

Prestige 202H Plus

ISDN Internet Access Router

User's Guide

Version 3.40

December 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

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

Federal Communications Commission (FCC) Interference Statement

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

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a CLASS B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the receiver.

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

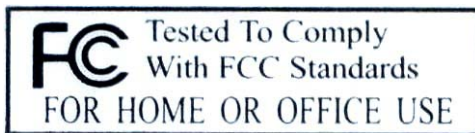
Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Certifications

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



Information for Canadian Users

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

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

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

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

Caution

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

Note

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

ZyXEL Limited Warranty

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

NOTE

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

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



Online Registration

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

Customer Support

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

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

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE ¹ / FAX ¹	WEB SITE / FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Niils 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

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

Table of Contents

- Copyright.....ii**
- Federal Communications Commission (FCC) Interference Statement..... iii**
- Information for Canadian Users.....iv**
- ZyXEL Limited Warranty.....v**
- Customer Support.....vi**
- List of Figures..... xiii**
- List of Tables.....xix**
- Preface..... xxiii**
- Getting Started I**
- Chapter 1 Getting to Know Your Prestige 1-1**
 - 1.1 Introducing the Prestige 202H Plus..... 1-1
 - 1.2 Features..... 1-1
 - 1.3 Internet Access With the Prestige..... 1-5
- Chapter 2 Introducing the Web Configurator 2-1**
 - 2.1 Web Configurator Overview 2-1
 - 2.2 Accessing Your Prestige Via Web Configurator..... 2-1
 - 2.3 Resetting the Prestige..... 2-2
 - 2.4 Configuring Password..... 2-4
 - 2.5 Navigating the Prestige Web Configurator..... 2-4
- Chapter 3 Wizard Setup 3-1**
 - 3.1 Wizard Setup Introduction 3-1
 - 3.2 IP Address and Subnet Mask..... 3-1
 - 3.3 IP Address Assignment..... 3-2
 - 3.4 NAT..... 3-2
 - 3.5 MSN (Multiple Subscriber Number) and Subaddress..... 3-2
 - 3.6 PABX Outside Line Prefix 3-3
 - 3.7 Wizard Setup Configuration: First Screen..... 3-3
 - 3.8 Wizard Setup Configuration: Second Screen 3-5
 - 3.9 Wizard Setup Configuration: Third Screen 3-8
 - 3.10 DHCP Setup 3-9
 - 3.11 Wizard Setup Configuration: Connection Tests 3-11
 - 3.12 Test Your Internet Connection..... 3-12
- Advanced Settings.....II**
- Chapter 4 LAN Settings..... 4-1**
 - 4.1 LAN Overview..... 4-1
 - 4.2 DHCP Setup..... 4-1
 - 4.3 IP Address and Subnet Mask..... 4-1
 - 4.4 DNS Server Address Assignment..... 4-2
 - 4.5 LAN TCP/IP..... 4-2

4.6	Configuring IP	4-2
Chapter 5	WAN Setup	5-1
5.1	WAN Overview.....	5-1
5.2	Configuring WAN Setup.....	5-1
Chapter 6	Network Address Translation (NAT).....	6-1
6.1	NAT Overview	6-1
6.2	SUA (Single User Account) Versus NAT	6-4
6.3	SUA Server.....	6-5
6.4	Selecting the NAT Mode.....	6-6
6.5	Configuring SUA Server.....	6-7
6.6	Configuring Address Mapping.....	6-9
6.7	Editing an Address Mapping Rule	6-11
Chapter 7	Dynamic DNS.....	7-1
7.1	Dynamic DNS.....	7-1
7.2	Configuring Dynamic DNS	7-1
Chapter 8	Firewalls.....	8-1
8.1	Firewall Overview	8-1
8.2	Types of Firewalls.....	8-1
8.3	Introduction to ZyXEL's Firewall.....	8-2
8.4	Denial of Service	8-3
8.5	Stateful Inspection	8-7
8.6	Guidelines for Enhancing Security with Your Firewall	8-11
8.7	Packet Filtering Vs Firewall	8-12
Chapter 9	Firewall Configuration	9-1
9.1	Remote Management and the Firewall	9-1
9.2	Enabling the Firewall.....	9-1
9.3	E-Mail	9-2
9.4	Attack Alert.....	9-3
Chapter 10	Creating Custom Rules	10-1
10.1	Rules Overview.....	10-1
10.2	Rule Logic Overview.....	10-1
10.3	Connection Direction.....	10-3
10.4	Rule Summary	10-4
10.5	Predefined Services.....	10-6
10.6	Creating/Editing Firewall Rules.....	10-9
10.7	Timeout	10-12
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	Firewall Logs.....	12-1

12.1 Logs Screen 12-1

VPN/IPSec III

Chapter 13 Introduction to IPSec 13-1

13.1 VPN Overview 13-1

13.2 IPSec Architecture 13-3

13.3 Encapsulation 13-4

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

14.3 My IP Address 14-2

14.4 Secure Gateway IP Address 14-3

14.5 Summary Screen 14-3

14.6 Keep Alive 14-6

14.7 NAT Traversal 14-6

14.8 ID Type and Content 14-8

14.9 Pre-Shared Key 14-10

14.10 Editing VPN Rules 14-10

14.11 IKE Phases 14-17

14.12 Configuring Advanced IKE Settings 14-19

14.13 Manual Key Setup 14-23

14.14 Configuring Manual Key 14-24

14.15 Viewing SA Monitor 14-28

14.16 Configuring Global Setting 14-30

14.17 Telecommuter VPN/IPSec Examples 14-31

14.18 Logs 14-34

NetAPI and Supplementary Phone Services IV

Chapter 15 NetAPI 15-1

15.1 NetAPI Overview 15-1

15.1 CAPI 15-1

15.2 Configuring NetAPI 15-1

Chapter 16 Supplementary Phone Services 16-1

16.1 Overview 16-1

16.2 Setting Up Supplemental Phone Service 16-1

16.3 The Flash Key 16-2

16.4 Call Waiting 16-2

16.5 Three Way Calling 16-2

16.6 Call Transfer 16-3

16.7 Call Forwarding 16-4

16.8 Reminder Ring 16-4

16.9 Multiple Subscriber Number (MSN) 16-4

16.10	Using MSN	16-5
16.11	Terminal Portability (Suspend/Resume)	16-5
Maintenance		V
Chapter 17 Maintenance		17-1
17.1	Maintenance Overview	17-1
17.2	System Status Screen	17-1
17.3	DHCP Table Screen	17-6
17.4	Firmware Screen	17-7
17.5	Budget Control	17-9
General SMT Menus		VI
Chapter 18 Introducing the SMT		18-1
18.1	Introduction to the SMT	18-1
18.2	Accessing the Prestige via Console Port	18-1
18.3	Accessing the Prestige via Telnet	18-2
18.4	Navigating the SMT Interface	18-2
18.5	SMT Menu Overview	18-5
18.6	Changing the System Password	18-6
Chapter 19 SMT Menu 1 General Setup		19-1
19.1	General Setup Overview	19-1
19.2	Configuring General Setup	19-1
19.3	Configuring Dynamic DNS	19-2
Chapter 20 ISDN Setup		20-1
20.1	ISDN Setup Overview	20-1
20.2	ISDN Setup	20-3
20.3	NetCAPI	20-7
Chapter 21 Ethernet Setup		21-1
21.1	Ethernet Setup	21-1
21.2	Ethernet TCP/IP and DHCP Server	21-2
21.3	Configuring TCP/IP Ethernet and DHCP	21-2
21.4	IP Alias Setup	21-3
Chapter 22 Internet Access Setup		22-1
22.1	Internet Access Overview	22-1
22.2	Internet Access Setup	22-1
Advanced SMT Applications		VII
Chapter 23 Remote Node Configuration		23-1
23.1	Remote Node Overview	23-1
23.2	Remote Node Setup	23-1
23.3	Outgoing Authentication Protocol	23-6
23.4	PPP Multilink	23-6
23.5	Bandwidth on Demand	23-6
23.6	Editing PPP Options	23-7

- 23.7 LAN-to-LAN Application 23-9
- 23.8 Configuring Network Layer Options 23-11
- 23.9 Configuring Filter..... 23-14
- Chapter 24 Static Route Setup 24-1**
- 24.1 Static Route Overview 24-1
- Chapter 25 Dial-in Setup 25-1**
- 25.1 Dial-in Users Overview..... 25-1
- 25.2 Default Dial-in User Setup..... 25-1
- 25.3 Setting Up Default Dial-in 25-2
- 25.4 Callback Overview..... 25-5
- 25.5 Dial-In User Setup..... 25-5
- 25.6 Telecommuting Application With Windows Example 25-7
- 25.7 LAN-to-LAN Server Application Example..... 25-10
- Chapter 26 Network Address Translation (NAT)..... 26-1**
- 26.1 NAT Overview 26-1
- 26.2 Applying NAT..... 26-1
- 26.3 NAT Setup..... 26-3
- 26.4 Configuring a Server behind NAT..... 26-8
- 26.5 General NAT Examples..... 26-10
- Advanced Management VIII**
- Chapter 27 Filter Configuration 27-1**
- 27.1 Filtering Overview 27-1
- 27.2 Configuring a Filter Set..... 27-4
- 27.3 Configuring a Filter Rule 27-9
- 27.4 Filter Types and NAT 27-16
- 27.5 Example Filter..... 27-16
- 27.6 Applying Filters and Factory Defaults 27-19
- Chapter 28 Enabling the Firewall..... 28-1**
- 28.1 Remote Management and the Firewall..... 28-1
- 28.2 Access Methods 28-1
- 28.3 Using Prestige SMT Menus 28-1
- Chapter 29 SNMP Configuration 29-1**
- 29.1 SNMP Configuration..... 29-1
- 29.2 SNMP Traps 29-2
- Chapter 30 External Server 30-1**
- 30.1 RADIUS..... 30-1
- 30.2 Configure External Server..... 30-2
- Chapter 31 System Information and Diagnosis..... 31-1**
- 31.1 System Status Overview..... 31-1
- 31.2 System Status 31-1
- 31.3 System Information and Console Port Speed..... 31-3

31.4	Log and Trace	31-5
31.5	Accounting Server	31-9
31.6	Call Triggering Packet	31-10
31.7	Diagnostic	31-11
Chapter 32	Firmware and Configuration File Maintenance	32-1
32.1	Filename Conventions	32-1
32.2	Backup Configuration	32-2
32.3	Restore Configuration	32-7
32.4	Uploading Firmware and Configuration Files	32-10
Chapter 33	SMT Menus 24.8 to 24.10	33-1
33.1	Command Interpreter Mode	33-1
33.2	Call Control Support	33-2
33.3	Time and Date	33-6
Chapter 34	Remote Management	34-1
34.1	Remote Management Overview	34-1
34.2	Remote Management	34-1
34.3	Remote Management and NAT	34-3
34.4	System Timeout	34-3
Chapter 35	Call Scheduling	35-1
35.1	Call Scheduling Overview	35-1
35.2	Configuring Call Scheduling	35-1
35.3	Applying Schedule Sets	35-3
Chapter 36	VPN/IPSec Setup	36-1
36.1	VPN/IPSec Overview	36-1
36.2	IPSec Summary	36-2
36.3	IPSec Setup	36-7
36.4	Configuring IKE Settings	36-12
36.5	Manual Key Setup	36-15
Chapter 37	SA Monitor	37-1
37.1	SA Monitor Overview	37-1
Chapter 38	IPSec Log	38-1
38.1	IPSec Logs	38-1
Appendices and Index	IX
	Appendix A Troubleshooting	A
	Appendix B Power Adaptor Specifications	E
	Appendix C IP Subnetting	G
	Appendix D Setting up Your Computer's IP Address	O
	Appendix E Splitters and Microfilters	AA
Index	i

List of Figures

Figure 1-1 Internet Access Application.....	1-5
Figure 1-2 LAN-to-LAN Connection Application.....	1-6
Figure 1-3 Remote Access.....	1-6
Figure 1-4 Secure Internet Access and VPN Application.....	1-7
Figure 2-1 Example Xmodem Upload.....	2-3
Figure 2-2 Reload the Configuration file: Via Console Port.....	2-3
Figure 2-3 Password.....	2-4
Figure 2-4 The Site Map Screen.....	2-5
Figure 3-1 Wizard 1: ISDN Line Set Up.....	3-3
Figure 3-2 Wizard 2: ISP Parameters For Internet Access.....	3-6
Figure 3-3 Wizard 3: Summary.....	3-9
Figure 3-4 Wizard: LAN Configuration.....	3-10
Figure 3-5 Wizard Screen 4.....	3-12
Figure 4-1 LAN Setup.....	4-3
Figure 5-1 Internet Access Setup.....	5-2
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.....	6-6
Figure 6-4 NAT Mode.....	6-7
Figure 6-5 Edit SUA/NAT Server Set.....	6-8
Figure 6-6 Address Mapping Rules.....	6-10
Figure 6-7 Address Mapping Rule Edit.....	6-11
Figure 7-1 DDNS.....	7-2
Figure 8-1 Prestige Firewall Application.....	8-3
Figure 8-2 Three-Way Handshake.....	8-4
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.....	9-5
Figure 10-1 LAN to WAN Traffic.....	10-3
Figure 10-2 WAN to LAN Traffic.....	10-4
Figure 10-3 Firewall Rules Summary: First Screen.....	10-5
Figure 10-4 Creating/Editing A Firewall Rule.....	10-10
Figure 10-5 Adding/Editing Source and Destination Addresses.....	10-12
Figure 10-6 Timeout.....	10-13
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 Log Screen	12-1
Figure 13-1 Encryption and Decryption	13-2
Figure 13-2 IPSec Architecture.....	13-3
Figure 13-3 Transport and Tunnel Mode IPSec Encapsulation.....	13-4
Figure 14-1 IPSec Summary Fields	14-4
Figure 14-2 VPN: Summary	14-4
Figure 14-3 NAT Router Between IPSec Routers.....	14-6
Figure 14-4 VPN Host using Intranet DNS Server Example.....	14-8
Figure 14-5 VPN: Rule Setup (Basic).....	14-11
Figure 14-6 Two Phases to Set Up the IPSec SA.....	14-17
Figure 14-7 VPN IKE: Advanced	14-20
Figure 14-8 Rule Setup: Manual.....	14-25
Figure 14-9 SA Monitor.....	14-29
Figure 14-10 VPN: Global Setting	14-30
Figure 14-11 Telecommuters Sharing One VPN Rule Example.....	14-31
Figure 14-12 Telecommuters Using Unique VPN Rules Example	14-33
Figure 14-13 VPN Logs.....	14-35
Figure 15-1 Configuring NetCAPI	15-2
Figure 15-2 Configuration Example	15-3
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 Firmware Upgrade	17-8
Figure 17-5 Network Temporarily Disconnected.....	17-9
Figure 17-6 Error Message	17-9
Figure 17-7 Budget Control.....	17-10
Figure 18-1 Initial Screen	18-1
Figure 18-2 Login Screen	18-2
Figure 18-3 SMT Main Menu.....	18-4
Figure 18-4 SMT Menu Overview	18-6
Figure 18-5 Menu 23.1 System Password	18-7
Figure 18-6 Menu 23.1 - System Security - Change Password	18-7
Figure 19-1 Menu 1 General Setup.....	19-1
Figure 19-2 Configure Dynamic DNS.....	19-2
Figure 20-1 Prestige Behind a PABX	20-2
Figure 20-2 Menu 2 ISDN Setup.....	20-3

Figure 20-3 Menu 2.1 ISDN Advanced Setup	20-5
Figure 20-4 Loopback Test	20-6
Figure 20-5 Menu 2.2 NetCAPI Setup	20-7
Figure 21-1 Menu 3 Ethernet Setup	21-1
Figure 21-2 Menu 3.1 General Ethernet Setup	21-1
Figure 21-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup	21-2
Figure 21-4 Menu 3.2.1 IP Alias Setup	21-4
Figure 22-1 Menu 4 Internet Access Setup	22-1
Figure 23-1 Menu 11 Remote Node Setup	23-2
Figure 23-2 Menu 11.1 Remote Node Profile	23-2
Figure 23-3 Menu 11.2 Remote Node PPP Options	23-8
Figure 23-4 TCP/IP LAN-to-LAN Application	23-9
Figure 23-5 LAN 1 Setup	23-10
Figure 23-6 LAN 2 Setup	23-10
Figure 23-7 Sample IP Addresses for LAN-to-LAN Connection	23-14
Figure 23-8 Menu 11.5 Remote Node Filter	23-15
Figure 24-1 Sample Static Routing Topology	24-1
Figure 24-2 Menu 12 IP Static Route Setup	24-2
Figure 24-3 Menu 12.1 Edit IP Static Route	24-2
Figure 25-1 Menu 13 Default Dial-in Setup	25-2
Figure 25-2 Menu 13.1 Default Dial-in Filter	25-5
Figure 25-3 Menu 14 Dial-in User Setup	25-6
Figure 25-4 Menu 14.1 Edit Dial-in User	25-6
Figure 25-5 Example of Telecommuting	25-8
Figure 25-6 Configuring Menu 13 for Remote Access	25-9
Figure 25-7 Edit Dial-in-User	25-9
Figure 25-8 Example of a LAN-to-LAN Server Application	25-10
Figure 25-9 LAN 1 LAN-to-LAN Application	25-11
Figure 25-10 LAN 2 LAN-to-LAN Application	25-11
Figure 25-11 Testing Callback With Your Connection	25-12
Figure 25-12 Callback With CLID Configuration	25-13
Figure 25-13 Configuring CLID With Callback	25-13
Figure 25-14 Callback and CLID Connection Test	25-14
Figure 26-1 Applying NAT for Internet Access	26-2
Figure 26-2 Applying NAT to the Remote Node	26-3
Figure 26-3 Menu 15 NAT Setup	26-4
Figure 26-4 Menu 15.1 Address Mapping Sets	26-4
Figure 26-5 Menu 15.1.255 SUA Address Mapping Rules	26-5
Figure 26-6 Menu 15.1.1 Address Mapping Rules First Set	26-6
Figure 26-7 Menu 15.1.1.1 Address Mapping Rule	26-7
Figure 26-8 Menu 15.2 NAT Server Setup	26-9

Figure 26-9 Menu 15.2.1 NAT Server Setup	26-9
Figure 26-10 Multiple Servers Behind NAT Example	26-10
Figure 26-11 NAT Example 1	26-11
Figure 26-12 Menu 4 Internet Access & NAT Example	26-11
Figure 26-13 NAT Example 2	26-12
Figure 26-14 Menu 15.2.1 Specifying an Inside Server	26-12
Figure 26-15 NAT Example 3	26-13
Figure 26-16 Example 3: Menu 11.3	26-14
Figure 26-17 Example 3: Menu 15.1.1.1	26-14
Figure 26-18 Example 3: Final Menu 15.1.1	26-15
Figure 26-19 NAT Example 4	26-16
Figure 26-20 Example 4: Menu 15.1.1.1 Address Mapping Rule	26-17
Figure 26-21 Example 4: Menu 15.1.1 Address Mapping Rules	26-17
Figure 27-1 Outgoing Packet Filtering Process	27-2
Figure 27-2 Filter Rule Process	27-3
Figure 27-3 Menu 21 Filter and Firewall Setup	27-4
Figure 27-4 Menu 21.1 Filter Set Configuration	27-5
Figure 27-5 NetBIOS_WAN Filter Rules Summary	27-6
Figure 27-6 NetBIOS_LAN Filter Rules Summary	27-6
Figure 27-7 Telnet WAN Filter Rules Summary	27-7
Figure 27-8 FTP_WAN Filter Rules Summary	27-7
Figure 27-9 Menu 21.1.7.1 TCP/IP Filter Rule	27-10
Figure 27-10 Executing an IP Filter	27-13
Figure 27-11 Menu 21.1.8.1 Generic Filter Rule	27-14
Figure 27-12 Protocol and Device Filter Sets	27-16
Figure 27-13 Sample Telnet Filter	27-17
Figure 27-14 Sample Filter Menu 21.1.9.1	27-18
Figure 27-15 Sample Filter Rules Summary Menu 21.1.9	27-19
Figure 27-16 Filtering Ethernet Traffic	27-20
Figure 27-17 Filtering Remote Node Traffic	27-21
Figure 28-1 Menu 21 Filter and Firewall Setup	28-1
Figure 28-2 Menu 21.2 Firewall Setup	28-2
Figure 28-3 Example Firewall Log	28-2
Figure 28-4 E-mail Log	28-4
Figure 29-1 Menu 22 SNMP Configuration	29-1
Figure 30-1 RADIUS Server	30-1
Figure 30-2 Menu 23.2 System Security - External Server	30-2
Figure 31-1 Menu 24 System Maintenance	31-1
Figure 31-2 Menu 24.1 System Maintenance Status	31-2
Figure 31-3 Menu 24.2 System Information and Console Port Speed	31-4
Figure 31-4 Menu 24.2.1 System Maintenance Information	31-4

Figure 31-5 Menu 24.2.2 System Maintenance Change Console Port Speed	31-5
Figure 31-6 Menu 24.3 System Maintenance Log and Trace	31-6
Figure 31-7 Sample Error and Information Messages	31-6
Figure 31-8 Menu 24.3.2 System Maintenance Unix Syslog	31-7
Figure 31-9 Menu 24.3.3 System Maintenance Accounting Server	31-10
Figure 31-10 Menu 24.3.4 Call Triggering Packet	31-11
Figure 31-11 Menu 24.4 System Maintenance Diagnostic	31-12
Figure 31-12 Display for a Successful Manual Call	31-13
Figure 32-1 Menu 24.5 System Maintenance – Backup Configuration	32-3
Figure 32-2 FTP Session Example	32-4
Figure 32-3 System Maintenance Backup Configuration	32-6
Figure 32-4 System Maintenance: Starting Xmodem Download Screen	32-7
Figure 32-5 Backup Configuration Example	32-7
Figure 32-6 Successful Backup Confirmation Screen	32-7
Figure 32-7 Telnet into Menu 24.6	32-8
Figure 32-8 Restore Using FTP Session Example	32-9
Figure 32-9 System Maintenance: Restore Configuration	32-9
Figure 32-10 System Maintenance: Starting Xmodem Download Screen	32-9
Figure 32-11 Restore Configuration Example	32-10
Figure 32-12 Successful Restoration Confirmation Screen	32-10
Figure 32-13 - System Maintenance Upload Firmware	32-11
Figure 32-14 Menu 24.7.1 Upload System Firmware	32-11
Figure 32-15 Menu 24.7.2 - System Maintenance – Upload Configuration File	32-12
Figure 32-16 FTP Session Example of Firmware File Upload	32-13
Figure 32-17 Menu 24.7.1 as Seen Using the Console Port	32-14
Figure 32-18 Example Xmodem Upload	32-15
Figure 32-19 Menu 24.7.2 as Seen Using the Console Port	32-16
Figure 32-20 Example Xmodem Upload	32-17
Figure 33-1 Command Mode in Menu 24	33-1
Figure 33-2 Valid Commands	33-2
Figure 33-3 Menu 24.9 Call Control	33-2
Figure 33-4 Menu 24.9.1 Call Control Parameters	33-3
Figure 33-5 Menu 24.9.2 Blacklist	33-4
Figure 33-6 Menu 24.9.1 Budget Management	33-4
Figure 33-7 Menu 24.9.4 Call History	33-5
Figure 33-8 Menu 24: System Maintenance	33-6
Figure 33-9 Menu 24.10 System Maintenance: Time and Date Setting	33-7
Figure 34-1 Menu 24.11 Remote Management Control	34-2
Figure 35-1 Menu 26 Schedule Setup	35-1
Figure 35-2 Menu 26.1 Schedule Set Setup	35-2
Figure 35-3 Applying Schedule Set(s)	35-4

Figure 36-1 VPN SMT Menu Tree	36-1
Figure 36-2 Menu 27 VPN/IPSec Setup	36-2
Figure 36-3 IPSec Summary Fields Illustration.....	36-2
Figure 36-4 Menu 27.1 IPSec Summary.....	36-3
Figure 36-5 Menu 27.1.1 IPSec Setup	36-8
Figure 36-6 Menu 27.1.1.1 IKE Setup.....	36-13
Figure 36-7 Menu 27.1.1.2 Manual Setup	36-15
Figure 37-1 Menu 27.2 SA Monitor	37-1
Figure 38-1 Example VPN Initiator IPSec Log.....	38-1
Figure 38-2 Example VPN Responder IPSec Log.....	38-2

List of Tables

Table 2-1 Password	2-4
Table 2-2 Web Configurator Screens Summary	2-5
Table 3-1 Wizard 1: ISDN Line Set Up	3-4
Table 3-2 Wizard 2: ISP Parameters For Internet Access	3-6
Table 3-3 Wizard: LAN Configuration	3-11
Table 4-1 LAN Setup	4-3
Table 5-1 Internet Access Setup	5-3
Table 6-1 NAT Definitions	6-1
Table 6-2 NAT Mapping Types	6-4
Table 6-3 Services and Port Numbers	6-5
Table 6-4 NAT Mode	6-7
Table 6-5 Edit SUA/NAT Server Set	6-8
Table 6-6 Address Mapping Rules	6-10
Table 6-7 Address Mapping Rule Edit	6-12
Table 7-1 DDNS	7-2
Table 8-1 Common IP Ports	8-3
Table 8-2 ICMP Commands That Trigger Alerts	8-6
Table 8-3 Legal NetBIOS Commands	8-6
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 Rules Summary: First Screen	10-5
Table 10-2 Predefined Services	10-7
Table 10-3 Creating/Editing A Firewall Rule	10-10
Table 10-4 Adding/Editing Source and Destination Addresses	10-12
Table 10-5 Timeout	10-13
Table 11-1 Customized Services	11-2
Table 11-2 Creating/Editing A Customized Service	11-3
Table 12-1 Log Screen	12-2
Table 13-1 VPN and NAT	13-5
Table 14-1 ESP and AH	14-2
Table 14-2 VPN: Summary	14-5
Table 14-3 Local ID Type and Content Fields	14-9
Table 14-4 Peer ID Type and Content Fields	14-9
Table 14-5 Matching ID Type and Content Configuration Example	14-10
Table 14-6 Mismatching ID Type and Content Configuration Example	14-10
Table 14-7 VPN: Rule Setup (Basic)	14-12
Table 14-8 VPN IKE: Advanced	14-21
Table 14-9 Rule Setup: Manual	14-26

Table 14-10 SA Monitor	14-29
Table 14-11 VPN: Global Setting	14-30
Table 14-12 Telecommuters Sharing One VPN Rule Example	14-32
Table 14-13 Telecommuters Using Unique VPN Rules Example.....	14-33
Table 14-14 VPN Logs	14-35
Table 15-1 Configuring NetCAPI	15-2
Table 16-1 Supplemental Services In Europe	16-1
Table 16-2 Phone Flash Commands	16-4
Table 17-1 System Status	17-3
Table 17-2 System Status: Show Statistics	17-4
Table 17-3 DHCP Table	17-7
Table 17-4 Firmware Upgrade	17-8
Table 17-5 Budget Control	17-10
Table 18-1 Main Menu Commands	18-2
Table 18-2 Main Menu Summary	18-4
Table 19-1 Menu 1 General Setup	19-2
Table 20-1 Menu 2 ISDN Setup.....	20-3
Table 20-2 Menu 2.1 ISDN Advanced Setup.....	20-5
Table 20-3 Menu 2.2 NetCAPI Setup	20-7
Table 22-1 Menu 4 Internet Access Setup	22-2
Table 23-1 Menu 11.1 Remote Node Profile	23-3
Table 23-2 BTR vs MTR for BOD	23-7
Table 23-3 Menu 11.2 Remote Node PPP Options	23-8
Table 23-4 TCP/IP-related Fields in Remote Node Profile.....	23-11
Table 23-5 Remote Node Network Layer Options	23-12
Table 23-6 Remote Node Network Layer Options	23-12
Table 24-1 Menu 12.1 Edit IP Static Route	24-2
Table 25-1 Remote Dial-in Users/Remote Nodes Comparison Chart.....	25-1
Table 25-2 Menu 13 Default Dial-in Setup.....	25-2
Table 25-3 Edit Dial-in User.....	25-6
Table 26-1 Applying NAT to the Remote Node.....	26-3
Table 26-2 Menu 15.1.255 SUA Address Mapping Rules	26-5
Table 26-3 Fields in Menu 15.1.1	26-7
Table 26-4 Menu 15.1.1.1 Address Mapping Rule	26-8
Table 27-1 Filter Rules Summary Menu Abbreviations.....	27-8
Table 27-2 Rule Abbreviations Used	27-8
Table 27-3 Menu 21.1.7.1 TCP/IP Filter Rule	27-10
Table 27-4 Menu 21.1.8.1 Generic Filter Rule	27-14
Table 27-5 Filter Sets Table	27-19
Table 28-1 View Firewall Log	28-3
Table 29-1 Menu 22 SNMP Configuration	29-1

Table 29-2 SNMP Traps.....	29-2
Table 29-3 Ports and Permanent Virtual Circuits.....	29-2
Table 30-1 Menu 23.2 System Security - External Server.....	30-2
Table 31-1 Menu 24.1 System Maintenance Status.....	31-2
Table 31-2 Menu 24.2.1 System Maintenance Information.....	31-4
Table 31-3 Menu 24.3.2 System Maintenance Unix Syslog.....	31-7
Table 31-4 System Maintenance Menu Diagnostic.....	31-12
Table 32-1 Filename Conventions.....	32-2
Table 32-2 General Commands for GUI-based FTP Clients.....	32-4
Table 32-3 General Commands for GUI-based TFTP Clients.....	32-6
Table 33-1 Menu 24.9.1 Call Control Parameters.....	33-3
Table 33-2 Menu 24.9.1 Budget Management.....	33-5
Table 33-3 Menu 24.9.4 Call History.....	33-6
Table 33-4 Time and Date Setting Fields.....	33-7
Table 34-1 Menu 24.11 Remote Management Control.....	34-2
Table 35-1 Menu 26.1 Schedule Set Setup.....	35-2
Table 36-1 Menu 27.1 IPSec Summary.....	36-3
Table 36-2 Local ID Type and Content Fields.....	36-6
Table 36-3 Peer ID Type and Content Fields.....	36-6
Table 36-4 Matching ID Type and Content Configuration Example.....	36-7
Table 36-5 Mismatching ID Type and Content Configuration Example.....	36-7
Table 36-6 Menu 27.1.1 IPSec Setup.....	36-8
Table 36-7 Menu 27.1.1.1 IKE Setup.....	36-13
Table 36-8 Menu 27.1.1.2 Manual Setup.....	36-15
Table 37-1 Menu 27.2 SA Monitor.....	37-2
Table 38-1 Sample IKE Key Exchange Logs.....	38-2
Table 38-2 Sample IPSec Logs During Packet Transmission.....	38-4
Table 38-3 RFC-2408 ISAKMP Payload Types.....	38-4

Preface

Congratulations on your purchase of the Prestige 202H Plus ISDN Internet access router.

About This User's Manual

This manual is designed to guide you through the configuration of your Prestige for its various applications. This manual may refer to the Prestige 202H Plus ISDN Internet access router as the Prestige.

You may use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your Prestige. Not all features can be configured through all interfaces.

Related Documentation

- Support Disk
Refer to the included CD for support documents.
- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains general connection and initial configuration instructions.
- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.
- Packing List Card
The Packing List Card lists all items that should have come in the package.
- Certifications
Refer to the product page at www.zyxel.com for information on product certifications.
- ZyXEL Glossary and Web Site
Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback









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

Syntax Conventions

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

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

Graphics Icons Key

 Prestige	 Computer	 Notebook computer
 Server	 Telephone	 Firewall
 Router	 Switch	

Part I:

Getting Started

This part is structured as a step-by-step guide to help you access your Prestige. It covers key features and applications, accessing the web configurator and configuring the wizard screens for initial setup.

Chapter 1

Getting to Know Your Prestige

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

1.1 Introducing the Prestige 202H Plus

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

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

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

1.2 Features

This section describes the Prestige's key features.

IPSec VPN Capability

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

Firewall

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

4-Port Switch

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

Auto-negotiating 10/100 Mbps Ethernet LAN

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

Auto-crossover 10/100 Mbps Ethernet LAN

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

Call Scheduling

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

Network Address Translation (NAT)

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

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

SNMP, a member of the TCP/IP protocol suite, allows you to exchange management information between network devices. Your 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 Alias

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

ISDN Data Link Connections

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

ISDN Basic Rate Interface (BRI) Support

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

Extensive Analog Phone Support

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

Incoming Call Support

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

Outgoing Data Call Bumping Support

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

CLID Callback Support For Dial-In Users

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

TCP/IP and PPP Support

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

Dial-on-Demand

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

PPP Multilink

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

Bandwidth-On-Demand

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

Full Network Management

- ◆ You can access the SMT (System Management Terminal) through a telnet connection or console port.
- ◆ The embedded web configurator is an all-platform web-based utility that allows you to easily access the Prestige's management interface.

Logging and Tracing

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

PAP and CHAP Security

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

DHCP (Dynamic Host Configuration Protocol)

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

Call Control

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

Data Compression

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

Upgrade Firmware via LAN

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

Supplementary Voice Features

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

- ◆ Call Waiting
- ◆ Three Way Calling (Conference Calling)
- ◆ Call Transfer
- ◆ Call Forwarding

◆ Reminder Ring

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

Caller ID Display Services on Analog PSTN Lines

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

1.3 Internet Access With the Prestige

These sections provide example applications for your Prestige.

1.3.1 Internet Access

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

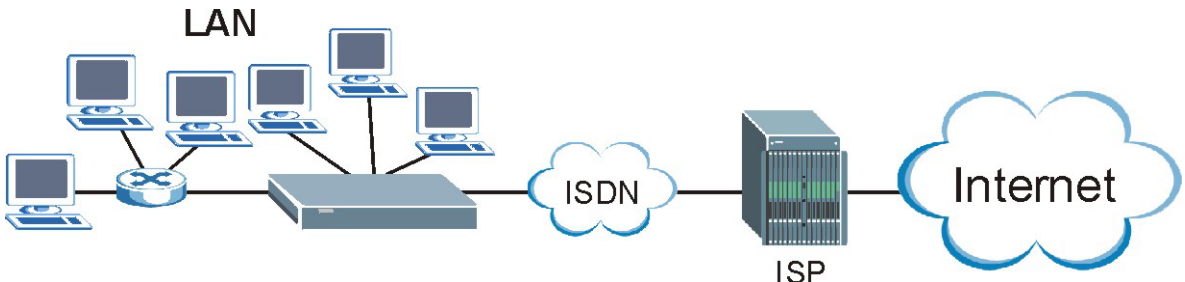


Figure 1-1 Internet Access Application

Internet Single User Account

For a SOHO (Small Office/Home Office) environment, your Prestige offers the NAT (Network Address Translation) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single user. NAT address mapping can also be used for other LAN-to-LAN connections.

1.3.2 LAN-to-LAN Connection

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

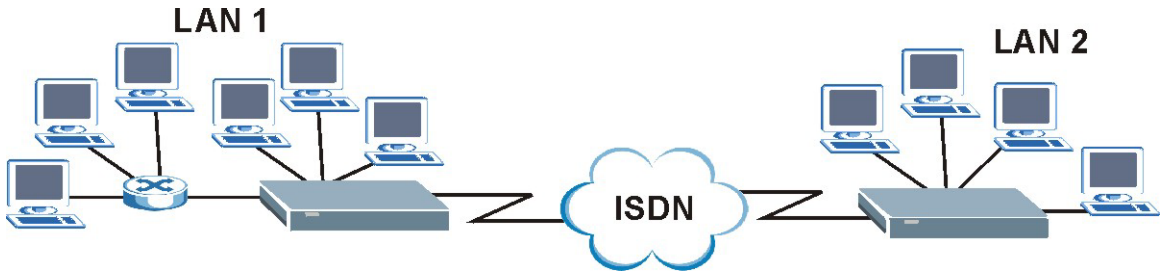


Figure 1-2 LAN-to-LAN Connection Application

1.3.3 Remote Access Server

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

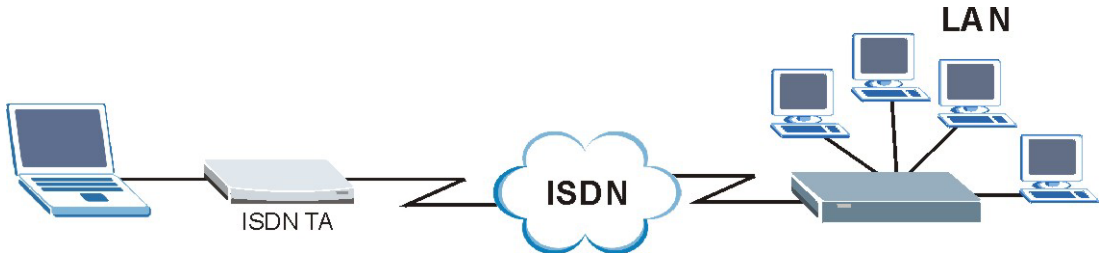


Figure 1-3 Remote Access

1.3.4 Secure Broadband Internet Access and VPN

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

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

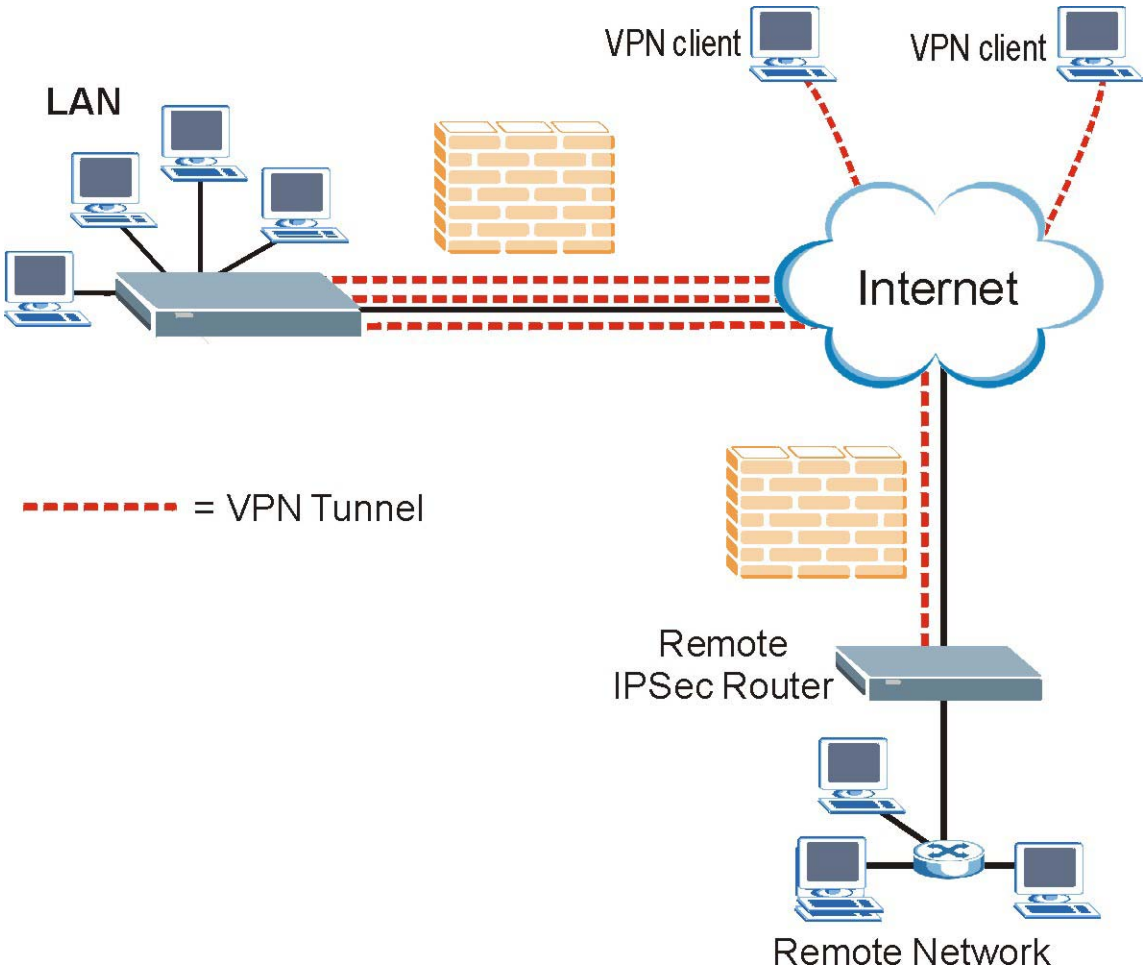


Figure 1-4 Secure Internet Access and VPN Application

Chapter 2

Introducing the Web Configurator

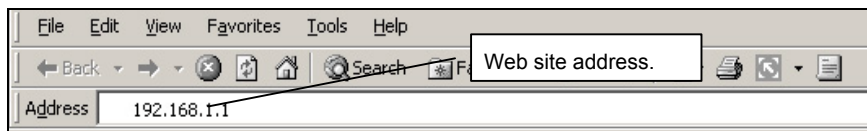
This chapter describes how to access the Prestige web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The embedded web configurator (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 Your Prestige Via Web Configurator

Step 1. Launch your web browser. Enter “192.168.1.1” as the web site address.

