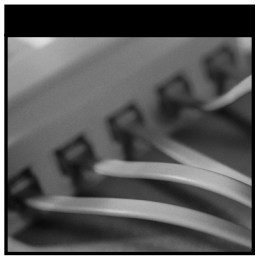
WILEY

Nortel® Guide to VPN Routing for Security and VoIP

James Edwards
Richard Bramante
Al Martin



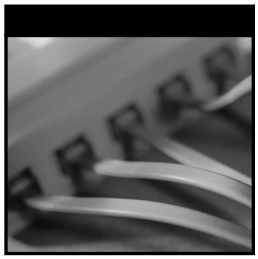


Nortel Guide to VPN Routing for Security and VoIP

James Edwards
Richard Bramante
Al Martin

WILEY
Wiley Publishing, Inc.

Nortel Guide to VPN Routing for Security and VoIP



Nortel Guide to VPN Routing for Security and VoIP

James Edwards
Richard Bramante
Al Martin

WILEY
Wiley Publishing, Inc.

Nortel Guide to VPN Routing for Security and VoIP
Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2006 by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN-13: 978-0-471-78127-1
ISBN-10: 0-471-78127-4

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

1MA/SU/QX/QW/IN

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4355, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware that Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (800) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Library of Congress Cataloging-in-Publication Data
Edwards, James, 1962-
Nortel guide to VPN routing / James Edwards, Richard Bramante, Al Martin.
p. cm.
"Wiley Technology Publishing."
Includes index.
ISBN-13: 978-0-471-78127-1 (cloth)
ISBN-10: 0-471-78127-4 (cloth)
1. Routing (Computer network management) 2. Extranets (Computer networks) I. Bramante, Richard, 1944- II. Martin, Al, 1964- III. Title.
TK5105.543.E39 2006
004.6'2--dc22
2006011213

Trademarks: Wiley and related trade dress are registered trademarks of Wiley Publishing, Inc., in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

This book is dedicated to my wife, Denise, and our children:
Natasia, Shaun, Nick, Emily, and Samantha.
For the support, pride, admiration, love, laughter,
life lessons, and so much more that they give to me each
and every day of my life.

—Jim Edwards

This book is dedicated to my beloved departed wife, Barbara,
who showed great courage and perseverance in facing and
battling the illnesses that eventually took her from this life.
Her constant encouragement in whatever I wanted to pursue is
not forgotten, nor will her memory fade. For without her in my life,
I would not have my son, Richard, who is a source of joy and pride.
I thank him and his loving wife, Michelle, for the three beautiful
grandchildren they blessed me with, my three amigos,
Vanessa, Ethan, and Olivia.

—Richard Bramante

About the Authors

James Edwards (Nashua, NH) is a Nortel Networks Certified Support Specialist (NNCSS) in VPN Routers. Working in the Premium Support Group (consisting of Nortel's largest Enterprise customers), he has extensive experience with many Nortel products, in particular in support for VPN Routers for the last two years. Jim has previous technical writing experience and is also author of *Nortel Networks: A Beginner's Guide* (McGraw-Hill, 2001).

Richard Bramante (Tewksbury, MA) is a Nortel Networks Certified Support Specialist (NNCSS) in VPN Routers. Richard has been in Nortel VPN Router support for three years and prior to this, was a technology lead on the Instant Internet (now part of the VPN Router portfolio) for four years. He has previous technical writing experience drafting functional specifications and testing procedures for various technologies and devices.

Credits

Executive Editor
Carol Long

Development Editor
Kevin Shafer

Production Editor
Angela Smith

Copy Editor
Nancy Rapoport

Editorial Manager
Mary Beth Wakefield

Production Manager
Tim Tate

Vice President and Executive Group Publisher
Richard Swadley

Vice President and Executive Publisher
Joseph B. Wikert

Project Coordinator
Jennifer Theriot

Graphics and Production Specialists
Jennifer Click
Lauren Goddard
Denny Hager
Stephanie D. Jumper
Lynsey Osborn
Heather Ryan
Alicia B. South

Quality Control Technician
Leeann Harney
Joe Niesen

Proofreading and Indexing
Techbooks

Cover Image
Kristin Corley

Contents

Chapter 1 Networking and VPN Basics 1

Networking Basics 2
- The OSI Reference Model 2
  - The Application Layer (Layer 7) 3
  - The Presentation Layer (Layer 6) 4
  - The Session Layer (Layer 5) 4
  - The Transport Layer (Layer 4) 4
  - The Network Layer (Layer 3) 5
  - The Data Link Layer (Layer 2) 6
  - The Physical Layer (Layer 1) 6
- Overview of a Local Area Network 7
- Overview of a Wide Area Network 8
- Media Access Control Addressing 8
- Internet Protocol Addressing 9
  - IP Address Classes 10
  - Class A Addresses 10
  - Class B Addresses 11
  - Class C Addresses 11
  - Class D Addresses 11
- Protocols and Other Standards 12
  - Internet Protocol 12
  - Interior Gateway Protocol 13
  - Exterior Gateway Protocol 14
  - Routing Information Protocol 14
  - Open Shortest Path First 15
  - Virtual Router Redundancy Protocol 16
  - Digital Subscriber Line 16

