The Prestige supports MIB II that is defined in RFC-1213 and RFC-1215. The Prestige can also respond with specific data from the ZyXEL private MIB (ZYXEL-MIB). The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

The only implement MIBs in the Prestige as a SNMP agent. Users must implement their own GUI on SNMP platform (SNMP manager).

29.3 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 Hgst= 0.0.0.0
Trap:
Community= public
Destination= 0.0.0.0

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

Figure 29-2 SNMP Configuration**Table 29-1 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.		

29.4 SNMP Traps

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

Table 29-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (power on).

TRAP #	TRAP NAME	DESCRIPTION
2	warmStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (software reboot).
3	linkUp (<i>defined in RFC-1215</i>)	A trap is sent with the port number.
4	authenticationFailure (<i>defined in RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (<i>defined in RFC-1215</i>)	A trap is sent with the port number when any of the links are down. See the following table.

The port number is its interface index under the interface group.

Chapter 30

System Maintenance

This chapter covers the diagnostic tools that help you to maintain your Prestige.

30.1 System Maintenance Overview

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

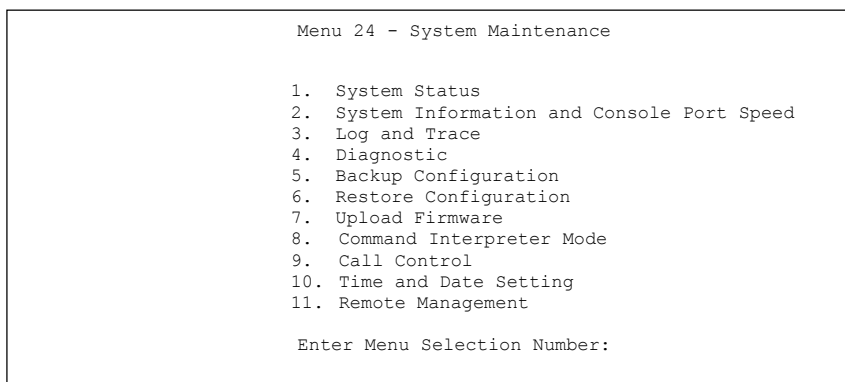


Figure 30-1 System Maintenance

30.2 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your ADSL telephone line status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 — System Maintenance**. From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

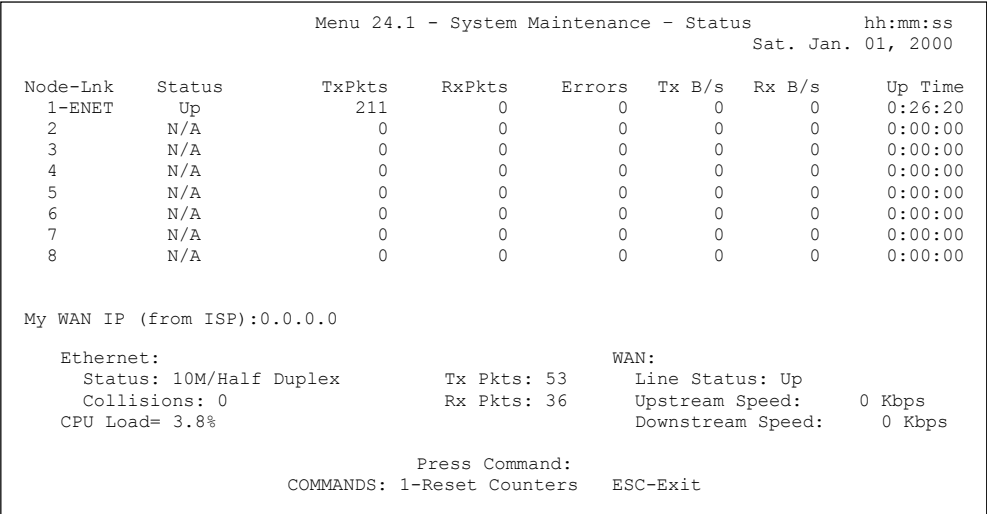


Figure 30-2 System Maintenance — Status

Table 30-1 System Maintenance — Status

FIELD	DESCRIPTION
Node-Lnk	This is the node index number and link type. Link types are: PPP, ENET, 1483.
Status	Shows the status of the remote node.
TxPkts	The number of transmitted packets to this remote node.
RxPkts	The number of received packets from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	Shows the transmission rate in bytes per second.
Rx B/s	Shows the receiving rate in bytes per second.
Up Time	Time this channel has been connected to the current remote node.
My WAN IP (from ISP)	The IP address of the ISP remote node.
Ethernet	Shows statistics for the LAN.
Status	Shows the current status of the LAN.
Tx Pkts	The number of transmitted packets to the LAN.

Table 30-1 System Maintenance — Status

FIELD	DESCRIPTION
Rx Pkts	The number of received packets from the LAN.
Collision	Number of collisions.
WAN	Shows statistics for the WAN.
Line Status	Shows the current status of the xDSL line, which can be Up or Down.
Upstream Speed	Shows the upstream transfer rate in kbps.
Downstream Speed	Shows the downstream transfer rate in kbps.
CPU Load	Specifies the percentage of CPU utilization.

30.3 System Information

To get to the System Information:

Step 1. Enter 24 to display **Menu 24 — System Maintenance**.

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

Step 3. From this menu you have two choices as shown in the next figure:

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

Please enter selection:
```

Figure 30-3 System Information and Console Port Speed

30.3.1 System Information

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

```
Menu 24.2.1 - System Maintenance - Information

Name:
Routing: IP
ZyNOS F/W Version: V3.40(BQ.0)b1 | 3/24/2003
xDSL F/W Version: R.2.3.1
Standard: ANSI (ANNEX_A)

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 30-4 System Maintenance — Information

Table 30-2 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.
xDSL F/W Version	Refers to the DSL version.
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
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.

30.3.2 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 and 38400 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: 115200

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

Figure 30-5 System Maintenance – Change Console Port Speed

Once you change the Prestige consol port speed, you must also set the speed parameter for the communication software you are using to connect to the Prestige.

30.4 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 UNIX syslog facility for message logging.

30.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

Step 1. Type 24 in the main menu to display **Menu 24 – System Maintenance**.

Step 2. From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

```
Menu 24.3 - System Maintenance - Log and Trace

1. View Error Log
2. UNIX Syslog

Please enter selection
```

Figure 30-6 System Maintenance — Log and Trace

Step 3. Enter 1 from **Menu 24.3 — System Maintenance — Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

```
59 Thu Jan 01 00:00:03 1970 PP0f INFO LAN promiscuous mode <0>
60 Thu Jan 01 00:00:03 1970 PP00 -WARN SNMP TRAP 0: cold start
61 Thu Jan 01 00:00:03 1970 PP00 INFO main: init completed
62 Thu Jan 01 00:00:19 1970 PP00 INFO SMT Session Begin
63 Thu Jan 01 00:00:24 1970 PP0a WARN MPOA Link Down
Clear Error Log (y/n):
```

Figure 30-7 Sample Error and Information Messages

30.4.2 Syslog

The Prestige uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog can be configured in **Menu 24.3.2 — System Maintenance — UNIX Syslog**, as shown next.

```
Menu 24.3.2 - System Maintenance - UNIX Syslog

UNIX Syslog:
Active= No
Syslog IP Address= ?
Log Facility= Local 1

Types:
CDR= No
Packet triggered= No
Filter Log= No
PPP Log= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 30-8 System Maintenance — Syslog and Accounting

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

Table 30-3 System Maintenance Menu — Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Type the IP address of your syslog server.
Log Facility	Use [SPACE BAR] and then [ENTER] to select one of seven different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to Yes .
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to Yes .
Filter Log	No filters are logged when this field is set to No . Filters with the individual filter Log Filter field set to Yes are logged when this field is set to Yes .
PPP Log	PPP events are logged when this field is set to Yes .

The following are examples of the four types of syslog messages sent by the Prestige:

1 - CDR	
SdcmSyslogSend (SYSLOG CDR, SYSLOG INFO, String);	
String = board xx line xx channel xx, call xx, str	
board = the hardware board ID	
line = the WAN ID in a board	
Channel = channel ID within the WAN	
call = the call reference number which starts from 1 and increments by 1 for each new call	
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)	
C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)	
C01 Incoming Call xxxxx (= connected speed) xxxxx (= Remote Call ID)	
L02 Tunnel Connected (L2TP)	
C02 OutCall Connected xxxxx (= connected speed) xxxxx (= Remote Call ID)	
C02 CLID call refused	
L02 Call Terminated	
C02 Call Terminated	
Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002	
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002	
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated	
2 - Packet Triggered	
SdcmSyslogSend (SYSLOG PKTRI, 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=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f70717273 74	

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
SdcmSyslogSend (SYSLOG FILLOG, SYSLOG NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m), drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol ("TCP", "UDP", "ICMP")
spo: Source port
dpo: Destination port
Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP spo=0208 dpo=0208}] S03>R01mF Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035}] S03>R01mF Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035}] S03>R01mF
4 - PPP Log
SdcmSyslogSend (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

30.5 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.

Menu 24.4 - System Maintenance - Diagnostic	
xDSL	System
1. Reset xDSL	21. Reboot System
	22. Command Mode
TCP/IP	
12. Ping Host	
Enter Menu Selection Number:	
Host IP Address= N/A	

Figure 30-9 System Maintenance — Diagnostic

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. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

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

Table 30-4 System Maintenance Menu — Diagnostic

FIELD	DESCRIPTION
Reset xDSL	Re-initialize the xDSL link to the telephone company.
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
Reboot System	Reboot the Prestige.
Command Mode	Type the mode to test and diagnose your Prestige using specified commands.
Host IP Address	If you typed 12 to Ping Host, now type the address of the computer you want to ping.

Chapter 31

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.

31.1 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.

```
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 31-1 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

31.2 Backup Configuration

The Prestige displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2; depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current 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. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don’t have to rename the files.

Please note that terms “download” and “upload” are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

31.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

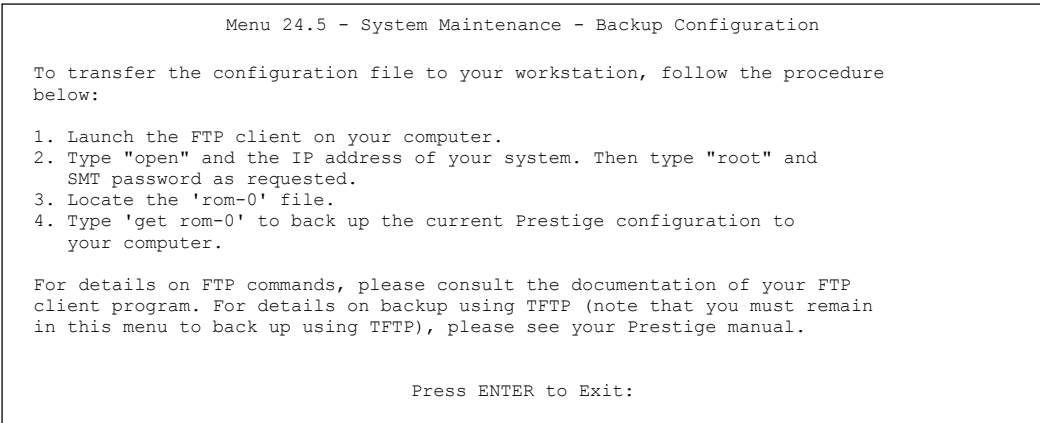


Figure 31-1 System Maintenance - Backup Configuration

31.2.2 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.