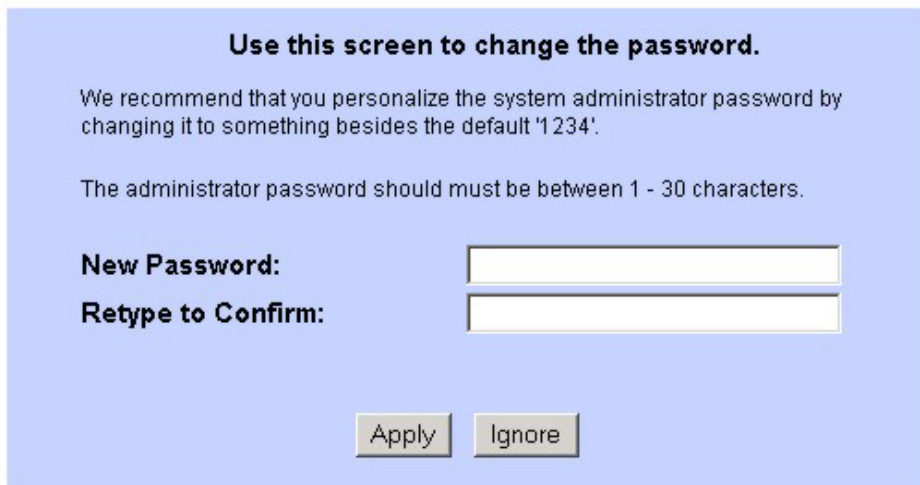


Step 2. Type the password (“1234” is the default), then click **Login** to proceed to the next screen. In some versions, the default password appears automatically - if this is the case, click **Login**.



Step 3. You should see a screen asking you to change your password (highly recommended). Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

If you do not change the password, the following screen appears every time you log in.



Use this screen to change the password.

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

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

New Password:

Retype to Confirm:

Step 4. You should now see the **Site Map** screen (see Figure 2-4).

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

2.3 Resetting the Prestige

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

2.3.1 Uploading a Configuration File Via Console Port

- Step 1.** Download the default configuration file from the ZyXEL Networks FTP site, unzip it and save it in a folder.
- Step 2.** 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 3.** Enter "atlc" after "Enter Debug Mode" message.
- Step 4.** Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.
- Step 5.** Click **Transfer**, then **Send File** to display the following screen.

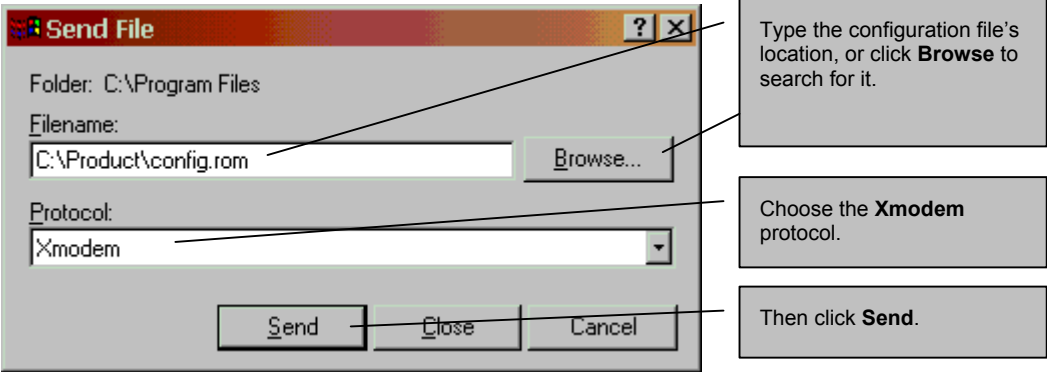


Figure 2-1 Example Xmodem Upload

- Step 6.** After successful firmware upload, enter "atgo" to restart the Prestige.

```
Bootbase Version: V2.09 | 9/26/2002 16:06:05
RAM: Size = 16384 Kbytes
DRAM POST: Testing: 16384K OK
FLASH: AMD 16M

ZyNOS Version: V3.40(QI.0)b5 | 9/7/2004 13:47:04
Press any key to enter debug mode within 3 seconds.
.....
Enter Debug Mode
atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCCCC
Total 16384 bytes received.

Erasing..
....
OK
atgo
```

Figure 2-2 Reload the Configuration file: Via Console Port

2.4 Configuring Password

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

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 Navigating the Prestige Web Configurator

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

Follow the instructions you see in the Site Map screen or click the **HELP ?** icon (located in the top right corner of most screens) to view online help.

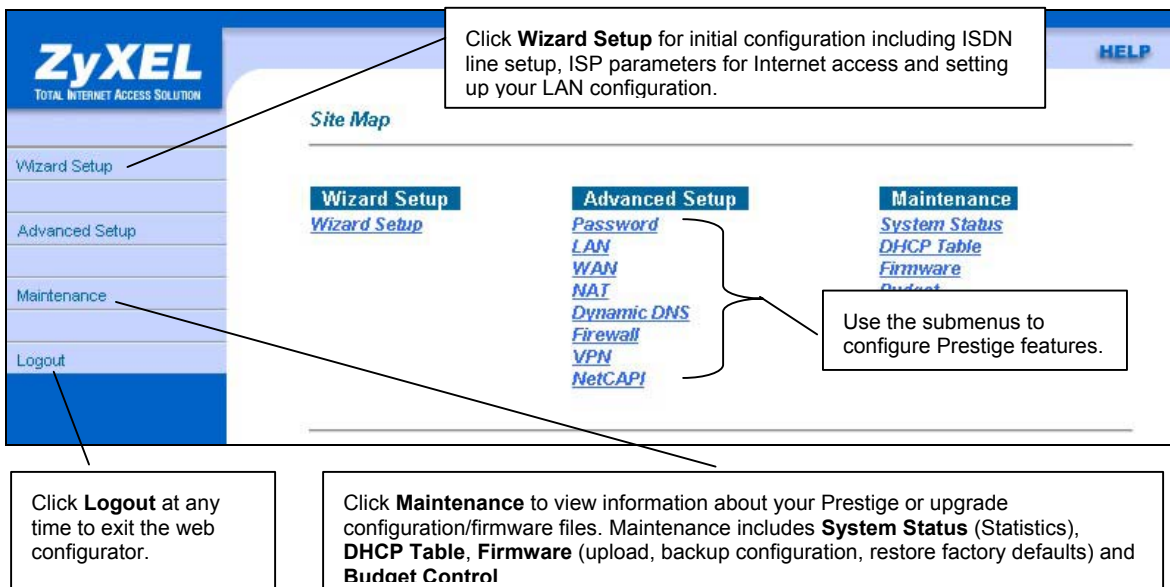


Figure 2-4 The Site Map Screen

The following table describes the sub-menus.

Table 2-2 Web Configurator Screens Summary

LINK	TAB	FUNCTION
Wizard Setup		Use these screens for initial configuration including general setup, ISP parameters for Internet access and WAN IP/DNS Server/MAC address assignment.
Advanced Setup		
Password		Use this screen to change your password.
LAN	IP	Use this screen to configure LAN DHCP and TCP/IP settings.
	Static DHCP	Use this screen to assign fixed IP addresses on the LAN.
	IP Alias	Use this screen to partition your LAN interface into subnets.

Table 2-2 Web Configurator Screens Summary

LINK	TAB	FUNCTION
WAN	Internet Access Setup	Use this screen to configure Internet Service Provider parameters.
NAT	SUA Server	Use this screen to configure servers behind the Prestige.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Trigger Port	Use this screen to change your Prestige's trigger port settings.
Dynamic DNS		Use this screen to allow the Prestige to use dynamic host name resolution.
Firewall	Config	Use this screen to enable the firewall.
	Email	Use this screen to send logs and alert messages to an email account.
	Alert	Use this screen to configure the threshold for DoS attacks.
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add firewall rules.
	Timeout	Use this screen to configure connection timeouts.
	Logs	This screen displays firewall logs.
VPN	Setup	Use this screen to configure VPN connections and view the rule summary.
	Monitor	Use this screen to display and manage active VPN connections.
	Global Setting	Use this screen to allow NetBIOS packets through the VPN connections.
	Logs	This screen displays VPN logs.
NetAPI		Use this screen to allow applications to access services over ISDN.
Maintenance		
System Status		This screen contains administrative and system-related information. Use this screen to access statistics.
DHCP Table		This screen shows current DHCP client information of all network clients using the Prestige's DHCP server.
Firmware		Use this screen to upload firmware to your Prestige, backup and restore the configuration or reset the factory defaults to your Prestige.

Table 2-2 Web Configurator Screens Summary

LINK	TAB	FUNCTION
Budget		This screen displays remote nodes their connected time and the time allocated for that connection.
Logout		Click Logout to exit the web configurator.

Chapter 3

Wizard Setup

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

3.1 Wizard Setup 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 in the *Quick Start Guide*. Your ISP may have already configured some of the fields in the wizard screens for you.

3.2 IP Address and Subnet Mask

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

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

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

3.3 IP Address Assignment

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

3.3.1 Private IP Addresses

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

```
10.0.0.0      - 10.255.255.255
172.16.0.0   - 172.31.255.255
192.168.0.0  - 192.168.255.255
```

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

3.4 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.

3.5 MSN (Multiple Subscriber Number) and Subaddress

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

3.6 PABX Outside Line Prefix

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

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

3.7 Wizard Setup Configuration: First Screen

Click **Wizard Setup** in the main menu to display the first wizard screen.

Wizard Setup - ISDN Line Setup

B Channel Usage

Incoming Phone Numbers:

ISDN Data

Subaddress

A/B Adapter 1

Subaddress

A/B Adapter 2

Subaddress

Outside Line Prefix

Incoming Phone Numbers Matching:

Analog Call Routing

Global Analog Call

Figure 3-1 Wizard 1: ISDN Line Set Up

The following table describes the labels in this screen.

Table 3-1 Wizard 1: ISDN Line Set Up

LABEL	DESCRIPTION
B Channel Usage	<p>This is the bearer channel in an ISDN connection. B channel is a 64 Kbps full-duplex channel in both primary and basic rate ISDN.</p> <p>Select Switch/Switch (default). If you are only using one B channel (e.g., your Prestige is sharing the ISDN line with another device), then select Switch/Unused. If your second B channel is a leased line, select Switch/Leased.</p>
Incoming Phone Numbers:	
ISDN Data	<p>Type the phone number assigned to you by your telephone company. The maximum number of digits is 25 for the telephone number.</p>
Subaddress	<p>Enter the subaddress assigned to A/B Adapter 1 (PHONE1). The maximum number of digits is 25 for the subaddress.</p>
A/B Adapter1	<p>Enter the telephone number assigned to A/B Adapter 1 (PHONE1).</p>
Subaddress	<p>Enter the subaddress assigned to A/B Adapter 2 (PHONE2). The maximum number of digits is 25 for the subaddress.</p>
A/B Adapter2	<p>Enter the telephone number assigned to A/B Adapter 2 (PHONE2).</p>
Outside Line Prefix	<p>If it's necessary to dial an additional number to reach an outside line, type in your prefix in this field. The maximum number of digits is 4.</p>
Incoming Phone Numbers Matching:	<p>The Incoming Phone Number Matching setting governs how incoming calls are routed. If you select Multiple Subscriber Number (MSN) or Called Party Subaddress, a call (either ISDN data or analog) is routed to the port that matches the dialed number; if no match is found, the call is dropped.</p> <p>If you select Don't Care, then all data calls are routed to the Prestige itself. Analog calls, however, are routed to either A/B adapter 1 or 2, or simply ignored, depending on the Analog Call Routing field.</p>
Analog Call Routing	<p>Select the destination for analog calls.</p> <p>The choices are A/B Adapter 2, A/B Adapter 1, Both or Ignore. This field is only applicable when Incoming Phone Number Matching is Don't Care.</p>

Table 3-1 Wizard 1: ISDN Line Set Up

LABEL	DESCRIPTION
Global Analog Call	<p>A global call is an incoming analog call where the switch did not send the dialed number. This happens most often when the call originates from an analog telephone line.</p> <p>If you specify explicit matching, i.e., Incoming Phone Number Matching is either MSN or Called Party Subaddress, then global calls are always ignored. If it is Don't Care and Analog Call Routing is either A/B Adapter 1, A/B Adapter 2 or Both, then the Prestige uses Global Analog Call to decide how to handle global calls. If you set Global Analog Call to Accept, then global calls are routed to the port according to the Analog Call Routing setting; if you set Global Analog Call to Ignore, then the Prestige ignores all global calls. If Analog Call Routing is Ignore to begin with, then all analog calls, including global calls, are ignored.</p>
Next	Click this button to set up your Prestige for Internet access.

3.8 Wizard Setup Configuration: Second Screen

The second wizard screen helps you set up your Prestige for Internet access.

Wizard Setup - ISP Parameters for Internet Access

Service Name

Login Information

Primary Phone #

Secondary Phone #

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Network Address Translation

▾

Dial out Channel Setting

Transfer Type ▾

Multilink ▾

Connection

Max Idle Timeout Secs

Figure 3-2 Wizard 2: ISP Parameters For Internet Access

The following table describes the labels in this screen.

Table 3-2 Wizard 2: ISP Parameters For Internet Access

LABEL	DESCRIPTION
Service Name	Type the name of your service provider.

Table 3-2 Wizard 2: ISP Parameters For Internet Access

LABEL	DESCRIPTION
Login Information	
Primary Phone #	Your Prestige always calls your ISP using the primary phone number first. Type the number exactly as your ISP gave you.
Secondary Phone #	If the primary phone number is busy or does not answer, your Prestige will dial the secondary phone number if available. Some areas require dialing the pound sign (#) before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.
User name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
IP Address	
Obtain an IP Address Automatically	Select this option to have the Prestige obtain an IP address from a DHCP server.
Static IP Address	Select this option to manually configure your Prestige IP address.
IP Address	Type an IP address to identify your Prestige on the LAN.
Network Address Translation	Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that maps one public IP address to many private IP addresses. Choose Full Feature if you have multiple public IP addresses. When you select Full Feature , you must use the NAT address mapping rules screen to configure at least one address mapping set! Full Feature mapping types include: One-to-One , Many-to-One (SUA), Many-to-Many Overload , Many-to-Many No Overload and Server . Choose None to disable NAT. Refer to the NAT chapter for more details.
Dial Out Channel Setting	
Transfer Type	This field specifies the type of connection between the Prestige and your ISP. Select 64K or Leased .

Table 3-2 Wizard 2: ISP Parameters For Internet Access

LABEL	DESCRIPTION
Multilink	The Prestige uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is 64K. Options for this field are: Off , BOD and Always .
Connection	
Max Idle Timeout	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your Prestige. Administrative packets such as RIP are not counted as data. The default time is 100 seconds.
Back	Click this button to reconfigure your ISDN line settings.
Next	Click this button to display a summary of all your settings.

3.9 Wizard Setup Configuration: Third Screen

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.

Wizard Setup - ISP Parameters for Internet Access

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

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

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

Change LAN Configuration

Save Settings

Figure 3-3 Wizard 3: Summary

3.10 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.

3.10.1 IP Pool Setup

The Prestige is pre-configured with a pool of 6 IP addresses starting from 192.168.1.33 to 192.168.1.38 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.

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

Wizard Setup - ISP Parameters for Internet Access

TCP/IP

LAN IP Address

LAN Subnet Mask

DHCP

DHCP Server

Client IP Pool Starting Address

Size of Client IP Pool

Primary DNS Server

Secondary DNS Server

Figure 3-4 Wizard: LAN Configuration

The following table describes the labels in this screen.

Table 3-3 Wizard: LAN Configuration

LABEL	DESCRIPTION
TCP/IP	
LAN IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default). <hr/> <p style="text-align: center;">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.</p> <hr/>
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
DHCP	
DHCP Server	From the DHCP Server drop-down list box, select On to allow your Prestige to assign IP addresses, a default gateway and DNS servers to computer systems that support the DHCP client feature. Select Off to disable DHCP server. When DHCP server is used, set the following items:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Back	Click Back to go back to the previous screen.
Finish	Click Finish to save the settings and begin testing your connection.

3.11 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.

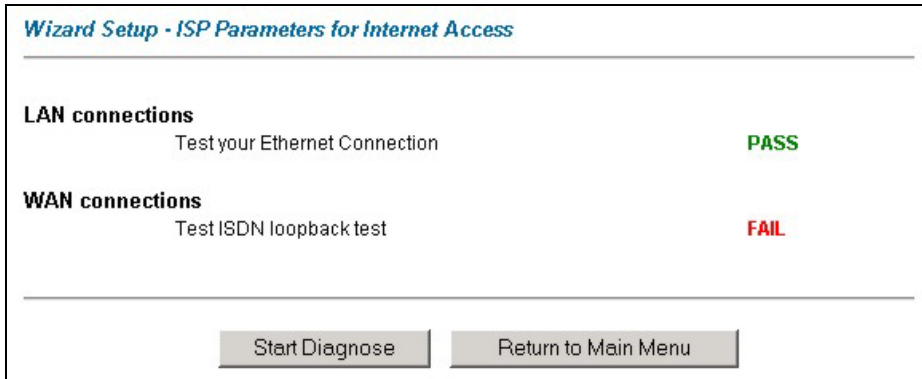


Figure 3-5 Wizard Screen 4

3.12 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.

Part II:

Advanced Settings

This part covers configuration of the Advanced screens.

Chapter 4

LAN Settings

This chapter describes how to configure LAN settings.

4.1 LAN Overview

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

4.2 DHCP Setup

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

4.2.1 IP Pool Setup

The Prestige is pre-configured with a pool of 6 IP addresses starting from 192.168.1.33 to 192.168.1.38. This configuration leaves 31 IP addresses (excluding the Prestige itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

4.3 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 192.168.10 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.

4.4 DNS Server Address Assignment

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

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

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

4.5 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.

4.5.1 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 6 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.

4.6 Configuring IP

Click **Advanced**, and then click **LAN** to open the **LAN Setup** screen.

LAN - LAN Setup

DHCP

DHCP

Client IP Pool Starting Address

Size of Client IP Pool

Primary DNS Server

Secondary DNS Server

Remote DHCP Server

TCP/IP

IP Address

IP Subnet Mask

Figure 4-1 LAN Setup

The following table describes the labels in this screen.

Table 4-1 LAN Setup

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 server is used, set the following items:</p>
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.

Table 4-1 LAN Setup

LABEL	DESCRIPTION
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary/Secondary DNS Servers	Type the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask. Leave these entries at 0.0.0.0 if they are provided by a WAN DHCP server.
Remote DHCP Server	If Relay is selected in the DHCP Server field, type the IP address of a WAN DHCP server.
TCP/IP	
IP Address	Type the IP address of your Prestige in dotted decimal notation. 192.168.1.1 is the factory default.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Prestige automatically selects the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to begin configuring this screen afresh.

Chapter 5

WAN Setup

This chapter describes how to configure WAN settings.

5.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet. See the *Wizard Setup* chapter for more information on the fields in the WAN screens.

5.2 Configuring WAN Setup

To change your Prestige's WAN remote node settings, click **WAN**.

Internet Access Setup

Name

Login Information

Primary Phone #

Secondary Phone #

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Dial out Channel Setting

Transfer Type

Multilink

Connection

Nailed-Up Connection

Connect on Demand

Max Idle Timeout Secs

Budget Control

Budget (min)

Period (hr)

Figure 5-1 Internet Access Setup

The following table describes the labels in this screen.

Table 5-1 Internet Access Setup

LABEL	DESCRIPTION
Name	Type the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Login Information	
Primary Phone #	Your Prestige always calls your ISP using the primary phone number first. Type the number exactly as your ISP gave you.
Secondary Phone #	If the primary phone number is busy or does not answer, your Prestige will dial the secondary phone number if available. Some areas require dialing the pound sign (#) before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.
User name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
IP Address	
Obtain an IP Address Automatically	Select this option to have your Prestige use a dynamically assigned IP address from your ISP each time.
Static IP Address	Select this option and type a fixed IP that your ISP gives you in the field below.
IP Address	Enter the IP address in dotted decimal notation.
Network Address Translation	Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that maps one public IP address to many private IP addresses. Choose Full Feature if you have multiple public IP addresses. When you select Full Feature , you must use the NAT address mapping rules screen to configure at least one address mapping set! Full Feature mapping types include: One-to-One , Many-to-One (SUA), Many-to-Many Overload , Many-to-Many No Overload and Server . Choose None to disable NAT. Refer to the NAT chapter for more details.
Dial Out Channel Setting	
Transfer Type	This field specifies the type of connection between the Prestige and your ISP. Select 64K , or Leased .

Table 5-1 Internet Access Setup

LABEL	DESCRIPTION
Multilink	The Prestige uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is 64K. Options for this field are: Off , BOD and Always .
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	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your Prestige. Administrative packets such as RIP are not counted as data. The default time is 100 seconds.
Budget Control	
Budget	This field sets the budget callback time for all the remote dial-in users. The default for this field is 0 for no budget control.
Period	This field sets the time interval to reset the above callback budget control.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to begin configuring this screen afresh.

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. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 6-2*), NAT offers the additional benefit of firewall protection. With no servers defined, your Prestige filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

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.

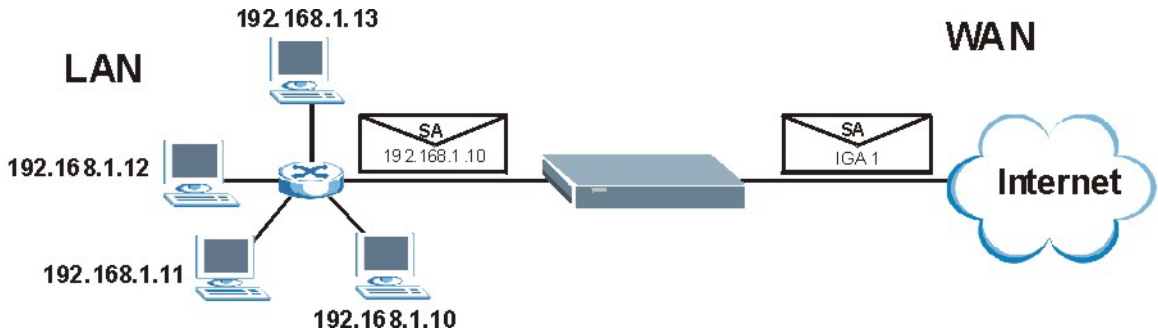


Figure 6-1 How NAT Works

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.

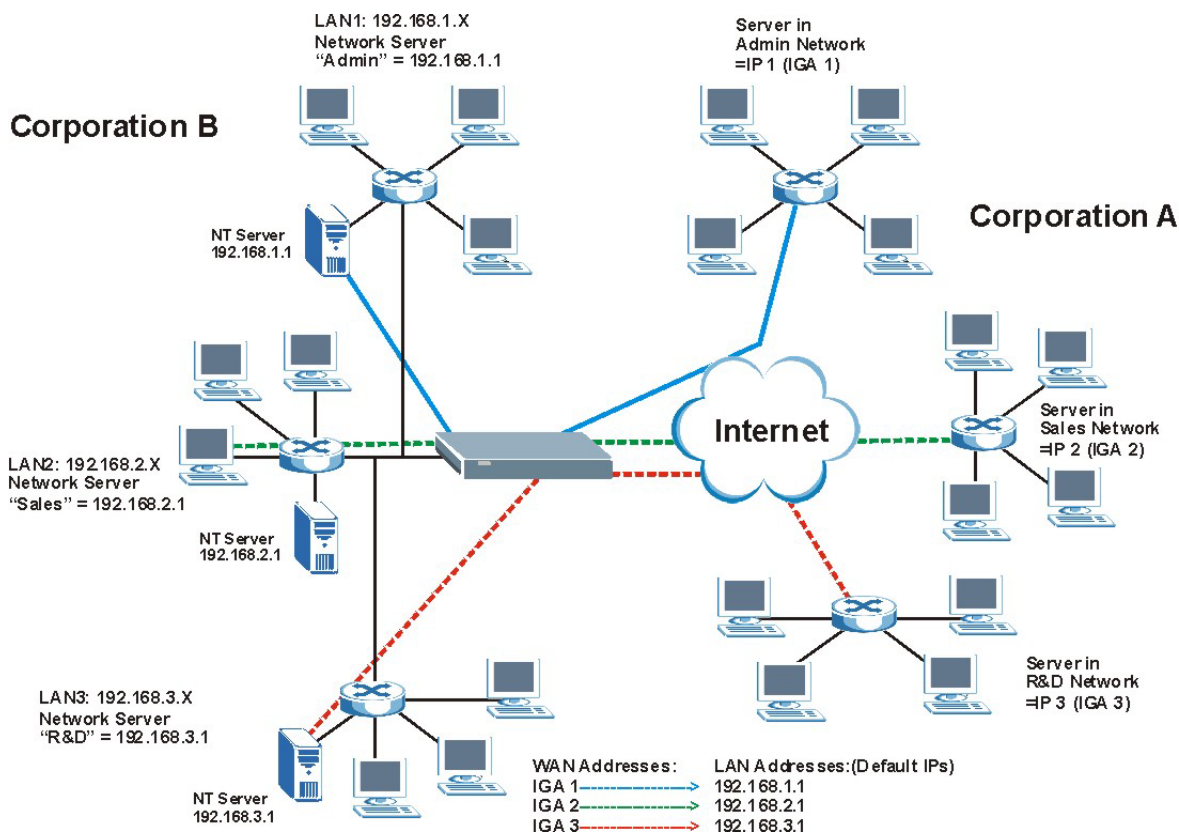


Figure 6-2 NAT Application With IP Alias

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*.

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

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

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

Table 6-3 Services and Port Numbers

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

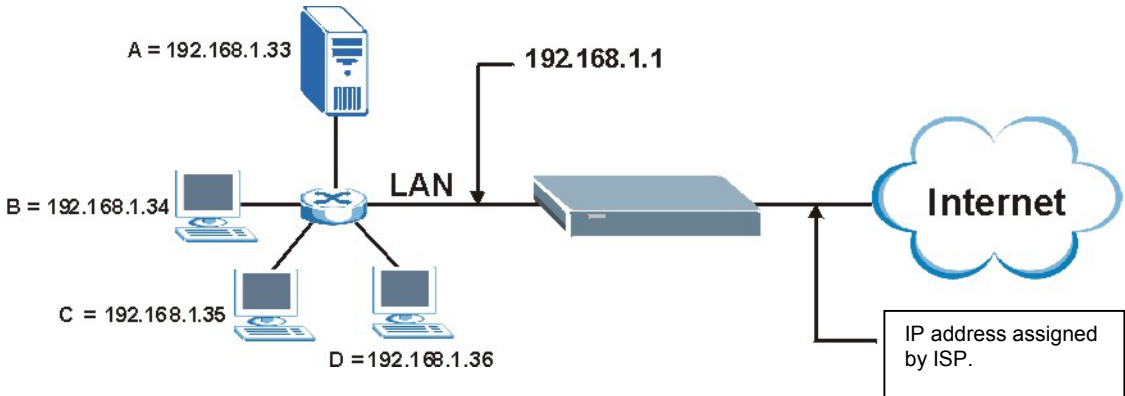


Figure 6-3 Multiple Servers Behind NAT Example

6.4 Selecting the NAT Mode

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

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.

Refer to *Table 6-3* for port numbers commonly used for particular services.

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	<input type="text"/>	<input type="text"/>	0.0.0.0
3	<input type="text"/>	<input type="text"/>	0.0.0.0
4	<input type="text"/>	<input type="text"/>	0.0.0.0
5	<input type="text"/>	<input type="text"/>	0.0.0.0
6	<input type="text"/>	<input type="text"/>	0.0.0.0
7	<input type="text"/>	<input type="text"/>	0.0.0.0
8	<input type="text"/>	<input type="text"/>	0.0.0.0
9	<input type="text"/>	<input type="text"/>	0.0.0.0
10	<input type="text"/>	<input type="text"/>	0.0.0.0
11	<input type="text"/>	<input type="text"/>	0.0.0.0
12	<input type="text"/>	<input type="text"/>	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.	Enter a port number in this field. To forward only one port, enter the port number again in the End Port No. field. To forward a series of ports, enter the start port number here and the end port number in the End Port No. field.

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.
Server 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 the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-one and Server mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for Many-to-One and Server mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is N/A for One-to-one , Many-to-One and Server mapping types.

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"> One-to-One: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. Many-to-One: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. Many-to-Many No Overload: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	<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

This chapter describes 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 **Advanced**, then click **Dynamic DNS**. The screen appears as shown.

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	This is the name of your Dynamic DNS service provider.
Host Name	Enter the host name You can specify up to two host names in each field separated by a comma (",").
E-mail Address	Enter your e-mail address.
User	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to begin configuring this screen afresh.

Chapter 8

Firewalls

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:

- i. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

- ii. Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

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 four Ethernet LAN ports, which physically separate the network into two areas.

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

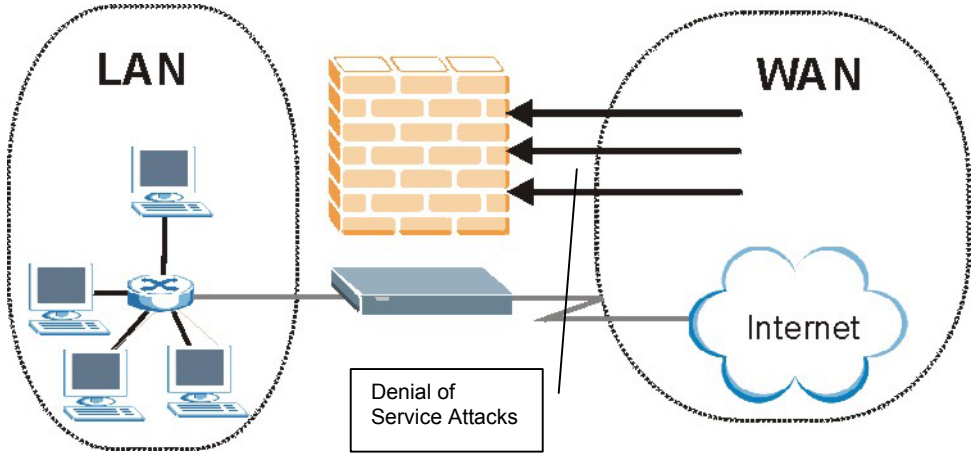


Figure 8-1 Prestige Firewall Application

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.

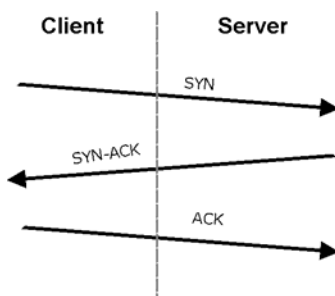


Figure 8-2 Three-Way Handshake

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.

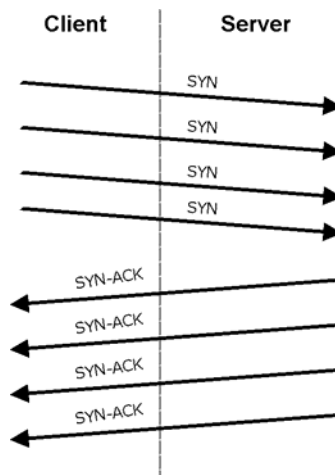


Figure 8-3 SYN Flood

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.

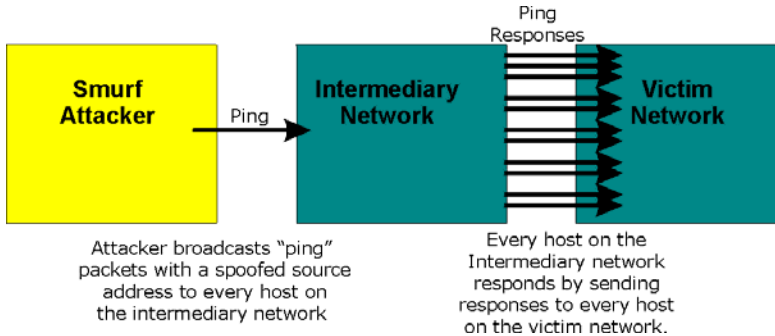


Figure 8-4 Smurf Attack

❑ 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.

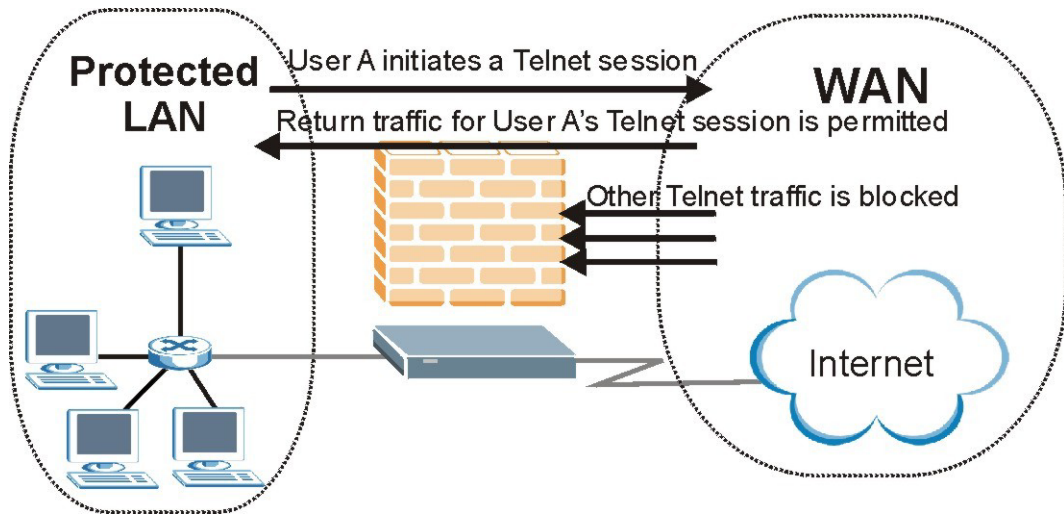


Figure 8-5 Stateful Inspection

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 10-3*) determines the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.

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

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:

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

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

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

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the 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. Limit who can telnet into your Prestige.
3. 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.
4. 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.
5. Protect against IP spoofing by making sure the firewall is active.
6. 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.

When To Use The Firewall

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

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

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

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.

Chapter 9

Firewall Configuration

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

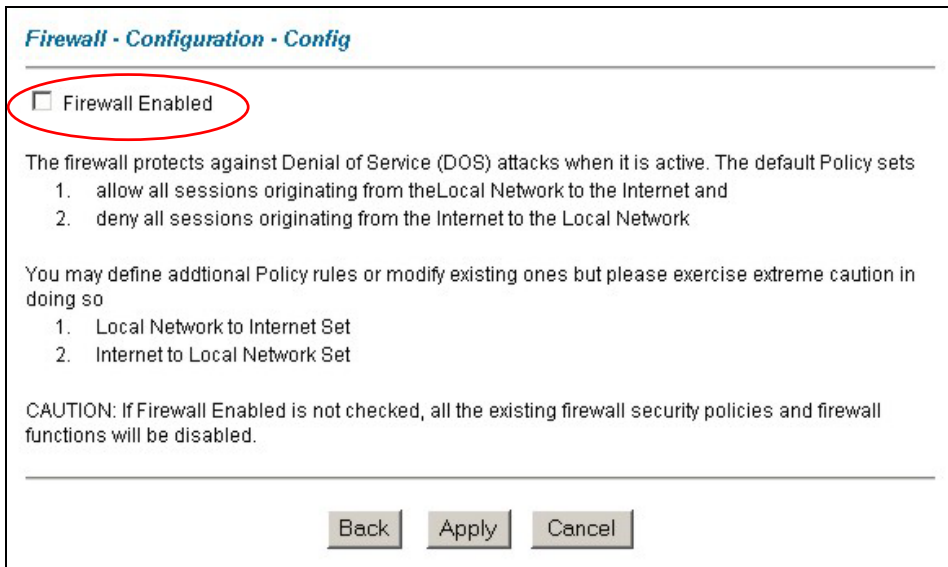
9.1 Remote Management and the Firewall

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 **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 E-Mail

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

Use the **E-Mail** screen to configure to where the 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

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.
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.

Table 9-1 E-mail

LABEL	DESCRIPTION
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> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. <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 **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 10-4*). 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 **Firewall**, and **Alert** to bring up the next screen.