Integrated Services Digital Network 17
Lightweight Directory Access Protocol 18
Remote Authentication Dial-In User Service 18
Networking Hardware 19
Random Access Memory 19
Modem 19
Channel Service Unit/Data Service Unit 20
Computer Workstations 20
Servers 20
Network Interface Cards 21
Switch 21
Hub 22
Router 22
Repeater 22
Remote Access 24
Remote Access Services 24
Dial Access to a Single Workstation 25
Remote Access System 25
Terminal Servers 25
Network Security 26
The Firewall 26
Proxy Server 27
Packet Filtering 27
Stateful Packet Inspection 27
Demilitarized Zone 27
Hackers 28
VPN Basics 29
VPN Overview 29
VPN Tunneling Protocols and Standards 30
Secure Sockets Layer 30
Public Key Infrastructure 32
SecurID 32
Internet Protocol Security 33
Layer 2 Forwarding 34
Point-to-Point Tunneling Protocol 35
Layer 2 Tunneling Protocol 36
Generic Routing Encapsulation 37
Summary 38

Chapter 2 The Nortel VPN Router 39
The Nortel VPN Router Portfolio 40
Modules and Interfaces 41
SSL VPN Module 1000 41
Hardware Interface Options 42
Peripheral Component Interconnect Expansion Slots 42
10/100Base-T Ethernet 42
1000Base-SX/1000Base-T Ethernet 42

CSU/DSU 43
T1/E1 43
ADSL 44
Serial Interfaces (V.35, X.21, RS-232) 44
V.90 Dial Access Modem 45
High Speed Serial Interface 45
Encryption Accelerator Modules 45
Console Port (DB-9) 45
Nortel VPN Router Solutions 46
VPN Router 100 48
Overview 50
Technical Specifications 50
VPN Router 200 Series 50
VPN Router 221 50
VPN Router 251 52
VPN Router 600 53
VPN Router 1000 Series 55
VPN Router 1010 55
VPN Router 1050 57
VPN Router 1100 58
VPN Router 1700 Series 59
VPN Router 1700 60
VPN Router 1740 61
VPN Router 1750 62
VPN Router 2700 63
Overview 64
VPN Router 5000 66
Overview 66
VPN Router Features Comparison 67
Deployment Examples 70
Branch Office Tunnel VPN Solution 70
Extranet VPN Solution 71
Remote Access VPN Solution 72
Summary 74

Chapter 3 The Nortel VPN Router Software Overview 75
Nortel VPN Software 76
Accounting Services 76
Bandwidth Management Services 76
Certifications 77
Encryption Services 77
IP Routing Services 77
Management Services 78
Stateful Firewall 78
User Authentication 78
VPN Tunneling Protocols 79
Secure Sockets Layer Services 79
WAN Services 79

VPN Router Software Version 6.00 79
Memory Requirements 80
Optional Software Licenses 80
Advanced Router License Key 80
Contivity Stateful Firewall License Key 81
Additional VPN Tunnel Support License Key 81
Features Introduced in VPN Router Version 6.00 81
Loading, Verifying, and Upgrading the VPN Router Software 82
Release Notes 83
Loading a New Version of VPN Router Software 83
Removing Unused Versions 102
VPN Client Software 106
Installing the VPN Client Software 106
Release Notes 107
Installing the VPN Client 107
Upgrading the VPN Client Software 113
Uninstalling the Existing Version of VPN Client Software 113
Installing the Upgrade 115
Starting the VPN Client 122
The VPN Client Connection Wizard Process 125
Selecting Username and Password Authentication Type 126
Selecting Hardware or Software Token Card Authentication Type 130
Summary 132

Chapter 4 The Nortel VPN Router in the Network 133
What Is a Virtual Private Network? 133
Tunneling Basics 135
Branch Office Tunnel 136
Aggressive Mode Branch Office Tunnel 138
User/Client Tunnel 141
PC-Based VPN Tunnels 142
VPN-Enabled Device Acting in Client Mode 145
Small Office or Home Office 148
DMZ Creation and Usages 154
The Regional Office 158
Nortel 100 VPN Router Added to Existing Regional Office Network 160
Upgrading a Regional Office to VPN Technology 162
The Central Office 164
The VPN Router as an Access Point 166
Client Access to the Corporate Network 168
Client Load Balancing and Failover 171
Corporate User Access to the Internet 172
Backup Interface Services 173
Interface Group Fails 175
Route Unreachable 175