31.2.3 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 31-2 FTP Session Example

31.2.4 GUI-based FTP Clients

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

Table 31-2 General Commands for GUI-based FTP Clients

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

31.2.5 TFTP and FTP over WAN Management Limitations

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

- 1. You have disabled Telnet service and remote management.
- 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.

31.2.6 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.

31.2.7 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.

31.2.8 GUI-based TFTP Clients

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

Table 31-3 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 31.2.5* to read about configurations that disallow TFTP and FTP over WAN.

31.2.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.5 and enter “y” at the following screen.

```
Ready to backup Configuration via Xmodem.  
Do you want to continue (y/n):
```

Figure 31-3 System Maintenance – Backup Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
You can enter ctrl-x to terminate operation any time.  
Starting XMODEM download...
```

Figure 31-4 System Maintenance – Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

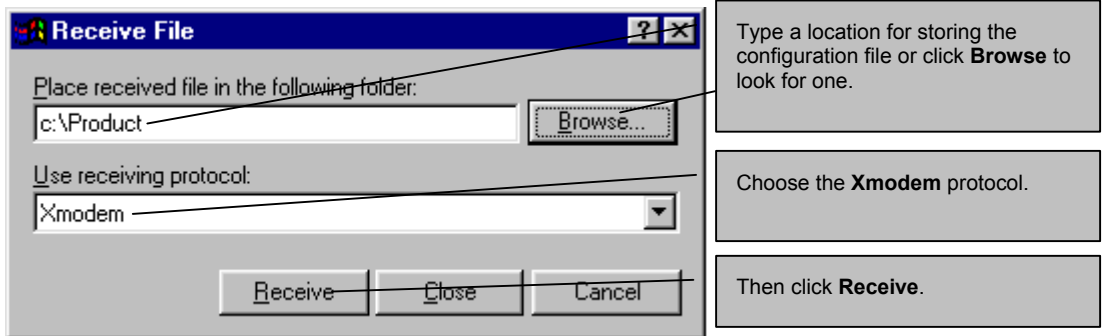


Figure 31-5 Backup Configuration Example

Step 4. After a successful backup you will see the following screen. Press any key to return to the SMT menu.

```

** Backup Configuration completed. OK.
### Hit any key to continue.###

```

Figure 31-6 Successful Backup Confirmation Screen

31.3 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.

31.3.1 Restore Using FTP

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

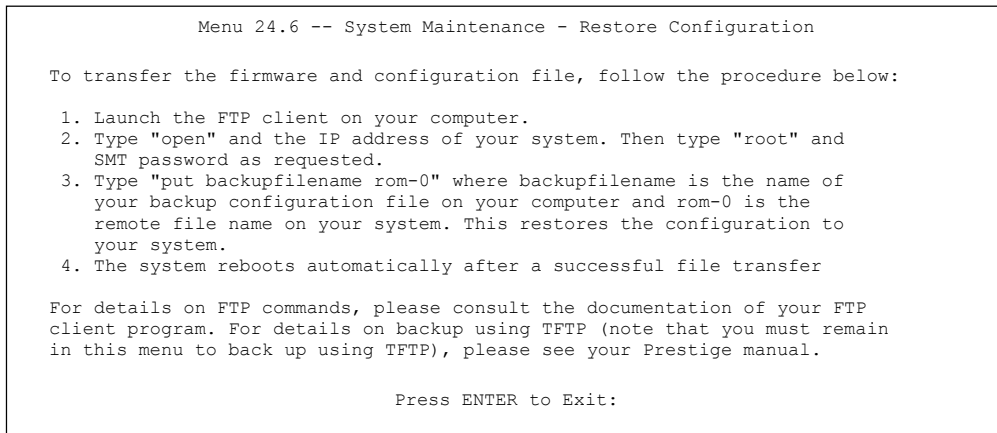


Figure 31-7 System Maintenance - Restore Configuration

- 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.

31.3.2 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 31-8 Restore Using FTP Session Example

Refer to *section 31.2.5* to read about configurations that disallow TFTP and FTP over WAN.

31.3.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.6 and enter “y” at the following screen.

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 31-9 System Maintenance – Restore Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
Starting XMODEM download (CRC mode) ...
CCCCCCCC
```

Figure 31-10 System Maintenance – Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

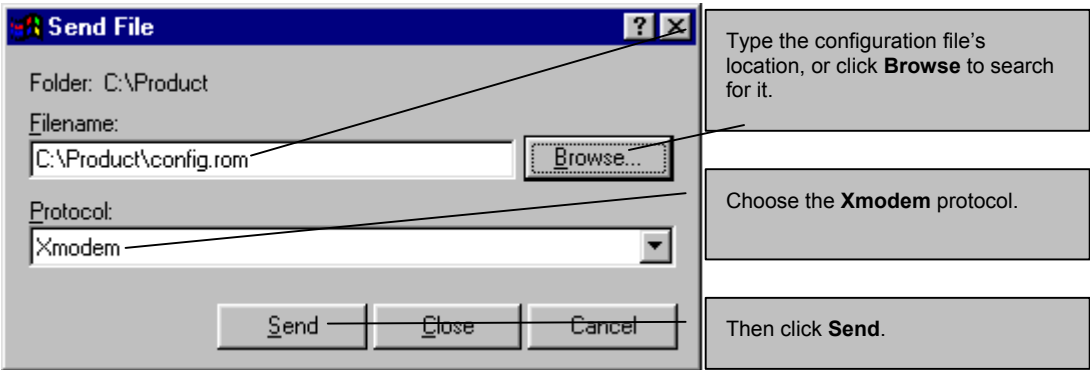


Figure 31-11 Restore Configuration Example

Step 4. After a successful restoration you will see the following screen. Press any key to restart the Prestige and return to the SMT menu.

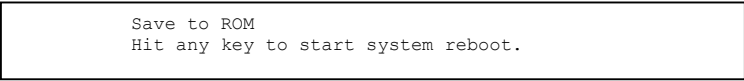


Figure 31-12 Successful Restoration Confirmation Screen

31.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File** (for console port).

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

31.4.1 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 firmwarefilename ras" where "firmwarefilename" is the name of your firmware upgrade file on your workstation and "ras" is the remote file name on the system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP client program. For details on uploading system firmware using TFTP (note that you must remain on this menu to upload system firmware using TFTP), please see your manual.

Press ENTER to Exit:

Figure 31-13 System Maintenance - Upload System Firmware

31.4.2 Configuration File Upload

You will see the following screen when you telnet into menu 24.7.2.

Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and SMT password as requested.
3. Type "put configurationfilename rom-0" where "configurationfilename" is the name of your system configuration file on your workstation, which will be transferred to the "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration file process is complete.

For details on FTP commands, please consult the documentation of your FTP client program. For details on uploading 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 31-14 Telnet Into Menu 24.7.2 – System Maintenance

To upload the firmware and the configuration file, follow these examples

31.4.3 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.

31.4.4 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 31-15 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 31.2.5* to read about configurations that disallow TFTP and FTP over WAN.

31.4.5 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.

31.4.6 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.

31.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your Prestige. However, in the event of your network being down, uploading files is only possible with a direct connection to your Prestige via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

31.4.8 Uploading Firmware File Via Console Port

Step 1. Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 – System Maintenance – Upload System Firmware**, then follow the instructions as shown in the following screen.

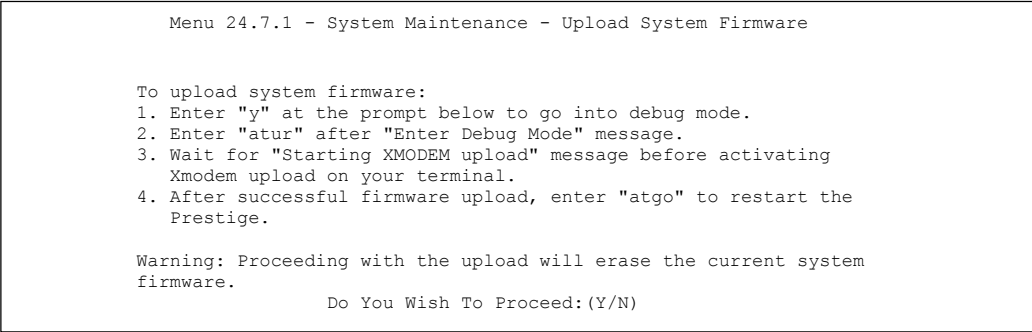


Figure 31-16 Menu 24.7.1 as seen using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

31.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

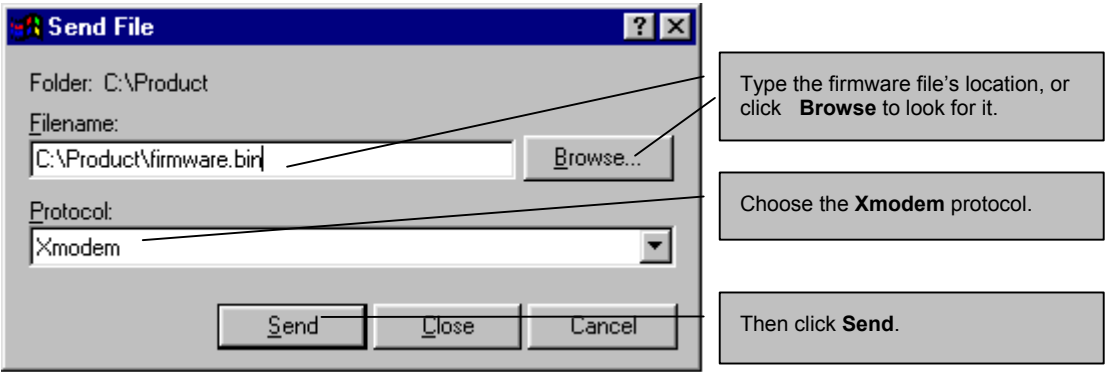


Figure 31-17 Example Xmodem Upload

After the configuration upload process has completed, restart the Prestige by entering "atgo".

31.4.10 Uploading Configuration File Via Console Port

- Step 1.** Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 – System Maintenance – Upload System Configuration File**. Follow the instructions as shown in the next screen.

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   system.

Warning:
1. Proceeding with the upload will erase the current
   configuration file.
2. The system's console port speed (Menu 24.2.2) may change
   when it is restarted; please adjust your terminal's speed
   accordingly. The password may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
   port speed will be reset to 9600 bps and the password to
   "1234".