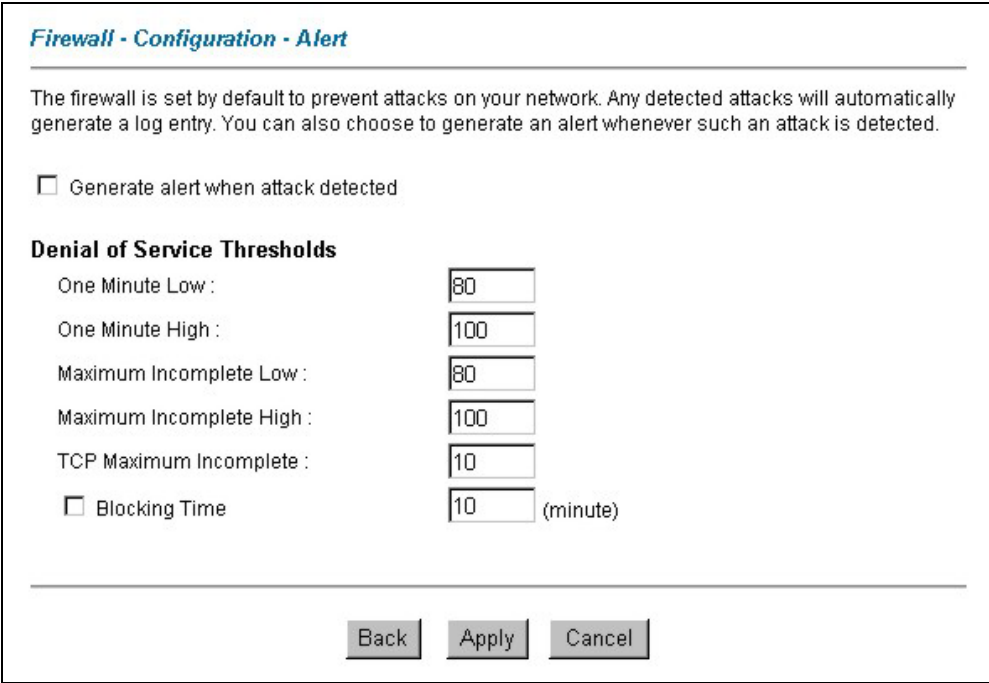


Figure 9-3 Alert

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.
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 (minute) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.
(minute)	Type the length of Blocking Time in minutes (1-256). The default is "0".

Table 9-2 Alert

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 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 10.5* 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 a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

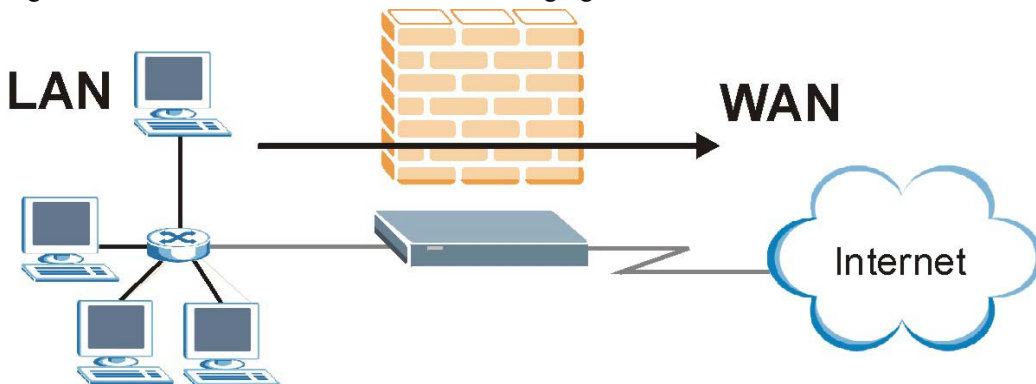


Figure 10-1 LAN to WAN Traffic

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.

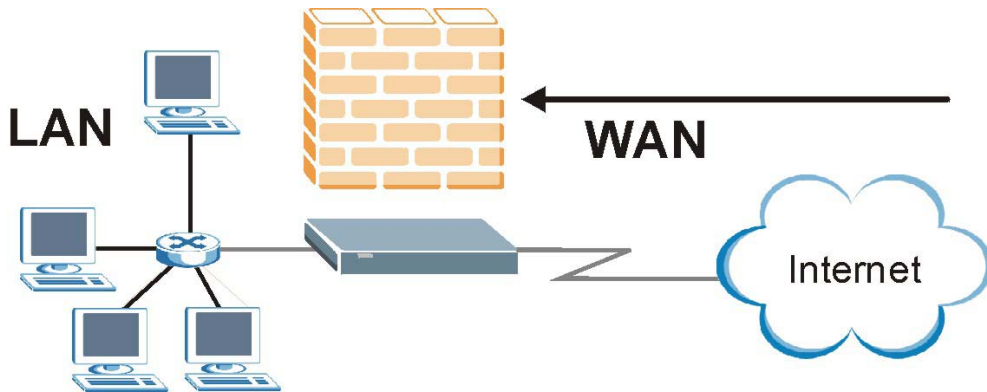


Figure 10-2 WAN to LAN Traffic

10.4 Rule Summary

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

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

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="button" value="v"/>	<input type="text" value="Any"/> <input type="button" value="v"/>	<input type="text" value="Any(UDP)"/> <input type="button" value="v"/>	Forward	None
2	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>		
3	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>		
4	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>		
5	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>		
6	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>		
7	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>		
8	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>		
9	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>		
10	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>		

Rules Reorder: Move rule number to rule number

Figure 10-3 Firewall Rules Summary: First Screen

The following table describes the labels in this screen.

Table 10-1 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.

Table 10-1 Firewall Rules Summary: First Screen

LABEL	DESCRIPTION
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 10-2</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.

10.5 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see *Figure 10-4*) 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 10-2 Predefined Services

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

Table 10-2 Predefined Services

SERVICE	DESCRIPTION
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS (TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
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.

Table 10-2 Predefined Services

SERVICE	DESCRIPTION
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.

10.6 Creating/Editing Firewall Rules

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

Figure 10-4 Creating/Editing A Firewall Rule

The following table describes the labels in this screen.

Table 10-3 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.

Table 10-3 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 11</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.
Back	Click Back to return to the previous screen.
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.

10.6.1 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.

Figure 10-5 Adding/Editing Source and Destination Addresses

The following table describes the labels in this screen.

Table 10-4 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.

10.7 Timeout

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

10.7.1 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 to Internet Set** or **Internet to Local Network Set**.

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 10-6 Timeout

The following table describes the labels in this screen.

Table 10-5 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 10-5 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 10-4*). 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 10.5*. To configure a custom service, click **Edit Available Service** in an edit rule screen to bring up the following screen.

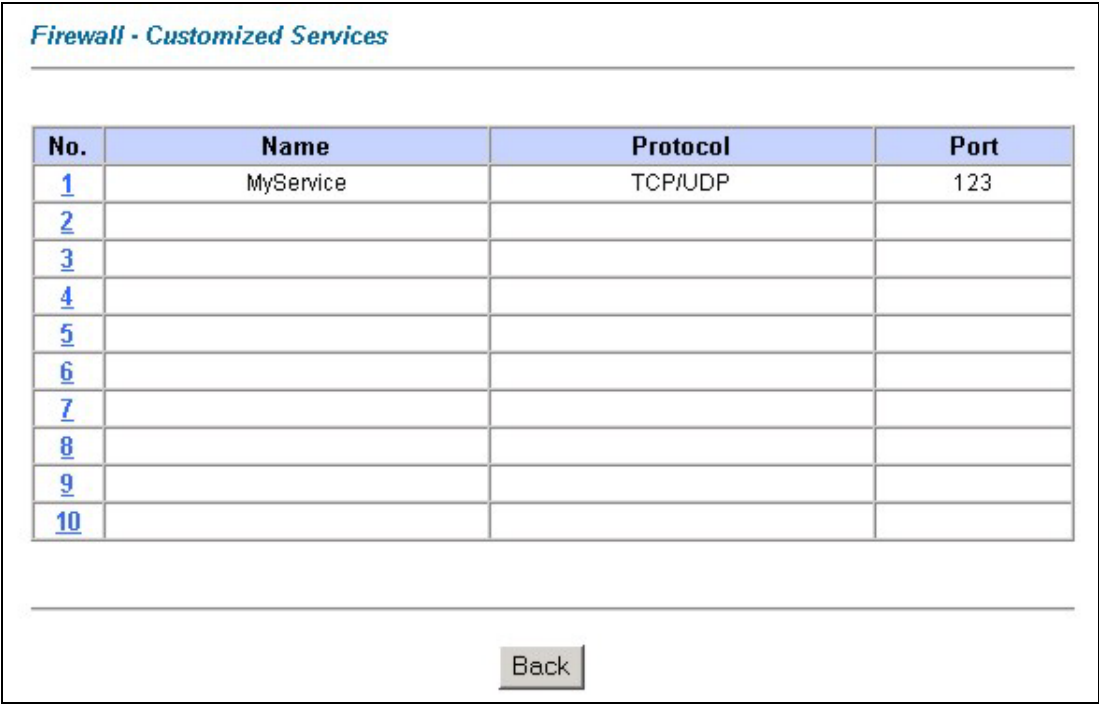


Figure 11-1 Customized Services

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 TCP/UDP) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click Back to return 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:

Port Configuration

Type: Single Range

Port Number: -

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.

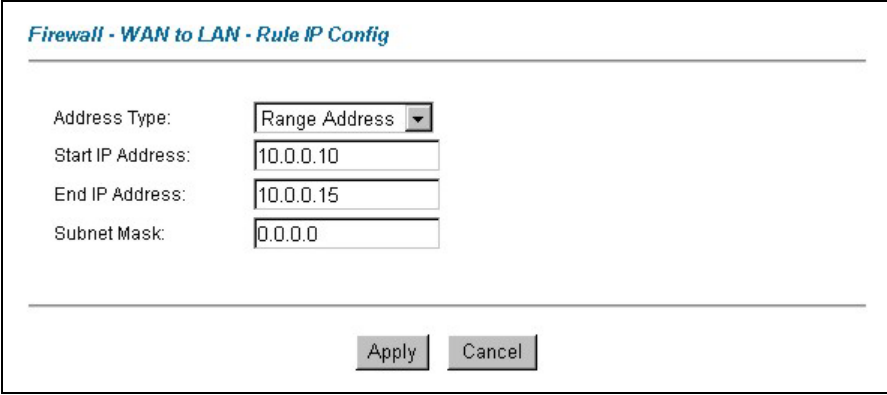
11.3 Example Custom Service Firewall Rule

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



Firewall - WAN to LAN - Rule IP Config

Address Type:

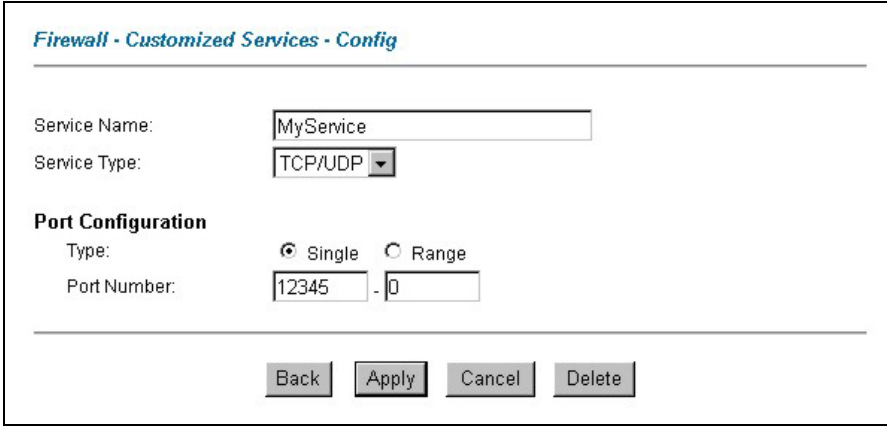
Start IP Address:

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.

The screenshot shows the 'Firewall - WAN to LAN - Edit Rule 1' configuration window. It is divided into several sections: Source Address, Destination Address, Service, Action for Matched Packets, and Log. Callouts are present: one pointing to the Source Address field containing '10.0.0.10 - 10.0.0.15', another pointing to the Selected Services field containing '*MyService(TCP/UDP:12345)', and a third pointing to the 'Apply' button at the bottom. The 'Action for Matched Packets' is set to 'Forward' and 'Log' is set to 'None'. There is also an unchecked 'Alert' checkbox.

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

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:

Default Permit Log

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

Rules Reorder: Move rule number to rule number

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

Chapter 12

Firewall Logs

This chapter contains information about using the log screen to view the results of the rules you have configured.

12.1 Logs Screen

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

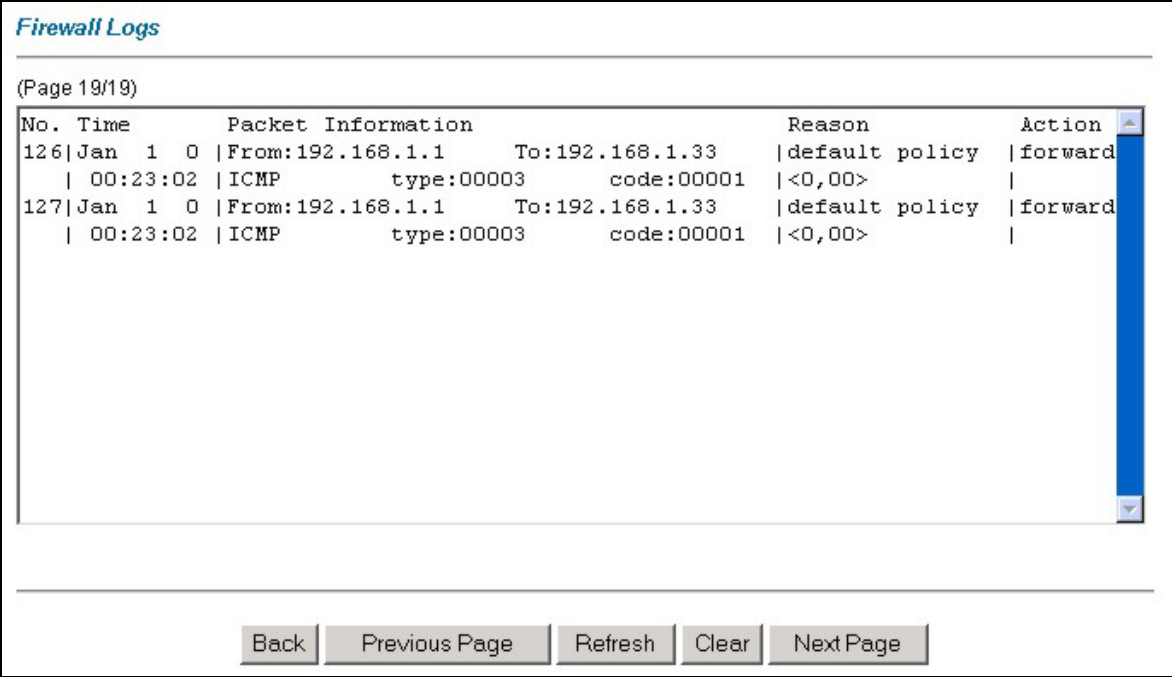


Figure 12-1 Log Screen

The following table describes the labels in this screen.

Table 12-1 Log Screen

FIELD	DESCRIPTION	EXAMPLE
No.	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real-time; otherwise the time shown in these examples is displayed.	dd: e.g., Jan 1 0 mm: yy
		hh: e.g., 00:00:00 mm: ss
Packet Information	This field lists packet information such as:	From and To IP addresses ----- protocol and port numbers.
Reason	This field states the reason for the log; i.e., was the rule matched, not matched, or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol.
	This is a log for a DoS attack	attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop, or syn flood.
Action	This field displays whether the packet was blocked (i.e., silently discarded), forwarded or neither (Block, Forward or None). "None" means that no action is dictated by this rule.	Block, Forward or None
Click Back to return to the previous screen. Click Previous Page or Next Page to view other pages in your log. Click Refresh to renew the log screen or Clear to clear all the logs. Click the Help icon for field descriptions.		

Part III:

VPN/IPSec

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

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.

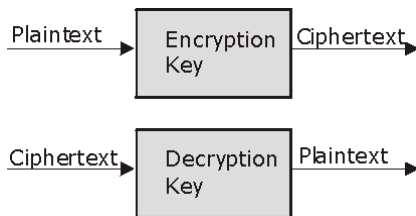


Figure 13-1 Encryption and Decryption

➤ **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. See the chapter on *Getting to Know Your Prestige* for an example of a VPN application.

13.2 IPsec Architecture

The overall IPsec architecture is shown as follows.

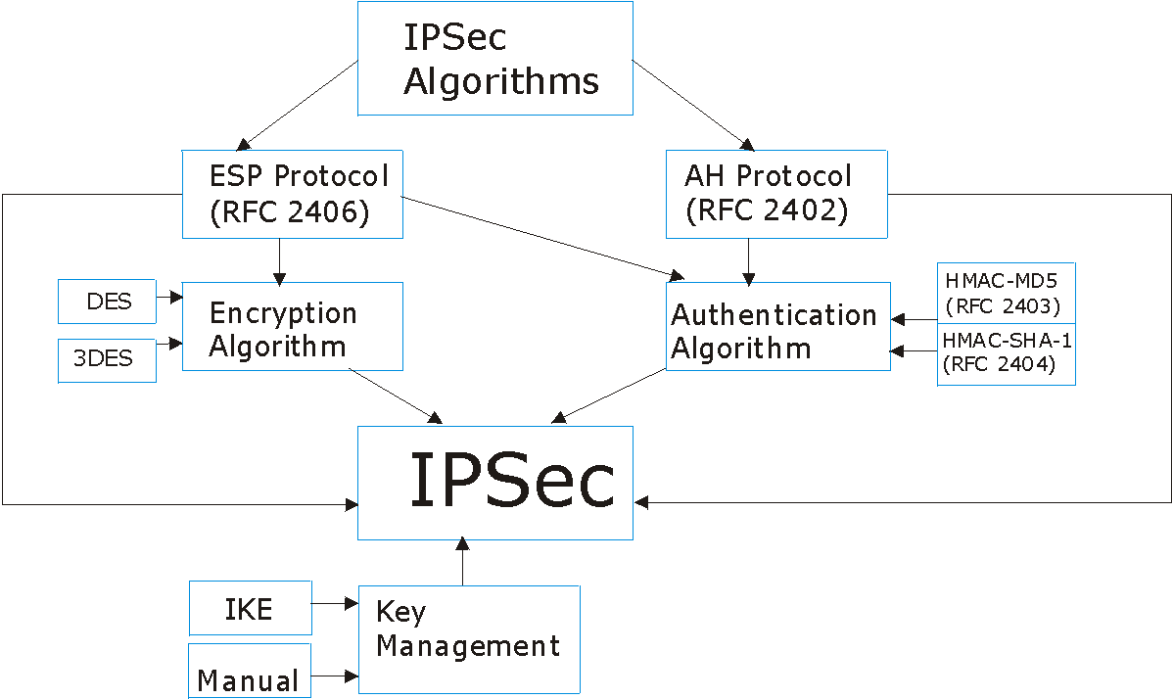


Figure 13-2 IPsec Architecture

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.

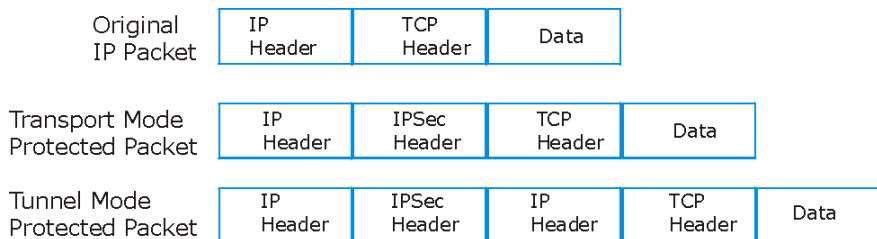


Figure 13-3 Transport and Tunnel Mode IPsec Encapsulation

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, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (see *section 14.7* for details).

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

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 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 ESP and AH

	ESP	AH
Encryption	DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys ($3 \times 56 = 168$ bits), effectively doubling the strength of DES.	
Authentication	MD5 (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	MD5 (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select MD5 for minimal security and SHA-1 for maximum security.	

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 IP Address

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

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

You can also enter a remote secure gateway's domain name in the **Secure Gateway IP Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The 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 14.17* for configuration examples.

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

14.5 Summary Screen

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

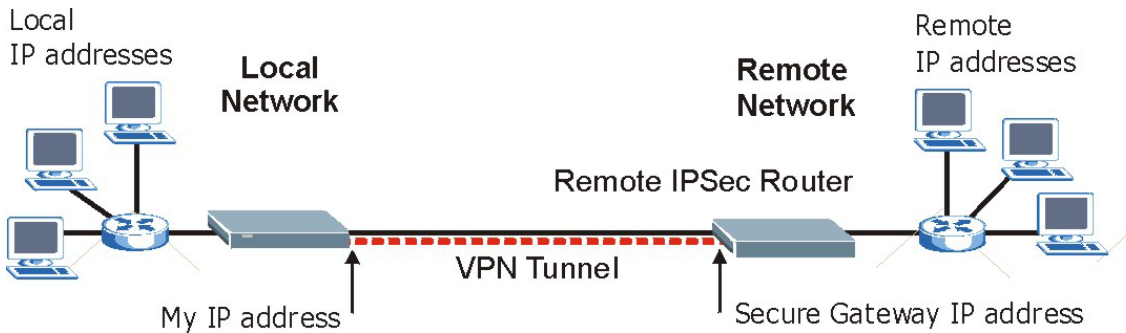


Figure 14-1 IPsec Summary Fields

Local and remote IP addresses must be static.

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

VPN - Summary

No.	Name	Active	Local Address	Remote Address	Encap.	IPsec Algorithm	Secure Gateway IP
1	Taiwan	Yes	192.168.1.35 - 192.168.1.38	172.16.2.40 - 172.16.2.46	Tunnel	ESP DES SHA1	193.81.13.2
2							
3							
4							
5							

Back

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

Table 14-2 VPN: Summary

LABEL	DESCRIPTION
	Select the hyperlink next to a VPN index number and then click Edit to edit a specific VPN policy. Click the radio button next to an empty VPN policy index number and then Edit to add a new VPN policy.
	Select the radio button next to a VPN policy number you want to delete and then click Delete . When a VPN policy is deleted, subsequent policies do not move up in the list.

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 14.11* for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both IPSec routers must have a Prestige-compatible keep alive feature enabled in order for this feature to work.

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

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

14.7 NAT Traversal

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

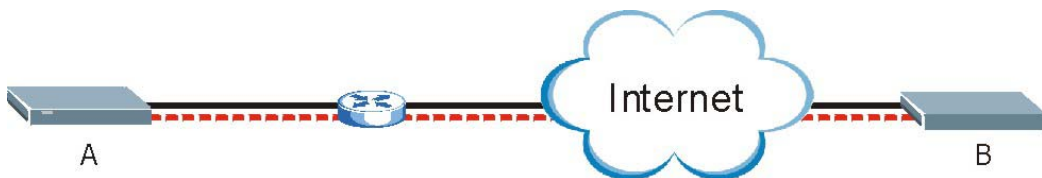


Figure 14-3 NAT Router Between IPSec Routers

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

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

14.7.1 NAT Traversal Configuration

For NAT traversal to work you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPsec endpoints.

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

14.7.2 Remote DNS Server

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

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

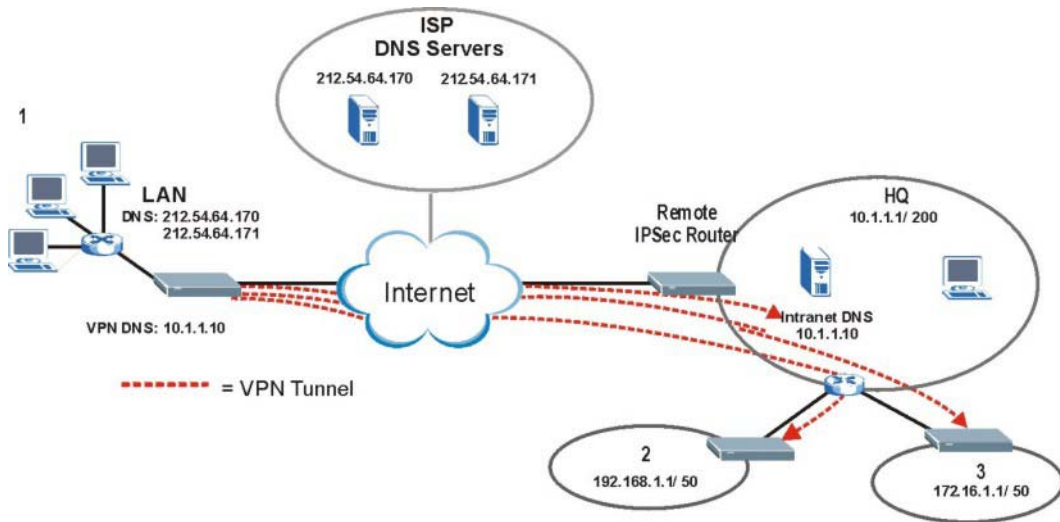


Figure 14-4 VPN Host using Intranet DNS Server Example

If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote network.

14.8 ID Type and Content

With aggressive negotiation mode (see *Section 14.11.1*), the Prestige identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Prestige to distinguish between multiple rules for SAs that connect from remote IPsec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the Prestige from IPsec routers with dynamic IP addresses (see *Section 0* for a telecommuter configuration example).

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

With main mode (see *Section 14.11.1*), the ID type and content are encrypted to provide identity protection. In this case the Prestige can only distinguish between up to eight different incoming SAs that connect from remote IPsec routers that have dynamic WAN IP addresses. The Prestige can distinguish up to eight

incoming SAs because you can select between three encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see *Section 14.12*). The ID type and content act as an extra level of identification for incoming SAs.

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

Table 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.	

14.8.1 ID Type and Content Examples

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

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

Table 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

14.9 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see *Section 14.11* for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

14.10 Editing VPN Rules

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

VPN - IKE

IPSec Setup

Active Keep Alive

Name

IPSec Key Mode

Negotiation Mode

Local:

Local Address Type

IP Address Start

End / Subnet Mask

Remote:

Remote Address Type

IP Address Start

End / Subnet Mask

Local ID Type

Content

My IP Address

Peer ID Type

Content

Secure Gateway IP Address

Encapsulation Mode

Security Protocol

VPN Protocol

Pre-Shared Key

VPN - Setup

Authentication Algorithm

Figure 14-5 VPN: Rule Setup (Basic)

The following table describes the labels in this screen.

Table 14-7 VPN: Rule Setup (Basic)

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select this check box to have the Prestige automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPsec router must also have keep alive enabled in order for this feature to work.
IPsec Key Mode	Select IKE or Manual from the drop-down list box. IKE provides more protection so it is generally recommended. Manual is a useful option for troubleshooting if you have problems using IKE key management.
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.
<p>Local</p> <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 IP 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 IP Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway IP Address field set to 0.0.0.0.</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.
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.

Table 14-7 VPN: Rule Setup (Basic)

LABEL	DESCRIPTION
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 IP 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 cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</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.
Local ID Type	Select IP to identify this Prestige by its IP address. Select DNS to identify this Prestige by a domain name. Select E-mail to identify this Prestige by an e-mail address.

Table 14-7 VPN: Rule Setup (Basic)

LABEL	DESCRIPTION
Content	<p>When you select IP in the Local ID Type field, type the IP address of your computer in the local Content field. The Prestige automatically uses the IP address in the My IP Address field (refer to the My IP Address field description) if you configure the local Content field to 0.0.0.0 or leave it blank.</p> <p>It is recommended that you type an IP address other than 0.0.0.0 in the local Content field or use the DNS or E-mail ID type in the following situations.</p> <ul style="list-style-type: none"> ➤ When there is a NAT router between the two IPSec routers. ➤ When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. <p>When you select DNS or E-mail in the Local ID Type field, type a domain name or e-mail address by which to identify this Prestige in the local Content field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.</p>
My IP Address	<p>Enter the WAN IP address of your Prestige. The VPN tunnel has to be rebuilt if this IP address changes.</p> <p>The Prestige uses its current WAN IP address (static or dynamic) to set up the VPN tunnel if you leave this field as 0.0.0.0.</p>
Peer ID Type	<p>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.</p>

Table 14-7 VPN: Rule Setup (Basic)

LABEL	DESCRIPTION
Content	<p>The configuration of the peer content depends on the peer ID type.</p> <ul style="list-style-type: none"> ➤ For IP, type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the Prestige will use the address in the Secure Gateway IP Address field (refer to the Secure Gateway IP Address field description). ➤ For DNS or E-mail, type a domain name or e-mail address by which to identify the remote IPsec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. <p>It is recommended that you type an IP address other than 0.0.0.0 or use the DNS or E-mail ID type in the following situations:</p> <ul style="list-style-type: none"> ➤ When there is a NAT router between the two IPsec routers. ➤ When you want the Prestige to distinguish between VPN connection requests that come in from remote IPsec routers with dynamic WAN IP addresses.
Secure Gateway IP Address	<p>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).</p> <p>In order to have more than one active rule with the Secure Gateway IP Address field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with 0.0.0.0 in the Secure Gateway IP Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway IP Address field set to 0.0.0.0.</p>
Encapsulation Mode	Select Tunnel mode or Transport mode from the drop-down list box.
Security Protocol	

Table 14-7 VPN: Rule Setup (Basic)

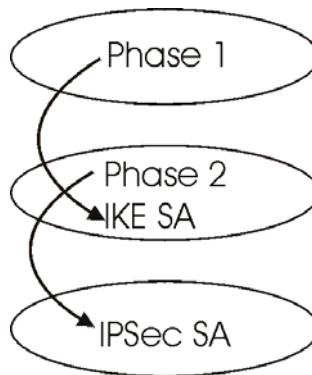
LABEL	DESCRIPTION
VPN Protocol	<p>Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described next).</p> <p>Select AH if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select AH here, you must select options from the Authentication Algorithm field (described later).</p>
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>
VPN - Setup	<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>
Advanced	Click Advanced to configure more detailed settings of your IKE key management.
Apply	Click Apply to save your changes back to the Prestige.

Table 14-7 VPN: Rule Setup (Basic)

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

14.11 IKE Phases

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

**Figure 14-6 Two Phases to Set Up the IPsec SA**

In phase 1 you must:

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

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

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see *Section 14.11.3*. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The Prestige automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The Prestige also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

14.11.1 Negotiation Mode

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

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

useful in remote access situations where the address of the initiator is not known by the responder and both parties want to use pre-shared key authentication.

14.11.2 Diffie-Hellman (DH) Key Groups

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

14.11.3 Perfect Forward Secrecy (PFS)

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

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

14.12 Configuring Advanced IKE Settings

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

VPN - IKE - Advanced Setup

VPN - IKE

Protocol

Enable Replay Detection

Local Start Port End

Remote Start Port End

Phase1

Negotiation Mode

Pre-Shared Key

Encryption Algorithm

Authentication Algorithm

SA Life Time (Seconds)

Key Group

Phase2

Active Protocol

Encryption Algorithm

Authentication Algorithm

SA Life Time (Seconds)

Encapsulation

Perfect Forward Secrecy(PFS)

Figure 14-7 VPN IKE: Advanced

The following table describes the labels in this screen.

Table 14-8 VPN IKE: Advanced

LABEL	DESCRIPTION
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select YES 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 Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
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.
<p>Phase 1</p> <p>A phase 1 exchange establishes an IKE SA (Security Association).</p>	
Negotiation Mode	Select Main or Aggressive from the drop-down list box. The Prestige's negotiation mode should be identical to that on the remote secure gateway.
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>

Table 14-8 VPN IKE: Advanced

LABEL	DESCRIPTION
Encryption Algorithm	Select DES or 3DES from the drop-down list box. The Prestige's encryption algorithm should be identical to the secure remote gateway. When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slower. Select MD5 for minimal security and SHA-1 for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
<p>Phase 2</p> <p>A phase 2 exchange uses the IKE SA established in phase 1 to negotiate the SA for IPSec.</p>	
Active Protocol	Use the drop-down list box to choose from ESP or AH . The Prestige's IPSec protocol should be identical to the secure remote gateway.
Encryption Algorithm	<p>The encryption algorithm for the Prestige and the secure remote gateway should be identical.</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 14-8 VPN IKE: Advanced

LABEL	DESCRIPTION
Authentication Algorithm	Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select MD5 for minimal security and SHA-1 for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select Tunnel mode or Transport mode from the drop down list-box. The Prestige's encapsulation mode should be identical to the secure remote gateway.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (None) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose from DH1 or DH2 to enable PFS. DH1 refers to Diffie-Hellman Group 1, a 768 bit random number. DH2 refers to Diffie-Hellman Group 2, a 1024 bit (1Kb) random number (more secure, yet slower).
Apply	Click Apply to save your changes back to the Prestige and return to the VPN-IKE screen.
Cancel	Click Cancel to return to the VPN-IKE screen without saving your changes.

14.13 Manual Key Setup

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

14.13.1 Security Parameter Index (SPI)

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

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

14.14 Configuring Manual Key

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

VPN - Manual Key

IPSec Setup

Active

Name

IPSec Key Mode

Local Address Type

IP Address Start

End / Subnet Mask

Remote Address Type

IP Address Start

End / Subnet Mask

My IP Address

Secure Gateway IP Address

SPI

Encapsulation Mode

Security Protocol

IPSec Protocol

Encapsulation Algorithm

Encapsulation Key

Authentication Algorithm

Authentication Key

Figure 14-8 Rule Setup: Manual

The following table describes the labels in this screen.

Table 14-9 Rule Setup: Manual

LABEL	DESCRIPTION
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 Keying Mode	Select IKE or Manual from the drop-down list box. Manual is a useful option for troubleshooting if you have problems using IKE key management.
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 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.
IP Address End/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 LAN behind your Prestige. When the Remote Address Type field is configured to Subnet , this is a subnet mask on the LAN behind your Prestige.

Table 14-9 Rule Setup: Manual

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 IP Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
Encapsulation Mode	Select Tunnel mode or Transport mode from the drop-down list box.
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 Encryption Algorithm and Authentication Algorithm fields (described next).
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>
Encryption Key (Only with ESP)	With DES , type a unique key 8 characters long. With 3DES , type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slower. Select MD5 for minimal security and SHA-1 for maximum security.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for MD5 authentication or 20 characters for SHA-1 authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the Prestige.

Table 14-9 Rule Setup: Manual

LABEL	DESCRIPTION
Cancel	Click Cancel to begin configuring this screen afresh.
Delete	Click Delete to remove the current rule.

14.15 Viewing SA Monitor

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

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

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"/>

Back Apply Refresh

Figure 14-9 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.
IP Sec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase Prestige processing requirements and communications latency (delay).
Disconnect	Click the radio button next to a security association and then Apply to stop that security association.

Table 14-10 SA Monitor

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

14.16 Configuring Global Setting

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

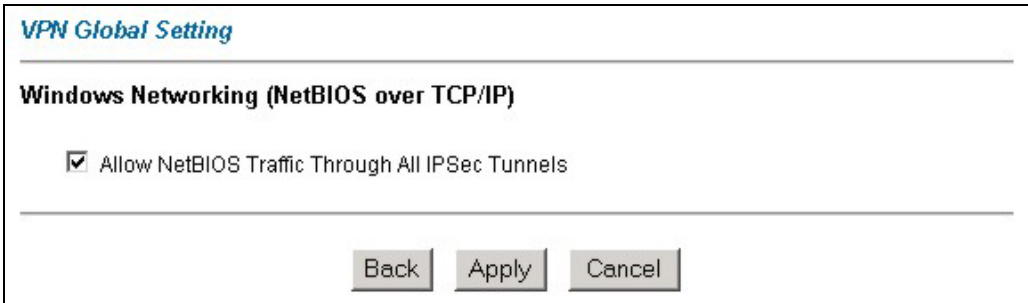


Figure 14-10 VPN: Global Setting

The following table describes the labels in this screen.

Table 14-11 VPN: Global Setting

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

Table 14-11 VPN: Global Setting

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

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.

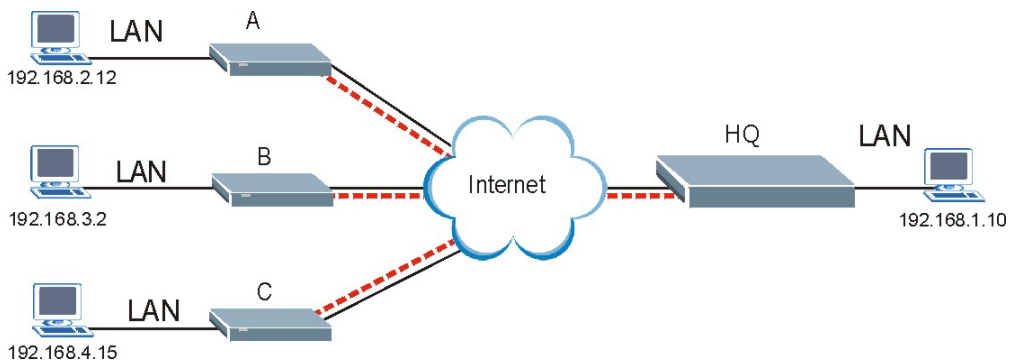
**Figure 14-11 Telecommuters Sharing One VPN Rule Example**

Table 14-12 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.
Local IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote IP Address:	192.168.1.10	0.0.0.0 (N/A)

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 14.11.1*), the Prestige can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a Prestige at headquarters. They can use different IPSec parameters. 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.