Ping Failure 175
Time of Day or Day of the Week 176
Placement in the Network 177
Network Administration of VPN Routers 180
Direct Access 181
Control Tunnels 181
Out-of-Band Management 181
Logging 182
SNMP 182
Other Management Considerations 184
Summary 184

Chapter 5 Management Options and Overview 185
Serial Port Management 186
Command Line Interface 187
Accessing the CLI Through a Telnet Session 187
Accessing the CLI Through the Serial Port 188
CLI Command Modes 188
User EXEC Mode 189
Privileged EXEC Mode 189
Global Configuration Mode 190
CLI Help 191
CLI Keystroke Shortcuts 196
Web-Based Management 197
System 200
Services 200
Routing 201
QoS 201
Profiles 201
Servers 202
Admin 202
Status 203
Help 203
VPN Router Administrator 204
File Management 205
Checking the Current Status of Your VPN Router 206
Logs 206
Configuration Log 206
Event Log 208
Security Log 210
System Log 212
VPN Router System Status Tools 214
Sessions 214
Reports 215
System 215
Health Check 216
Statistics 217
Accounting 218

Other VPN Router Tools 218
Trace Route 218
Ping 219
Address Resolution Protocol 219
VPN Router Administration 221
Software Upgrades 221
Lightweight Directory Access Protocol 222
Remote Authentication Dial-In User Service 222
Automatic System Backups 223
System Recovery 223
System Shutdown 224
Bandwidth Management 225
Configuring Bandwidth Management 225
Summary 227

Chapter 6 Authentication 229
Understanding LDAP 230
LDAP Principles 231
LDAP Request Flowchart 232
Configuring Internal LDAP 232
External LDAP 235
Enabling LDAP Proxy 237
Monitoring LDAP Servers 240
Using Remote Authentication Dial-in User Service 242
Enabling RADIUS Authentication 242
RADIUS Server Selection 243
RADIUS Authentication Options 245
RADIUS Diagnostics 246
RADIUS Proxy 246
Enabling RADIUS Accounting 248
Understanding Certificates 250
SSL Encryption with LDAP Server 251
LDAP Certificate Installation 251
LDAP Special Characters 252
External LDAP Proxy 252
Tunnel Certificates 253
Using Public Key Infrastructure 254
PKI Setup 254
CA and X.509 Certificates 254
Loading Certificates 255
Requesting a Server Certificate 255
Server Certificates Using CMP 255
Trusted CA Certificate Installation 260
Trusted CA Certificate Settings 261
Certificate Revocation List Configuration 264
CRL Server Configuration 265
CRL Distribution Points 267

CRL Retrieval 268
Enabling Certificate Use for Tunnels 268
Identifying Individual Users with Certificates 269
Identifying Branch Offices with Certificates 270
IPSec Authentication 271
L2TP/IPSec Authentication 273
Adding L2TP Access Concentrators 274
Summary 275

Chapter 7 Security 277
Stateful Firewall Basics 277
Using Stateful Inspection 278
Interfaces 278
Filter Rules 279
Anti-Spoofing 280
Attack Detection 280
Access Control Filters 281
Network Address Translation 282
Configuring Stateful Firewall 283
Configuration Prerequisites 283
Stateful Firewall Manager System Requirements 284
Enabling Firewall Options 284
Enabling the Stateful Firewall Feature 285
Connection Limitation and Logging 286
Application-Specific Logging 286
Remote Logging of Firewall Events 287
Anti-Spoofing Configuration 288
Malicious Scan Detection Configuration 289
Firewall Policies 290
Firewall Policy Creation and Editing 290
Policy Creation 290
Rules 292
Implied Rules 292
Static Pre-Implied Rules 293
Dynamic Implied Rules 294
Override Rules 295
Interface Specific Rules 295
Default Rules 296
Rule Creation 296
Header Row Menu 297
Row Menu 297
Cell Menus 297
Rule Columns 298
Creating a New Policy 305
Firewall Configuration Verification 306
Sample Security Policy Configuration 306