Do You Wish To Proceed:(Y/N)
```

Figure 31-18 Menu 24.7.2 as seen using the Console Port

- Step 2.** After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.
- Step 3.** Enter "atgo" to restart the Prestige.

31.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

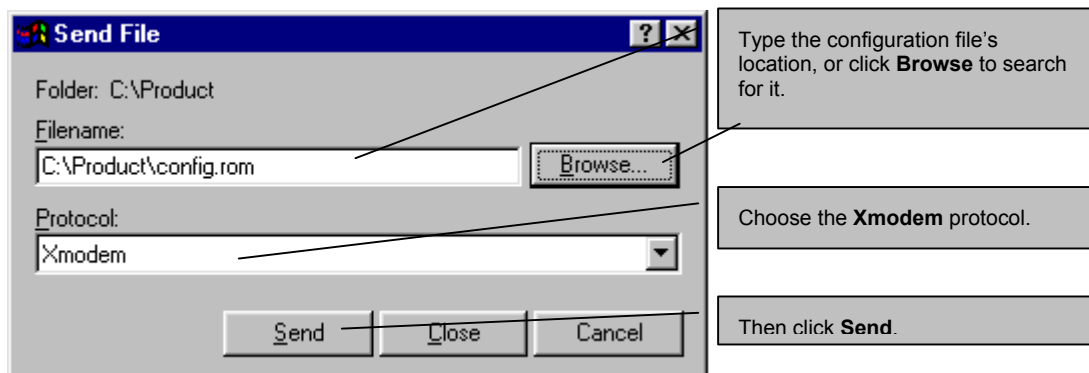


Figure 31-19 Example Xmodem Upload

After the configuration upload process has completed, restart the Prestige by entering "atgo".

Chapter 32

System Maintenance and Information

This chapter leads you through SMT menus 24.8 to 24.10.

32.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.

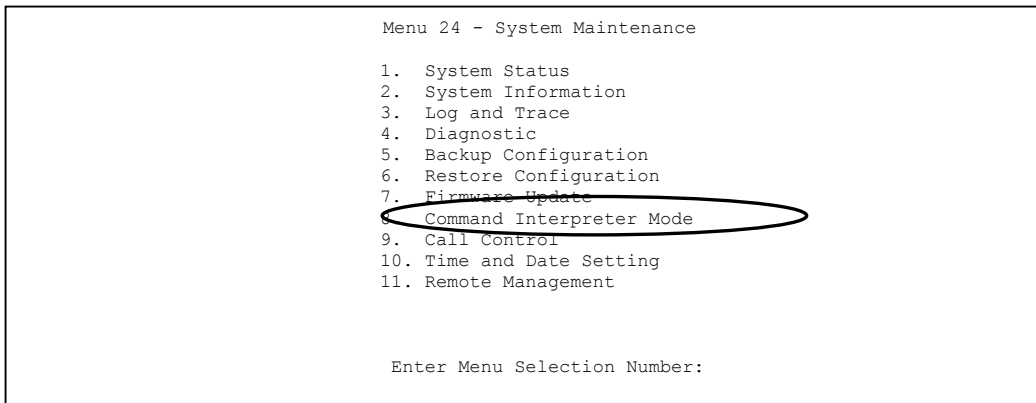


Figure 32-1 Command Mode in Menu 24

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys      exit      device      ether
wan      poe       xdsl       ip
ppp      bridge    hdap
ras>
```

Figure 32-2 Valid Commands

32.2 Call Control Support

Call Control Support 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

Enter Menu Selection Number:
```

Figure 32-3 Call Control

32.2.1 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 - System Maintenance - Budget Management

Remote Node      Connection Time/Total Budget      Elapsed Time/Total Period
1.MyISP          No Budget                                No Budget
2.-----
3.-----
4.-----
5.-----
6.-----
7.-----
8.-----

Reset Node (0 to update screen):

```

Figure 32-4 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 when PPPoE encapsulation is selected.

Table 32-1 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.		

32.3 Time and Date Setting

The Prestige keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 — System Maintenance**, as shown next.

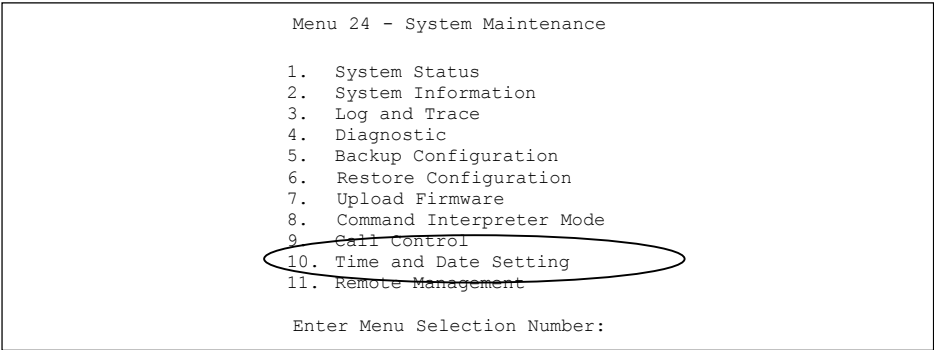


Figure 32-5 System Maintenance

Then enter 10 to go to **Menu 24.10 — System Maintenance — Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

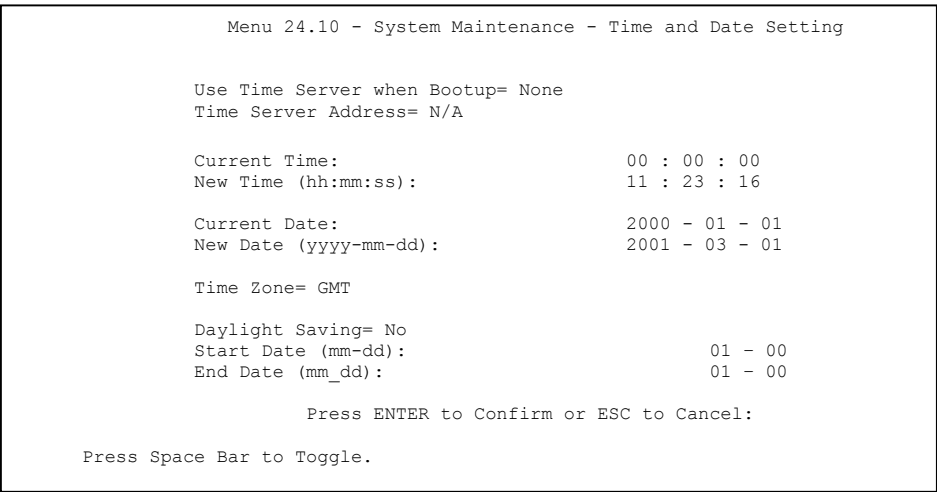


Figure 32-6 System Maintenance — Time and Date Setting

Table 32-2 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	<p>Enter 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 differences between them are the format.</p> <p>Daytime (RFC 867) format is day/month/year/time zone of the server.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) is similar to Time (RFC-868).</p> <p>None. The default, enter the time manually.</p>
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
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 re-enter 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	If you use daylight savings time, then choose Yes .
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
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.	

32.3.1 Resetting the Time

The Prestige resets the time in three instances:

- On leaving menu 24.10 after making changes.
- When the Prestige starts up, if there is a timeserver configured in menu 24.10.
- 24-hour intervals after starting.

Chapter 33

IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

33.1 IP Policy Routing Overview

Traditionally, routing is based on the destination address only and the IAD takes the shortest path to forward a packet. IP Routing Policy (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

33.1.1 IP Policy Routing Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

33.1.2 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, for example, telnet, tend to have short packets, while bulk traffic, for example, file transfer, tends to have large packets.

The actions that can be taken include:

- Routing the packet to a different gateway (and hence the outgoing interface).
- Setting the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

33.2 IP Routing Policy Setup

Menu 25 shows all the policies defined.

Menu 25 - IP Routing Policy Setup

Policy Set #	Name	Policy Set #	Name
1	test	7	
2		8	
3		9	
4		10	
5		11	
6		12	

Enter Policy Set Number to Configure= 0

Edit Name= N/A

Press ENTER to Confirm or ESC to Cancel:

Figure 33-1 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

- Step 1. Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup**.
- Step 2. Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator “|” means the action is taken on criteria matched and separator “=” means the action is taken on criteria not matched.


```

Menu 25.1 - IP Routing Policy Setup

# A          Criteria/Action
- - - - -
1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
   SP=20-25,DP=20-25,P=6,T=NM,PR=0      |GW=192.168.1.1,T=MT,PR=0
2 N _____
3 N _____
4 N _____
5 N _____
6 N _____

Enter Policy Rule Number (1-6) to Configure:

```

Figure 33-2 Sample IP Routing Policy Setup

Table 33-1 IP Routing Policy Setup Abbreviations

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17...)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
Service	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

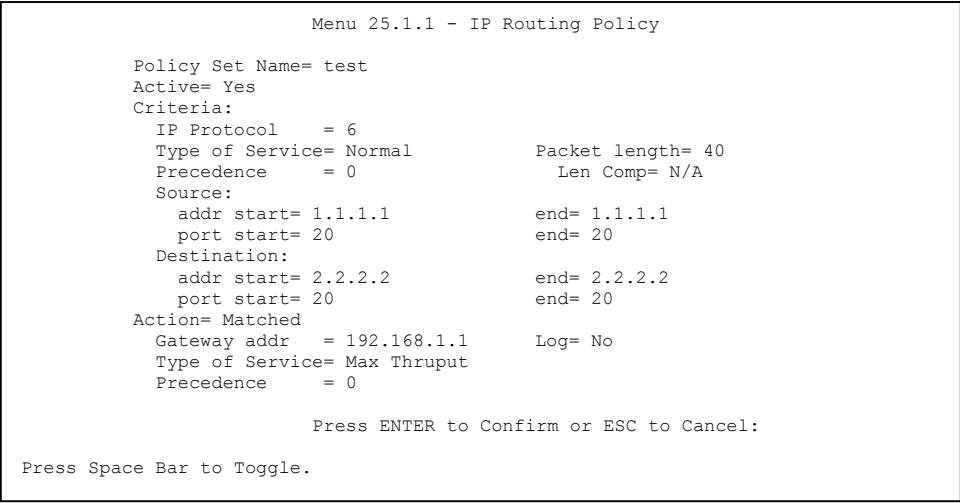


Figure 33-3 IP Routing Policy

Table 33-2 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in Menu 25 – IP Routing Policy Setup .
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate or No to deactivate the policy. Inactive policies are displayed with a minus sign “-“ in SMT menu 25.
Criteria	
IP Protocol	IP layer 4 protocol, for example, UDP , TCP , ICMP , etc.
Type of Service	Prioritize incoming network traffic by choosing from Don’t Care , Normal , Min Delay , Max Thruput , Min Cost or Max Reliable .
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from 0 to 7 or Don’t Care .
Packet Length	Type the length of incoming packets (in bytes). The operators in the Len Comp (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from Equal , Not Equal ,

Table 33-2 IP Routing Policy

FIELD	DESCRIPTION
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from Equal , Not Equal , Less , Greater , Less or Equal or Greater or Equal .
Source:	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria Matched or Not Matched .
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing No Change , Normal , Min Delay , Max Thruput , Max Reliable or Min Cost .
Precedence	Set the new outgoing packet precedence value. Values are 0 to 7 or No Change .
Log	Press [SPACE BAR] and then [ENTER] to select Yes to make an entry in the system log when a policy is executed.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

33.3 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

33.3.1 Ethernet IP Policies

From **Menu 3 — Ethernet Setup**, type 2 to go to **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**.