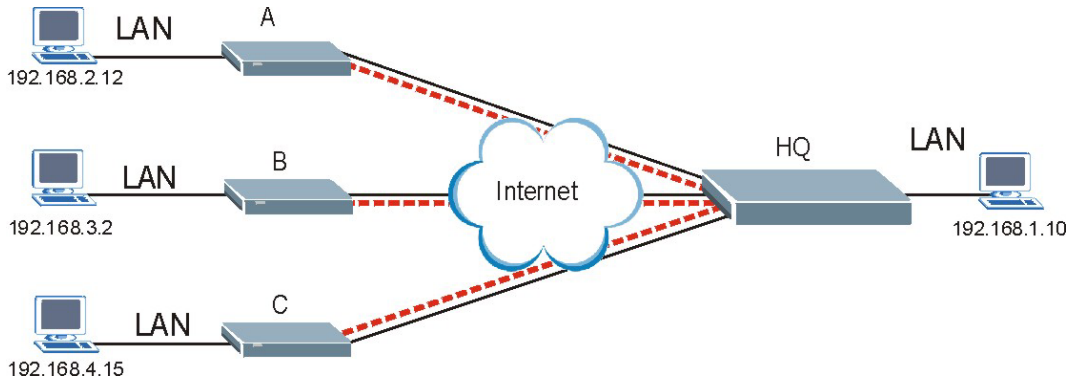


Figure 14-12 Telecommuters Using Unique VPN Rules Example

Table 14-13 Telecommuters Using Unique VPN Rules Example

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

Table 14-13 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters Prestige Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

14.18 Logs

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

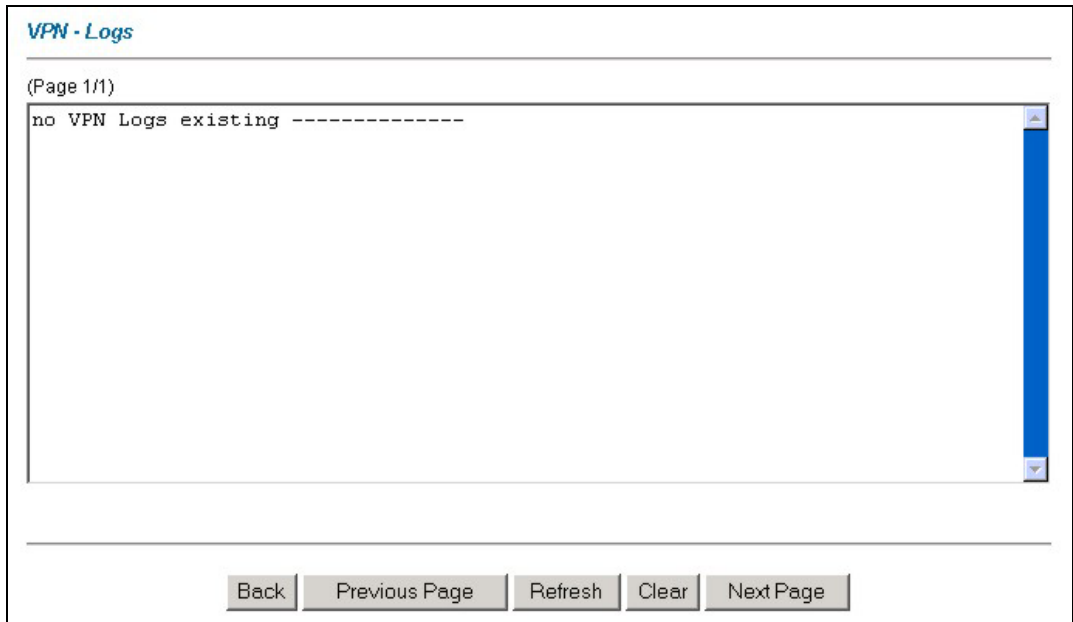


Figure 14-13 VPN Logs

The following table describes the labels in this screen.

Table 14-14 VPN Logs

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

Part IV:

NetCAPI and Supplementary Phone Services

This part contains information on configuring NetCAPI and supplementary phone services.

Chapter 15

NetAPI

This chapter covers the NetAPI screen.

15.1 NetAPI Overview

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

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

15.1 CAPI

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

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

15.1.1 ISDN-DCP

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

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

15.2 Configuring NetAPI

To edit your Prestige's NetAPI settings, click **Advanced**, **NetAPI**. The screen appears as shown.

NetCAPI

Active

Max Number of Registered Users

Incoming Data Call Number Matching

Start IP	End IP	Operation
<input type="text" value="192.168.1.132"/>	<input type="text" value="192.168.1.145"/>	<input type="text" value="Both"/>
<input type="text" value="192.168.14.1"/>	<input type="text" value="192.168.14.32"/>	<input type="text" value="Incoming"/>
<input type="text" value="192.168.20.7"/>	<input type="text" value="192.168.20.12"/>	<input type="text" value="Outgoing"/>
<input type="text" value="192.168.30.1"/>	<input type="text" value="192.168.30.3"/>	<input type="text" value="Both"/>
<input type="text" value="10.0.0.0"/>	<input type="text" value="10.255.255.255"/>	<input type="text" value="Incoming"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="None"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="None"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="None"/>
Default		<input type="text" value="Both"/>

Figure 15-1 Configuring NetCAPI

The following table describes the fields in this screen.

Table 15-1 Configuring NetCAPI

LABEL	Description
Active	Select this check box to enable NetCAPI.
Max Number of Registered Users	When you want to use NetCAPI to place outgoing calls or to listen to incoming calls, you must start RVSCOM on your computer, and RVSCOM registers itself to the Prestige. Enter the maximum number of clients (no more than 5) for which you want the Prestige to allow connections at the same time.

Table 15-1 Configuring NetCAPI

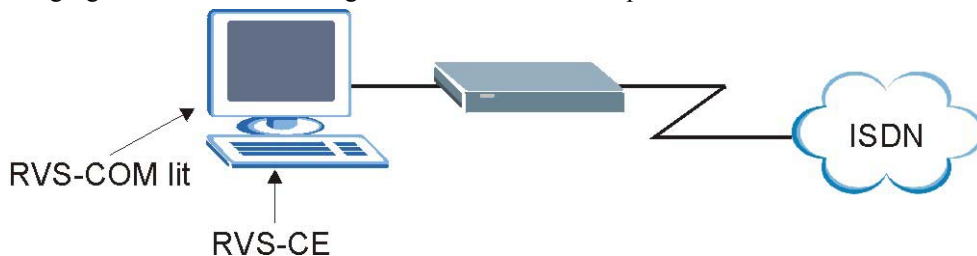
LABEL	Description
Incoming Data Call Number Matching	This field determines how incoming calls are routed. Select NetCAPI if you want to direct all incoming data calls to NetCAPI. Select Subscriber Number (MSN) if you want to direct all incoming call to the Prestige only when the incoming phone number matches the ISDN DATA number. If the incoming phone number does not match the ISDN DATA number, then the call will be routed to NetCAPI. Select Called Party Subaddress if you want to direct all incoming calls to the Prestige only when the incoming call matches the subaddress of ISDN DATA. If the incoming call does not match the subaddress of ISDN DATA, then the call will be routed to NetCAPI.
Start IP	Enter the first IP address of a group of NetCAPI clients. Each group contains contiguous IP addresses.
End IP	Enter the last IP address in a NetCAPI client group.
Operation	Select Incoming if you wish to grant incoming calls permission. Select Outgoing if you wish to grant outgoing calls permission. Select Both if you wish to grant both incoming calls and outgoing calls permissions. Select None if you wish to deny all calls.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to begin configuring this screen afresh.

15.2.1 Configuring the Prestige as a NetCAPI Server

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

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

The following figure illustrates the configuration used in this example.

**Figure 15-2 Configuration Example**

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

15.2.2 RVS-COM

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

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

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

15.2.3 Example of Installing a CAPI driver and Communication Software

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

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

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

Chapter 16

Supplementary Phone Services

This chapter discusses the European ISDN supplemental services.

16.1 Overview

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

Table 16-1 Supplemental Services In Europe

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

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

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

16.2 Setting Up Supplemental Phone Service

All Supplemental Phone Services are enabled by default except for Call Waiting, which is disabled by default but can be enabled in **Menu 2.1 – ISDN Advanced Setup**. The **Calling Line Indication**, or Caller ID, also

in this menu decides whether the other party can see your number when you call. If set to **Enable** (default), the Prestige sends the caller ID and the party you call can see your number, otherwise if set to **Disable**, the caller ID is blocked.

16.3 The Flash Key

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

16.4 Call Waiting

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

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

16.4.1 How to Use Call Waiting

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

Placing the Current Call on Hold

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

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

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

An incoming caller receives a busy signal if

- You have two calls active (one active and one on hold, or both active using Three-Way Calling) already.
- You are dialing a number on the B-channel the incoming caller is attempting to reach, but have not yet established a connection.

16.5 Three Way Calling

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

16.5.1 How to Use Three-Way Calling

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

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

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

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

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

To drop yourself from the conference call:

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

16.6 Call Transfer

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

16.6.1 How to Use Call Transfer

Transferring an active call to a third party:

1. Once you have an active call (Caller A), press the flash key to put Caller A on hold and receive a dial tone.
2. Dial the third party's telephone number (Caller B).
3. When you are ready to conference the two calls together, press the flash key to establish a three-way-conference call.
4. Hang up the telephone. The ISDN network does an implicit transfer to directly connect Caller A with Caller B.

16.6.2 To Do a Blind Transfer:

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

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

16.7 Call Forwarding

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

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

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

Table 16-2 Phone Flash Commands

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

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

16.8 Reminder Ring

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

16.9 Multiple Subscriber Number (MSN)

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

If you choose **MSN** to determine routing for all incoming calls, the Prestige will compare the incoming call's **Called Party Number** or **Subaddress** to the number you set and route the incoming call to the destination

that matches the number set. This feature is useful for those who connect a fax machine to one analog port while connecting a telephone set to the other analog port.

16.10 Using MSN

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

16.11 Terminal Portability (Suspend/Resume)

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

16.11.1 How to Suspend/Resume a Phone Call:

To suspend an active phone call

1. Press the flash key twice.
2. Dial *3n*#, where n is any number from 1 to 9.

To resume your phone call

1. Reconnect at a(n) (ISDN) telephone that is linked to the same S/T interface (Network Terminator-1, NT1) where you suspended the call.
2. Pick up the handset and press the flash key.
3. Dial #3n#, where n is any number from 1 to 9, but should be identical to that used above.

Part V:

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

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

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 only for diagnostic purposes.

System Status

System Status

System Name :
ZyNOS FW Version: V3.40(QI.0)b5 | 9/7/2004
Country: 225

WAN Information

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

LAN Information

MAC Address: 00:a0:c5:9a:c0:ba
IP Address: 192.168.1.1
IP Subnet Mask: 255.255.255.0
DHCP: Server
DHCP Start IP: 192.168.1.33
DHCP Pool Size: 6

Show Statistics

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 Firmware Version	This is the ZyNOS firmware version and the date the firmware was created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Country	This is the country code value (in decimal notation).
WAN Information	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
LAN Information	
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 the 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: 0:12:18
CPU Load: **2.09%**

WAN Port Statistics:

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

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

LAN Port Statistics:

Interface	Status	TxPkts	RxPkts	Collisions
Ethernet	100M/Full Duplex	426	730	0

Poll Interval(s) :

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.
CPU Load	This specifies the percentage of CPU utilization.

Table 17-2 System Status: Show Statistics

LABEL	DESCRIPTION
WAN Port Statistics	
Channel	This shows statistics for B1 and B2 channels respectively. This is the information displayed for each channel.
Link	This shows the name of the remote node or the user the channel is currently connected to or the status of the channel (e.g., Down, Idle, Calling, Answering, NetCAPi, etc.).
Type	This is the current connecting speed.
TxPkts	This is the number of transmitted packets on this channel.
RxPkts	This is the number of received packets on this channel.
Errors	This displays the number of error packets on this channel.
CLU	The CLU (Current Line Utilization) is the percentage of current bandwidth used on this channel.
ALU	The ALU (Average Line Utilization) is a 5-second moving average of usage for this channel.
Up Time	Time this channel has been connected to the current remote node.
Channel	This shows statistics for B1 and B2 channels respectively. This is the information displayed for each channel.
Own IP Addr	This refers to the IP address of the Prestige.
Own CLID	This shows your Caller ID.
Peer IP Addr	This refers to the IP address of the peer.
Peer CLID	This refers to the Caller ID of the peer.
LAN Port Statistics	
Interface	This shows the type of LAN interface connection.

Table 17-2 System Status: Show Statistics

LABEL	DESCRIPTION
Status	This displays the port speed and duplex setting.
TxPkts	This is the number of transmitted packets to the LAN.
RxPkts	This is the number of received packets from the LAN.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval(s) field.
Stop	Click Stop to stop refreshing statistics.

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

DHCP Table

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

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

17.4 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 device's specific model. Refer to the label on the bottom of your device.

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

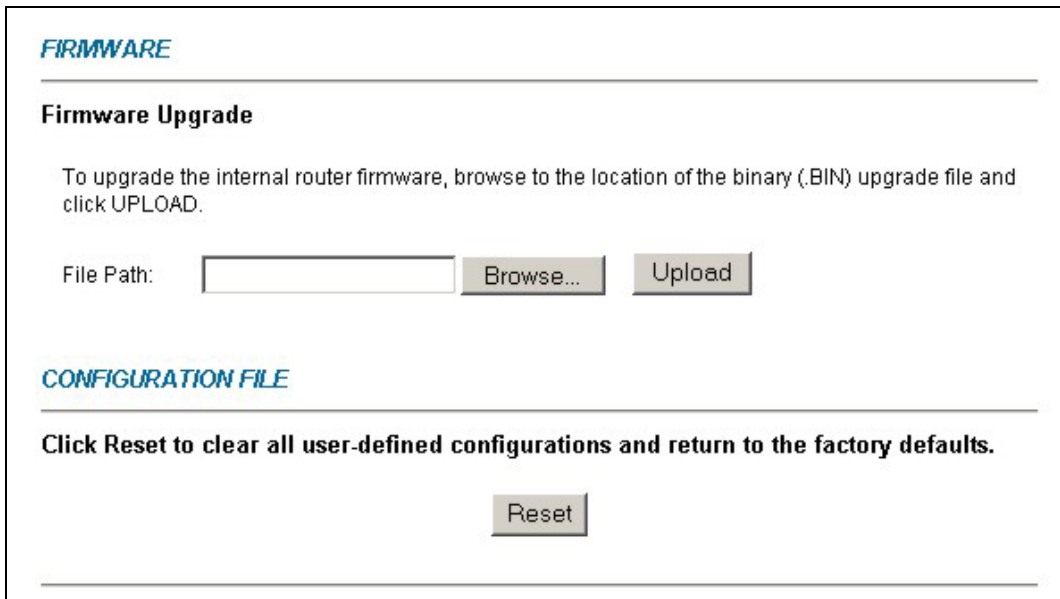


Figure 17-4 Firmware Upgrade

The following table describes the labels in this screen.

Table 17-4 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 Progress** 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.

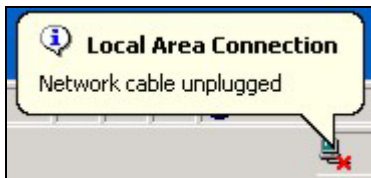


Figure 17-5 Network Temporarily Disconnected

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 17-6 Error Message

17.5 Budget Control

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

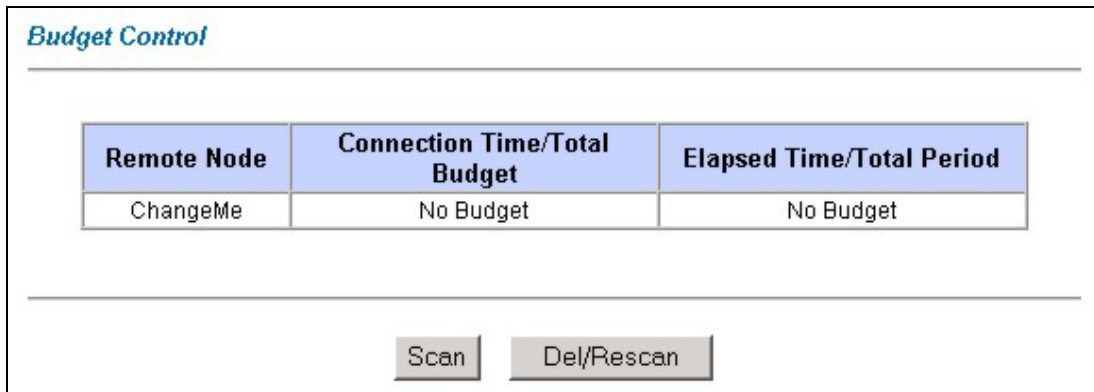


Figure 17-7 Budget Control

The following table describes the labels in this screen.

Table 17-5 Budget Control

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

Part VI:

General SMT Menus

This part explains how to access the System Management Terminal and covers LAN, ISDN and Ethernet Settings.

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 the System Management Terminal and gives an overview of its menus.

18.1 Introduction to the SMT

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

18.2 Accessing the Prestige 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.

18.2.1 Initial Screen

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

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

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.  
initialize ch =0, ethernet address: 00:a0:c5:9a:c0:ba  
(2) DSS1:  
Resetting ISDN .....  
Press ENTER to continue...
```

Figure 18-1 Initial Screen

18.2.2 Entering the Password

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

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

Please note that if there is no activity for longer than 5 minutes after you log in, the Prestige automatically logs you out and displays a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

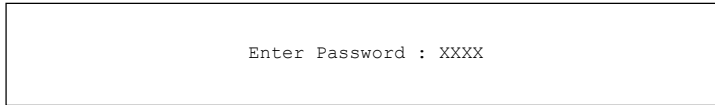


Figure 18-2 Login Screen

18.3 Accessing the Prestige 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.

18.4 Navigating the SMT Interface

The SMT (System Management Terminal) interface allows you to configure and manage your Prestige.

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

Table 18-1 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].

Table 18-1 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change No to Yes then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of No . Press [SPACE BAR] to change No to Yes , and then press [ENTER] to go to a "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively. When you are at the top of a menu, press the [UP] arrow key to move to the bottom of a menu.
Entering information	Fill in, or press [SPACE BAR], then press [ENTER] to select from choices.	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? >	All fields with the symbol <?> must be filled in order 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. Make sure you save your settings in each screen that you configure.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the Main Menu, as shown.

```

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

F202H Plus Main Menu

Getting Started
1. General Setup
2. ISDN Setup
3. Ethernet Setup
4. Internet Access Setup

Advanced Applications
11. Remote Node Setup
12. Static Routing Setup
13. Default Dial-in Setup
14. Dial-in User Setup
15. NAT Setup

Advanced Management
21. Filter Set Configuration
22. SNMP Configuration
23. System Security
24. System Maintenance
26. Schedule Setup
27. VPN/IPSec Setup
99. Exit

Enter Menu Selection Number:
    
```

Figure 18-3 SMT Main Menu

18.4.1 System Management Terminal Interface Summary

Table 18-2 Main Menu Summary

NO.	Menu Title	FUNCTION
1	General Setup	Use this menu to set up administrative information.
2	ISDN Setup	Use this menu to set up the ISDN.
3	Ethernet Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure IP static routes in this menu.
13	Default Dial-in Setup	Use this menu to set up default dial-in parameters so that your Prestige can be used as a dial-in server.
14	Dial-in User Setup	Use this menu to configure settings for remote dial-in users.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter Set Configuration	Use this menu to setup filters to provide security, call control, etc.

Table 18-2 Main Menu Summary

NO.	Menu Title	FUNCTION
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Security	Use this menu to set up security-related parameters.
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN /IPSec Setup	Use this menu to configure VPN connections.
99	Exit	Use this menu to exit (necessary for remote configuration).

18.5 SMT Menu Overview

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

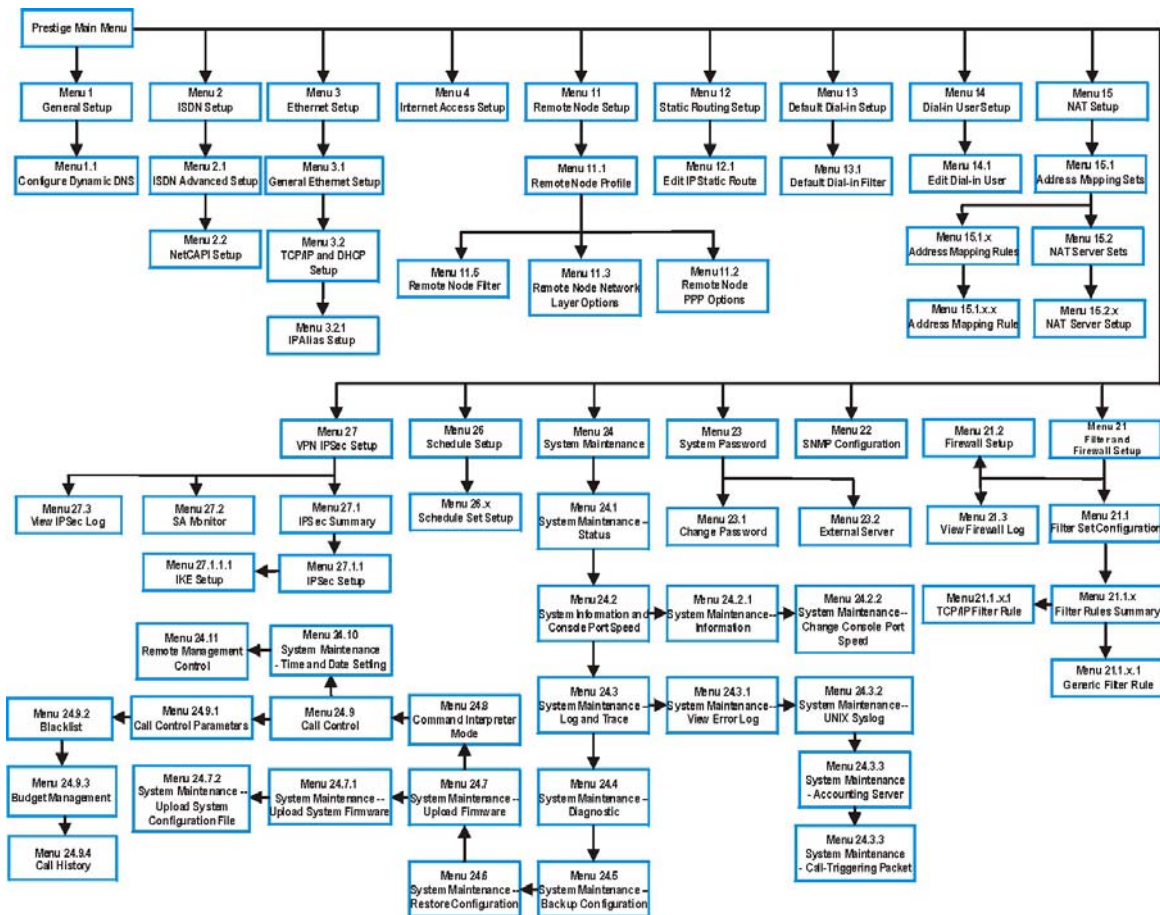


Figure 18-4 SMT Menu Overview

18.6 Changing the System Password

The first thing you should do is to change the system password by performing the following steps.

Step 1. Enter 23 in the Main Menu to open **Menu 23 - System Security** as shown below.

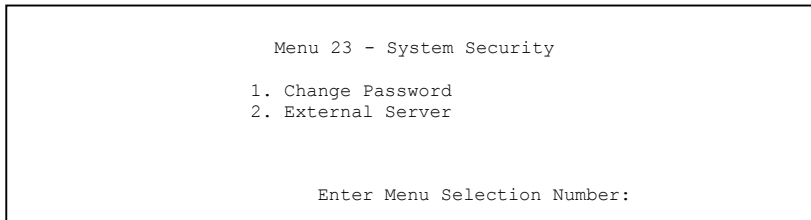


Figure 18-5 Menu 23.1 System Password

Step 2. Enter 1 in Menu 23 to open **Menu 23.1 - System Security - Change Password.**

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

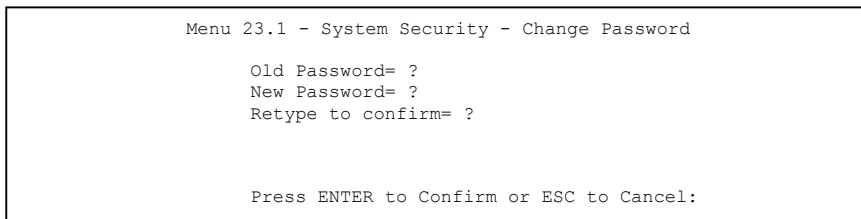


Figure 18-6 Menu 23.1 - System Security - Change Password

Step 4. Enter your new system password and press [ENTER].

Step 5. Re-type your new system password for confirmation and press [ENTER].

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

Chapter 19

SMT Menu 1 General Setup

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

19.1 General Setup Overview

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

19.1.1 General Setup and System Name

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

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

19.2 Configuring General Setup

Enter 1 in the Main Menu to open **Menu 1 – General Setup** as shown. Fill in the required fields for your applications, as explained in the following table.

```
Menu 1 - General Setup

System Name= ?
Location= MyHouse
Contact Person's Name= JohnDoe
Domain Name= zyxel.com.tw
Edit Dynamic DNS= No

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

Figure 19-1 Menu 1 General Setup

The following table describes the fields in this menu.

Table 19-1 Menu 1 General Setup

FIELD	DESCRIPTION
System Name	Choose 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.
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.
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.
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).
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.	

19.3 Configuring Dynamic DNS

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

```

      Menu 1.1 - Configure Dynamic DNS

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

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

Figure 19-2 Configure Dynamic DNS

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

FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select Yes and then press [ENTER] to make dynamic DNS active.
Host	Enter the domain name assigned to your Prestige by your Dynamic DNS provider.
EMAIL	Enter your e-mail address.
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.
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

ISDN Setup

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

20.1 ISDN Setup Overview

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

20.1.1 Supplementary Voice Services

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

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

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

20.1.2 ISDN Call Waiting

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

20.1.3 PABX Outside Line Prefix

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

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

20.1.4 Outgoing Calling Party Number

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

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

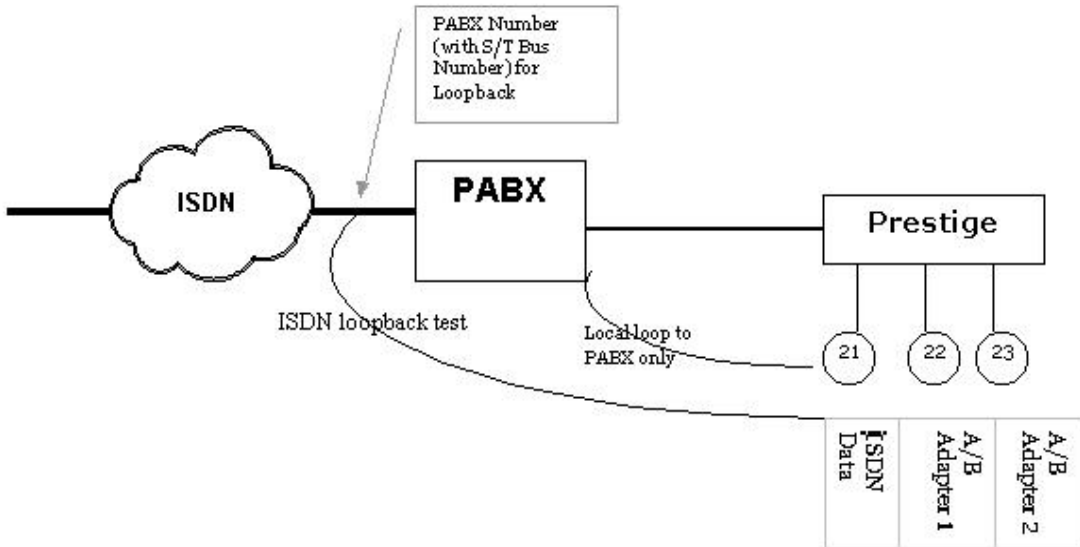


Figure 20-1 Prestige Behind a PABX

20.2 ISDN Setup

Enter 1 in the main menu to open menu 2 as shown next.

```

Menu 2 - ISDN Setup

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

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

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

Edit Advanced Setup = No
Edit NetCAPI Setup = No

Press ENTER to Confirm or ESC to Cancel:

```

Figure 20-2 Menu 2 ISDN Setup

The following table describes the fields in this menu.

Table 20-1 Menu 2 ISDN Setup

FIELD	DESCRIPTION								
Switch Type	This read only field displays your switch type, DSS-1.								
B Channel Usage	In general, this will be Switch/Switch (default). If you are only using one B channel (e.g., your Prestige is sharing the ISDN BRI line with another device), then select Switch/Unused . If your second B channel is a leased line, select Switch/Leased . Press [SPACE BAR] to toggle through all the options. The options are below.								
	<table border="0"> <tr> <td>◆ Switch/Unused</td> <td>◆ Leased/Unused</td> </tr> <tr> <td>◆ Switch/Switch</td> <td>◆ Unused/Leased</td> </tr> <tr> <td>◆ Switch/Leased</td> <td>◆ Leased/Leased</td> </tr> <tr> <td>◆ Leased/Switch</td> <td></td> </tr> </table>	◆ Switch/Unused	◆ Leased/Unused	◆ Switch/Switch	◆ Unused/Leased	◆ Switch/Leased	◆ Leased/Leased	◆ Leased/Switch	
◆ Switch/Unused	◆ Leased/Unused								
◆ Switch/Switch	◆ Unused/Leased								
◆ Switch/Leased	◆ Leased/Leased								
◆ Leased/Switch									
Incoming Phone Numbers:									
ISDN Data & Subaddress	Enter the telephone number and the subaddress assigned to ISDN data calls for the Prestige. The maximum number of digits is 25 for the telephone number and 5 for the subaddress.								

Table 20-1 Menu 2 ISDN Setup

FIELD	DESCRIPTION
A/B Adapter 1 & Subaddress	Enter the telephone number and the subaddress assigned to A/B Adapter 1 (PHONE1).
A/B Adapter 2 & Subaddress	Same as above for A/B Adapter 2 (PHONE2).
Incoming Phone Number Matching	Determines how incoming calls are routed. The choices for this field are Multiple Subscriber Number (MSN) , Called Party Subaddress and Don't Care .
Analog Call Routing	Select the destination for analog calls. The choices are A/B Adapter 1 , A/B Adapter 2 and Ignore . This field is only applicable when Incoming Phone Number Matching is Don't Care .
Global Analog Call	Select how to handle global analog calls. The choices are Accept and Ignore . This field is not applicable when the Analog Call Routing is Ignore .
Edit Advanced Setup	Advanced Setup features are configured when you select Yes to enter Menu 2.1 - ISDN Advanced Setup .
Edit NetCAPi Setup	Press the [SPACE BAR] to select Yes or No . Select Yes to configure Menu 2.2 - NetCAPi Setup (discussed next).
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

20.2.1 ISDN Advanced Setup

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


```

Menu 2.1 - ISDN Advanced Setup

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

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

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

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

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

Figure 20-3 Menu 2.1 ISDN Advanced Setup

The following table describes the fields in this menu.

Table 20-2 Menu 2.1 ISDN Advanced Setup

FIELD	DESCRIPTION
Phone 1/2 Call Waiting	The Call Waiting feature on your ISDN line works in exactly the same way as it does on a regular analog line. After hearing a call waiting indicator tone, press and immediately release the flash button on your telephone. This puts your current call on hold and answers the incoming call.
Calling Line Indication	The Calling Line Indication, or Caller ID, governs whether the other party can see your number when you call. If set to Enable, the Prestige sends the caller ID and the party you call can see your number; if it is set to Disable, the caller ID is blocked.
PABX Outside Line Prefix	Enter the number for outside line access if the Prestige is connected to a PABX; otherwise, leave it blank. The maximum number of digits is 4.
PABX Number (Include S/T Bus Number) for Loopback	Enter the S/T bus number if the Prestige is connected to an ISDN PABX. If this field is left as blank then the ISDN loopback test will be skipped.
Outgoing Calling Party Number	You only need to fill in this field if your switch requires a specific Outgoing Calling Party Number; otherwise, leave it blank.

Table 20-2 Menu 2.1 ISDN Advanced Setup

FIELD	DESCRIPTION
ISDN Data	Enter the telephone number(s) assigned to your ISDN line by your telephone company. Some switch types only have one telephone number. Note that the Prestige only accepts digits; please do not include '-' or spaces in this field. This field should be no longer than 25 digits.
A/B Adapter 1	Enter the telephone number assigned to A/B Adapter 1 (PHONE1).
A/B Adapter 2	Enter the telephone number assigned to A/B Adapter 2 (PHONE2).
Hangup Silence Time(sec)	Most answering machines automatically terminate a call after a predefined length of silence. Specify the time in seconds that elapses before the answering machine drops the call when the Prestige receives tones from the switch and send a silence tone to the answering machine.
Data Link Connection	There are two types of ISDN Data Link Connection namely: point-to-multipoint and point-to-point . When you select point-to-multipoint, the TE1 value will be assigned by negotiation with the switch. When you select point-to-point, the TE1 value will be assigned a unique value of 0.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

20.2.2 Configuring Advanced Setup

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

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

```

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

```

Figure 20-4 Loopback Test

20.3 NetCAPI

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

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

See *NetCAPI* chapter for more information regarding CAPI drivers.

20.3.1 Configuring NetCAPI

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

```

Menu 2.2 - NetCAPI Setup

Active= No

Max Number of Registered Users= 1
Incoming Data Call Number Matching= NetCAPI

Access List:
  Start IP      End IP      Operation
192.168.1.132  192.168.1.145  Both
192.168.14.1   192.168.14.32  Incoming
192.168.20.7   192.168.20.12  Outgoing
192.168.30.1   192.168.30.3   Both
10.0.0.0       10.255.255.255 Incoming
0.0.0.0        0.0.0.0        None
0.0.0.0        0.0.0.0        None
0.0.0.0        0.0.0.0        None
default        0.0.0.0        Both

Press ENTER to Confirm or ESC to Cancel:

```

Figure 20-5 Menu 2.2 NetCAPI Setup

The following table describes the fields in this screen.

Table 20-3 Menu 2.2 NetCAPI Setup

FIELD	DESCRIPTION
Active	This field allows you to enable or disable NetCAPI. Press the [SPACEBAR] to select Yes or No

Table 20-3 Menu 2.2 NetCAPI Setup

FIELD	DESCRIPTION
Max Number of Registered Users	When you want to use NetCAPI to place outgoing calls or to listen to incoming calls, you must start RVSCOM on your computer, and RVSCOM will register itself to the Prestige. This option is the maximum number of clients that the Prestige supports at the same time.
Incoming Data Call Number Matching	This field determines how incoming calls are routed. Select NetCAPI if you want to direct all incoming data calls to NetCAPI. Select Subscriber Number (MSN) if you want to direct all incoming call to the Prestige only when the incoming phone number matches the ISDN DATA number. If the incoming phone number does not match the ISDN DATA number, then the call will be routed to NetCAPI. Select Called Party Subaddress if you want to direct all incoming calls to the Prestige only when the incoming call matches the subaddress of ISDN DATA. If the incoming call does not match the subaddress of ISDN DATA, then the call will be routed to NetCAPI.
Access List:	
Start IP	Refers to the first IP address of a group of NetCAPI clients. Each group contains contiguous IP addresses
End IP	Refers to the last IP address in a NetCAPI client group.
Operation	Select Incoming if you wish to grant incoming calls permission. Select Outgoing if you wish to grant outgoing calls permission. Select Both if you wish to grant both incoming calls and outgoing calls permissions. Select None if you wish to deny all calls.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

Chapter 21

Ethernet Setup

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

21.1 Ethernet Setup

This section describes how to configure the Ethernet using **Menu 3 – Ethernet Setup**. From the Main Menu, enter 3 to open **Menu 3 - Ethernet Setup**.

```
Menu 3 - Ethernet Setup

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

Enter Menu Selection Number:
```

Figure 21-1 Menu 3 Ethernet Setup

21.1.1 General Ethernet Setup

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

```
Menu 3.1 - General Ethernet Setup

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

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

Figure 21-2 Menu 3.1 General Ethernet Setup

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

21.2 Ethernet TCP/IP and DHCP Server

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

21.3 Configuring TCP/IP Ethernet and DHCP

You will now use **Menu 3.2-TCP/IP and DHCP Ethernet Setup** to configure your Prestige for TCP/IP.

To edit menu 3.2, select the menu option **Ethernet Setup** in the Main Menu. When menu 3 appears, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2 – TCP/IP and DHCP Ethernet Setup**, as shown.

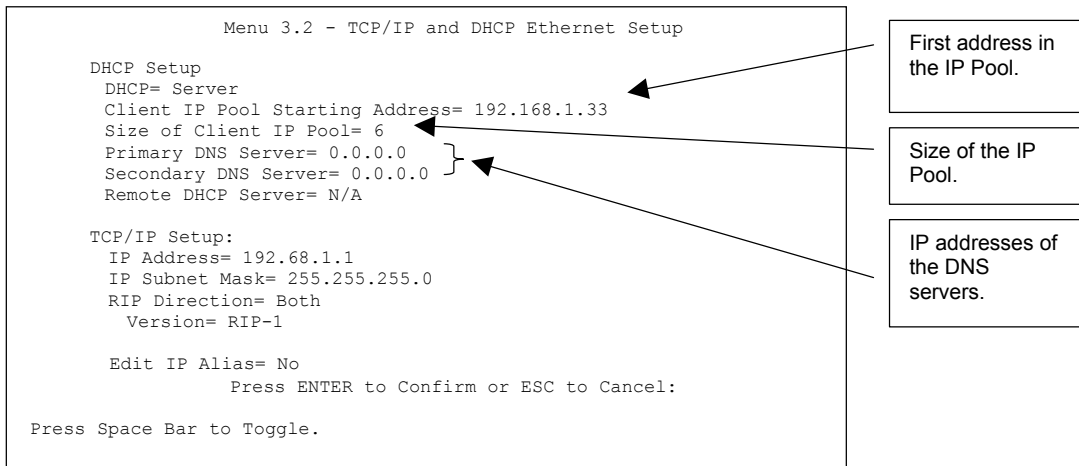


Figure 21-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup

The following table describes the fields in this screen.

FIELD	DESCRIPTION
DHCP Setup	
DHCP	<p>This field enables/disables the DHCP server. If set to Server, your Prestige will act as a DHCP server. If set to None, the DHCP server will be disabled. If set to Relay, the Prestige acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients.</p> <p>When set to Server, the following four items need to be set:</p>

FIELD	DESCRIPTION
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Remote DHCP Server	If Relay is selected in the DHCP field above, then enter the IP address of the actual, remote DHCP server here.

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

FIELD	DESCRIPTION
TCP/IP Setup	
IP Address	Enter the IP address of your Prestige in dotted decimal notation.
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.
RIP Direction	Press [SPACE BAR] to select the RIP direction from Both/None/In Only/ Out Only .
Version	Press [SPACE BAR] to select the RIP version from RIP-1/RIP-2B/ RIP-2M .
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to select Yes and then press [ENTER] to display menu 3.2.1
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

21.4 IP Alias Setup

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

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

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= Yes
IP Address= 192.168.2.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-1
Incoming protocol filters=
Outgoing protocol filters=
IP Alias 2= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A

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

Figure 21-4 Menu 3.2.1 IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1 or 2	Choose Yes to configure the LAN for the Prestige.
IP Address	Enter the IP address of your Prestige in dotted decimal notation.
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from Both , In Only and Out Only .
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from RIP-1 , RIP-2B and RIP-2M .
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

Chapter 22

Internet Access Setup

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

22.1 Internet Access Overview

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in Menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information from your ISP (see *Quick Start Guide*). From the Main Menu, enter option **Internet Access Setup** to go to **Menu 4 – Internet Access Setup**, as shown in the following figure.

22.2 Internet Access Setup

The table following this menu contains instructions on how to configure your Prestige for Internet access.

```
Menu 4 - Internet Access Setup
ISP's Name= ChangeMe
Pri Phone #= 1234
Sec Phone #=
My Login= ChangeMe
My Password= *****
My WAN IP Addr= 0.0.0.0

NAT= SUA Only
Address Mapping Set= N/A

Telco Options:
Transfer Type= 64K

Multilink= Off
Idle Timeout= 100

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

Enter the phone number of your ISP.

Enter login name and password.

Figure 22-1 Menu 4 Internet Access Setup

The following table describes the fields in this screen.

Table 22-1 Menu 4 Internet Access Setup

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Pri/Sec Phone #	Both the Primary and the Secondary Phone number refer to the number that the Prestige dials to connect to the ISP.
My Login	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
My WAN IP Addr	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige. NOTE: This is the address assigned to your local router WAN, not the remote router. If the remote router is a router, then this entry determines the local router Rem IP Addr in Menu 11.1.
NAT	Choose from None , Full Feature or SUA Only . When you select Full Feature you must configure at least one address mapping set. See the chapter on NAT for a full discussion of this new feature.
Address Mapping Set	A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu). You may enter any server set number up to 10, but the first one is used for SUA only.
Telco options: Transfer Type	This field specifies the type of connection between the Prestige and this remote node. Select 64K, or Leased.
Multilink	The Prestige uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is 64K. Options for this field are: Off , BOD and Always .
Idle Timeout	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your Prestige. Administrative packets such as RIP are not counted as data.

Idle Timeout only applies when the Prestige initiates the call.

When you are finished, press [ENTER] at the message: 'Press ENTER to confirm or ESC to Cancel'. At this point, the SMT will ask if you wish to test the Internet connection. If you select **Yes**, your Prestige will

call the ISP to test the Internet connection. If the test fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

Part VII:

Advanced SMT Applications

This part describes the advanced applications of your Prestige, such as Remote Node Configuration, Dial-in Configuration and NAT.

Chapter 23

Remote Node Configuration

This chapter covers the configuration of remote nodes.

23.1 Remote Node Overview

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use Menu 4 to set up Internet access, you are actually configuring one of the remote nodes. Once a remote node is configured correctly, traffic to the remote network will trigger your Prestige to make a call automatically, i.e., Dial on Demand.

23.1.1 Minimum Toll Period

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

23.2 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, enter the number of the remote node that you wish to configure.

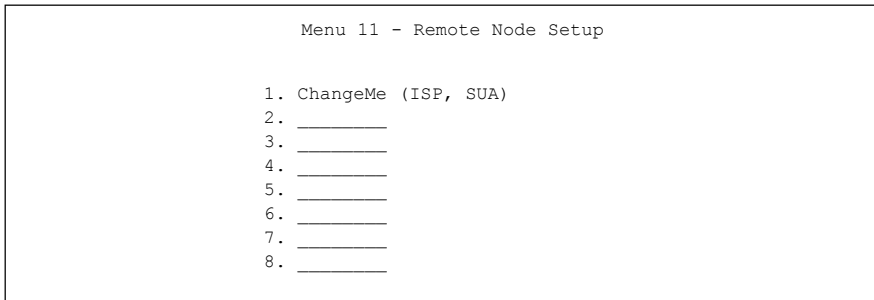


Figure 23-1 Menu 11 Remote Node Setup

When **Menu 11.1 – Remote Node Profile** appears, fill in the fields as described in the following table to define this remote profile. The following table shows you how to configure the Remote Node Menu.

<pre> Menu 11.1 - Remote Node Profile Rem Node Name= nodename Active= Yes Call Direction= Outgoing Incoming: Rem Login= N/A Rem Password= N/A Rem CLID= N/A Call Back= N/A Outgoing: My Login= ChangeMe My Password= ***** Authen= CHAP/PAP Pri Phone #= 1234567 Sec Phone #= Edit PPP Options= No Rem IP Addr= 0.0.0.0 Edit IP= No Telco Option: Transfer Type= 64K Allocated Budget(min)= 0 Period(hr)= Schedules= Carrier Access Code= Nailed-Up Connection= No Toll Period(sec)= 0 Session Options: Edit Filter Sets= No Idle Timeout(sec)= 100 </pre>	<div style="border: 1px solid black; padding: 5px; width: fit-content;">Edit PPP Options in menu 11.2.</div> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin-top: 20px;">Edit IP Options in menu 11.3.</div> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin-top: 20px;">Edit Filter Sets in menu 11.5.</div>
--	---

Figure 23-2 Menu 11.1 Remote Node Profile

Table 23-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	This is a required field [?]. Enter a descriptive name for the remote node, for example, Corp. This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name.	
Active	Press [SPACE BAR] and then [ENTER] to select Yes (activate remote node) or No (deactivate remote node).	Yes
Call Direction	<p>If this parameter is set to Both, your Prestige can both place and receive calls to/from this remote node.</p> <p>If set to Incoming, your Prestige will not place a call to this remote node.</p> <p>If set to Outgoing, your Prestige will drop any incoming calls from this remote node.</p> <p>Several other fields in this menu depend on this parameter. For example, in order to enable Callback, the Call Direction must be set to Both.</p>	Outgoing
Incoming:		
Rem Login	<p>Enter the login name that this remote node will use when it calls your Prestige.</p> <p>The login name in this field combined with the Rem Password will be used to authenticate this node.</p>	
Rem Password	Enter the password used when this remote node calls your Prestige.	
Rem CLID	<p>This field is applicable only if Call Direction is either set to Both or Incoming. Otherwise, a N/A appears in the field.</p> <p>This is the Calling Line ID (the telephone number of the calling party) of this remote node.</p> <p>If you enable the CLID Authen field in Menu 13 – Default Dial-In Setup, your Prestige will check the CLID in the incoming call against the CLIDs in the database. If no match is found and CLID Authen is set to Required, the call will be dropped.</p>	

Table 23-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Call Back	<p>This field is applicable only if Call Direction is set to Both. Otherwise, a N/A appears in the field.</p> <p>This field determines whether or not your Prestige will call back after receiving a call from this remote node.</p> <p>If this option is enabled, your Prestige will disconnect the initial call from this node and call it back at the Outgoing Primary Phone Number (see section <i>25.4 Callback Overview</i>).</p>	Yes
Outgoing:		
My Login	This is a required field [?] if Call Direction is either Both or Outgoing . Enter the login name for your Prestige when it calls this remote node.	
My Password	This is a required field [?] if Call Direction is either Both or Outgoing . Enter the password for your Prestige when it 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 only.</p> <p>PAP – accept PAP only.</p>	CHAP/PAP
Pri(mary) Sec(ondary) Phone #	<p>Your Prestige always calls this remote node using the Primary Phone number first for a dial-up line.</p> <p>If the Primary Phone number is busy or does not answer, your Prestige will dial the Secondary Phone number if available.</p> <p>Some areas require dialing the pound sign # before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.</p>	
Edit PPP Options	To edit the PPP options for this remote node, move the cursor to this field. Press [SPACE BAR] and then [ENTER] to select Yes and press [ENTER]. This will bring you to Menu 11.2 – Remote Node PPP Options. For more information on configuring PPP options, see section <i>23.6</i> .	No
Rem IP Addr	This is a required field [?] if Route is set to IP . Enter the IP address of the remote gateway.	

Table 23-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Edit IP	Press [SPACE BAR] to select Yes and press [ENTER] to go to Menu 11.3 – Remote Node Network Layer Options.	No
Telco Options:		
Transfer Type	This field specifies the type of connection between the Prestige and this remote node. When set to Leased , the Allocated Budget and Period do not apply.	64k
Allocated Budget (min)	This field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 for no budget control.	Default = 0
Period (hr)	This field sets the time interval to reset the above outgoing call budget control.	
Schedules	Apply up to 4 schedule sets, separated by commas to your remote node here. Please see ahead for a full discussion on schedules.	
Carrier Access Code	In some European countries, you need to enter the access code number of your preferred telecommunications service provider. Your telephone company should supply you with this number.	
Nailed-up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. See the following section for more details.	No
Toll Period	This is the basic unit of time for charging purposes, e.g., 25 cents every 3 minutes – 3 minutes is the Toll Period.	
Session Options:		
Edit Filter Sets	Press [SPACE BAR] and then [ENTER] to select Yes to open Menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.	Default = No
Idle Timeout (sec)	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your Prestige. Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes). Idle timeout only applies when the Prestige initiates the call. 0 sec means the remote node will never be automatically disconnected.	Default = 300 secs
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

23.3 Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. 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 you encounter the case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

23.4 PPP Multilink

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

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

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

23.5 Bandwidth on Demand

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

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

Table 23-2 BTR vs MTR for BOD

BTR AND MTR SETTING	No. of Channel(s) Used	Max. No. of Channel(s) Used	BANDWIDTH ON DEMAND
BTR = 64, MTR = 64	1	1	Off
BTR = 64, MTR = 128	1	2	On
BTR = 128, MTR = 128	2	2	Off

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

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

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

23.6 Editing PPP Options

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

```

Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No
BACP= Enable

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

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

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

Figure 23-3 Menu 11.2 Remote Node PPP Options

The following table describes the fields in this menu.

Table 23-3 Menu 11.2 Remote Node PPP Options

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

Table 23-3 Menu 11.2 Remote Node PPP Options

FIELD	DESCRIPTION	EXAMPLE
Target Utility (Kbps)	Enter the two thresholds separated by a [-] for subtracting and adding the second port.	Default = 32-48
Add Persist	This parameter specifies the number of seconds where traffic is above the adding threshold before the Prestige will bring up the second link.	Default = 5 sec
Subtract Persist	This parameter specifies the number of seconds where traffic is below the subtraction threshold before your Prestige drops the second link.	Default = 5 sec

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.

23.7 LAN-to-LAN Application

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

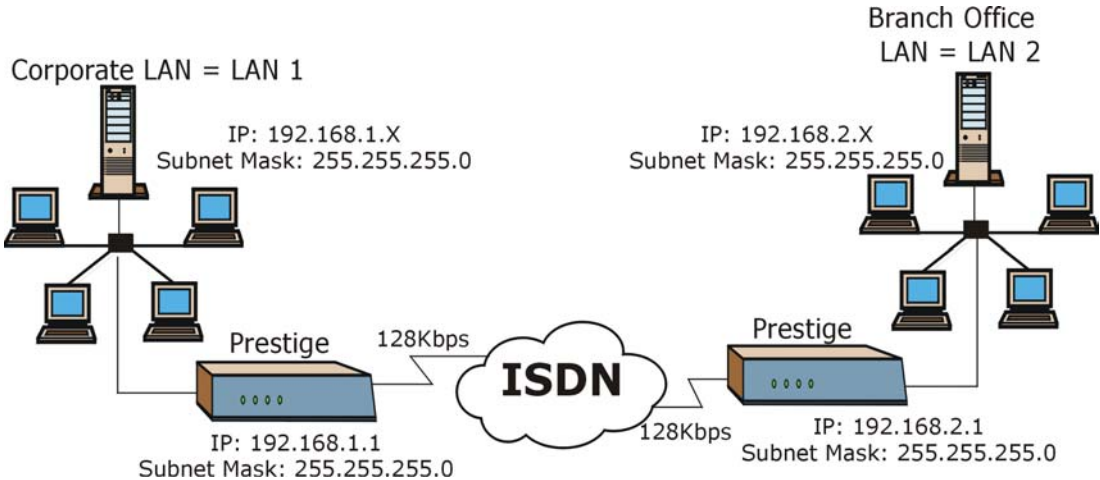


Figure 23-4 TCP/IP LAN-to-LAN Application

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

LAN 1 Setup

```
Menu 11.1 - Remote Node Profile

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

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

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

IP address of the Prestige on LAN 2.

Figure 23-5 LAN 1 Setup

LAN 2 Setup

```
Menu 11.1 - Remote Node Profile

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

Incoming:
  Rem Login= lan1            Telco Option:
  Rem Password= *****    Transfer Type= 64K
  Rem CLID=                  Allocated Budget(min)= 0
  Call Back= No              Period(hr)= 0
Outgoing:                    Schedules=
  My Login= lan2             Carrier Access Code=
  My Password= *****      Nailed-Up Connection= No
  Authen= CHAP/PAP           Toll Period(sec)= 0
  Pri Phone #= 027176324     Session Options:
  Sec Phone #=                Edit Filter Sets= No
                               Idle Timeout(sec)= 300

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

IP address of the Prestige on LAN 1.

Figure 23-6 LAN 2 Setup

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

23.8 Configuring Network Layer Options

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

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

Table 23-4 TCP/IP-related Fields in Remote Node Profile

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

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

```

Menu 11.3 - Remote Node Network Layer Options

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

NAT= Full Feature
    Address Mapping Set= 0

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

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

Table 23-5 Remote Node Network Layer Options

The following table describes the fields in this menu.

Table 23-6 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
Rem IP Addr	This will show the IP address you entered for this remote node in the previous menu.	
Rem Subnet Mask	Enter the subnet mask for the remote network.	
My WAN Addr	<p>Some implementations, especially the UNIX derivatives, require the ISDN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the ISDN port of your Prestige.</p> <p>NOTE: This is the address assigned to your local Prestige WAN, not the remote router. If the remote router is a Prestige, then this entry determines the local Prestige Rem IP Addr in Menu 11.1.</p>	

Table 23-6 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
NAT Address Mapping Set	Choose from None , Full Feature , or SUA Only . When you select Full Feature you must configure at least one address mapping set. For more information about NAT and the choices listed refer to the NAT Chapter. A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA Menu 15.1 before). You may enter any server set number up to 10 but the first one is used for SUA only.	Full Feature
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
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 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 from Both/In Only/Out Only/None .	None (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from RIP-1/RIP-2B/RIP-2M .	RIP-2B (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.		

The following diagram shows the sample IP addresses to help you understand the field of **My Wan Addr** in Menu 11.3.

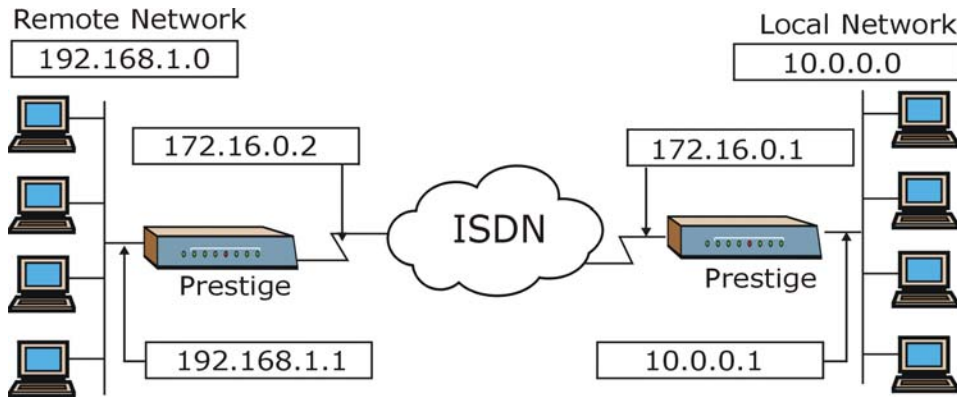


Figure 23-7 Sample IP Addresses for LAN-to-LAN Connection

23.9 Configuring 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, e.g., 1, 5, 9, 12, in each **filter** field. The default is no filters.

Note that spaces are accepted in this field. The Prestige comes with a prepackaged filter set, `NetBIOS_WAN`, that blocks NetBIOS packets (call protocol filter = 1). You can include this in the call filter sets if you wish to prevent NetBIOS packets from triggering calls to a remote node.

To specify remote node filters, move the cursor to the **Edit Filter Sets** field in **Menu 11.1 – Remote Node Profile**, and use [SPACE BAR] to select **Yes**. Press [ENTER] to open Menu 11.5, as shown next.

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Call Filter Sets:
  protocol filters= 1
  device filters=

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

Figure 23-8 Menu 11.5 Remote Node Filter

Chapter 24

Static Route Setup

This chapter shows how to set up static routes.

24.1 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 diagram 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 2. The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

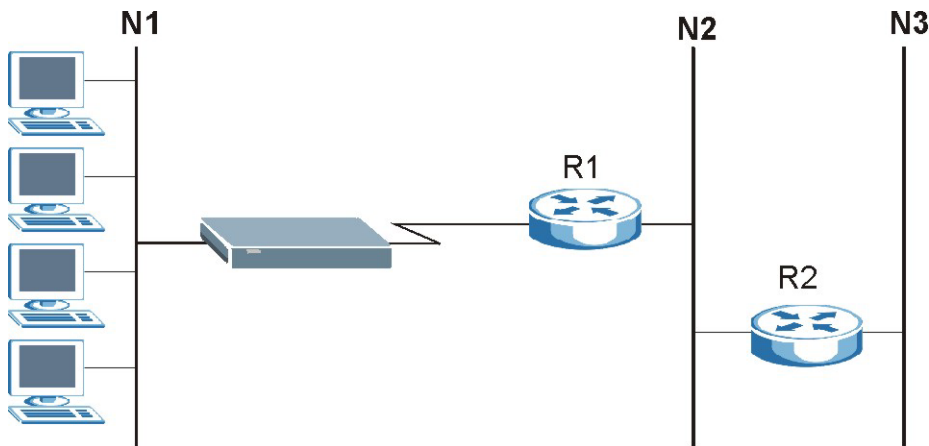


Figure 24-1 Sample Static Routing Topology

To configure an IP static route, use **Menu 12 – IP Static Route Setup**, as displayed next.

```

Menu 12 - IP Static Route Setup

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

Enter selection number:
    
```

Figure 24-2 Menu 12 IP Static Route Setup

From Menu 12, select one of the available IP static routes to open **Menu 12.1 – Edit IP Static Route**, as shown next.

```

Menu 12.1 - Edit IP Static Route

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

Figure 24-3 Menu 12.1 Edit IP Static Route

Table 24-1 Menu 12.1 Edit IP Static Route

FIELD	DESCRIPTION
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.

Table 24-1 Menu 12.1 Edit IP Static Route

FIELD	DESCRIPTION
IP Subnet Mask	Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include 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 broadcast. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] to cancel.	

Chapter 25

Dial-in Setup

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

25.1 Dial-in Users Overview

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

Table 25-1 Remote Dial-in Users/Remote Nodes Comparison Chart

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

25.2 Default Dial-in User Setup

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

25.2.1 CLID Callback Support For Dial-In Users

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

25.3 Setting Up Default Dial-in

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

```

Menu 13 - Default Dial-in Setup

Telco Options:                                IP Address Supplied By:
CLID Authen= Required                        Dial-in User= Yes
                                             IP Pool= No
                                             IP Start Addr= N/A
                                             IP Count(1,2)= N/A

PPP Options:                                  Session Options:
Recv Authen= CHAP/PAP                        Edit Filter Sets= No
Compression= Yes
Mutual Authen= No
O/G Username=
O/G Password= *****
Multiple Link Options:
  Max Trans Rate(Kbps)= 128

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

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

Figure 25-1 Menu 13 Default Dial-in Setup

Table 25-2 Menu 13 Default Dial-in Setup

FIELD	DESCRIPTION	EXAMPLE
Telco Options:		
CLID Authen	This field sets the CLID authentication parameter for all incoming calls. There are three options for this field: None – No CLID is required. Required – CLID must be available, or the Prestige will not answer the call. Preferred – If the CLID is available then CLID will be used; otherwise, authentication is performed in PPP negotiation.	Required
PPP Options:		

Table 25-2 Menu 13 Default Dial-in Setup

FIELD	DESCRIPTION	EXAMPLE
Recv Authen	This field sets the authentication protocol for incoming calls. For security reason, setting authentication to None is strongly discouraged. Options for this field are: CHAP/PAP – Your Prestige will try CHAP first, but PAP will be used if CHAP is not available. CHAP – Use CHAP only. PAP – Use PAP only. None – Your Prestige tries to acquire CHAP/PAP first, but no authentication is required if CHAP/PAP is not available.	CHAP/PAP
Compression	Turn on/off Stac Compression. The default for this field is No .	Yes
Mutual Authen	Some vendors, e.g., Cisco, require mutual authentication, i.e., the node that initiates the call will request a user name and password from the far end that it is dialing to. If the remote node requires mutual authentication, set this field to Yes .	No
O/G Username	Enter the login name to be used to respond to the peer's authentication request.	
O/G Password	Enter the outgoing password to be used to respond to the peer's authentication request.	
Multiple Link Options:		
Max Trans Rate(Kbps)	Enter the maximum data transfer rate between your Prestige and the remote dial-in user. 64 – At most, one B channel is used. 128 – A maximum of two channels can be used. When the Prestige calls back to the remote dial-in user, the maximum data transfer rate is always 64.	128
Callback Budget Management:		
Allocated Budget (min)	This field sets the budget callback time for all the remote dial-in users. The default for this field is 0 for no budget control.	0 (default)
Period (hr)	This field sets the time interval to reset the above callback budget control.	
IP Address Supplied By:		

Table 25-2 Menu 13 Default Dial-in Setup

FIELD	DESCRIPTION	EXAMPLE
Dial-in User	<p>If set to Yes, the Prestige will allow a remote host to specify its own IP address.</p> <p>If set to No, the remote host must use the IP address assigned by your Prestige from the IP pool, configured below. This is to prevent the remote host from using an invalid IP address and potentially disrupting the whole network.</p>	Yes (default)
IP Pool	<p>This field tells your Prestige to provide the remote host with an IP address from the pool. This field is required if Dial-In IP Address Supplied By: Dial-in User is set to No. You can configure this field even if Dial-in User is set to Yes, in which case your Prestige will accept the IP address if the remote peer specifies one; otherwise, an IP address is assigned from the pool.</p>	No (default)
IP Start Addr	<p>This field is applicable only if you selected Yes in the Dial-In IP Address Supplied By: IP Pool field.</p> <p>The IP pool contains contiguous IP addresses and this field specifies the first one in the pool. The IP start address is the start of a series of consecutive IP addresses.</p>	
IP Count (1, 2)	<p>In this field, enter the number (1 or 2) of addresses in the IP Pool. For example, if the starting address is 192.168.135.5 and the count is 2, then the pool will have 192.68.135.5 and 192.68.135.6. The IP count is the number of consecutive IP addresses allowed.</p>	1
Session Options: Edit Filter Sets	<p>Press [SPACE BAR] and then [ENTER] to select Yes to edit the filter sets. Keep in mind that the filter set(s) will only apply to remote dial-in users but not the remote nodes.</p> <p>NOTE: Spaces and [-] symbol are accepted in this field. For more information on customizing your filter sets, see <i>Chapter 9 – Filter Configuration</i>. The default is blank, i.e., no filters.</p>	No (default)
<p>Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] to cancel.</p>		

25.3.1 Default Dial-in Filter

Use **Menu 13.1 – Default Dial-in Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between all dial-in users and your Prestige. Note that the filter set(s) only applies to the dial-in users

but not the remote nodes. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each filter field. The default is no filters.

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

```
Menu 13.1 - Default Dial-in Filter

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

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

Figure 25-2 Menu 13.1 Default Dial-in Filter

25.4 Callback Overview

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

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

25.5 Dial-In User Setup

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

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

```

Menu 14 - Dial-in User Setup

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

Enter Menu Selection Number:
    
```

Figure 25-3 Menu 14 Dial-in User Setup

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

```

Menu 14.1 - Edit Dial-in User

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

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

Figure 25-4 Menu 14.1 Edit Dial-in User

Table 25-3 Edit Dial-in User

FIELD	DESCRIPTION	EXAMPLE
User Name	This is a required field. This will be used as the login name for authentication. Choose a descriptive word for login, for example, johndoe.	johndoe
Active	You can disallow dial-in access to this user by setting this field to inactive. Inactive users are displayed with a [-] (minus sign) at the beginning of the name in Menu 14.	Yes
Password	Enter the password for the remote dial-in user.	

Table 25-3 Edit Dial-in User

FIELD	DESCRIPTION	EXAMPLE
Callback	<p>This field determines if your Prestige will allow call back to this user upon dial-in. If this option is enabled, your Prestige will call back to the user if requested. In such a case, your Prestige will disconnect the initial call from this user and dial back to the specified callback number (see ahead).</p> <p>No – The default is no callback.</p> <p>Optional – The user can choose to disable callback.</p> <p>Mandatory – The user cannot disable callback.</p>	No (default)
Phone # Supplied by Caller	<p>This option allows the user to specify the call back telephone number on a call-by-call basis. This is useful when your Prestige returns a call back to a mobile user at different numbers, e.g., a sales rep. in a hotel.</p> <p>If the setting is Yes, the user can specify and send to the Prestige the callback number of his/her choice.</p> <p>The default is No, i.e., your Prestige always calls back to the fixed callback number.</p>	No (default)
Callback Phone #	If Phone # Supplied by Caller is No , then this is a required field. Otherwise, a N/A will appear in the field. Enter the telephone number to which your Prestige will call back.	
Rem CLID	If you enable CLID Authen field in Menu 13, then you need to specify the telephone number from which this user calls. Your Prestige will check the CLID in the incoming call against the CLIDs in the database. If they do not match and CLID Authen is Required , your Prestige will not answer the call.	
Idle Time-out	<p>Enter the idle time (in seconds). This time-out determines how long the dial-in user can be idle before your Prestige disconnects the call when the Prestige is calling back.</p> <p>Idle time is defined as the period of time where there is no data traffic between the dial-in user and your Prestige. The default is 100 seconds.</p>	100 seconds
Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] to cancel.		

25.6 Telecommuting Application With Windows Example

Telecommuting enables people to work at remote sites and yet still have access to the resources in the business office. Typically, a telecommuter will use a client workstation with TCP/IP and dial-out capabilities, e.g., a Windows® PC or a Macintosh. For telecommuters to call in to your Prestige, you need to configure a

dial-in user profile for each telecommuter. Additionally, you need to configure the Default Dial-in User Setup to set the operational parameters for all dial-in users.

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

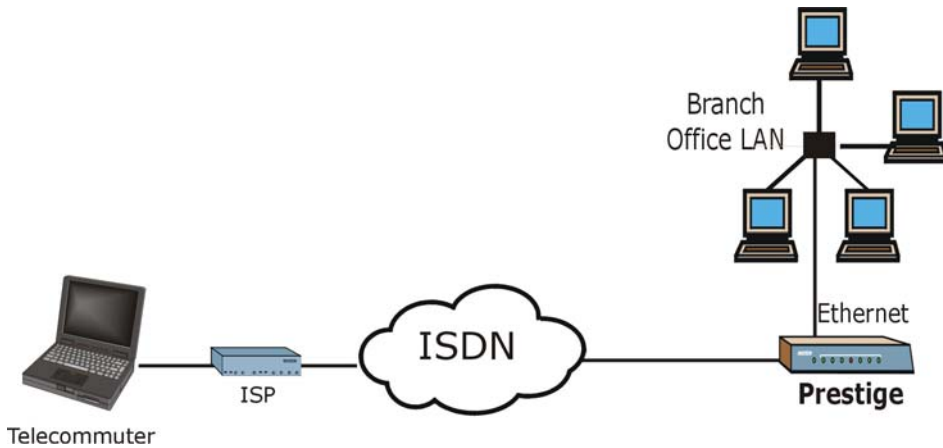


Figure 25-5 Example of Telecommuting

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

Configuring Menu 13:

```

Menu 13 - Default Dial-in Setup

Telco Options:
  CLID Authen= None

PPP Options:
  Recv Authen= PAP
  Compression= Yes
  Mutual Authen= No
  O/G Username=
  O/G Password= *****
  Multiple Link Options:
    Max Trans Rate(Kbps)= 128

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

IP Address Supplied By:
  Dial-in User= Yes
  IP Pool= Yes
  IP Start Addr= 192.168.250.250
  IP Count(1,2)= N/A

Session Options:
  Edit Filter Sets= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

IP Pool for RAS Clients.

This must be PAP for Windows®.

Figure 25-6 Configuring Menu 13 for Remote Access**Configuring Menu 14.1**

```

Menu 14.1 - Edit Dial-in User

User Name= Name
Active= Yes
Password= *****
Callback= No
  Phone # Supplied by Caller= N/A
  Callback Phone #= N/A
Rem CLID=
Idle Timeout= 300

Press ENTER to Confirm or ESC to Cancel:

```

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

Figure 25-7 Edit Dial-in-User

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

25.7 LAN-to-LAN Server Application Example

Your Prestige can also be used as a dial-in server for LAN-to-LAN application to provide access for the workstations on a remote network. For your Prestige to be set up as a LAN-to-LAN server, you need to configure the Default Dial-in User Setup to set the operational parameters for incoming calls. Additionally, you must create a remote node for the router on the remote network (see the chapter on *Remote Node Configuration*). An example of your Prestige being used as a LAN-to-LAN server is shown as follows.

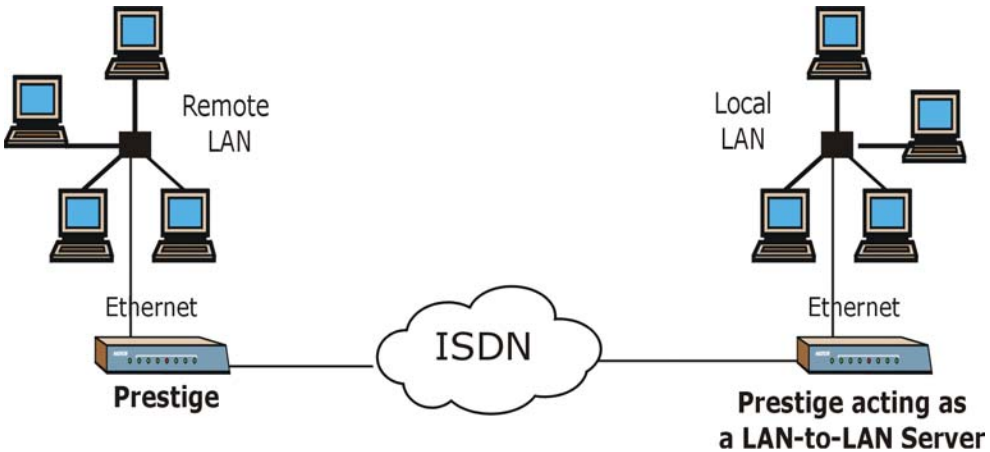


Figure 25-8 Example of a LAN-to-LAN Server Application

25.7.1 Configuring Callback in LAN-to-LAN Application

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

LAN 1

```

Menu 11.1 - Remote Node Profile

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

Incoming:                     Telco Option:
  Rem Login= lan2             Transfer Type= 64K
  Rem Password= *****      Allocated Budget(min)= 0
  Rem CLID=                   Period(hr)= 0
  Call Back= No               Schedules=
Outgoing:                     Carrier Access Code=
  My Login= lan1              Nailed-Up Connection= No
  My Password= *****        Toll Period(sec)= 0
  Authen= CHAP/PAP            Session Options:
  Pri Phone #= 1234           Edit Filter Sets= No
  Sec Phone #=                Idle Timeout(sec)= 300

Press ENTER to Confirm or ESC to Cancel:

```

Set **Call Direction** and **Call Back** to **Both** and **No** respectively.

Figure 25-9 LAN 1 LAN-to-LAN Application

LAN 2

```

Menu 11.1 - Remote Node Profile

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

Incoming:                     Telco Option:
  Rem Login= lan1             Transfer Type= 64K
  Rem Password= *****      Allocated Budget(min)= 0
  Rem CLID=                   Period(hr)= 0
  Call Back= Yes               Schedules=
Outgoing:                     Carrier Access Code=
  My Login= lan2              Nailed-Up Connection= No
  My Password= *****        Toll Period(sec)= 0
  Authen= CHAP/PAP            Session Options:
  Pri Phone #= 456           Edit Filter Sets= No
  Sec Phone #=                Idle Timeout(sec)= 300

Press ENTER to Confirm or ESC to Cancel:

```

Set **Call Direction** and **Call Back** to **Both** and **Yes** respectively.

Figure 25-10 LAN 2 LAN-to-LAN Application

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

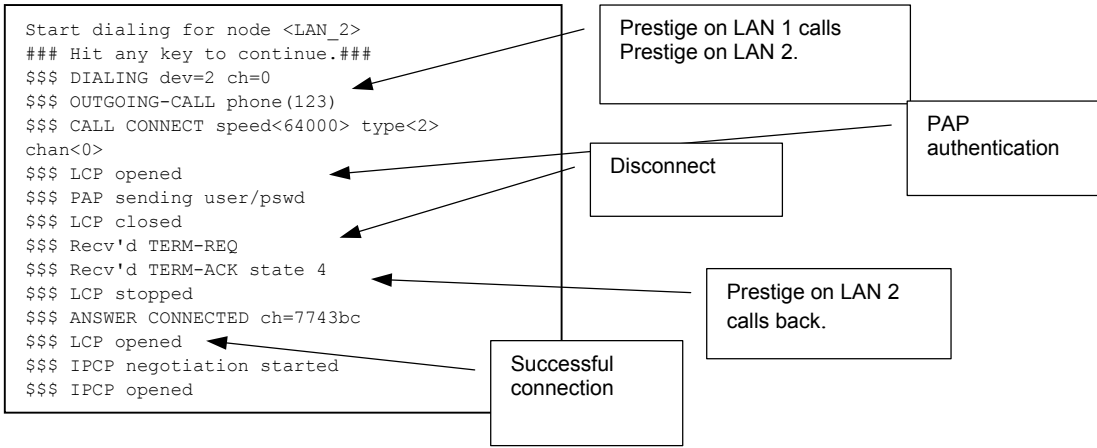


Figure 25-11 Testing Callback With Your Connection

25.7.2 Configuring With CLID in LAN-to-LAN Application

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

Prestige on LAN 2

```

Menu 11.1 - Remote Node Profile

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

Incoming:                      Telco Option:
  Rem Login= lan1              Transfer Type= 64K
  Rem Password= *←*****      Allocated Budget(min)= 0
  Rem CLID= 123                Period(hr)= 0
  Call Back= Yes               Schedules=
Outgoing:                      Carrier Access Code=
  My Login= lan2              Nailed-Up Connection= No
  My Password= *****        Toll Period(sec)= 0
  Authen= CHAP/PAP            Session Options:
  Pri Phone #= 456            Edit Filter Sets= No
  Sec Phone #=                Idle Timeout(sec)= 300

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

This is how the Prestige on LAN 2 identifies the Prestige on LAN 1.

Figure 25-12 Callback With CLID Configuration

Menu 13

```

Menu 13 - Default Dial-in Setup

Telco Options:                 IP Address Supplied By:
CLID Authen= Required         ← Dial-in User= Yes
                               IP Pool= No
                               IP Start Addr= N/A
                               IP Count(1,2)= N/A

PPP Options:
Recv Authen= PAP              Session Options:
Compression= No               Edit Filter Sets= No
Mutual Authen= No
O/G Username=
O/G Password= *****
Multiple Link Options:
Max Trans Rate(Kbps)= 128

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

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

Set this field to Required.

Figure 25-13 Configuring CLID With Callback

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

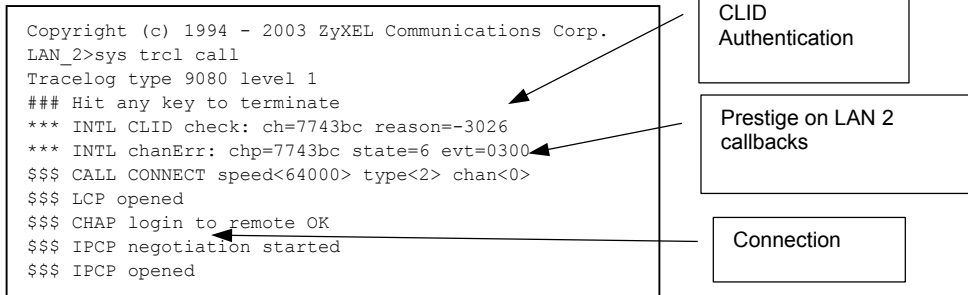


Figure 25-14 Callback and CLID Connection Test

Chapter 26

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

26.1 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.

Refer to the Web Configurator chapters for a full description of *NAT* and worked examples.

26.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See section 26.3.1 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.**
-

26.2 Applying NAT

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

```
Menu 4 - Internet Access Setup

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

NAT= SUA Only
Address Mapping Set= N/A

Telco Options:
Transfer Type= 64K

Multilink= Off
Idle Timeout= 100

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

Figure 26-1 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 select a remote node.
- Step 2.** Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**.

```

Menu 11.3 - Remote Node Network Layer Options

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

NAT= SUA Only
Address Mapping Set= N/A

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

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

Figure 26-2 Applying NAT to the Remote Node

Table 26-1 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 26.3.1). When you select Full Feature you must configure at least one address mapping set!	Full Feature
	Select None to disable NAT.	
	When you select SUA Only , the SMT uses Address Mapping Set 255 (menu 15.1 - see section 26.3.1). Choose SUA Only if you have just one public WAN IP address for your Prestige.	

26.3 NAT Setup

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in the chapter on NAT web

configurator screens for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

```
Menu 15 - NAT Setup

1. Address Mapping Sets
2. NAT Server Sets

Enter Menu Selection Number:
```

Figure 26-3 Menu 15 NAT Setup

26.3.1 Address Mapping Sets

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

```
Menu 15.1 - Address Mapping Sets

1.
2.
3.
4.
5.
6.
7.
8.
255. SUA (read only)

Enter Menu Selection Number:
```

Figure 26-4 Menu 15.1 Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 26.1.1*). The fields in this menu cannot be changed.