You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.

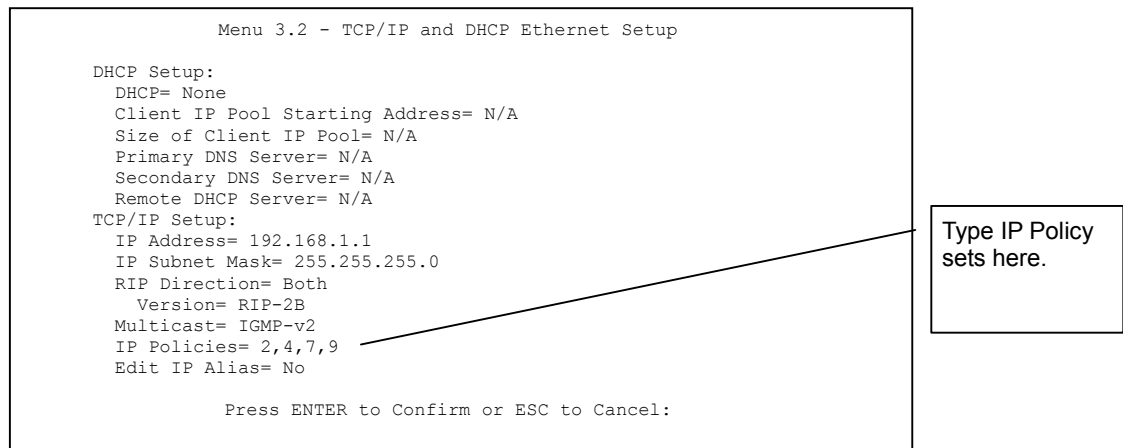


Figure 33-4 TCP/IP and DHCP Ethernet Setup

Go to menu 11.3 (shown next) and type the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by typing their numbers separated by commas.

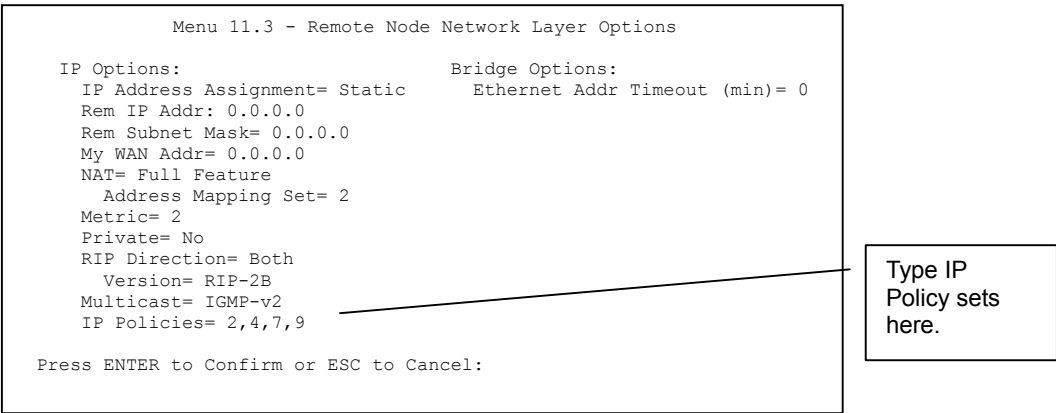


Figure 33-5 Remote Node Network Layer Options

33.4 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

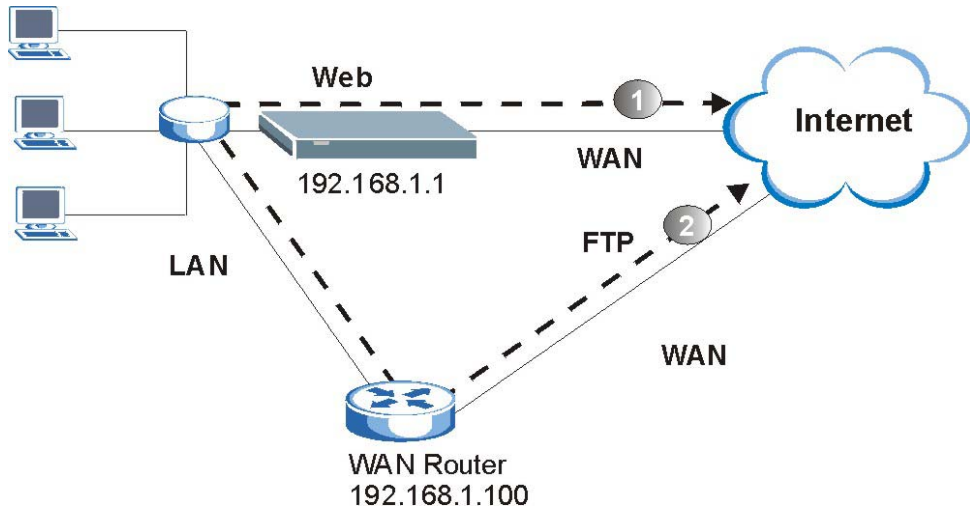


Figure 33-6 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the Prestige, follow the steps as shown next.

Step 1. Create a routing policy set in menu 25.

Step 2. Create a rule for this set in **Menu 25.1.1 — IP Routing Policy** as shown next.

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= set1
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care
  Precedence      = Don't Care
  Source:
    addr start= 192.168.1.2
    port start= 0
  Destination:
    addr start= 0.0.0.0
    port start= 80
  Action= Matched
  Gateway addr  = 192.168.1.1
  Type of Service= No Change
  Precedence    = No Change
  Packet length= 10
  Len Comp= N/A
  end= 192.168.1.64
  end= N/A
  end= N/A
  end= 80
  Log= No

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

```

Figure 33-7 IP Routing Policy Example

- Step 3.** Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.
- Step 4.** Create another policy set in menu 25.
- Step 5.** Create a rule in menu 25.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= set2
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care          Packet length= 10
  Precedence      = Don't Care          Len Comp= N/A
Source:
  addr start= 0.0.0.0                  end= N/A
  port start= 0                        end= N/A
Destination:
  addr start= 0.0.0.0                  end= N/A
  port start= 20                       end= 21
Action= Matched
Gateway addr =192.168.1.100           Log= No
Type of Service= No Change
Precedence   = No Change

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

```

Figure 33-8 IP Routing Policy

Step 6. Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.

Step 7. Apply both policy sets in menu 3.2 as shown next.

```

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 64
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
  Version= RIP-1
  Multicast= None
  IP Policies= 1,2
  Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 33-9 Applying IP Policies

Chapter 34

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.

34.1 Call Scheduling Overview

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 video cassette 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**.

34.2 Schedule Setup

From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

Menu 26 - Schedule Setup			
Schedule Set #	Name	Schedule Set #	Name
1	_____	7	_____
2	_____	8	_____
3	_____	9	_____
4	_____	10	_____
5	_____	11	_____
6	_____	12	_____

Enter Schedule Set Number to Configure=

Edit Name=

Press ENTER to Confirm or ESC to Cancel:

Figure 34-1 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(yy/yy/mm/dd) = 2000 - 01 - 01
How Often= Once
Once:
  Date(yy/yy/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 34-2 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 34-1 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

Table 34-1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
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
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	<p>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.</p> <p>Forced Down means that the connection is blocked whether or not there is a demand call on the line.</p> <p>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.</p>	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= ?
Active= Yes

Encapsulation= PPPoE
Multiplexing=VC-based
Service Name=
Incoming
 Rem Login=
 Rem Password= *****

Outgoing=
 My Login=?
 My Password= *****
 Authen= CHAP/PAP

Route= IP
Bridge= No

Edit IP/Bridge= No
Edit ATM Options= No
Telco Option:
 Allocated Budget (min)= 0
 Period (hr)= 0
 Schedules= 1,2,3,4
 Nailed-Up Connection= No

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

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

Apply your
schedule
sets here.

Figure 34-3 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).

Chapter 35

Remote Management

This chapter covers remote management (SMT menu 24.11).

35.1 Remote Management Overview

Remote management setup is for managing Telnet, FTP and Web services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your Prestige from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

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

If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

35.1.1 Remote Management and Telnet Services

You can configure your Prestige for remote Telnet access as shown next.

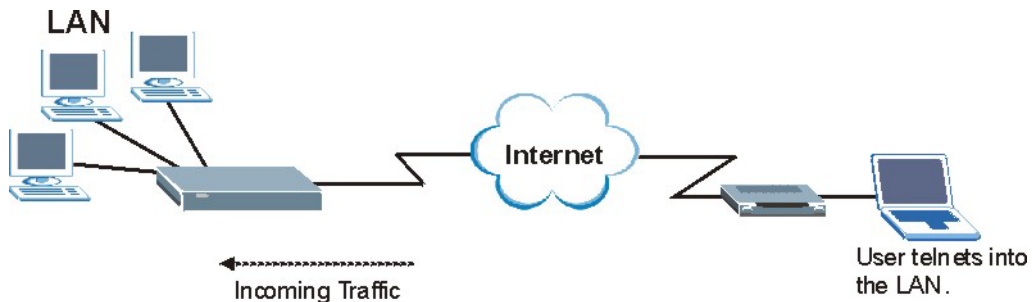


Figure 35-1 Telnet Configuration on a TCP/IP Network

35.1.2 Remote Management and FTP Services

You can upload and download Prestige firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

35.1.3 Remote Management and Web Services

You can use the Prestige’s embedded web configurator for configuration and file management. See the *online help* for details.

35.1.4 Disabling Remote Management

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

35.2 Remote Management Setup

Enter 11 in menu 24 to display **Menu 24.11 — Remote Management Control** (shown next).

```
Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                Server Access = LAN only
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                Server Access = LAN only
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                Server Access = LAN only
  Secured Client IP = 0.0.0.0

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

Figure 35-2 Remote Management Control

Table 35-1 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service that you may use to remotely manage the Prestige.	
Server Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	23
Server Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: LAN only , WAN only , All or Disable . The default is LAN only .	LAN only

Table 35-1 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the 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.		

35.2.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
5. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

35.3 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.

35.4 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your Prestige will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Part X:

SMT VPN/IPSec and Internal SPTGEN

This part provides information about configuring VPN/IPSec for secure communications and Internal SPTGEN for configuration of multiple Prestiges.

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

Chapter 36

VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

36.1 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.

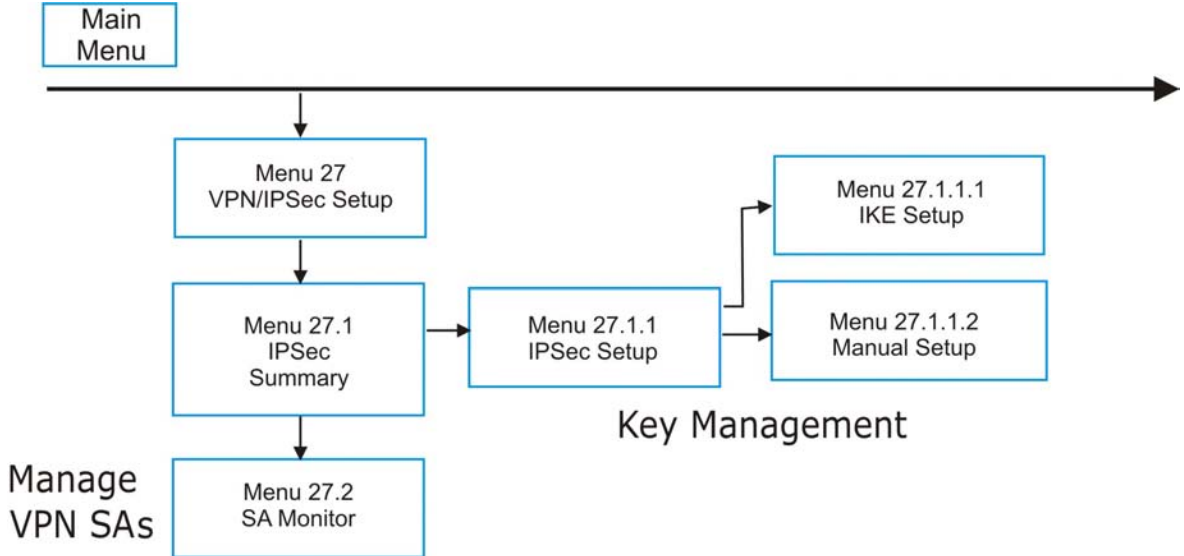


Figure 36-1 VPN SMT Menu Tree

From the main menu, enter 27 to display the first VPN menu (shown next).

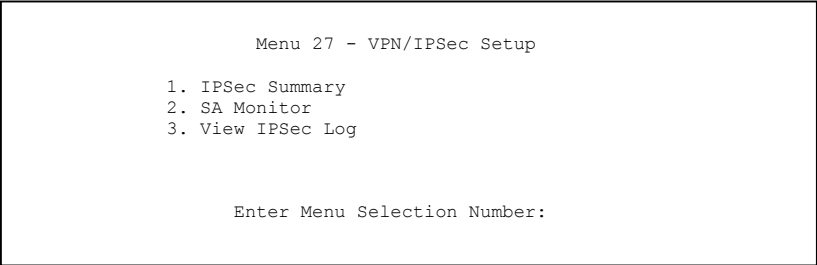


Figure 36-2 Menu 27 VPN/IPSec Setup

36.2 IPSec Summary Screen

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

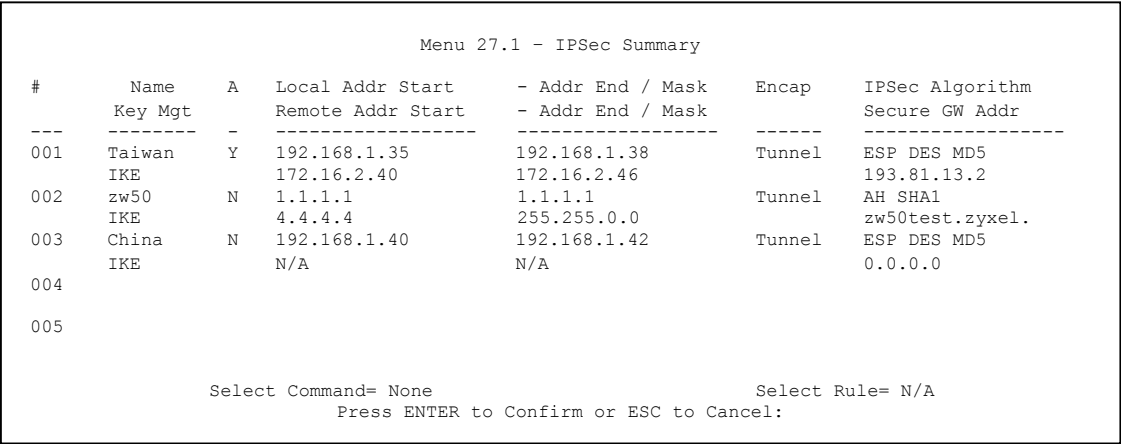


Figure 36-3 Menu 27.1 IPSec Summary

The following table describes the fields in this menu.

Table 36-1 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
#	This is the VPN policy index number.	1

Table 36-1 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
Addr End / Mask	When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Single , this is the same (static) IP address as in the Local Addr Start field. When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Range , this is the end (static) IP address, in a range of computers on the LAN behind your 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 36-1 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>This field displays N/A when you configure the Secure Gateway Addr field in SMT 27.1.1 to 0.0.0.0.</p>	172.16.2.40
Remote Addr End	<p>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.</p> <p>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.</p> <p>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.</p> <p>This field displays N/A when you configure the Secure Gateway Addr field in SMT 27.1.1 to 0.0.0.0.</p>	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 36-1 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Select Command	<p>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.</p> <p>Select None and then press [ENTER] to go to the “Press ENTER to Confirm...” prompt.</p> <p>Use Edit to create or edit a rule. Use Delete to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do <u>not</u> move up in the page list.</p> <p>Use Go To Rule to view the page where your desired rule is listed.</p> <p>Select Next Page or Previous Page to view the next or previous page of rules (respectively).</p>	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.		

36.3 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.

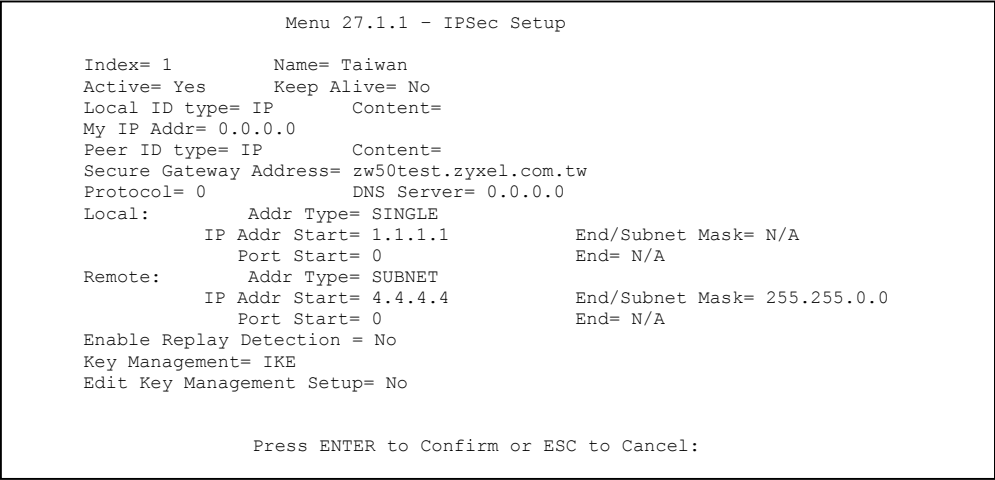


Figure 36-4 Menu 27.1.1 IPSec Setup

The following table describes the fields in this menu.

Table 36-2 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
Local ID type	Press [SPACE BAR] to choose IP , DNS , or E-mail and press [ENTER]. Select IP to identify this Prestige by its IP address. Select DNS to identify this Prestige by a domain name. Select E-mail to identify this Prestige by an e-mail address.	

Table 36-2 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Content	<p>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.</p> <p>When you select DNS in the Local ID Type field, type a domain name (up to 31 characters) by which to identify this Prestige.</p> <p>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.</p> <p>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.</p>	
My IP Addr	<p>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.</p> <p>The VPN tunnel has to be rebuilt if this IP address changes.</p>	0.0.0.0
Peer ID type	<p>Press [SPACE BAR] to choose IP, DNS, or E-mail and press [ENTER].</p> <p>Select IP to identify the remote IPSec router by its IP address.</p> <p>Select DNS to identify the remote IPSec router by a domain name.</p> <p>Select E-mail to identify the remote IPSec router by an e-mail address.</p>	
Content	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	

Table 36-2 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
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
DNS Server	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.	
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0 , the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0 .	
Addr Type	Press [SPACE BAR] to choose SINGLE , RANGE , or SUBNET and press [ENTER]. Select SINGLE with a single IP address. Select RANGE for a specific range of IP addresses. Select SUBNET to specify IP addresses on a network by their subnet mask.	SINGLE
IP Addr Start	When the Addr Type field is configured to Single , enter a static IP address on the LAN behind your Prestige. When the Addr Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige. When the Addr Type is configured to SUBNET , this is a (static) IP address on the LAN behind your Prestige.	192.168.1.35

Table 36-2 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
End/Subnet Mask	<p>When the Addr Type field is configured to Single, this field is N/A.</p> <p>When the Addr Type field is configured to Range, enter the end (static) IP address, in a range of computers on the LAN behind your Prestige.</p> <p>When the Addr Type field is configured to SUBNET, this is a subnet mask on the LAN behind your Prestige.</p>	192.168.1.38
Port Start	<p>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.</p> <p>Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3</p>	0
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is N/A when 0 is configured in the Port Start field.	N/A
Remote	<p>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.</p> <p>Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>	
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	<p>When the Addr Type field is configured to Single, enter a static IP address on the network behind the remote IPSec router.</p> <p>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.</p> <p>When the Addr Type field is configured to SUBNET, enter a static IP address on the network behind the remote IPSec router.</p> <p>This field displays N/A when you configure the Secure Gateway Address field to 0.0.0.0.</p>	4.4.4.4

Table 36-2 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
End/Subnet Mask	<p>When the Addr Type field is configured to Single, this field is N/A.</p> <p>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.</p> <p>When the Addr Type field is configured to SUBNET, enter a subnet mask on the network behind the remote IPSec router.</p> <p>This field displays N/A when you configure the Secure Gateway Address field to 0.0.0.0.</p>	255.255.0.0
Port Start	<p>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.</p> <p>Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.</p>	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	<p>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.</p> <p>Press [SPACE BAR] to select Yes or No. Choose Yes and press [ENTER] to enable replay detection.</p>	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.		