```

Menu 15.1.255 - Address Mapping Rules

Set Name= SUA

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

Press ENTER to Confirm or ESC to Cancel:

```

Figure 26-5 Menu 15.1.255 SUA Address Mapping Rules

Table 26-2 Menu 15.1.255 SUA Address Mapping Rules

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

26.3.2 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.

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

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=

Figure 26-6 Menu 15.1.1 Address Mapping Rules First Set

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

26.3.3 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 26-3 Fields in Menu 15.1.1

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

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

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

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

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start=
  End = N/A

Global IP:
  Start=
  End = N/A

Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Figure 26-7 Menu 15.1.1.1 Address Mapping Rule

The following table explains the fields in this menu.

Table 26-4 Menu 15.1.1.1 Address Mapping Rule

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. Server allows you to specify multiple servers of different types behind NAT to this computer. See <i>section 26.5.3</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.		

26.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

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

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

```

Menu 15.2 - NAT Server Sets

1. Server Set 1 (Used for SUA Only)
2. Server Set 2
3. Server Set 3
4. Server Set 4
5. Server Set 5
6. Server Set 6
7. Server Set 7
8. Server Set 8
9. Server Set 9
10. Server Set 10

Enter Set Number to Edit:

```

Figure 26-8 Menu 15.2 NAT Server Setup

Step 3. Enter 1 to go to **Menu 15.2.1 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                21             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 26-9 Menu 15.2.1 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

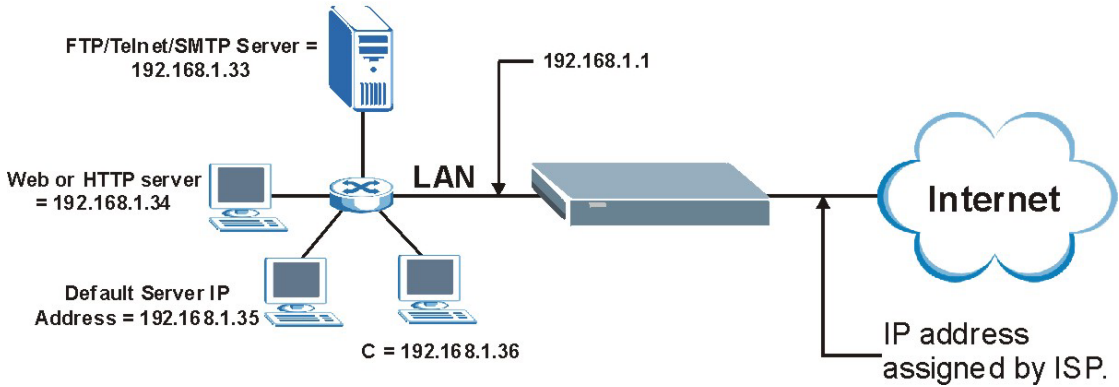


Figure 26-10 Multiple Servers Behind NAT Example

26.5 General NAT Examples

The following are some examples of NAT configuration.

26.5.1 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.

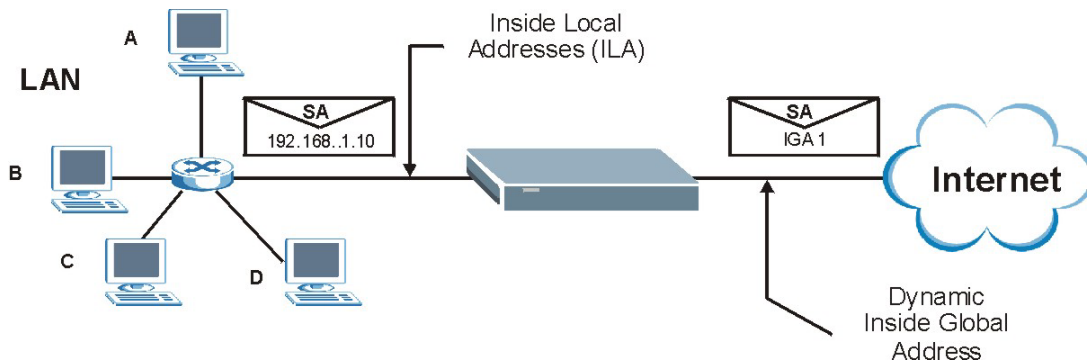


Figure 26-11 NAT Example 1

```

Menu 4 - Internet Access Setup

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

NAT= SUA Only
Address Mapping Set= N/A

Telco Options:
Transfer Type= 64K

Multilink= Off
Idle Timeout= 100

Press ENTER to Confirm or ESC to Cancel:

```

Figure 26-12 Menu 4 Internet Access & NAT Example

From menu 4, choose the **SUA Only** option from the **NAT** field. This is the Many-to-One mapping discussed in *section 26.5*. The **SUA Only** read-only option from the **NAT** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

26.5.2 Example 2: Internet Access with an Inside Server

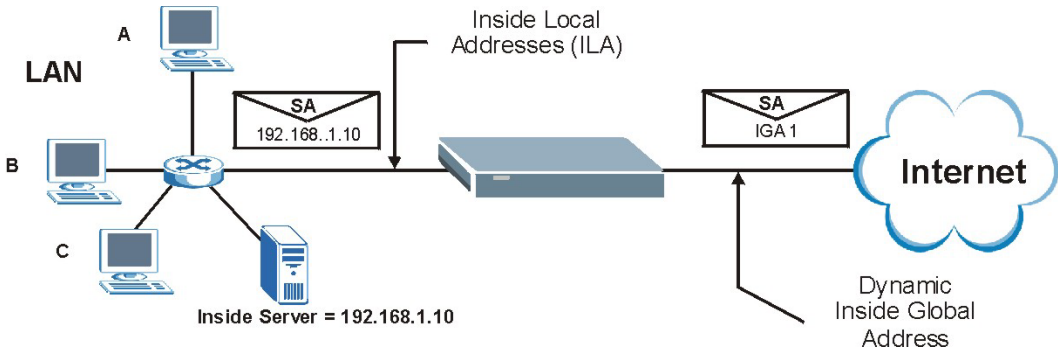


Figure 26-13 NAT Example 2

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 15.2.1 - NAT Server Setup (Used for SUA Only)

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 26-14 Menu 15.2.1 Specifying an Inside Server

26.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with

an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

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

The example situation looks somewhat like this:

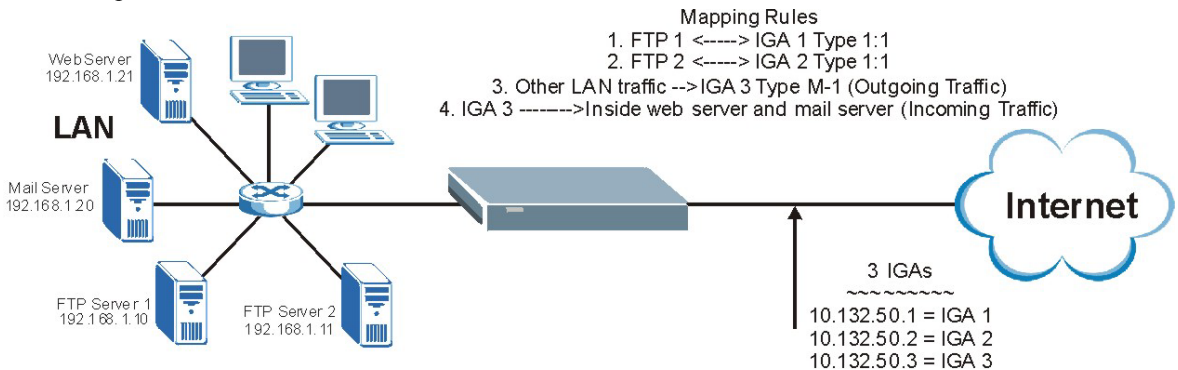


Figure 26-15 NAT Example 3

- 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 NAT field (in menu 4 or menu 11.3) in *Figure 26-16*.
- Step 2.** Then enter 15 from the main menu.
- Step 3.** Enter 1 to configure the Address Mapping Sets.
- Step 4.** Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- Step 5.** Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 26-17*).
- Step 6.** Repeat the previous step for rules 2 to 4 as outlined above.

Step 7. When finished, menu 15.1.1 should look like as shown in *Figure 26-18*.

```
Menu 11.3 - Remote Node Network Layer Options

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

NAT= Full Feature
Address Mapping Set= 2

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

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

Figure 26-16 Example 3: Menu 11.3

The following figures show how to configure the first rule

```
Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
Start= 192.168.1.10
End = N/A

Global IP:
Start= 10.132.50.1
End = N/A

Server Mapping Set= N/A

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

Figure 26-17 Example 3: Menu 15.1.1.1

Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	192.168.1.10		10.132.50.1		1-1
2.	192.168.1.11		10.132.50.2		1-1
3.	0.0.0.0	255.255.255.255	10.132.50.3		M-1
4.			10.132.50.3		Server
5.					
6.					
7.					
8.					
9.					
10.					

Action= Edit Select Rule=

Figure 26-18 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** to see the following menu. Configure it as shown.

Menu 15.2.1 - 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:

Example 3: Menu 15.2.1

26.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

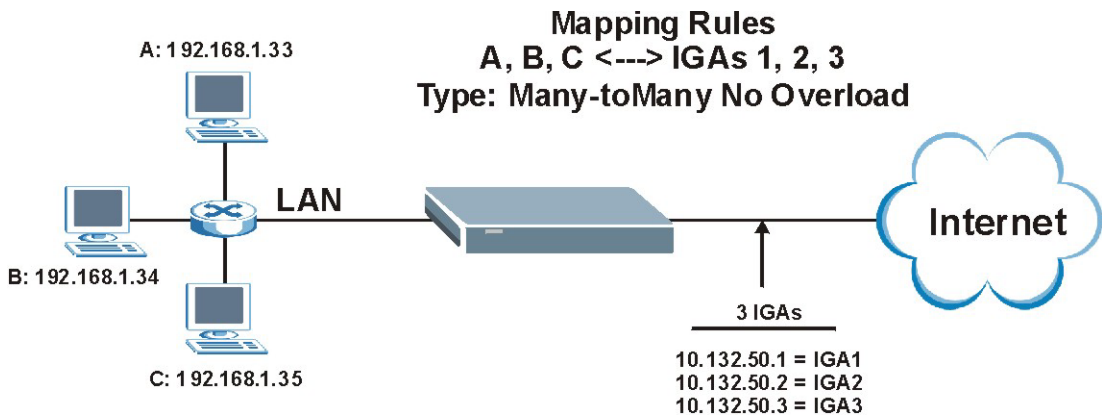


Figure 26-19 NAT Example 4

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 26-20 Example 4: Menu 15.1.1.1 Address Mapping Rule

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

```

Menu 15.1.1 - Address Mapping Rules

Set Name= Example4

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.   192.168.1.10    192.168.1.12  10.132.50.1     10.132.50.3   M-M No
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= None          Select Rule= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Figure 26-21 Example 4: Menu 15.1.1 Address Mapping Rules

Part VIII:

Advanced Management

This part discusses Filtering and Firewall setup, SNMP, System Information and Diagnosis, Firmware and Configuration File Maintenance, System Maintenance and Information, Call Scheduling, Remote Management and Virtual Private Networking (VPN/IPSec).

Chapter 27

Filter Configuration

This chapter shows you how to create and apply filters.

27.1 Filtering Overview

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 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, for example, 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.

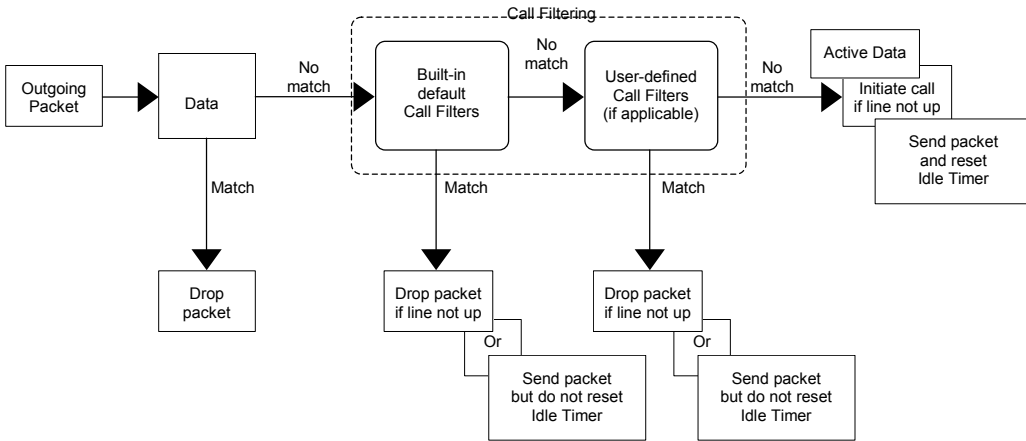


Figure 27-1 Outgoing Packet Filtering Process

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.

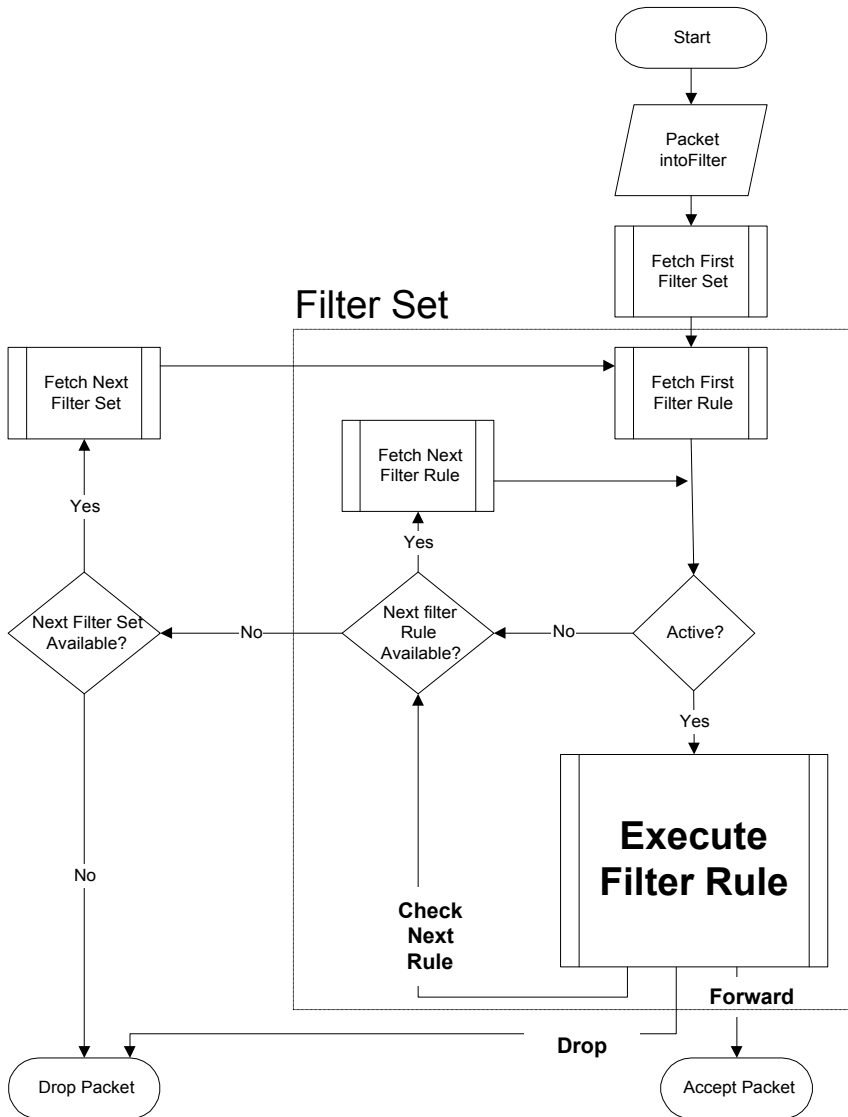


Figure 27-2 Filter Rule Process

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, for example, 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.

27.2 Configuring a Filter Set

To configure a filter set, follow the steps shown next.

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

```
Menu 21 - Filter and Firewall Setup

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

Enter Menu Selection Number:
```

Figure 27-3 Menu 21 Filter and Firewall Setup

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


```

Menu 21.1 - Filter Set Configuration

Filter          Filter
Set #          Set #
-----          -----
1             NetBIOS_WAN      7             _____
2             NetBIOS_LAN      8             _____
3             TELNET_WAN      9             _____
4             FTP_WAN         10            _____
5             _____      11            _____
6             _____      12            _____

Enter Filter Set Number to Configure= 0

Edit Comments= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Figure 27-4 Menu 21.1 Filter Set Configuration

- Step 3.** Select the filter set you wish to configure (1-12) and press [ENTER].
- Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.x- Filter Rules Summary**. The following shows filter rules summary screens for filter sets 1 through 4.

```

Menu 21.1.1 - Filter Rules Summary

# A Type                               Filter Rules                               M m n
-----
1 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137      N D N
2 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138      N D N
3 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139      N D N
4 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137     N D N
5 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138     N D N
6 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139     N D F

Enter Filter Rule Number (1-6) to Configure:

```

Figure 27-5 NetBIOS_WAN Filter Rules Summary

```

Menu 21.1.2 - Filter Rules Summary

# A Type                               Filter Rules                               M m n
-----
1 Y IP  Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53  N D F
2 N
3 N
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure:

```

Figure 27-6 NetBIOS_LAN Filter Rules Summary

```

Menu 21.1.3 - Filter Rules Summary

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

Enter Filter Rule Number (1-6) to Configure:
    
```

Figure 27-7 Telnet WAN Filter Rules Summary

```

Menu 21.1.4 - Filter Rules Summary

# A Type                               Filter Rules                               M m n
- - -----
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21   N D F
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=20   N D F
3 N
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure:
    
```

Figure 27-8 FTP_WAN Filter Rules Summary

27.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in the previous menus.

Table 27-1 Filter Rules Summary Menu Abbreviations

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.
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 27-2 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

Table 27-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
Len	Length

27.3 Configuring a Filter Rule

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

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

To speed up filtering, all rules in a filter set must be of the same class, 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.

27.3.1 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** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.x – TCP/IP Filter Rule**. The following example screen shows menu 21.1.7.1.

```

Menu 21.1.7.1 - TCP/IP Filter Rule

Filter #: 7,1
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= None
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= Check Next Rule
Action Not Matched= Check Next Rule

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

Figure 27-9 Menu 21.1.7.1 TCP/IP Filter Rule

The following table describes the labels in this menu.

Table 27-3 Menu 21.1.7.1 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.	7,1
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	Use [SPACE BAR] and then [ENTER] to select Yes to activate or No to deactivate the filter rule.	No (default)
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)

Table 27-3 Menu 21.1.7.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
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)
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

Table 27-3 Menu 21.1.7.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
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.

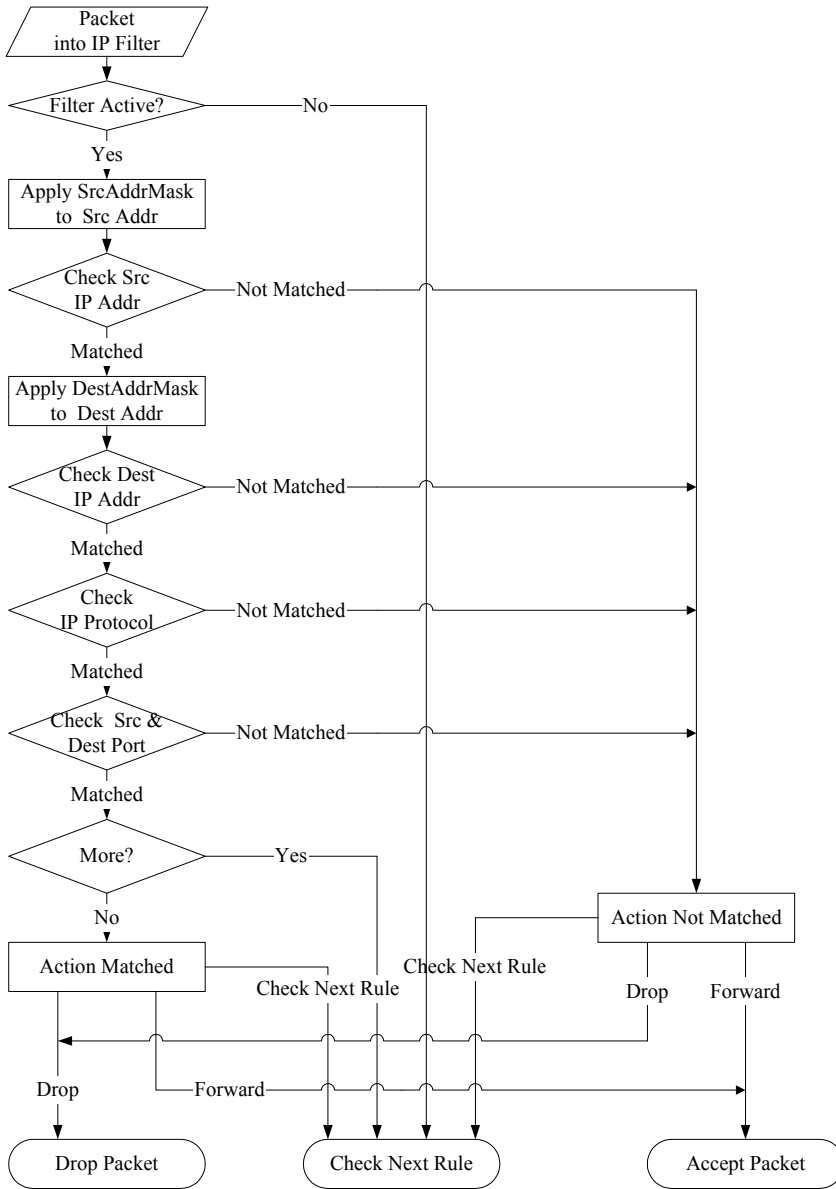


Figure 27-10 Executing an IP Filter

27.3.2 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 digits. 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 21.1, for example 8. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.x – Generic Filter Rule**. The following example screen shows menu 21.1.8.1.

```
Menu 21.1.8.1 - Generic Filter Rule

Filter #: 8,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

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

Figure 27-11 Menu 21.1.8.1 Generic Filter Rule

The following table describes the labels in this menu.

Table 27-4 Menu 21.1.8.1 Generic 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 rule of that set.	8,1

Table 27-4 Menu 21.1.8.1 Generic Filter Rule

FIELD	DESCRIPTION	EXAMPLE
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.		

27.4 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.

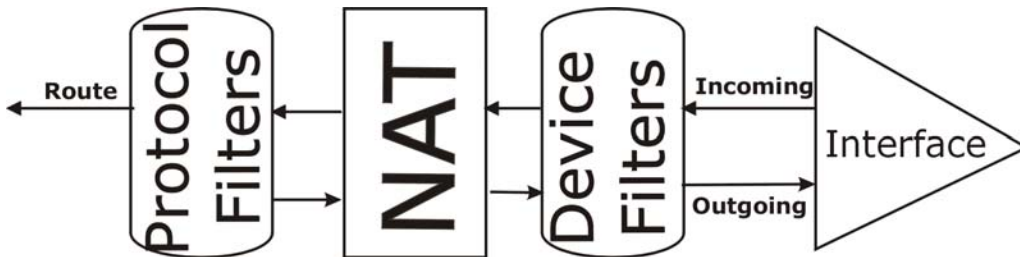


Figure 27-12 Protocol and Device Filter Sets

27.5 Example Filter

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

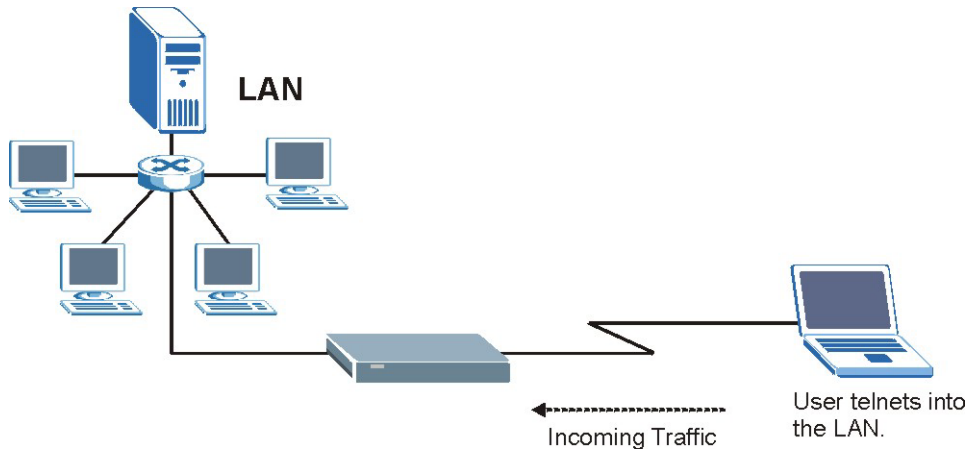


Figure 27-13 Sample Telnet Filter

- Step 1.** Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
- Step 2.** Enter 1 to open **Menu 21.1 - Filter Set Configuration**.
- Step 3.** Enter the index of the filter set you wish to configure (such as 9) and press [ENTER].
- Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.9 - Filter Rules Summary**.

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

Menu 21.1.9.1 - TCP/IP Filter Rule

```

Filter #: 9,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
              IP Mask= 0.0.0.0
              Port # = 23
              Port # Comp= Equal
Source: IP Addr= 0.0.0.0
        IP Mask= 0.0.0.0
        Port # =
        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.

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

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

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

There are no more rules to check.

Figure 27-14 Sample Filter Menu 21.1.9.1

Step 7. 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 21.1.9 - Filter Rules Summary

```

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

Enter Filter Rule Number (1-6) to Configure: 1
    
```

Callout 1 (Left): This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP, Pr = 6**) for destination telnet ports (**DP = 23**).

Callout 2 (Right): **M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

Figure 27-15 Sample Filter Rules Summary Menu 21.1.9

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

Step 8. Type 11 in the main menu to go to menu 11 and type the remote node number to edit.

Step 9. Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

Step 10. This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

27.6 Applying Filters and Factory Defaults

Table 27-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules.

Table 27-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

27.6.1 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.

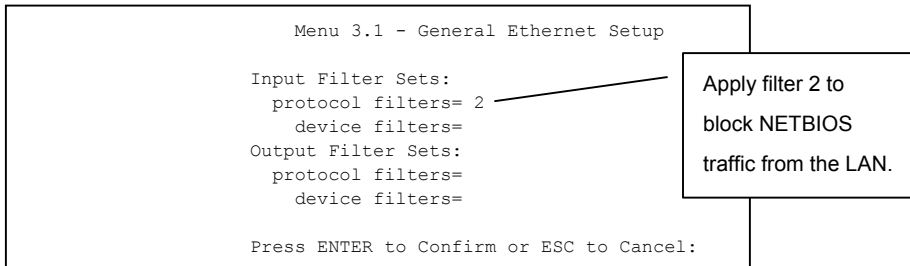
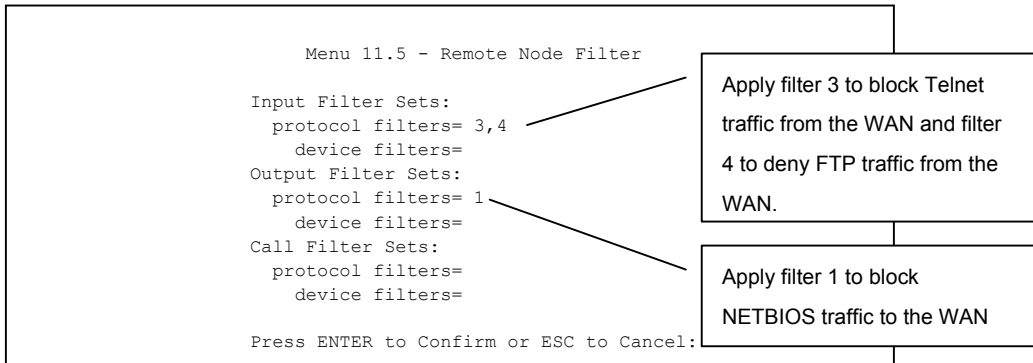


Figure 27-16 Filtering Ethernet Traffic

27.6.2 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.

**Figure 27-17 Filtering Remote Node Traffic**

Chapter 28

Enabling the Firewall

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

28.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management (see the *Remote Management* chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

28.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your Prestige has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

28.3 Using Prestige SMT Menus

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

```
Menu 21 - Filter and Firewall Setup

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

Enter Menu Selection Number:
```

Figure 28-1 Menu 21 Filter and Firewall Setup

28.3.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

```

Menu 21.2 - Firewall Setup

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

    1. allow all sessions originating from the LAN to the WAN and
    2. deny all sessions originating from the WAN to the LAN

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

Active: Yes

LAN-to-WAN Set Name: ACL Default Set
WAN-to-LAN Set Name: ACL Default Set

Please configure the Firewall function through Web Configurator.
    
```

Figure 28-2 Menu 21.2 Firewall Setup

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

28.3.2 Viewing the Firewall Log

In menu 21, enter 3 to view the firewall log. An example of a firewall log is shown next.

```

# Time      Packet Information          Reason          Action
0|Jan 1 00 |From:192.168.17.1 To:192.168.17.255 |default policy |block
  | 15:43:19|UDP src port:00520 dest port:00520  |<2,00>         |
1|Jan 1 00 |From:172.20.1.179 To:172.21.1.66  |default policy |block
  | 15:43:20|UDP src port:03571 dest port:00161  |<2,00>         |
2|Jan 1 00 |From:172.21.1.148 To:172.21.255.255 |default policy |block
  | 15:43:20|UDP src port:00137 dest port:00137  |<2,00>         |
Clear Firewall Log (y/n):
    
```

Figure 28-3 Example Firewall Log

An “End of Log” message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

Table 28-1 View Firewall Log

FIELD	DESCRIPTION	EXAMPLES
#	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log wraps around and the old logs are lost.	23
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real time; otherwise the clock will start at 2000/01/01 00:00:00 the last time the Prestige was reset.	mm:dd:yy e.g., Jan 1 00 ----- hh:mm:ss e.g., 00:00:00
Packet Information	This field lists packet information such as protocol and src/dest port numbers (TCP, UDP), or protocol, type and code (ICMP).	From and To IP addresses ----- Protocol and port numbers
Reason	This field states the reason for the log; i.e., was the rule matched, did not match or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule. This is a log for a DoS attack.	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. ----- attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop or syn flood
Action	This field displays whether the packet was blocked or forwarded. None means that no action is dictated by this rule.	block, forward or none
After viewing the firewall log, ENTER "y" to clear the log or "n" to retain it. With either option you will be returned to Menu 21- Filter and Firewall Setup .		

28.3.3 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

```

Subject:
  Firewall Alert From Prestige
Date:
  Fri, 07 Apr 2000 10:05:42
From:
  user@zyxel.com
To:
  user@zyxel.com

1|Apr 7 00|From:192.168.1.1    To:192.168.1.255  |default policy
|forward
  | 09:54:03 |UDP    src port:00520 dest port:00520  |<1,00>    |
  2|Apr 7 00|From:192.168.1.131   To:192.168.1.255  |default policy
|forward
  | 09:54:17 |UDP    src port:00520 dest port:00520  |<1,00>    |
  3|Apr 7 00|From:192.168.1.6     To:10.10.10.10   |match     |forward
  | 09:54:19 |UDP    src port:03516 dest port:00053  |<1,01>    |
.....{snip}.....
.....{snip}.....
126|Apr 7 00|From:192.168.1.1    To:192.168.1.255  |match
|forward
  | 10:05:00 |UDP    src port:00520 dest port:00520  |<1,02>    |
127|Apr 7 00|From:192.168.1.131   To:192.168.1.255  |match
|forward
  | 10:05:17 |UDP    src port:00520 dest port:00520  |<1,02>    |
128|Apr 7 00|From:192.168.1.1    To:192.168.1.255  |match
  
```

The date format here is Day-Month-Year.

You may edit the subject title

The date format here is Month-Day-Year. The time format is Hour-Minute-Second.

"End of Log" message shows that a complete log has been sent.

Figure 28-4 E-mail Log

Chapter 29

SNMP Configuration

This chapter explains SNMP Configuration menu 22.

29.1 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 29-1 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 29-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
Get Community	Type the Get Community , which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.
Trap:	

Table 29-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

29.2 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 (defined in RFC-1215)	A trap is sent after booting (power on).
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.

Table 29-3 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
...	...
13	12
14	DSL

Chapter 30

External Server

This chapter describes how to set up an external server.

30.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) is based on a client-server model that supports authentication, authorization and accounting. The RADIUS is an external server and handles the following tasks:

- **Authentication**
Determines the identity of the users.
- **Authorization**
Determines the network services available to authenticated users once they are connected to the network.
- **Accounting**
Keeps track of the client's network activity.

RADIUS authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

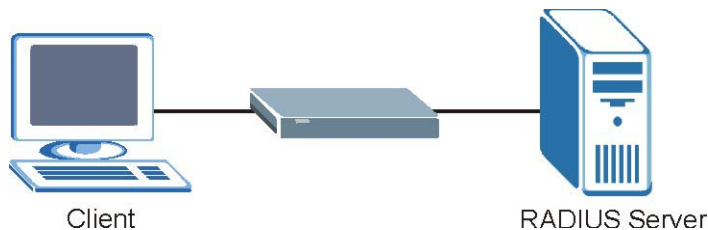


Figure 30-1 RADIUS Server

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

30.2 Configure External Server

To have the Prestige check the user database on the specified RADIUS server for a login username and password, you must configure an external server first. Select option 23 from the main menu to open **Menu 23 – System Security**. Enter 2 to open **Menu 23.2 - System Security - External Server**.

```

Menu 23.2 - System Security - External Server

Authentication Server:
Active= No
Type: RADIUS
Server Address= ?
Port #= 1645
Key= ?

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

Figure 30-2 Menu 23.2 System Security - External Server

The following table describes the labels in this menu.

Table 30-1 Menu 23.2 System Security - External Server

LABEL	DESCRIPTION
Authentication Server	
Active	Select Yes from the drop-down list box to enable user authentication through an external authentication server.
Type	This field displays the external server type.
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	The default port of the RADIUS server for authentication is 1645 . You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and Prestige.

Chapter 31

System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

31.1 System Status 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.

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

Figure 31-1 Menu 24 System Maintenance

31.2 System Status

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**. Typing 1 resets the counters, [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status** which are READ-ONLY and meant for diagnostic purposes.

```

Menu 24.1 - System Maintenance - Status                                01:36:21
                                                                    Sat. Jan. 01, 2000
Chan  Link      Type      TxPkts    RxPkts    Errors  CLU  ALU  Up Time
--    Down     0Kbps    0         0         0      0%  0%  0:00:00
--    Down     0Kbps    0         0         0      0%  0%  0:00:00

Chan  Own IP Address  Own CLID      Peer IP Address  Peer CLID
--
Ethernet  Status          TxPkts        RxPkts          Collision
100M/Full Duplex      2479          2363            0
Total Outcall Time:   0:00:00      CPU Load =     4.95%
LAN Packet Which Triggered Last Call: (Type: IP)
45 00 00 28 FE EB 00 00 FE 06 50 01 C0 A8 01 21 AC 16 00 03 04 61 02 0C
99 90 38 9D 00 00 00 00 50 04 FA F0 6E 72 00 00

Press Command:
COMMANDS: 1-Drop B1  2-Drop B2  3-Reset Counters  4-Drop All  ESC-Exit
    
```

Figure 31-2 Menu 24.1 System Maintenance Status

The following table describes the labels in this menu.

Table 31-1 Menu 24.1 System Maintenance Status

FIELD	DESCRIPTION
Chan	This shows statistics for B1 and B2 channels respectively. This is the information displayed for each channel.
Link	This shows the name of the remote node or the user the channel is currently connected to or the status of the channel (e.g., Down , Idle , Calling , Answering , NetCAPI , etc.).
Type	This is the current connecting speed.
TxPkts	This is the number of transmitted packets on this channel.
RxPkts	This is the number of received packets on this channel.
Errors	This is the number of error packets on this channel.
CLU	The CLU (Current Line Utilization) is the percentage of current bandwidth used on this channel.
ALU	The ALU (Average Line Utilization) is a 5-second moving average of usage for this channel.
Up Time	Time this channel has been connected to the current remote node.
Chan	This shows statistics for B1 and B2 channels respectively. This is the information displayed for each channel.

Table 31-1 Menu 24.1 System Maintenance Status

FIELD	DESCRIPTION
Own IP Address	This refers to the IP address of the Prestige.
Own CLID	Shows your Caller ID.
Peer IP Address	This refers to the IP address of the peer.
Peer CLID	This shows the Caller ID of the peer.
Ethernet	This shows statistics for the LAN.
Status	This displays the port speed and duplex setting.
TxPkts	This is the number of transmitted packets to the LAN.
RxPkts	This is the number of received packets from the LAN.
Collision	This is the number of collisions.
Total Outcall Time	This shows the total outgoing call time for both B1 and B2 channels since the system has been powered up.
CPU Load	This specifies the percentage of CPU utilization.
LAN Packet Which Triggered Last Call	This shows the first 48 octets of the LAN packet that triggered the last outgoing call.
Commands	
Drop B1	This command drops the B1 channel.
Drop B2	This command drops the B2 channel.
Reset Counters	This command resets all counters.
Drop All	This command drops all channels.

31.3 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

- Step 1.** Enter 24 to go to **Menu 24 – System Maintenance**.
- Step 2.** Enter 2 to open **Menu 24.2 – System Information and Console Port Speed**.
- Step 3.** From this menu you have two choices as shown in the next figure:

```

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

Please enter selection:
    
```

Figure 31-3 Menu 24.2 System Information and Console Port Speed

31.3.1 System Information

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

```

Menu 24.2.1 - System Maintenance - Information

Name: name
Routing: IP
ZyNOS F/W Version: V3.40(QI.0)b5 | 9/7/2004
Country Code: 255

LAN
  Ethernet Address: 00:a0:c5:01:23:45
  IP Address: 192.168.1.1
  IP Mask: 255.255.255.0
  DHCP: Server
    
```

Figure 31-4 Menu 24.2.1 System Maintenance Information

The following table describes the labels in this menu.

Table 31-2 Menu 24.2.1 System Maintenance Information

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in Menu 1 – General Setup .
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Country Code	This is the country code value (in decimal notation).
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.

Table 31-2 Menu 24.2.1 System Maintenance Information

FIELD	DESCRIPTION
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

31.3.2 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, 38400 and 57600bps. Use [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

```

Menu 24.2.2 - System Maintenance - Change Console Port Speed

Console Port Speed: 9600

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 31-5 Menu 24.2.2 System Maintenance Change Console Port Speed

31.4 Log and Trace

Type 3 in menu 24 to open **Menu 24.3-Log and Trace**. This menu allows you to view the error log and the Unix Syslog, configure an accounting server, and see call-triggering packet information.

31.4.1 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 and Accounting
3. Accounting Server
4. Call-Triggering Packet

Please enter selection:
```

Figure 31-6 Menu 24.3 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.