36.4 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= 123456789
Encryption Algorithm= DES
Authentication Algorithm= SHA1
SA Life Time (Seconds)= 28800
Key Group= DH1

Phase 2
Active Protocol   = ESP
Encryption Algorithm = DES
Authentication Algorithm = SHA1
SA Life Time (Seconds)= 28800
Encapsulation    = Tunnel
Perfect Forward Secrecy (PFS)= None

Press ENTER to Confirm or ESC to Cancel:

```

Figure 36-5 Menu 27.1.1.1 IKE Setup

The following table describes the fields in this menu.

Table 36-3 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 (Pre-Shared Key)	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 36-3 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Encryption Algorithm	<p>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.</p> <p>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.</p> <p>Press [SPACE BAR] to choose from 3DES or DES and then press [ENTER].</p>	DES
Authentication Algorithm	<p>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.</p> <p>Press [SPACE BAR] to choose from SHA1 or MD5 and then press [ENTER].</p>	SHA1
SA Life Time (Seconds)	<p>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).</p> <p>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.</p>	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 36-3 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.		

36.5 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.

36.5.1 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 36-4 Active Protocol: Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

36.5.2 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 36-6 Menu 27.1.1.2 Manual Setup

The following table describes the fields in this menu.

Table 36-5 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)	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.	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).	
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	

Table 36-5 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION	EXAMPLE
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)	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.	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 37

SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

37.1 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 User's Guide* on keep alive to have the Prestige renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

37.2 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 37-1 Menu 27.2 SA Monitor

The following table describes the fields in this menu.

Table 37-1 Menu 27.2 SA Monitor

FIELD	DESCRIPTION	EXAMPLE
#	This is the security association index number.	
Name	<p>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.</p> <p>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.</p>	Taiwan
Encap.	This field displays Tunnel mode or Transport mode. See previous for discussion.	Tunnel
IPSec ALgorithm	<p>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.</p> <p>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).</p> <p>Both AH and ESP increase Prestige processing requirements and communications latency (delay).</p>	ESP DES MD5
Select Command	<p>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.</p> <p>Select Next Page or Previous Page to view the next or previous page of rules (respectively).</p>	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.		

37.3 Viewing IPSec Log

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log as shown next. The following figure shows a typical log from the initiator of a VPN connection.

Index:	Date/Time:	Log:
001	01 Jan 08:02:22	Send Main Mode request to <192.168.100.101>
002	01 Jan 08:02:22	Send:<SA>
003	01 Jan 08:02:22	Recv:<SA>
004	01 Jan 08:02:24	Send:<KE><NONCE>
005	01 Jan 08:02:24	Recv:<KE><NONCE>
006	01 Jan 08:02:26	Send:<ID><HASH>
007	01 Jan 08:02:26	Recv:<ID><HASH>
008	01 Jan 08:02:26	Phase 1 IKE SA process done
009	01 Jan 08:02:26	Start Phase 2: Quick Mode
010	01 Jan 08:02:26	Send:<HASH><SA><NONCE><ID><ID>
011	01 Jan 08:02:26	Recv:<HASH><SA><NONCE><ID><ID>
012	01 Jan 08:02:26	Send:<HASH>
Clear IPSec Log (y/n):		

Figure 37-2 Example VPN Initiator IPSec Log

37.3.1 VPN Responder IPSec Log

The following figure shows a typical log from the VPN connection peer.

Index:	Date/Time:	Log:
001	01 Jan 08:08:07	Recv Main Mode request from <192.168.100.100>
002	01 Jan 08:08:07	Recv:<SA>
003	01 Jan 08:08:08	Send:<SA>
004	01 Jan 08:08:08	Recv:<KE><NONCE>
005	01 Jan 08:08:10	Send:<KE><NONCE>
006	01 Jan 08:08:10	Recv:<ID><HASH>
007	01 Jan 08:08:10	Send:<ID><HASH>
008	01 Jan 08:08:10	Phase 1 IKE SA process done
009	01 Jan 08:08:10	Recv:<HASH><SA><NONCE><ID><ID>
010	01 Jan 08:08:10	Start Phase 2: Quick Mode
011	01 Jan 08:08:10	Send:<HASH><SA><NONCE><ID><ID>
012	01 Jan 08:08:10	Recv:<HASH>
Clear IPSec Log (y/n):		

Diagram 37-1 Example VPN Responder IPSec Log

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message is displayed.

Double exclamation marks (!!) denote an error or warning message.

Chapter 38

Internal SPTGEN

38.1 Internal SPTGEN Overview

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple Prestiges. Internal SPTGEN lets you configure, save and upload multiple menus at the same time using just one configuration text file – eliminating the need to navigate and configure individual SMT menus for each Prestige.

38.2 The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

```
<field identification number = field name = parameter values allowed =  
input>,
```

where <input> is your input conforming to <parameter values allowed>.

The figure shown next is an example of an Internal SPTGEN text file.

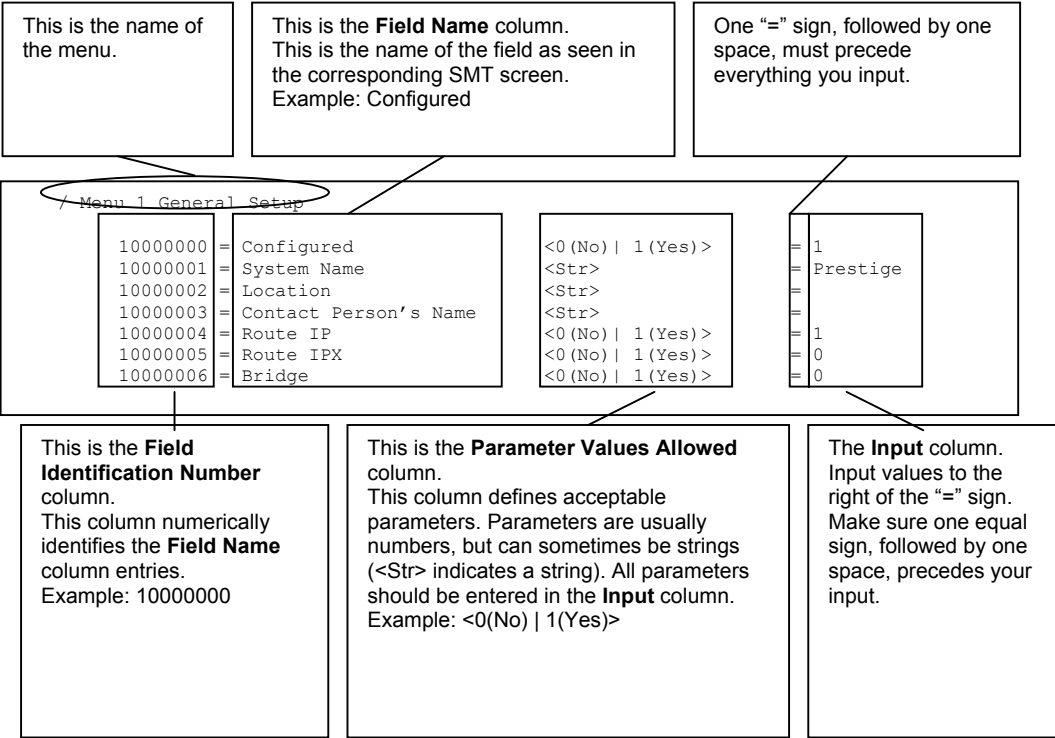


Figure 38-1 Configuration Text File Format: Column Descriptions

DO NOT alter or delete any field except parameters in the Input column.

For more text file examples, refer to the *Example Internal SPTGEN Screens Appendix*.

38.2.1 Internal SPTGEN File Modification - Important Points to Remember

- Each parameter you enter must be preceded by one “=” sign and one space.
- Some parameters are dependent on others. For example, if you disable the **Configured** field in menu 1 (see *Figure 38-1*), then you disable every field in this menu.
- If you enter a parameter that is invalid in the **Input** column, the Prestige will not save the configuration and the command line will display the **Field Identification Number**. *Figure 38-2*, shown next, is an example of what the Prestige displays if you enter a value other than “0” or “1” in the **Input** column of **Field Identification Number** 1000000 (refer to *Figure 38-1*).


```

field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2

```

Figure 38-2 Invalid Parameter Entered: Command Line Example

The Prestige will display the following if you enter parameter(s) that *are* valid.

```

Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2

```

Figure 38-3 Valid Parameter Entered: Command Line Example

38.3 Internal SPTGEN FTP Download Example

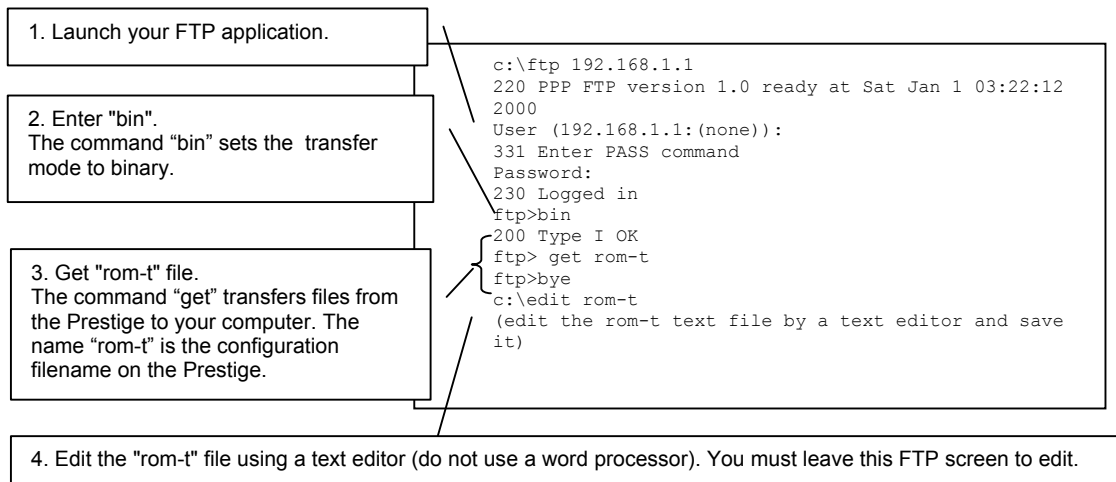


Figure 38-4 Internal SPTGEN FTP Download Example

You can rename your "rom-t" file when you save it to your computer but it must be named "rom-t" when you upload it to your Prestige.

38.4 Internal SPTGEN FTP Upload Example

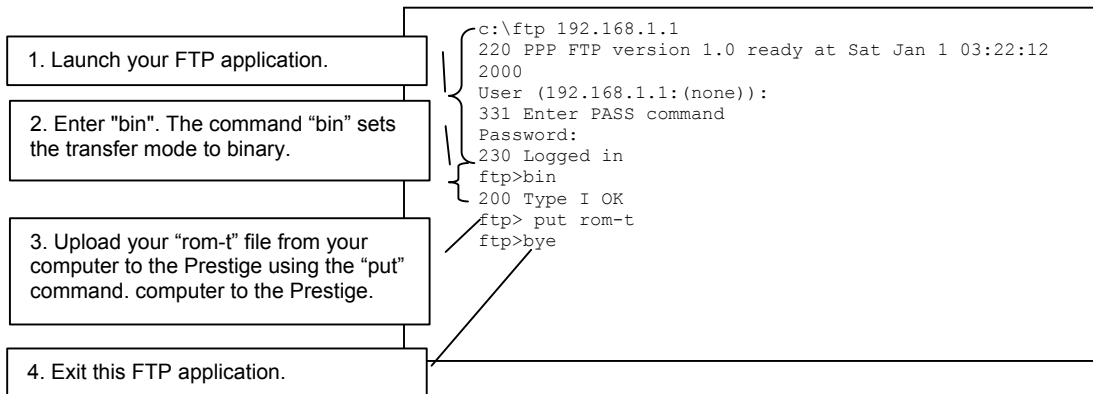


Figure 38-5 Internal SPTGEN FTP Upload Example

Part XI:

Appendices and Index

This section provides some Appendices and an Index.

Appendix A

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

Problems Starting Up the Prestige

Table A-1 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION	
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adapter is connected to the Prestige and plugged in to an appropriate power source. Check that the Prestige and the power source are both turned on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
I cannot access the Prestige via the console port.	1. Make sure the Prestige is connected to your computer's serial port.	
	2. Make sure the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation.
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
		No parity, 8 data bits, 1 stop bit, data flow set to none.

Problems with the LAN Interface

Table A-2 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige from the LAN.	If the 10M/100M LEDs on the front panel are off, check the Ethernet cable connections between your Prestige and computer.
	Check for faulty Ethernet cables.
	Make sure your NIC (Network Interface Card) is installed and functioning properly.
	Check the TCP/IP configuration on your computer. Make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.

Problems with the WAN Interface

Table A-3 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The WAN IP is provided when the ISP recognizes the user as an authorized user after verifying the MAC address, Host Name or User ID. Find out the verification method used by your ISP.
	If the ISP checks the host name, enter your computer's name in the System Name field in Menu 1 — General Setup .
	If the ISP checks the User ID, make sure that you have entered the correct user name (in the My Login field) and password (in the My Password field) in Menu 4 — Internet Access Setup .
I cannot connect to a remote node or ISP.	Check menu 4 or menu 11.1 to verify the Encapsulation for the remote node.

Problems with Internet Access

Table A-4 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet	Verify your settings in menu LAN and Internet settings.
	Make sure the Prestige is turned on and connected to the network. If the Prestige's DSL LED is off, check the cable between the Prestige and the telephone wall jack.
	Make sure you entered your user name and password correctly. Your username and password may be case-sensitive.
Internet connection disconnects	Check the schedule rules in SMT menu 26.
	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting in SMT menu 11.5.
	If the problem persists, contact your ISP.

Problems with Passwords

Table A-5 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	<p>The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.</p> <p>Restore the factory default configuration file. This will restore all of the factory defaults including the password. Refer to the <i>Reset Button</i> section in the <i>User's Guide</i> for details.</p>

Problems with Telnet

Table A-6 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige from the LAN or WAN.	Refer to the <i>Remote Management Limitations</i> section for scenarios when remote management may not be possible.
	<p>When NAT is enabled:</p> <ul style="list-style-type: none">➤ Use the Prestige's WAN IP address when configuring from the WAN.➤ Use the Prestige's LAN IP address when configuring from the LAN.
	Refer to the <i>Problems with the LAN Interface</i> section in Troubleshooting for instructions on checking your LAN connection.
	Refer to the <i>Problems with the WAN Interface</i> section in Troubleshooting for instructions on checking your WAN connection.

Appendix B

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.

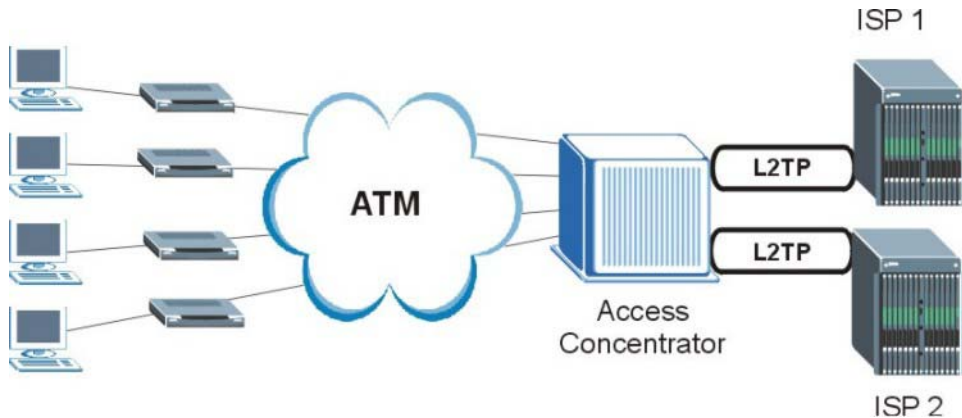


Diagram B-1 Single-PC per Modem Hardware Configuration

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.

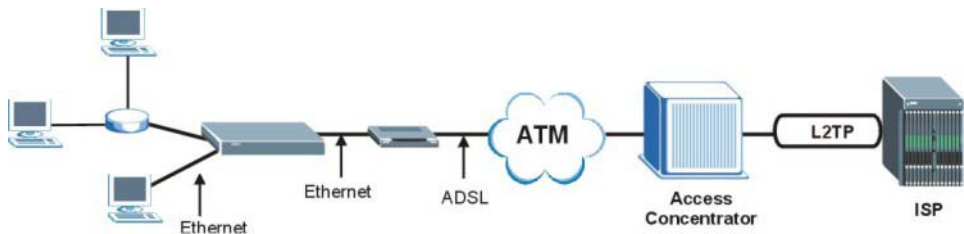


Diagram B-2 The Prestige as a PPPoE Client

Appendix C

Virtual Circuit Topology

ATM is a connection-oriented technology, meaning that it sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- **Virtual Channel** Logical connections between ATM switches
- **Virtual Path** A bundle of virtual channels
- **Virtual Circuit** A series of virtual paths between circuit end points

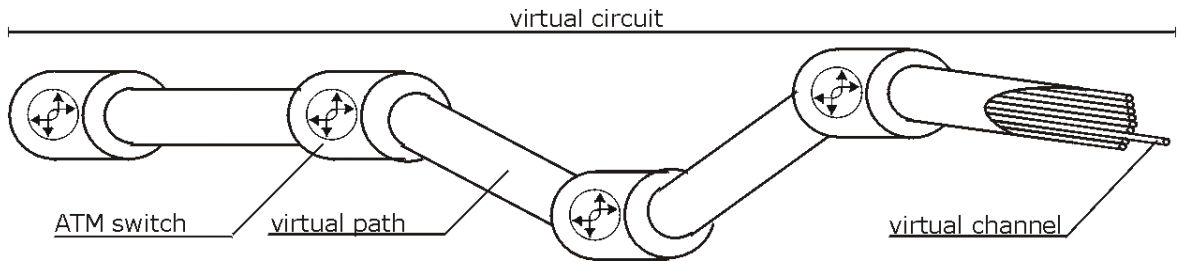


Diagram C-1 Virtual Circuit Topology

Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path.

The VPI and VCI identify a virtual path, that is, termination points between ATM switches. A series of virtual paths make up a virtual circuit.

Your service provider should supply you with VPI/VCI numbers.

Appendix D

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.

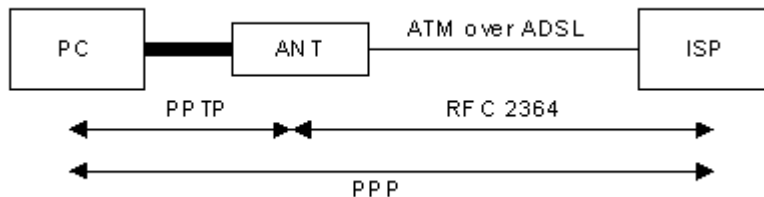


Diagram D-1 Transport PPP frames over Ethernet

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 – NAT Server 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 D-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.

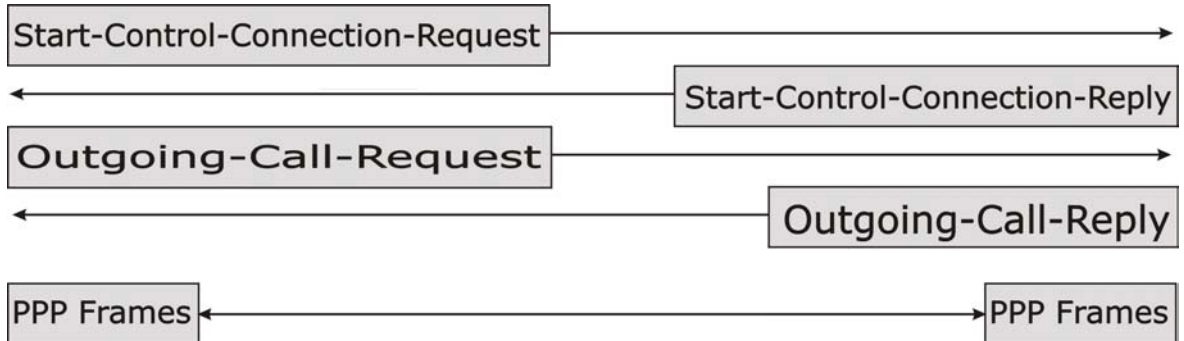


Diagram D-3 Example Message Exchange between PC and an ANT

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 E

Index

1	
10/100 MB Auto-negotiation	1-3
A	
Action for Matched Packets	10-13
Active.....	21-5, 21-7
Address Assignment	4-2
ADSL, what is it?.....	xxxi
Allocated Budget	21-6
Application Scenario.....	1-5
Application-level Firewalls.....	8-1
AT command	21-2, 21-3, 31-1
Attack Alert...9-2, 9-3, 9-5, 9-6, 10-5, 12-5, 14-27	
Attack Types	8-6
Authen.....	21-5
Authentication.....	5-12, 21-5, 24-4
auto-negotiation	1-3
B	
Backup	31-2
Blocking Time	9-5
Bridging	
Ether Address	26-3
Ethernet.....	26-1
Ethernet Addr Timeout.....	26-2
Remote Node	26-1
Static Route Setup.....	26-2
Brute-force Attack.....	8-6
Budget Management	32-2, 32-3
C	
Call Back Delay	21-4
Call Filtering	28-1
Call Filters	
Built-In	28-1
User-Defined	28-1
Call Scheduling.....	34-1
Maximum Number of Schedule Sets.....	34-1
PPPoE.....	34-3
Precedence.....	34-1
Precedence Example.....	See precedence
Canada	iv
Caution.....	iv
CDR.....	30-7
CDR (Call Detail Record).....	30-6
CHAP	21-5, 24-4
CHAP (Challenge Handshake Authentication Protocol).....	1-3
Collision.....	30-3
Command Interpreter Mode.....	32-1
Community	29-2
Computer Name.....	19-1
Conditions that prevent TFTP and FTP from working over WAN	31-4
Configuration.....	3-15, 17-6
Content Filtering.....	12-1
Categories.....	12-1
Exempt Computers	12-4
Keywords	12-1, 12-3
Copyright.....	ii
Cost Of Transmission	24-7, 25-3
Country Code.....	30-4
CPU Load	30-3
Custom Ports	
Creating/Editing	11-2
Introduction	11-1
Customer Support	vi

Customized Services..... 11-2

D

Data Filtering..... 28-1
 Default Policy Log..... 10-8
 Denial of Service 8-2, 8-3, 9-4, 9-5
 Destination Address..... 10-3, 10-13
 Device Filter rules..... 28-16
 DHCP 1-3, 3-15, 4-2, 4-3, 7-1, 17-6, 30-4
 Diagnostic 30-8
 Diagnostic Tools..... 30-1
 Dial Timeout..... 21-4
 DNS 22-5
 Domain Name..... 4-2, 6-6
 Domain Name System 4-1
 DoS
 Basics 8-3
 Types 8-4
 DoS (Denial of Service)..... 1-2
 Drop Timeout 21-4
 DSL (Digital Subscriber Line).....xxxi
 DSL, What Is It?xxxi
 DTR 5-18, 21-3
 Dynamic DNS..... 7-1, 19-2
 DYNDNS Wildcard..... 7-1

E

ECHO 6-6