```
40 Sat Jan 1 00:00:00 2000 PP06 -WARN SNMP TRAP 2: link down
41 Sat Jan 1 00:00:20 2000 PINI -WARN Last errorlog repeat 14 Times
45 Sat Jan 1 00:00:20 2000 PINI -WARN SNMP TRAP 0: cold start
46 Sat Jan 1 00:00:20 2000 PINI -WARN Last errorlog repeat 1 Times
47 Sat Jan 1 00:00:20 2000 PINI INFO main: init completed
48 Sat Jan 1 00:00:21 2000 PP06 -WARN SNMP TRAP 2: link down
49 Sat Jan 1 00:00:27 2000 PINI INFO SMT Session Begin
50 Sat Jan 1 00:07:01 2000 PINI INFO SMT Session End
Clear Error Log (y/n):
```

Figure 31-7 Sample Error and Information Messages

31.4.2 Unix Syslog

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


```

Menu 24.3.2 - System Maintenance - UNIX Syslog

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

Types:
CDR= No
Packet triggered= No
Filter log= No
PPP log= No
Firewall log= No

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

Figure 31-8 Menu 24.3.2 System Maintenance Unix Syslog

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

Table 31-3 Menu 24.3.2 System Maintenance Unix Syslog

FIELD	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to your UNIX manual for more details.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to Yes .
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to Yes .
Filter log	No filters are logged when this field is set to No . Filters with the individual filter Log Filter field set to Yes are logged when this field is set to Yes .
PPP log	PPP events are logged when this field is set to Yes .
Firewall log	Firewall events are logged when this field is set to Yes .
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

The following are examples of syslog messages sent by the Prestige:

1. CDR

```
CDR Message Format
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.)
      L02 Tunnel Connected(L2TP)
      C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call
Number)
      L02 Call Terminated
      C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2
ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected
64000 40002
Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
```

2. Packet triggered

```
Packet triggered Message Format
SdcmSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
String = Packet trigger: Protocol=xx Data=xxxxxxxxxxxx...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=4500003c100100001f010004c0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
7374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

3. Filter log

Filter log Message Format
<pre>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 Mar 03 10:39:43 202.132.155.97 ZyXEL: GEN[fffffffffnordff0080] }S05>R01mF Mar 03 10:41:29 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 10:41:34 202.132.155.97 ZyXEL: IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF Mar 03 11:59:20 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 12:00:52 202.132.155.97 ZyXEL: GEN[fffffffffff0080] }S05>R01mF Mar 03 12:00:57 202.132.155.97 ZyXEL: GEN[00a0c5f502010080] }S05>R01mF Mar 03 12:01:06 202.132.155.97 ZyXEL: IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF</pre>

4. PPP log

PPP Log Message Format
<pre>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</pre>

5. POTS log

POTS Log Message Format
<pre>SdcmSyslogSend (SYSLOG_POTSLOG, SYSLOG_NOTICE, String); String = Call Connect / Disconnect: Dir = xx Remote Call= xxxxx Local Call= xxxxx Dir = Call Direction 1: Incoming call 2: Outgoing call Remote Call = a string type which represents as the remote call number</pre>

31.5 Accounting Server

Type 3 in menu 24.3 to open **Menu 24.3.3-Accounting Server**. This menu allows you to activate and configure an accounting server.

```

Menu 24.3.3 - System Maintenance - Accounting Server

Accounting Server:
Active= No
Type: RADIUS
Server Address= ?
Port #= 1646
Key= *****

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
    
```

Figure 31-9 Menu 24.3.3 System Maintenance Accounting Server

FIELD	DESCRIPTION	EXAMPLE
Accounting Server		
Active	Press the [SPACE BAR] to select Yes and press [ENTER] to enable wireless client authentication through an external accounting server.	Yes
Type	This non-editable field shows the type of accounting server being used.	RADIUS
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.	10.11.12.133
Port #	The default port for the Radius server for accounting is 1646. You do not need to change this value unless your network administrator instructs you to do so.	1646
Key	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the Prestige.	
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

31.6 Call Triggering Packet

Type 3 in menu 24.3 to open **Menu 24.3.4-Call Triggering Packet**. This menu allows you to view the packets that triggered dial-out calls in a human-readable format. An example is shown next.

```

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

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

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

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

Press any key to continue...

```

Figure 31-10 Menu 24.3.4 Call Triggering Packet.

31.7 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

ISDN                                System
1. Hang Up B1 Call                  21. Reboot System
2. Hang Up B2 Call                  22. Command Mode
3. Reset ISDN
4. ISDN Connection Test
5. Manual Call

TCP/IP
11. Internet Setup Test
12. Ping Host

Enter Menu Selection Number:

Manual Call Remote Node= N/A
Host IP Address= N/A
    
```

Figure 31-11 Menu 24.4 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**.

Table 31-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Hang Up B1 Call	This tool hangs up the B1 channel. It is only applicable if the B1 channel is currently in use.
Hang Up B2 Call	This tool hangs up the B2 channel. It is only applicable if the B2 channel is currently in use.
Reset ISDN	This command re-initializes the ISDN link to the telephone company.
ISDN Connection Test	You can test to see if your ISDN line is working properly by using this option. This command triggers the Prestige to perform a loop-back test to check the functionality of the ISDN line. If the test is not successful, note the error message that you receive and consult your network administrator.
Manual Call	This provides a way for you to place a call to a remote node manually. This tests the connectivity to that remote node. When you use this command, the screen displays what is happening during the call setup and protocol negotiation. The following is an example of a successful connection.

Table 31-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Internet Setup Test	This test checks to see if your Internet access configuration has been done correctly. When this option is chosen, the Prestige places a manual call to the ISP remote node. If everything is working properly, you will receive an appropriate response. Otherwise, note the error message and consult your network administrator.
Ping Host	This diagnostic test pings the host, which determines the functionality of the TCP/IP protocol on both systems and the links in between.
Reboot System	This option reboots the Prestige.
Command Mode	This option allows you to enter the command mode. It allows you to diagnose and test your Prestige using a specified set of commands.
Manual Call Remote Node	If you entered 5 above, then enter the remote node number (with reference to the remote node listing on Menu 11 – Remote Node Setup) you wish to call.
Host IP Address	If you entered 12 above, then enter the IP address of the machine you want to ping in this field.

The following figure shows an example of a successful connection after selecting option **Manual Call** in Menu 24.4.

```

Start dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:12345
Call CONNECT speed<64000> chan<2> prot<1>
LCP up
CHAP send response
CHAP login to remote OK!
IPCP negotiation started
IPCP up

```

Figure 31-12 Display for a Successful Manual Call

Chapter 32

Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

32.1 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 32-1 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

32.2 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 method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

32.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

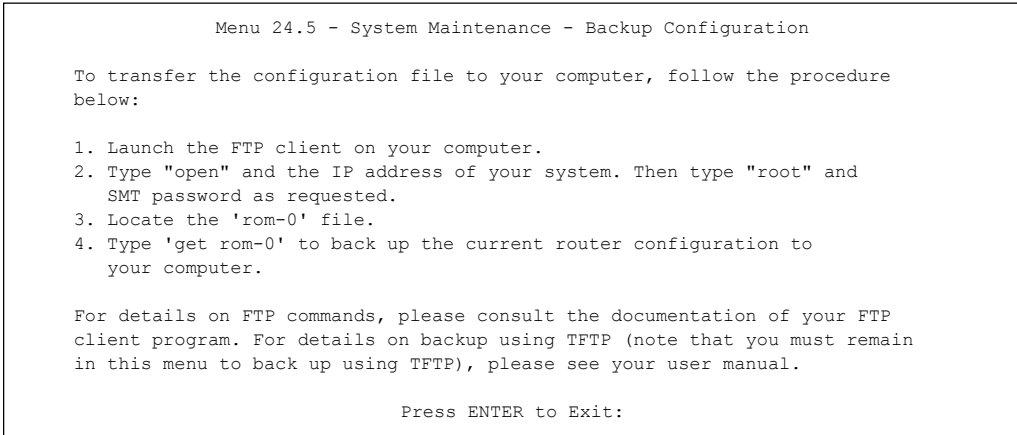


Figure 32-1 Menu 24.5 System Maintenance – Backup Configuration

32.2.2 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.

32.2.3 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.
    
```

Figure 32-2 FTP Session Example

32.2.4 GUI-based FTP Clients

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

Table 32-2 General Commands for GUI-based FTP Clients

COM IAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	<p>Anonymous.</p> <p>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.</p> <p>Normal.</p> <p>The server requires a unique User ID and Password to login.</p>
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).

32.2.5 Remote Management Limitations

TFTP, FTP and Telnet from the 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. There is an SMT console session running.

3. 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.
4. 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 is already a web session.

32.2.6 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.

32.2.7 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.

32.2.8 GUI-based TFTP Clients

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

Table 32-3 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 32.2.5* to read about configurations that disallow TFTP and FTP from the WAN.

32.2.9 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 32-3 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 32-4 System Maintenance: Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

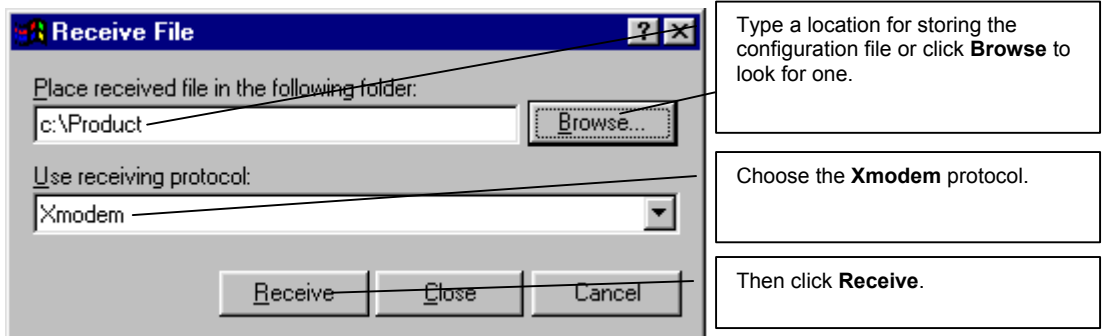


Figure 32-5 Backup Configuration Example

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 32-6 Successful Backup Confirmation Screen

32.3 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 a previously saved 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, WHEN THE UPLOAD CONFIGURATION/FIRMWARE PROCESS IS COMPLETE, THE PRESTIGE WILL AUTOMATICALLY RESET.

32.3.1 Restore Using FTP

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

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

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

1. Launch the FTP client on your computer.
2. Type "open" and the IP address of your router. Then type "root" and SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of your backup configuration file on your computer and rom-0 is the remote file name on the system. This restores the configuration to your system.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP client program. For details on backup using TFTP (note that you must remain in this menu to back up using TFTP), please see your user manual.
```

Figure 32-7 Telnet into Menu 24.6

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter “open”, followed by a space and the IP address of your 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.

32.3.2 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 32-8 Restore Using FTP Session Example

Refer to *section 32.2.5* to read about configurations that disallow TFTP and FTP from the WAN.

32.3.3 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 32-9 System Maintenance: Restore Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
Starting XMODEM download (CRC mode) ...
CCCCCCCC
```

Figure 32-10 System Maintenance: Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

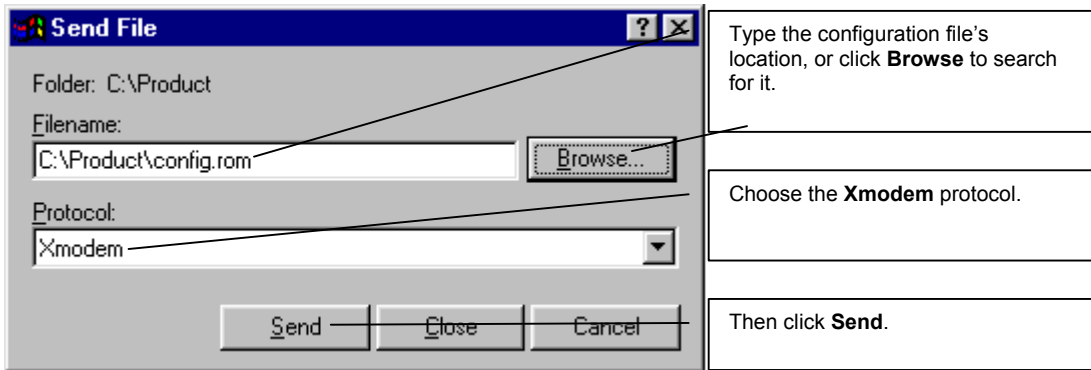


Figure 32-11 Restore Configuration Example

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.

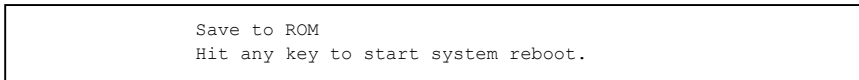


Figure 32-12 Successful Restoration Confirmation Screen

32.4 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, WHEN THE UPLOAD CONFIGURATION/FIRMWARE PROCESS IS COMPLETE, THE PRESTIGE WILL AUTOMATICALLY RESET.

32.4.1 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, type 7 in menu 24. You will see **Menu 24.7 – System Maintenance – Upload Firmware** as shown.

```
Menu 24.7 - System Maintenance - Upload Firmware

1. Upload Router Firmware
2. Upload Router Configuration File

Enter Menu Selection Number:
```

Figure 32-13 - System Maintenance Upload Firmware

Enter 1 in menu 24.7 to display the following screen an upload firmware 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 computer.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
   of your firmware upgrade file on your computer and "ras" is the
   remote file name on the system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

Figure 32-14 Menu 24.7.1 Upload System Firmware

32.4.2 Configuration File Upload

You can see the following screen when you enter 2 in menu 24.7.

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

1. Launch the FTP client on your computer.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put configurationfilename rom-0" where "configurationfilename"
   is the name of your system configuration file on your computer, which
   will be transferred to the "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration
   file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit.
```

Figure 32-15 Menu 24.7.2 - System Maintenance – Upload Configuration File

To upload the firmware and the configuration file, follow these examples

32.4.3 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.

32.4.4 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
fto: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
```

Figure 32-16 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 32.2.5* to read about configurations that disallow TFTP and FTP over WAN.

32.4.5 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.

32.4.6 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.

32.4.7 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.

32.4.8 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.

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload system firmware:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   router.

Warning: Proceeding with the upload will erase the current system
firmware.

Do You Wish To Proceed:(Y/N)
```

Figure 32-17 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.

32.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

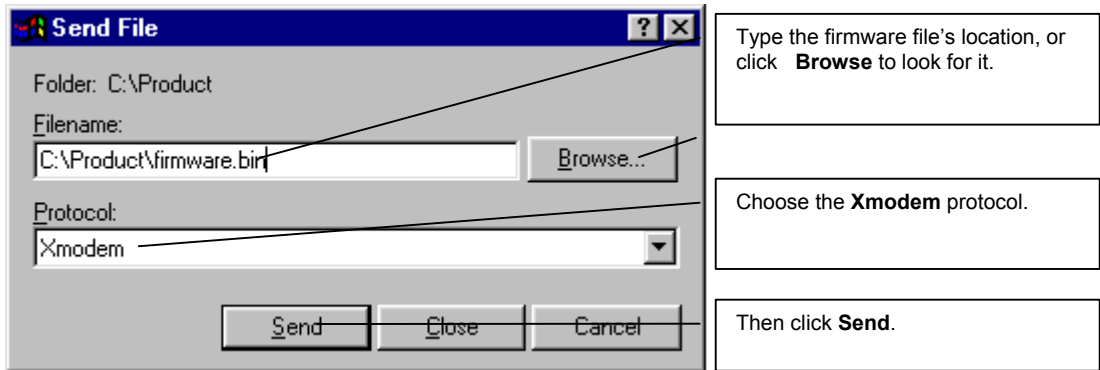


Figure 32-18 Example Xmodem Upload

After the configuration upload process has completed, restart the Prestige by entering “atgo”.

32.4.10 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 32-19 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.

32.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

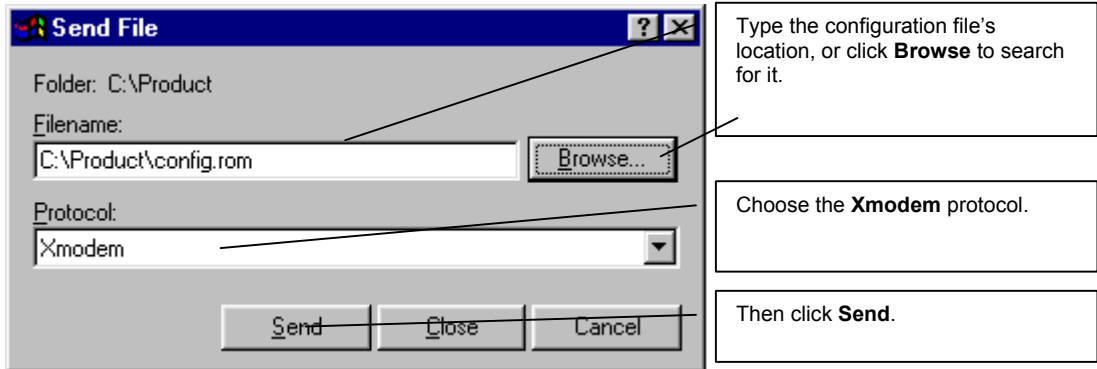


Figure 32-20 Example Xmodem Upload

After the configuration upload process has completed, restart the Prestige by entering "atgo".

Chapter 33

SMT Menus 24.8 to 24.10

This chapter leads you through System Maintenance SMT menus 24.8 to 24.10.

33.1 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. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

Figure 33-1 Command Mode in Menu 24

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          ether          isdn
ip          ipsec
ras>
```

Figure 33-2 Valid Commands

33.2 Call Control Support

The Prestige provides four call control functions: call control parameters, blacklist, budget management and call history.

Call control parameters allows you to set a dial out time limit, the number of times a number should be called before it is added to the blacklist and the interim between calls.

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

The blacklist function prevents the Prestige from re-dialing to an unreachable phone number. It is a list of phone numbers, up to a maximum of 14, to which the Prestige will not make an outgoing call. If the Prestige tries to dial to a phone number and fails a certain number of times (configurable in Menu 24.9.1), then the phone number is placed on the blacklist. You will have to enable the number manually before the Prestige will dial that number again.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

```
Menu 24.9 - System Maintenance - Call Control

1. Call Control Parameters
2. Black List
3. Budget Management
4. Call History

Enter Menu Selection Number:
```

Figure 33-3 Menu 24.9 Call Control

33.2.1 Call Control Parameters

Menu 24.9.1 shows the call control parameters. Enter 1 from Menu 24.9 to bring up the following menu.

```

Menu 24.9.1 - Call Control Parameters

Dialer Timeout:
  Digital Call(sec)= 60

Retry Counter= 0
Retry Interval(sec)= N/A

Press ENTER to confirm or ESC to Cancel:
Please enter a number from 5 to 300

```

Figure 33-4 Menu 24.9.1 Call Control Parameters

The following table describes the labels in this menu.

Table 33-1 Menu 24.9.1 Call Control Parameters

FIELD	DESCRIPTION
Dialer Timeout: Digital Call (sec)	The Prestige will timeout if it cannot set up an outgoing digital call within the timeout value. The default is 30 .
Retry Counter	How many times a busy or 'no answer' telephone number is retried before it is put on the blacklist. The default is 0 and the blacklist control is not enabled.
Retry Interval (sec)	Elapsed time after a call fails before another call may be retried. This applies before a telephone number is blacklisted.

33.2.2 Black List

Menu 24.9.2 shows the blacklist. The phone numbers on the blacklist are numbers that the Prestige had problems connecting to in the past. The only operation allowed is taking a number off the list by entering its index number. Enter 2 from Menu 24.9 to bring up the following menu.

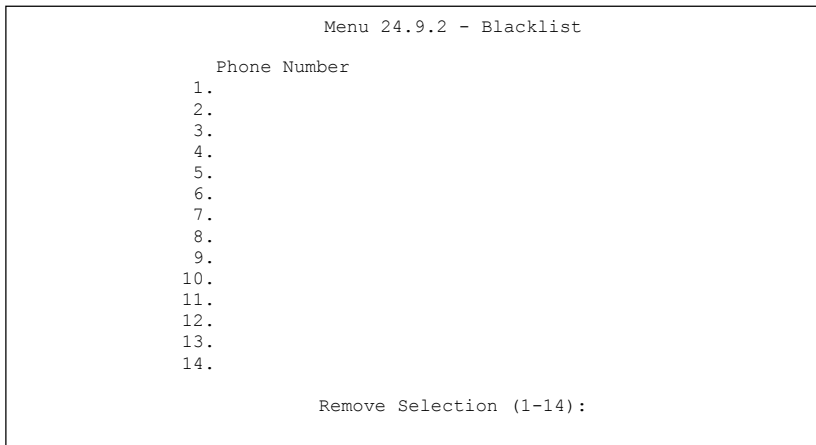


Figure 33-5 Menu 24.9.2 Blacklist

33.2.3 Budget Management

Menu 24.9.3 shows the budget management statistics for outgoing calls. Enter 3 from Menu 24.9 to bring up the following menu.

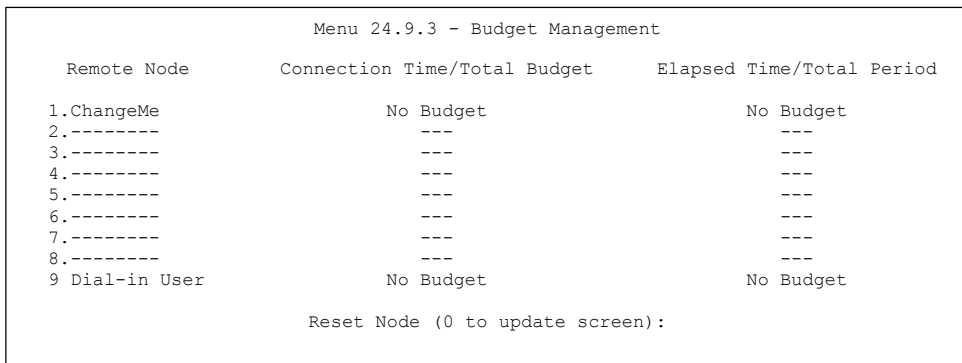


Figure 33-6 Menu 24.9.1 Budget Management

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 33-2 Menu 24.9.1 Budget Management

FILED	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.		

33.2.4 Call History

Menu 24.9.1 shows the call history for incoming and outgoing calls. Enter 4 from Menu 24.9 to bring up the following menu.

```

Menu 24.9.4 - Call History

  Phone Number  Dir    Rate    #call    Max    Min    Total
  1.
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

Enter Entry to Delete (0 to exit):
    
```

Figure 33-7 Menu 24.9.4 Call History

The following table describes the labels in this menu.

Table 33-3 Menu 24.9.4 Call History

FIELD	DESCRIPTION
Phone Number	This is the telephone number of past incoming and outgoing calls.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.

33.3 Time and Date

There is a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

Figure 33-8 Menu 24: System Maintenance

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

```

Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= None
Time Server IP Address= N/A

Current Time:                04 : 06 : 11
New Time (hh:mm:ss):        04 : 06 : 01

Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2000 - 01 - 01

Time Zone= GMT

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

Figure 33-9 Menu 24.10 System Maintenance: Time and Date Setting

The following table describes the fields in this menu.

Table 33-4 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your timeserver sends when you turn on the Prestige. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. NTP (RFC-1305) the default, is similar to Time (RFC-868) . None enter the time manually.
Time Server IP Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.

Table 33-4 Time and Date Setting Fields

FIELD	DESCRIPTION
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

33.3.1 Resetting the Time

The Prestige resets the time in three instances:

- i. On leaving menu 24.10 after making changes.
- ii. When the Prestige starts up, if there is a timeserver configured in menu 24.10.
- iii. 24-hour intervals after starting.

Chapter 34

Remote Management

This chapter covers remote management (SMT menu 24.11).

34.1 Remote Management Overview

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

When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

34.2 Remote Management

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

Enter 11 from menu 24 to display **Menu 24.11 — Remote Management Control**.

34.2.1 Remote Management Setup

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.

Enter 11, from 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 34-1 Menu 24.11 Remote Management Control

The following table describes the fields in this menu.

Table 34-1 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service or protocol.	
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the Prestige.	23
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
Secured Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the Prestige. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

34.2.2 Remote Management Limitations

Remote management over LAN or WAN will not work when:

5. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
6. You have disabled that service in menu 24.11.
7. 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.
8. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
9. There is a firewall rule that blocks it.

34.3 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.

34.4 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The Prestige automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Chapter 35

Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

35.1 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 videocassette recorder (you can specify a time period for the VCR to record).

35.2 Configuring Call Scheduling

From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next. You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**.

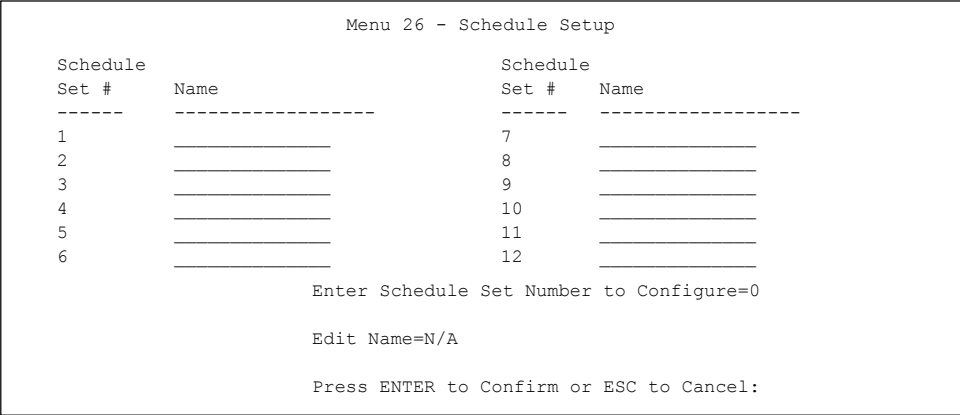


Figure 35-1 Menu 26 Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node, then set 1 will take precedence over set 2, 3 and 4 as the 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 [DEL] in the Edit Name field.

To set up a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

```

Menu 26.1 - Schedule Set Setup

Active= Yes
Start Date(yyyy/mm/dd) = 2000 - 01 - 01
How Often= Once
Once:
  Date(yyyy/mm/dd)= 2000 - 01 - 01
Weekdays:
  Sunday= N/A
  Monday= N/A
  Tuesday= N/A
  Wednesday= N/A
  Thursday= N/A
  Friday= N/A
  Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On
    
```

Figure 35-2 Menu 26.1 Schedule Set Setup

The following table describes the labels in this menu.

Table 35-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	OPTIONS
Active	Press [SPACE BAR] to select Yes or No . Choose Yes and press [ENTER] to activate the schedule set.	Yes No
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.	
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select Once or Weekly . Both these options are mutually exclusive. If Once is selected, then all weekday settings are N/A . When Once is selected, the schedule rule deletes automatically after the scheduled time elapses.	Once Weekly
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.	

Table 35-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	OPTIONS
Weekday: Day	If you selected Weekly in the How Often field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select Yes , then press [ENTER].	Yes No N/A
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	
Action	<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.</p> <p>Disable Dial-On-Demand means that this schedule prevents a demand call on the line.</p>	Forced On Forced Down Enable Dial-On-Demand Disable Dial-On-Demand
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

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**.

35.3 Applying Schedule Sets

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the Main Menu and then enter the target remote node index. You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

```
Menu 11.1 - Remote Node Profile

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

Incoming:                  Telco Option:
  Rem Login= ?             Transfer Type= 64K
  Rem Password= ?         Allocated Budget(min)=
  Rem CLID=                Period(hr)=
  Call Back= No           Schedules= 1,3,4,11
Outgoing:                  Carrier Access Code=
  My Login=                Nailed-Up Connection= N/A
  My Password= *****    Toll Period(sec)= 0
  Authen= CHAP/PAP        Session Options:
  Pri Phone #= ?          Edit Filter Sets= No
  Sec Phone #=            Idle Timeout(sec)= 100

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 35-3 Applying Schedule Set(s)

Chapter 36

VPN/IPSec Setup

This chapter shows you how to set up VPN/IPSec on your Prestige.

36.1 VPN/IPSec Overview

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

36.1.1 VPN/IPSec SMT Menus

The VPN/IPSec main SMT menu has three 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. Manage (refresh or disconnect) your SA connections in menu 27.2.
3. View the IPSec connection log in menu 27.4. This menu is also useful for troubleshooting.

This is an overview of the VPN menu tree.

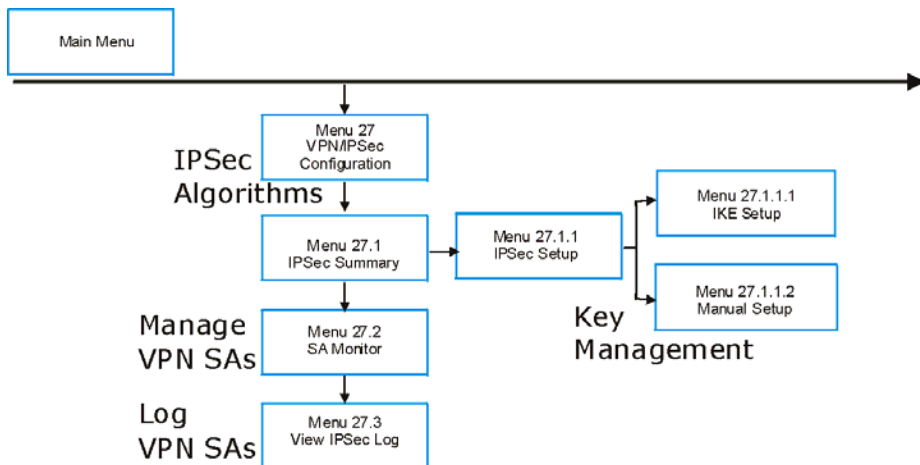


Figure 36-1 VPN SMT Menu Tree

From the main menu, enter 27 to display the first VPN/IPSec menu (shown next).

```
Menu 27 - VPN/IPSec Setup

1. IPSec Summary
2. SA Monitor
3. View IPSec Log

Enter Menu Selection Number:
```

Figure 36-2 Menu 27 VPN/IPSec Setup

36.2 IPSec Summary

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 — IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

The following figure helps explain the main fields in menu 27.1.

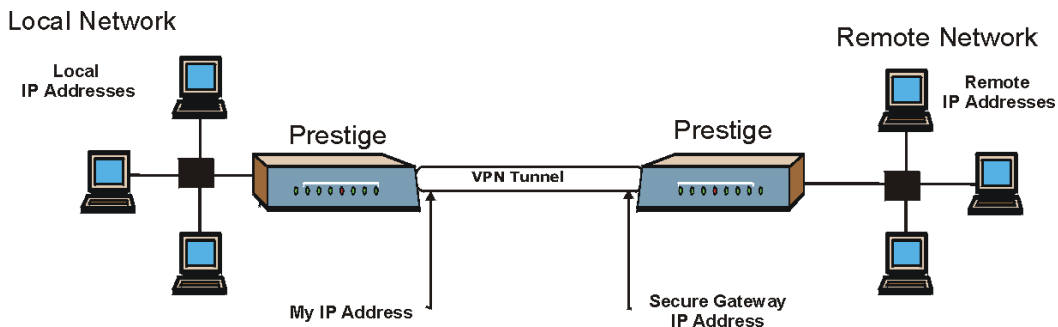


Figure 36-3 IPSec Summary Fields Illustration

Local and remote IP addresses must be static. The VPN initiator local IP address range should be identical to the peer remote IP address range. Similarly, the VPN initiator remote IP address range should be identical to the peer local IP address range. If they are not, the connection will fail and this will display in the IPSec log as a local or remote ID failure.

```

Menu 27.1 - IPSec Summary

#      Name      A  Local Addr Start      - Local Addr End      Encap      IPSec Algorithm
Key Mgt      Remote Addr Start      - Remote Addr End
-----
001    Taiwan    Y  192.168.1.35          192.168.1.38          Tunnel     ESP DES MD5
      IKE      172.16.2.40          172.16.2.46          Tunnel     193.81.13.2
002    zw50      N  1.1.1.1              1.1.1.1              Tunnel     AH SHA1
      IKE      4.4.4.4              255.255.0.0          Tunnel     zw50test.zyxel.
003    China     N  192.168.1.40         192.168.1.42         Tunnel     ESP DES MD5
      IKE      N/A                  N/A                  Tunnel     0.0.0.0
004
005

Select Command= None          Select Rule= N/A
Press ENTER to Confirm or ESC to Cancel:
    
```

Figure 36-4 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.	001
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. N means inactive.	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

Table 36-1 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Local 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 Local 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 LAN behind your Prestige.</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 LAN behind your Prestige.</p>	192.168.1.38
Encap	This field displays Tunnel mode or Transport mode. 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	<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>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).</p> <p>Both AH and ESP increase the Prestige's processing requirements and communications latency (delay).</p> <p>You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if ??? is displayed.</p>	ESP DES MD5
Key Mgt	This field displays the SA's type of key management, (IKE or Manual).	IKE

Table 36-1 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
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
Select Command	<p>Press [SPACE BAR] to choose from None, Edit or Delete and then press [ENTER]. You must select a rule in the next field when you choose the Edit, 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>	None

Table 36-1 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
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.		

Table 36-2 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 36-3 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 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 Addr field below.	

36.2.1 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 36-4 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 36-5 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

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.

```

Menu 27.1.1 - IPSec Setup

Index #= 1      Name= ?
Active= No     Keep Alive= No
Local ID type= IP      Content=
My IP Addr= 0.0.0.0
Peer ID type= IP      Content=
Secure Gateway Addr= 0.0.0.0
Protocol= 0
Local:  Addr Type= SINGLE
        IP Addr Start= 0.0.0.0      End/Subnet Mask= N/A
        Port Start= 0              End= N/A
Remote: Addr Type= N/A
        IP Addr Start= N/A         End/Subnet Mask= N/A
        Port Start= N/A           End= N/A
Enable Replay Detection= N/A
Key Management= N/A
Edit Key Management Setup= N/A
    
```

Figure 36-5 Menu 27.1.1 IPSec Setup

The following table describes the fields in this menu.

Table 36-6 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 . Select Yes 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 . 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.	IP

Table 36-6 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 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.</p> <p>The VPN tunnel has to be rebuilt if this IP address changes.</p>	0.0.0.0
Peer ID Type	<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>	IP
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 Addr 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 Addr field below.</p>	
Secure Gateway Addr	<p>Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection.</p> <p>Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the Key Management field must be set to IKE, see later). See the <i>Secure Gateway Address</i> section for more details.</p>	Zytest.com.tw

Table 36-6 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.	0
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.	
Addr Type	Press [SPACE BAR] to choose SINGLE , RANGE , or SUBNET and press [ENTER]. Select SINGLE with a single IP address. Select RANGE for a specific range of IP addresses. Select SUBNET to specify IP addresses on a network by their subnet mask.	SINGLE
IP Addr Start	When the Addr Type field is configured to Single , enter a (static) IP address on the LAN behind your 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
End/Subnet Mask	When the Addr Type field is configured to Single , this field is N/A . When the Addr Type field is configured to Range , enter the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the Addr Type field is configured to SUBNET , this is a subnet mask on the LAN behind your Prestige.	192.168.1.38
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3	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

Table 36-6 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
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 Addr field is configured to 0.0.0.0.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</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 Addr field to 0.0.0.0.</p>	4.4.4.4
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 Addr 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. Some of the most common IP ports are:</p> <p>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.	

Table 36-6 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
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	<p>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.</p>	IKE
Edit Key Management Setup	<p>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.</p>	No
<p>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.</p>		

36.4 Configuring IKE Settings

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).

```

Menu 27.1.1.1 - IKE Setup

Phase 1
Negotiation Mode= Main
Pre-Shared Key= ?
Encryption Algorithm = DES
Authentication Algorithm = MD5
SA Life Time (Seconds)= 28800
Key Group= DH1

Phase 2
Active Protocol = ESP
Encryption Algorithm = DES
Authentication Algorithm = SHA1
SA Life Time (Seconds)= 28800
Encapsulation = Tunnel
Perfect Forward Secrecy (PFS)= None

```

Figure 36-6 Menu 27.1.1.1 IKE Setup

The following table describes the fields in this menu.

Table 36-7 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]. Multiple SAs connecting through a secure gateway must have the same negotiation mode.	Main
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. Multiple SAs connecting through a secure gateway must have the same pre-shared key.	
Encryption Algorithm	When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Prestige DES encryption algorithm uses a 56-bit key. Triple DES (3DES), is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES . It also requires more processing power, resulting in slightly increased latency and decreased throughput. Press [SPACE BAR] to choose from 3DES or DES and then press [ENTER].	DES

Table 36-7 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Authentication Algorithm	MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slightly slower. Press [SPACE BAR] to choose from SHA1 or MD5 and then press [ENTER].	MD5
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.	28800 (default)
Key Group	You must choose a key group for phase 1 IKE setup. DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.	DH1
Phase 2		
Active Protocol	Press [SPACE BAR] to choose from ESP or AH and then press [ENTER]. See earlier for a discussion of these protocols.	ESP
Encryption Algorithm	Press [SPACE BAR] to choose from NULL , 3DES or DES and then press [ENTER]. Select NULL to set up a tunnel without encryption.	DES
Authentication Algorithm	Press [SPACE BAR] to choose from SHA1 or MD5 and then press [ENTER].	SHA1
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).	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
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 Key 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.

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= SHA1
Key=

AH Setup
SPI (Decimal)= N/A
Authentication Algorithm= N/A
Key= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Figure 36-7 Menu 27.1.1.2 Manual Setup

The following table describes the fields in this menu.

Table 36-8 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Active Protocol	Press [SPACE BAR] to choose from ESP Tunnel , ESP Transport , AH Tunnel or AH Transport and then press [ENTER]. Choosing an ESP combination causes the AH Setup fields to be non-applicable (N/A)	ESP Tunnel
ESP Setup	The ESP Setup fields are N/A if you chose an AH Active Protocol .	
SPI (Decimal)	The SPI must be unique and from one to four integers ("0" to "9").	1234
Encryption Algorithm	Press [SPACE BAR] to choose from NULL , 3DES or DES and then press [ENTER]. Fill in the Key1 field below when you choose DES and fill in fields Key1 to Key3 when you choose 3DES . Select NULL to set up a tunnel without encryption. When you select NULL , you do not enter any encryption keys.	DES

Table 36-8 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION	EXAMPLE
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).	
Authentication Algorithm	Press [SPACE BAR] to choose from MD5 or SHA1 and then press [ENTER].	SHA1
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for MD5 authentication and 20 characters for SHA-1 authentication. Any character may be used, including spaces, but trailing spaces are truncated.	123456789abcde
AH Setup	The AH Setup fields are N/A if you chose an ESP Active Protocol .	
SPI (Decimal)	The SPI must be from one to four unique decimal characters ("0" to "9") long.	N/A
Authentication Algorithm	Press [SPACE BAR] to choose from MD5 or SHA1 and then press [ENTER].	N/A
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for MD5 authentication and 20 characters for SHA-1 authentication. Any character may be used, including spaces, but trailing spaces are truncated.	N/A
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

Chapter 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.

An SA times out automatically after one minute if there is no traffic.

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
1	Taiwan : 3.3.3.1 - 3.3.3.3.100	Tunnel	ESP DES MD5
2			
3			
4			
5			
6			
7			
8			
9			
10			

Select Command= Refresh
Select Connection= N/A

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.	1
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	Press [SPACE BAR] to choose from Refresh , Disconnect or None and then press [ENTER]. You must select a connection in the next field when you choose the Disconnect command. Refresh displays current active VPN connections. None allows you to jump to the "Press ENTER to Confirm..." prompt.	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.		

Chapter 38

IPSec Log

This chapter interprets common IPSec log messages.

38.1 IPSec Logs

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log as shown next. The following figure shows a typical log from the initiator of a VPN connection.

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 38-1 Example VPN Initiator 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):

```

Figure 38-2 Example VPN Responder IPsec Log

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

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

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

Table 38-1 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 38-3</i> .