 Edit IP..... 21-6
 Encapsulation..... 1-3, 3-2, 23-2, 24-2
 ENET ENCAP..... 3-2
 PPP over Ethernet..... B-1, 3-2
 PPPoA 3-3
 RFC 1483 3-3
 ENET ENCAP 1-3
 Error Log 30-5
 Error/Information Messages
 Sample..... 30-6
 Ethernet..... 22-1
 Ethernet Encapsulation 6-5
 Ethernet Traffic..... 28-21

Ethernet/802.3 bridged 1-5

F

Factory LAN Defaults 4-3
 FCCiii
 Features 1-1
 Filename Conventions..... 31-1
 Filter 21-9, 28-1
 Applying Filters 28-20
 Ethernet Setup 22-1
 Ethernet traffic 28-21
 Ethernet Traffic 28-20
 Filter Rules 28-8
 Filter Structure 28-4
 Generic Filter Rule 28-14
 Remote Node..... 24-8
 Remote Node Filter 24-8
 Remote Node Filters 28-21
 SUA..... 28-16
 TCP/IP Filter Rule..... 28-10
 Filter Log 30-7, 30-8
 Filter Rule Process..... 28-3
 Filter Rule Setup..... 28-9
 Filter Rules Summary
 Sample..... 28-18, 28-19, 28-20
 Filter Set
 Class 28-9
 Filter Set Configuration..... 28-4
 Filtering 28-1, 28-9
 Filtering Process
 Outgoing Packets 28-2
 Finger 6-6
 Firewall
 Address Type 10-14
 Alerts..... 9-4
 Connection Direction 10-3
 Creating/Editing Rules 10-11
 Custom Ports See Custom Ports
 Enabling 9-1
 Firewall Vs Filters..... 8-12
 Guidelines For Enhancing Security..... 8-11

Gateway.....	33-5
IP Pool Setup	3-16
IP Ports	36-9, 36-10
IP Protocol.....	33-4
IP Routing Policy (IPPR).....	33-1
Benefits.....	33-1
Cost Savings.....	33-1
Criteria.....	33-1
Load Sharing	33-1
Setup.....	33-2
IP Routing Policy Setup.....	33-3
IP Spoofing	8-4, 8-7
IP Static Route	25-1
IP Static Route Setup	25-2
IP Subnet Mask.....	21-8
Remote	21-8
IPSec Setup.....	36-5
IPSec standard	1-2
IPSec VPN Capability	1-2

K

Key Fields For Configuring Rules.....	10-2
---------------------------------------	------

L

LAN.....	30-2, 30-3
LAN Setup.....	4-1, 5-1
LAN TCP/IP	4-2
LAN to WAN Rules	10-3
LAND.....	8-4, 8-6
Link type.....	30-2
LLC-based Multiplexing.....	24-10
Local Network	
Rule Summary.....	10-7
Log and Trace.....	30-6
Log Facility.....	30-7
Logging Option.....	28-12, 28-15
Login.....	24-3

M

MAC address	26-3
Main Menu	18-4

Management Information Base (MIB)	29-2
Max-incomplete High.....	9-4
Max-incomplete Low	9-4
MBS	See Maximum Burst Size
Media Access Control	26-1
Message Logging	30-5
Metric	5-1, 21-8, 24-7, 25-3
Multicast.....	4-3, 21-9, 24-7
Multiple Protocol over ATM.....	1-3
Multiplexing	
LLC-based.....	3-3
VC-based.....	3-3
Multiplexing	3-3, 23-2, 24-2
Multiprotocol Encapsulation	3-3
My Login.....	21-5
My Password	21-5
My WAN Address.....	21-8, 24-6

N

Nailed-Up Connection.....	3-8, 21-6
NAT.....	3-7, 6-5, 6-7, 21-8, 28-16
Application.....	6-2
Applying NAT in the SMT Menus.....	27-1
Configuring	27-3
Definitions.....	6-1
Examples	27-11
How NAT Works	6-2
Mapping Types	6-3
Non NAT Friendly Application Programs.....	27-18
Ordering Rules	27-6
Server Sets.....	6-5
What NAT does.....	6-1
NAT Traversal.....	16-1
NetBIOS commands.....	8-7
Network Address Translation.....	23-3
Network Address Translation (NAT)	27-1
Network Management	1-4, 6-6
NNTP	6-6

O

One-Minute High	9-4
-----------------------	-----

P

Packet	
Error.....	30-2
Received	30-3
Transmitted	30-2
Packet Filtering	8-13
Packet Filtering Firewalls	8-1
Packet Triggered	30-7
Packets	30-2
PAP	21-5, 24-4
PAP (Password Authentication Protocol)	1-3
Password	2-3, 18-1, 18-6, 24-4, 29-2
Period(hr)	21-6
Ping	30-9
Ping of Death	8-4
Point-to-Point.....	xxxi
Point-to-Point Tunneling Protocol	6-6
policy-based routing.....	33-1
POP3	6-6, 8-3, 8-4
Port Configuration.....	11-3
Port Numbers	6-5
PPP	21-7
PPP Encapsulation	24-10
PPP Log	30-7, 30-8
PPP over ATM.....	1-3
PPPoA	24-2
PPTP	6-6
PPTP and the Prestige	D-1
PPTP Protocol Overview	D-2
PPTP, What is it?	D-1
Precedence	33-1, 33-4
Prestige as a PPPoE Client.....	B-3
Prestige Firewall Application.....	8-3
Private	21-9, 24-7, 25-3
Protocol	28-11
Protocol Filter Rules	28-16
Protocols Supported	1-3
PSK	36-11

Q

Quality of Service	33-1
--------------------------	------

Quick Start Guide	2-1, 16-2
-------------------------	-----------

R

RAS	30-4, 33-2
Rate	
Receiving.....	30-2
Transmission	30-2
Read Me First	xxix
Related Documentation.....	xxix
Rem IP Address	21-8
Rem Node Name.....	21-5, 21-7
Remote DHCP Server.....	22-5
Remote Management	
Firewall.....	9-1
Remote Management and NAT	15-1
Remote Management Limitations.....	15-1, 35-3
Remote Management Setup	35-2
Remote Node	24-1, 30-2
Remote Node Setup.....	24-1, 24-2
Remote Node Filter.....	21-9
Remote Node Index Number	30-2
Remote Node Traffic	28-21
Required fields.....	18-4
Restore Configuration.....	31-7
retry count.....	21-4
retry interval	21-4
RFC-1483	1-3, 1-5, 24-2
RFC-2364	1-3, 24-2, 24-3
RIP.....	21-9, 22-5, 24-7. See Routing Information Protocol
Routing Information Protocol.....	4-3
Direction.....	4-3
Version	4-3
Routing Policy	33-1
Rule Summary	10-6, 11-6
Rules	10-1, 10-4
Checklist.....	10-1
Creating Custom.....	10-1
Key Fields	10-2
LAN to WAN	10-3
Logic.....	10-1

Predefined Services	10-8
Source and Destination Addresses	10-13
Summary	10-6
Timeout	10-14

S

SA Monitor	37-1
Sample IP Addresses	24-8
Saving the State	8-7
Scalability	1-1
Schedule Sets	
Duration	34-2
SCR	See Sustain Cell Rate
Security	1-3
Security Association	37-1
Security In General	8-11
Security Ramifications	10-2
Server	6-4, 27-3, 27-5, 27-8, 27-9, 27-10, 27-13, 27-14, 32-5
Service	v, 10-2
Service Type	11-3, 20-2
Services	6-5, 6-6
Session Initiation Protocol	1-4
setup a schedule	34-2
SIP	1-4
SMT Menu Overview	18-2
SMTP	6-6
Smurf	8-6
SNMP	1-2, 6-6
Community	29-3
Configuration	29-2
Get	29-2
Manager	29-2
MIBs	29-2
Trap	29-2
Trusted Host	29-3
Source & Destination Addresses	10-13
Source Address	10-3, 10-12
Source-Based Routing	33-1
Speed	1-1
SPI	36-13

Stateful Inspection	1-2, 8-1, 8-2, 8-7, 8-8
Prestige	8-9
Process	8-8
Static Routing Topology	25-1
SUA	1-3, 6-5, 6-6
SUA (Single User Account)	See NAT
Subnet Mask	3-6, 4-3, 10-14, 21-8, 22-5, 24-6, 25-3, 30-4
Supporting Disk	xxix
SYN Flood	8-4, 8-5
SYN-ACK	8-5
Syntax Conventions	xxix
Syslog	11-3, 30-6
Syslog IP Address	30-7
Syslog Server	30-6
System	
Console Port Speed	30-5
Diagnostic	30-8
Log and Trace	30-5
Syslog and Accounting	30-6
System Information	30-3
System Status	30-1
System Information	30-3
System Maintenance	30-1, 30-3, 31-2, 31-5, 31-13, 31-14, 32-1, 32-2, 32-4
System Management Terminal	18-4
System Parameter Table Generator	38-1
System Status	30-2
System Timeout	15-2, 35-3

T

TCP Maximum Incomplete	9-5
TCP Security	8-10
TCP/IP	8-3, 8-4, 15-2, 21-7, 28-16, 30-9, 35-1
TCP/IP Options	24-9
Teardrop	8-4
Telnet	15-2, 35-1
Telnet Configuration	15-2, 35-1
Telnet Under NAT	35-1
Text File Format	38-1
TFTP	

And FTP Over WAN	35-3
Restrictions	35-3
TFTP and FTP over WAN Will Not Work	
When	31-4
TFTP and FTP Over WAN	15-1
TFTP File Transfer	31-12
TFTP Restrictions	15-1, 31-4
Three-Way Handshake	8-5
Threshold Values	9-4
Time and Date Setting	32-4, 32-5
Time Zone	32-5
Timeout	10-14, 10-15, 21-6
TOS (Type of Service)	33-1
Trace Records	30-5
Traceroute	8-7
Traffic Redirect	5-8, 5-9
Type of Service	33-1, 33-3, 33-4, 33-5

U

UDP/ICMP Security	8-10
Universal Plug and Play	16-1
Application	16-1
Security issues	16-1
Universal Plug and Play Forum	16-2
UNIX Syslog	30-5, 30-7
UNIX syslog parameters	30-6
Upload Firmware	31-10
UPnP	See Universal Plug and Play
Upper Layer Protocols	8-10, 8-11

User Name	7-2
-----------------	-----

V

VC-based Multiplexing	24-2, 24-10
Virtual Private Network	1-2
VoIP	1-4
VPI & VCI	3-4
VPN/IPSec Setup	36-1

W

WAN Setup	3-1, 20-1, 20-2
WAN to LAN Rules	10-4
Web Configurator ...	2-1, 2-2, 2-3, 8-2, 8-11, 10-2, 16-2
What is PPTP?	D-1
Wizard Setup	3-1

X

XMODEM protocol	31-2
-----------------------	------

Z

ZyNOS	31-1, 31-2
ZyNOS F/W Version	31-1
ZyXEL Limited Warranty	
Note	v
ZyXEL's Firewall	
Introduction	8-2