Table 38-1 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
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.
!! 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 38-2 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.
!! 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 38-3 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

Table 38-3 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Part IX:

Appendices and Index

This part provides appendices and an index of key terms.

Appendix A

Troubleshooting

This Appendix covers potential problems and the corresponding remedies.

Problems Starting Up the Prestige

Chart 1 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION	
None of the LEDs turn on when you turn on the Prestige.	Make sure that you have the included power adaptor connected to the Prestige and to an appropriate power source.	
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
Cannot access the Prestige via the console port.	1. Check to see if the Prestige is connected to your computer's console port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
No parity, 8 data bits, 1 stop bit, data flow set to none.		

Problems With the ISDN Line

Chart 2 Troubleshooting the ISDN Line

PROBLEM	CORRECTIVE ACTION
<p>The ISDN initialization failed. This problem occurs when you attempt to save the parameters entered in Menu 2, but receive the message, 'Save successful, but Failed to initialize ISDN; Press [Esc] to exit'.</p>	<p>Check the error log (in Menu 24.3.1), you should see a log entry for the ISDN initialization failure in the format, 'ISDN init failed. code<n> . . .'. Note the code number, n.</p> <p>If the code is 1, the ISDN link is not up. This problem could be either the ISDN line is not properly connected to the Prestige or the ISDN line is not activated. Verify that the ISDN line is connected to the Prestige and to the wall telephone jack.</p> <p>If the code is 3, this indicates a general failure. Verify the provisioning information for your switch by contacting your telephone company.</p> <p>Check your SPID numbers if the ISDN LED is blinking slowly as this indicates that SPID negotiation has failed (North America only).</p>
<p>The ISDN loopback test failed.</p>	<p>If the ISDN initialization is successful, then the loopback test should also work. Verify the telephone numbers that have been entered in Menu 2. The loopback test dials the number entered in the second Phone # field (except for switch types with only one phone number). If you need to dial a prefix (e.g., '9') to get an outside line, then you have to enter the telephone number as '95551212' or '914085551212'. If it is an internal line, you may only need to enter the last four or five digits (according to your internal dialing plan), e.g., 51212.</p>

Problems With a LAN Interface

Chart 3 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
<p>Cannot access the Prestige from the LAN.</p>	<p>Check your Ethernet cable type and connections. Refer to the <i>Rear Panel and Connections</i> section for LAN connection instructions.</p>
	<p>Make sure your Ethernet card is installed and functioning properly.</p>
<p>Cannot ping any computer on the LAN.</p>	<p>Check the Ethernet LEDs on the front panel. One of these LEDs should be on. If they are all off, check the cables between your Prestige and hub or the computer.</p>
	<p>Verify that the IP address and the subnet mask of the Prestige and the computers are on the same subnet.</p>

Problems Connecting to a Remote Node or ISP

Chart 4 Troubleshooting a Connection to a Remote Node or ISP

PROBLEM	CORRECTIVE ACTION
Cannot connect to a remote node or ISP.	Check Menu 24.1 to verify the line status. If it indicates [down], then refer to the section on the line problems.
	In Menu 24.4.5, do a manual call to that remote node. Observe the messages and take appropriate actions.

Remote User Dial-in Problems

Chart 5 Troubleshooting Remote User Dial-in Problems

PROBLEM	CORRECTIVE ACTION
A remote user cannot dial-in.	First verify that you have configured the authentication parameters in Menu 13. These would be CLID Authen and Recv Authen .
	In Menu 14.1, verify the user name and password for the remote dial-in user.
	If the remote dial-in user is negotiating IP, verify that the IP address is supplied correctly in Menu 13. Check that either the remote dial-in user is supplying a valid IP address, or that the Prestige is assigning a valid address from the IP pool.
	If the remote dial-in user is negotiating IPX, verify that the IPX network number is valid from the IPX pool (if it is being used).

Problems With the Password

Chart 6 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	See the <i>Resetting the Prestige</i> section for details on restoring all of the factory default settings.

Problems With Remote Management

Chart 7 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige from the LAN or WAN.	When NAT is enabled: <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 for instructions on checking your LAN connection.

Appendix B

Power Adaptor Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adaptor Model	DV-121AACS
Input Power	AC120Volts/60Hz/23W max
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adaptor Model	AA-121A
Input Power	AC120Volts/60Hz/18W max
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adaptor Model	DSA-009F-12A
Input Power	AC100-250V/47-63Hz/0.3A
Output Power	DC 12 Volts/0.75A
Power Consumption	8 W
Safety Standards	UL, CUL, T-mark (UL 1950, CSA C22.2 No.950)
UNITED KINGDOM PLUG STANDARDS	
AC Power Adaptor Model	AA-121AD
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	ITS-GS, CE (EN 60950, BS 7002)

EUROPEAN PLUG STANDARDS	
AC Power Adaptor Model	DV-121AACCP-5716
Input Power	AC230Volts/50Hz/100mA
Output Power	AC12Volts/1.0A
Power Consumption	8W
Safety Standards	TUV-GS, CE (EN 60950)
EUROPEAN PLUG STANDARDS	
AC Power Adaptor Model	AA-121ABN
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	ITS-GS, CE (EN 60950)
china Standards	
AC Power Adaptor Model	DV-121AACCP-5720
Input Power	AC220Volts/50Hz/18W
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	CCEE (GB8898)
china Standards	
AC Power Adaptor Model	BH-48 (AA-121AP)
Input Power	AC220Volts/50Hz
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	CCEE (GB8898)

Appendix C

IP Subnetting

IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.
- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

Chart 8 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Host IDs of all zeros or all ones are not allowed.

Therefore:

- A class “C” network (8 host bits) can have $2^8 - 2$ or 254 hosts.
- A class “B” address (16 host bits) can have $2^{16} - 2$ or 65534 hosts.

A class “A” address (24 host bits) can have $2^{24} - 2$ hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Chart 9 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

Chart 10 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

Chart 11 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class “C” natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class “C” address 192.168.1.0 with subnet mask of 255.255.255.0.

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class “C”). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The “borrowed” host ID bit can be either “0” or “1” thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

Chart 12 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Chart 13 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart 14 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Chart 15 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Chart 16 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Chart 17 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Chart 18 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class “C” subnet planning.

Chart 19 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Chart 8) available for subnetting.

The following table is a summary for class "B" subnet planning.

Chart 20 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126

Chart 20 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix D

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

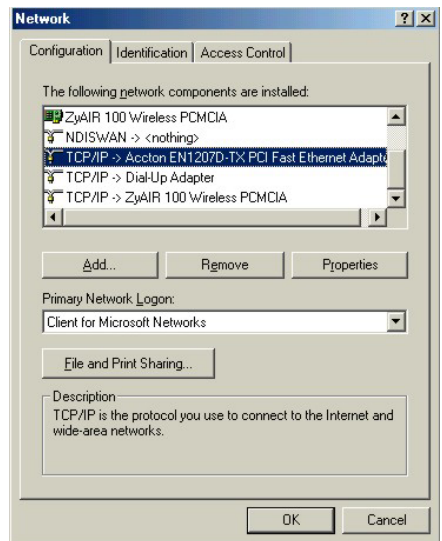
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- a. In the **Network** window, click **Add**.
- b. Select **Adapter** and then click **Add**.
- c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- a. In the **Network** window, click **Add**.
- b. Select **Protocol** and then click **Add**.
- c. Select **Microsoft** from the list of **manufacturers**.
- d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

- a. Click **Add**.
- b. Select **Client** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.
- d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e. Restart your computer so the changes you made take effect.

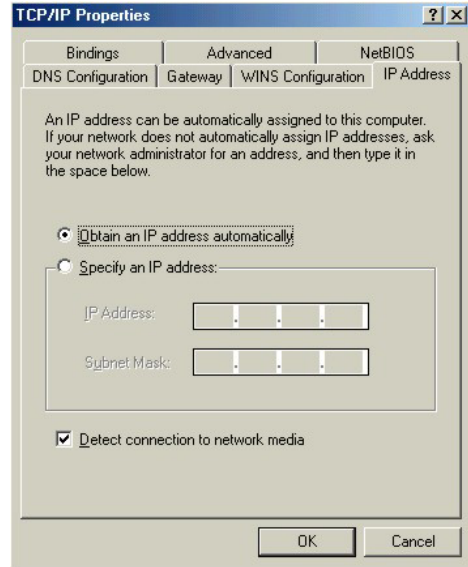
Configuring

1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

2. Click the **IP Address** tab.

-If your IP address is dynamic, select **Obtain an IP address automatically**.

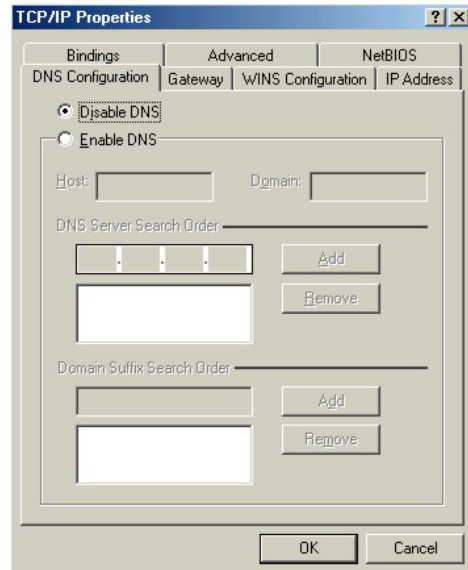
-If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



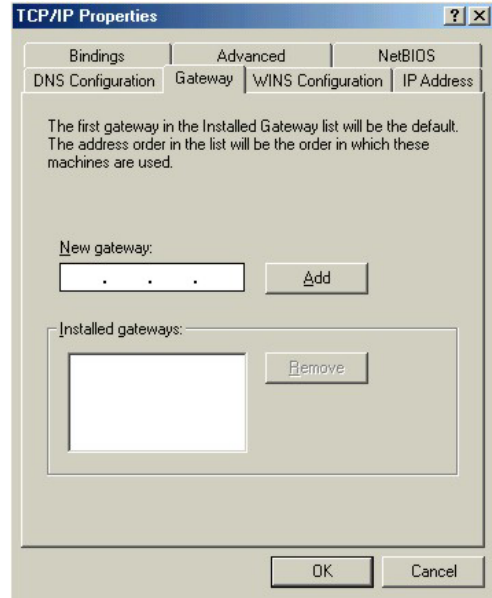
3. Click the **DNS Configuration** tab.

-If you do not know your DNS information, select **Disable DNS**.

-If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



4. Click the **Gateway** tab.
 - If you do not know your gateway's IP address, remove previously installed gateways.
 - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.



5. Click **OK** to save and close the **TCP/IP Properties** window.
6. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7. Turn on your Prestige and restart your computer when prompted.

Verifying Settings

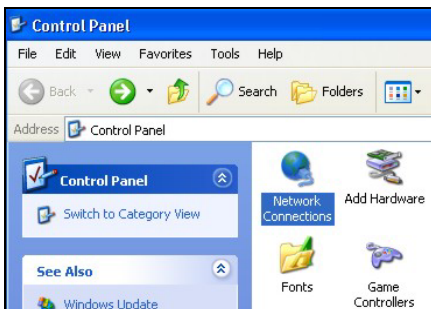
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

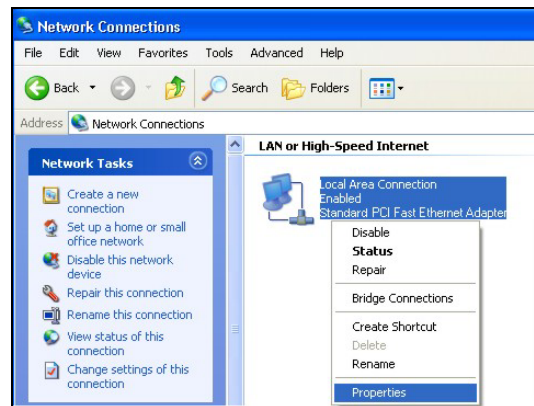
1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.



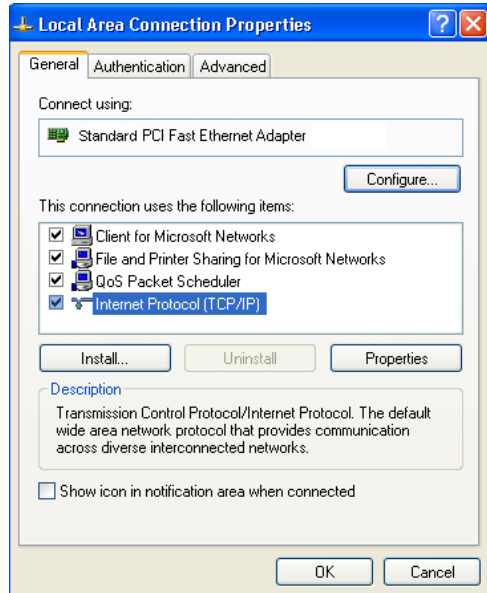
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.



3. Right-click **Local Area Connection** and then click **Properties**.



4. Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

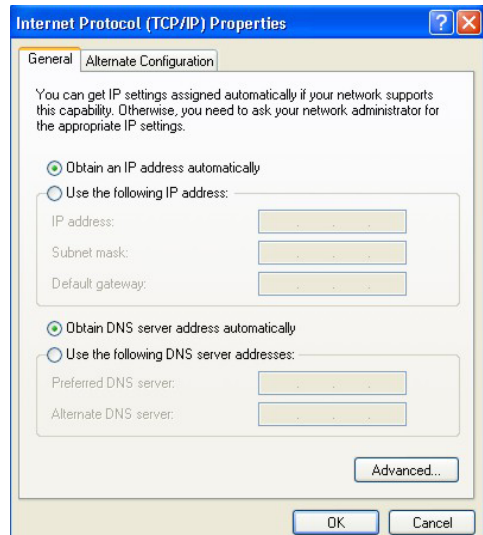


5. The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

-If you have a dynamic IP address click **Obtain an IP address automatically**.

-If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

Click **Advanced**.



6. -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

-In the **IP Settings** tab, in IP addresses, click **Add**.

-In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

-Repeat the above two steps for each IP address you want to add.

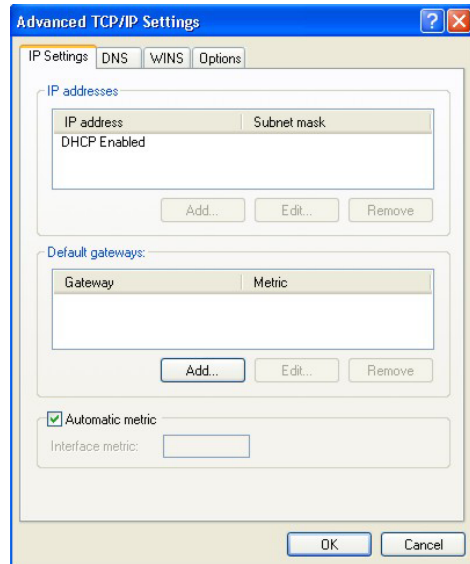
-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

-Click **Add**.

-Repeat the previous three steps for each default gateway you want to add.

-Click **OK** when finished.

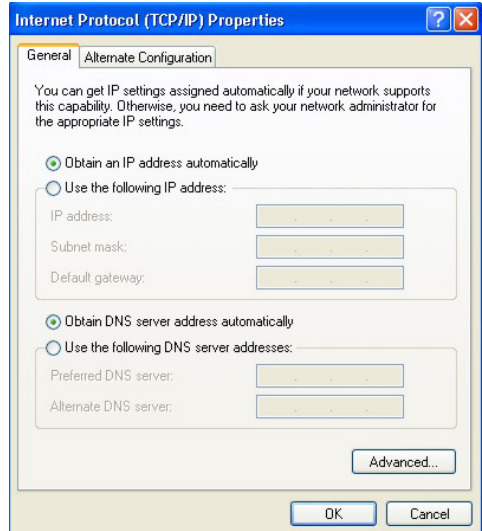


7. In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

-Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

-If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.



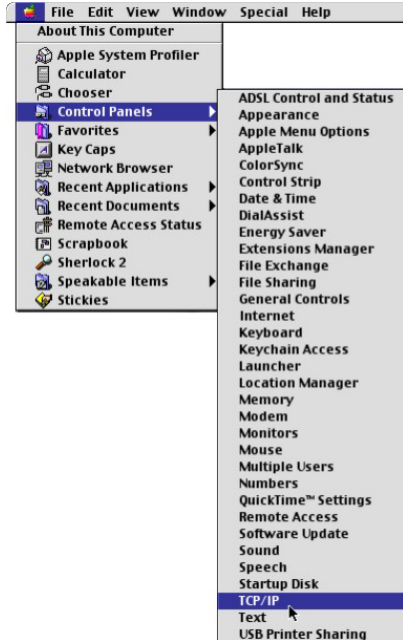
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

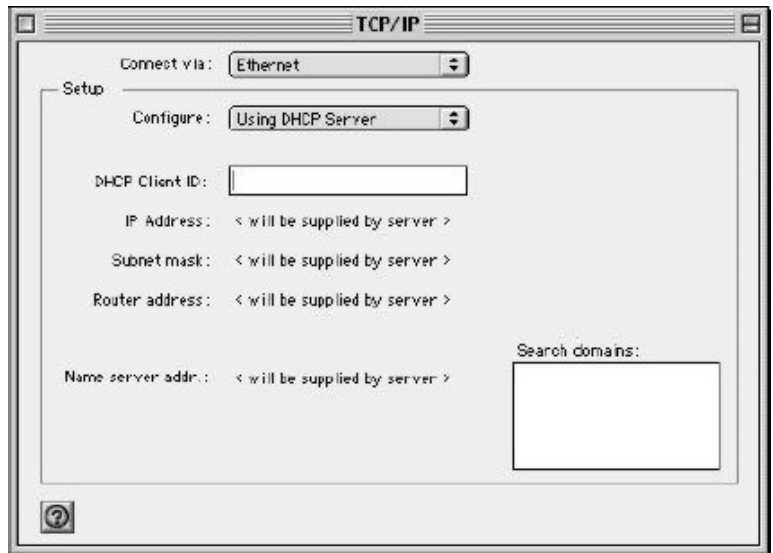
1. Click **Start, All Programs, Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

1. Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.



2. Select **Ethernet built-in** from the **Connect via** list.



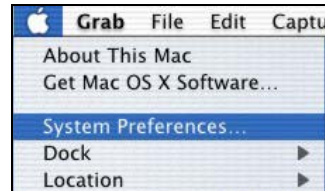
3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
4. For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Prestige in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

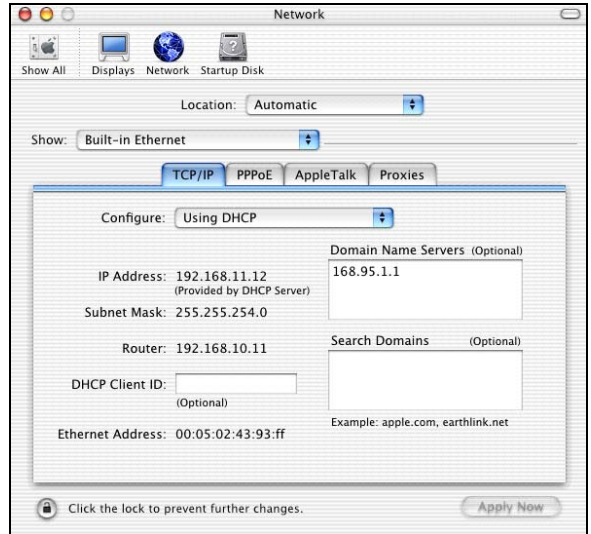
Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1. Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.



2. Click **Network** in the icon bar.
 - Select **Automatic** from the **Location** list.
 - Select **Built-in Ethernet** from the **Show** list.
 - Click the **TCP/IP** tab.



3. For dynamically assigned settings, select **Using DHCP** from the **Configure** list.
4. For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Prestige in the **Router address** box.
5. Click **Apply Now** and close the window.
6. Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix E

Splitters and Microfilters

This appendix tells you how to install a POTS splitter or a telephone microfilter.

Connecting a POTS Splitter

When you use the Full Rate (G.dmt) ADSL standard, you can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitter at the point where the telephone line enters your residence, as shown in the following figure.

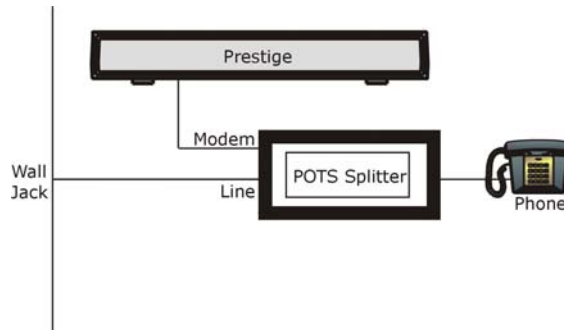


Diagram 1 Connecting a POTS Splitter

- Step 1.** Connect the side labeled “Phone” to your telephone.
- Step 2.** Connect the side labeled “Modem” to your Prestige.
- Step 3.** Connect the side labeled “Line” to the telephone wall jack.

Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The use of a telephone microfilter is optional.

- Step 1.** Connect a phone cable from the wall jack to the single jack end of the Y- Connector.
- Step 2.** Connect a cable from the double jack end of the Y-Connector to the “wall side” of the microfilter.

Step 3. Connect another cable from the double jack end of the Y-Connector to the Prestige.

Step 4. Connect the “phone side” of the microfilter to your telephone as shown in the following figure.

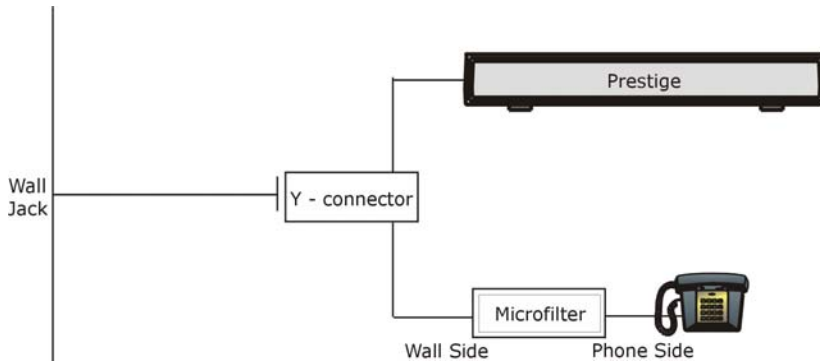


Diagram 2 Connecting a Microfilter

Prestige With ISDN

This section relates to people who use their Prestige with ADSL over ISDN (digital telephone service) only. The following is an example installation for the Prestige with ISDN.

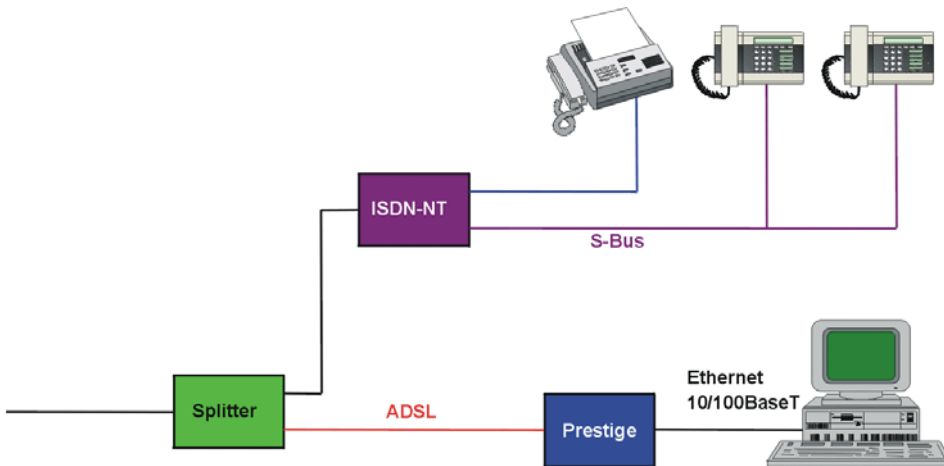


Diagram 3 Prestige with ISDN

Index

4

4-Port Switch 1-1

A

Action for Matched Packets 10-11
 Address Assignment 4-2
 Allocated Budget 23-5
 Alternative Subnet Mask Notation K
 Analog Phone Support 1-2
 Application-level Firewalls 8-1
 AT command 32-1
 Attack
 Reasons 12-2
 Attack Alert 9-2, 9-3, 9-5
 Attack Types 8-6
 Reason 28-3
 Authentication 23-4, 23-6, 25-2
 Auto-negotiating 10/100 Mbps Ethernet LAN. 1-2
 Auto-sensing 10/100 Mbps Ethernet LAN 1-2
 Average Line Utilization 31-2

B

Backup 32-2
 BACP 23-6
 Bandwidth-On-Demand 1-3
 BAP 23-6
 Base Transmission Rate 23-6
 Basic Rate Interface 1-2
 Blacklist 33-2, 33-3
 Blocking Time 9-4, 9-5
 BOD *See* Bandwidth on Demand . *See* Bandwidth
 on Demand
 Bold Times font *See* Syntax Conventions
 BRI 1-2
 Broadband Access Security Gateway xxiii

Brute-force Attack, 8-5
 BTR *See* Base Transmission Rate
 budget control 23-5, 25-3
 Budget Management 33-2, 33-4, 33-5

C

Call Control 1-4
 Call Direction 23-3
 Call Filtering 27-1
 Call Filters
 Built-In 27-1
 User-Defined 27-1
 Call Scheduling 1-2, 35-1
 maximum number of schedule sets 35-1
 Precedence 35-1
 Callback 1-6, 23-4, 25-3, 25-5, 25-7, 25-12
 Callback Support 25-1
 Callback with CLID 25-12
 Caller ID 1-5
 Canada iv
 Caution iv
 CDR 31-7
 CDR (Call Detail Record) 31-6
 CHAP 23-4, 25-3
 CHAP/PAP 25-3
 Classes of IP Addresses I
 CLID 1-3, 23-3, 25-1, 25-2, 25-7
 CLID Callback Support 1-3
 Command Interpreter Mode 33-1
 Command Mode 31-13
 Community 29-1
 Compression 23-8, 25-3
 Configuration 3-9, 4-1, 17-6
 Console Port 18-1, 31-3, 31-4
 Copyright ii
 Country Code 31-4
 CPU Load 31-3
 Current Line Utilization 31-2

Custom Ports	
Creating/Editing.....	11-2
Introduction	11-1
Customer Support	vi
Customized Services.....	11-2

D

data compression	1-4
Data Filtering.....	27-1
DDNS	
Configuration.....	19-2
Default Dial-In Setup.....	25-1
Default Policy Log.....	10-5
Denial of Service	8-2, 8-3, 9-4, 28-2
Destination Address.....	10-2, 10-11
Device Filter rules.....	27-16
DHCP	3-9, 4-1, 4-2, 7-1, 17-6, 21-2, 31-5
DHCP (Dynamic Host Configuration Protocol) 1-4	
DHCP Setup	21-2
Diagnostic.....	31-12
Diagnostic Tools.....	31-1
dial-in user	25-1
Dial-in User	25-4
Dial-On-Demand	1-3
Disclaimer.....	ii
DNS Server	
For VPN Host.....	14-7
Domain Name.....	4-2, 6-5
DoS	
Basics.....	8-3
Types	8-4
DoS (Denial of Service).....	1-1
Dynamic DNS.....	7-1, 19-2
DYNDNS Wildcard.....	7-1

E

e.g.	<i>See Syntax Conventions</i>
ECHO	6-5
E-mail	

Log Example	28-4
EMAIL	19-3
E-mail Address	19-3
Enable Wildcard	19-3
Encapsulation	23-8
Enter	<i>See Syntax Conventions</i>
Entering Information	18-3
Error Log	31-5
Error/Information Messages	
Sample	31-6
Ethernet	21-1
Ethernet Traffic	27-20
European (DSS1) ISDN Setup Menus.....	20-4

F

Factory LAN Defaults	4-2
FCC	iii
Features	1-1
Filename Conventions.....	32-1
Filter	
Applying Filters.....	27-19
Default Dial-in Filter	25-4
Ethernet Setup	21-1
Ethernet traffic.....	27-20
Ethernet Traffic	27-20
Filter Rules	27-7
Filter Structure.....	27-4
Generic Filter Rule	27-14
Remote Node Filter	23-14
Remote Node Filters.....	27-20
Sample	27-18
SUA	27-16
TCP/IP Filter Rule.....	27-9
Filter Log.....	31-7
Filter Rule Process.....	27-3
Filter Rule Setup.....	27-9
Filter Rules Summary	
Sample	27-19
Filter Set	
Class	27-9
Filtering	27-1, 27-9

Filtering Process	
Outgoing Packets	27-2
Finger	6-5
Firewall	1-1
Access Methods	28-1
Address Type	10-12
Alerts	9-3
Connection Direction	10-3
Creating/Editing Rules	10-9
Custom Ports	<i>See</i> Custom Ports
Enabling	9-1
Firewall Vs Filters	8-12
Guidelines For Enhancing Security	8-11
Introduction	8-2
LAN to WAN Rules	10-3
Log	28-2
Policies	10-1
Remote Management	9-1, 28-1
Rule Checklist	10-1
Rule Logic	10-1
Rule Precedence	10-4
Rule Security Ramifications	10-2
Services	10-6
SMT Menus	28-1
Types	8-1
When To Use	8-12
Firmware File	
Maintenance	17-7
Firmware Upgrade	1-4
FTP	4-1, 6-5, 7-1, 32-4, 34-3
Restrictions	34-3
FTP File Transfer	32-10
FTP Restrictions	32-4
FTP Server	26-13
Full Network Management	1-3
Full Rate	BB

G

Gateway	24-3
General Setup	19-1, 20-1
Graphics Icons Key	xxiv

H

Half-Open Sessions	9-4
Hidden Menus	18-3
Host	2-4
Host IDs	I
HTTP	6-5, 8-1, 8-3, 36-10, 36-11
HyperTerminal program	32-6, 32-9

I

i.e.	<i>See</i> Syntax Conventions
IANA	3-2
ICMP echo	8-5
Idle Timeout	23-5, 25-9
Incoming Call Support	1-3
Industry Canada	iv
Initial Screen	18-1
Internet Access	1-5
Internet Access Setup	26-1
Internet Assigned Numbers Authority ..	<i>See</i> IANA
Internet Control Message Protocol (ICMP)	8-5
IP Address 3-1, 4-1, 6-5, 6-7, 17-6, 21-3, 23-4, 23-11, 23-12, 24-2, 25-3, 27-11, 31-4	
IP Address Assignment	3-2
IP Addressing	I
IP Alias	1-2
IP Alias Setup	21-3
IP Classes	I
IP Filter	27-13
Logic Flow	27-12
IP mask	27-11
IP Packet	27-14
IP Pool	21-3, 25-4
IP Pool Setup	3-10, 4-1
IP Ports	36-10, 36-11
IP Spoofing	8-4, 8-7
IP Static Route	24-1
IP Static Route Setup	24-2
IPSec VPN Capability	1-1
ISDN	CC
ISDN initialization failure	B

ISDN loopback test failure B
 ISDN Setup 20-1

K

Key Fields For Configuring Rules 10-2

L

LAN 31-3
 LAN Setup 4-1, 5-1, 7-1, 21-1
 LAN TCP/IP 4-2, 21-2
 LAN to WAN Rules 10-3
 LAND 8-4, 8-5
 LAN-to-LAN 23-9, 25-10
 Local Network
 Rule Summary 10-4
 Log and Trace 31-6
 Log Facility 31-7
 Log Screen 12-1
 Logging 1-4
 Logging Option 27-11, 27-15
 Login 23-3
 login screen 18-2
 Logs 12-1
 Loop-back Test 20-6

M

Main Menu 18-3
 Main Menu Commands 18-2
 Max. Transmission Rate 23-6
 Max-incomplete High 9-4
 Max-incomplete Low 9-4
 Metric 23-13, 24-3
 MP 3-8, 5-4, 22-2. *See* Multilink
 Multilink 1-3, 23-6. *See* MP. *See* MP. *See* MP
 Mutual Authentication 25-3

N

Nailed-up Connection 23-5

NAT 3-1, 4-1, 6-5, 6-6, 27-16
 Application 6-2
 Applying NAT in the SMT Menus 26-1
 Configuring 26-3
 Definitions 6-1
 Examples 26-10
 How NAT Works 6-2
 Mapping Types 6-3
 Non NAT Friendly Application Programs 26-16
 Ordering Rules 26-6
 What NAT does 6-1
 NetBIOS commands 8-6
 Network Address Translation (NAT) 1-2, 26-1
 Network Management 6-6
 NNTP 6-5
 Notice iii

O

One-Minute High 9-4
 Online Registration v
 Outgoing Calling Party Number 20-2
 Outgoing Data Call Bumping Support 1-3

P

PABX 20-2
 PABX Outside Line Prefix 20-2
 Packet Filtering 8-12
 Packet Filtering Firewalls 8-1
 Packet Information 12-2
 Packet Triggered 31-7
 packets 31-2
 Packing List Card xxiii
 PAP 23-4, 25-3
 Password 2-4, 18-2, 18-6, 23-3, 23-4, 29-1
 Ping 31-13
 Ping of Death 8-4
 Point-to-Point Tunneling Protocol 6-6
 POP3 6-5, 8-3
 Port Configuration 11-3
 Port Numbers 6-5

Power Adapter Specifications	A, G
PPP	23-4, 23-7
PPP Log	31-7
PPP Multilink.....	1-3
PPTP	6-6
Prestige Firewall Application.....	8-3
Private	23-13, 24-3
Protocol.....	27-10
Protocol Filter rules.....	27-16

R

RADIUS	
Shared Secret Key.....	30-1
RADIUS (Remote Authentication Dial-In User Service).....	30-1
RAS.....	31-4
Read Me First.....	xxiii
Related Documentation.....	xxiii
Relay	21-2
Remote Access Server	1-6, 25-7
Remote Access under Windows.....	25-8
Remote Dial-in Users.....	25-1
Remote Management	
Firewall	9-1, 28-1
Remote Management Limitations	32-4, 34-3
Remote Management Setup	34-1
Remote Node	23-1, 23-8, 31-2, 31-12
Remote Node Profile.....	23-2
Remote Node Setup	23-1, 23-2
Repairs	v
Replacement.....	v
Required fields.....	18-3
Resetting the Time	33-8
Restore Configuration.....	32-7
Return Material Authorization Number	v
RIP	21-3, 23-13
RIP direction	21-4
RIP version.....	21-4
Rule Summary	10-4, 11-6
Rules	
Checklist	10-1

Creating Custom	10-1
Key Fields.....	10-2
LAN to WAN	10-3
Logic.....	10-1
Predefined Services	10-6
Source and Destination Addresses.....	10-11
Summary.....	10-4
Timeout.....	10-12

S

SA Monitor	37-1
Sample IP Addresses	23-13
Saving the State	8-7
Schedule Sets	
Duration	35-3
Security	1-4
Security Association	37-1
Security In General	8-11
Security Ramifications.....	10-2
Select	<i>See Syntax Conventions</i>
Server.....	6-4, 22-2, 26-3, 26-5, 26-8, 26-9, 26-12, 26-13, 33-7
Service	v, 10-2
Service Type	11-3
Services.....	6-5
Set Up a Schedule.....	35-2
Single User Account.....	22-2
SMTP.....	6-5
Smurf.....	8-5, 8-6
SNMP	
Community	29-1, 31-10
Configuration.....	29-1
Trusted Host	29-1
Source & Destination Addresses	10-11
Source Address	10-2, 10-10
Splitters.....	BB
Stac data compression.....	1-4
Stateful Inspection	
Prestige	1-1, 8-1, 8-2, 8-7, 8-8
Process.....	8-9
Process.....	8-8
Static Route Setup.....	24-1

Static Routing Topology	24-1
SUA	6-5, 6-6
SUA (Single User Account) ..	<i>See</i> NAT. <i>See</i> NAT
Subnet Mask ...	3-1, 4-1, 10-12, 21-3, 23-12, 24-3, 31-5
Subnet Masks	J
Subnetting	J
Supplementary Voice Features	1-4
Support Disk	xxiii
Switch Type	B
SYN Flood	8-4, 8-5
SYN-ACK	8-4
Syntax Conventions	xxiii
Syslog	11-3, 31-6
Syslog IP Address	31-7
Syslog Server	31-6
System	
Call Control	33-2
Console Port Speed	31-5
Diagnostic	31-11
Log and Trace	31-5
Syslog and Accounting	31-6
System Information	31-4
System Information	31-3, 31-4
System Information & Diagnosis	31-1
System Maintenance ...	31-1, 31-3, 32-2, 32-5, 32-13, 32-14, 33-1, 33-2, 33-7
System Management Terminal	18-2
System Status	31-2
System Timeout	34-3

T

Target Utility	23-7
TCP Maximum Incomplete	9-4, 9-5
TCP Security	8-9
TCP/IP	8-3, 8-4, 21-3, 27-16, 31-13
TCP/IP Ethernet Setup and DHCP	21-2
TCP/IP Setup	21-3
Teardrop	8-4
Telco Options	22-2
Telecommuting	25-7, 25-8

Telephone Microfilters	BB
TFTP	
And FTP Over WAN}	34-3
Restrictions	34-3
TFTP and FTP Over WAN}	32-4
TFTP File Transfer	32-13
TFTP Restrictions	32-4
Three-Way Handshake	8-4
Threshold Values	9-4
Time and Date Setting	33-6, 33-7
Timeout	10-12, 10-13
Toll Period	23-5
Traceroute	8-7
Tracing	1-4
Trademarks	ii
Troubleshooting	A
ISDN Line	B
LAN Interface	B
Remote Node or ISP	C
Remote User to Dial-in	C

U

UDP/ICMP Security	8-10
UNIX Syslog	31-7
UNIX syslog parameters	31-7
Upload Firmware	32-10
Upper Layer Protocols	8-9, 8-10
User Name	19-3

W

WAN address	23-12
WAN to LAN Rules	10-3
Warranty	v
Web Configurator 2-4, 8-2, 8-10, 8-11, 10-2, 28-2	
Wizard Setup	3-1
www.zyxel.com	v

X

XMODEM protocol	32-2
-----------------------	------

Z

ZyNOS 32-1, 32-2
ZyNOS F/W Version 32-1
ZyXEL Limited Warranty

Note v
ZyXEL website v
ZyXEL's Firewall
 Introduction 8-2