Firewall Examples 308
Residential Example 309
Business Example 309
Filters 311
Adding / Editing Filters 311
Next Hop Traffic Filter 314
NAT 315
Types of Address Translation 315
Dynamic Many-to-One NAT 316
Dynamic Many-to-Many NAT 317
Static One-to-One NAT 318
Port Forwarding NAT 319
Double NAT 320
IPSec Aware NAT 321
NAT Modes 322
Full Cone NAT 322
Restricted Cone NAT 322
Port Restricted Cone NAT 323
Symmetric NAT 324
NAT Traversal 325
NAT and VoIP 326
Address/Port Discovery 327
NAT Usage 327
Branch Office Tunnel NAT 328
Interface NAT 329
Dynamic Routing Protocols 329
Configuring a NAT Policy 330
NAT Policy Sets 330
Creating Rules 331
NAT ALG for SIP 331
Application Level Gateways 331
Configuring NAT ALG for SIP 332
Firewall SIP ALG 332
Hairpinning 332
Hairpinning with SIP 333
Hairpinning with a UNIStim Call Server 333
Hairpinning with a STUN Server 333
Hairpinning Requirements 334
Hairpinning Configuration 334
Time-Outs 334
NAT Statistics 334
Proxy ARP 335
Summary 335

Chapter 8 Overview of Ethernet LANs and Network Routing 337
Ethernet Networking 338
Basic Physical Topology Types 339
Bus Topology 339
Star Topology 339
Carrier Sense Multiple Access with Collision Detection 340
Ethernet Variants 341
Traditional Ethernet 342
Fast Ethernet 342
Gigabit Ethernet 343
Network Cables 343
Coaxial Cable 343
Twisted-Pair 344
Fiber-Optic 345
Data Transmission Modes 346
Simplex 346
Half-Duplex 346
Full-Duplex 347
Collision Domains 347
Broadcast Domains 348
Network Addressing 349
Media Access Control (MAC Addressing) 350
Internet Protocol (IP Addressing) 351
Address Resolution Protocol 351
Reverse Address Resolution Protocol 353
Virtual Local Area Network 353
Network Routing 355
Routing Basics 356
Routing Tables 358
Routing Algorithms 359
Distance-Vector Routing 360
Link-State Routing 361
Routing Protocols 362
Routing Protocol Types 363
Routing Protocol Concepts 363
Routing Information Protocol 364
RIP History Overview 366
RIP Route Determination 367
RIP Updates 368
RIP Request 368
RIP Response 368
Timelines 369
Open Shortest Path First 370
OSPF History 371
OSPF Considerations 371
Router Unique Name 372
Adjacencies 372
OSPF Processes 372

OSPF Areas 373
OSPF Overview 374
Hello Messages 375
LSDB 375
Shortest Path First 375
Border Gateway Protocol 376
BGP History 376
BGP Overview 376
BGP Topologies 377
Routing Concepts 378
Routing Information 379
Path Vector Routing Algorithm 380
Virtual Router Redundancy Protocol 381
VRRP Failover 382
Summary 382

Chapter 9 Tunneling, VoIP, and Other Features 385
Layer 2 Forwarding 386
Point-to-Point Tunneling Protocol 390
Layer 2 Tunneling Protocol 396
IP Security Tunneling Protocol 400
Quality of Service 405
Voice over IP 410
Point-to-Point Protocol over Ethernet 413
Client Address Redistribution 416
Circuitless IP 418
Backup Interface Services 419
Summary 421

Chapter 10 The Nortel VPN Client 423
Overview of the Nortel VPN Client 424
Operating System Compatibility 424
Supported Operating Systems 425
Operating Systems Supported Prior to the Nortel VPN Client Version 4.91 426
Operating Systems Supported in the Nortel VPN Client Version 6.01 426
Optional Licensing Operating Systems Supported 426
Installing the Nortel VPN Client 426
Using the Nortel VPN Client 433
Status and Monitoring 434
VPN Client Main Menu Items 435
The File Menu Option 436
The Edit Menu Option 437
The Options Menu Option 437
The Help Menu Option 439

Nortel VPN Client Customization 440
VPN Custom Client Installation Modes 441
VPN Customer Client Group Profiles Overview 442
VPN Custom Client Icons and Custom Bitmaps 442
VPN Client Event Logging and Keepalives Overview 442
VPN Client Event Log 443
VPN Client Keepalive 445
Internet Security Association and Key Management Protocol Keepalive 446
Network Address Translation Traversal Keepalive 446
Silent Keepalive 447
IPSec Mobility 447
Security Banner 449
Split Tunneling 451
Considerations 453
Inverse Split Tunneling 454
Support for All Zeros Addressing in Inverse Split Mode 455
TunnelGuard 455
TunnelGuard Daemon 455
Software Requirement Set Builder 456
TunnelGuard Agent 456
TunnelGuard Features Overview 457
TunnelGuard Icon Information 457
TunnelGuard Installation Considerations 457
TunnelGuard Event Logs 457
Banner Messages 458
VPN Client Failover 458
Summary 461

Chapter 11 VPN Router Administration Lab Exercises 463
Installing the VPN Client Software 464
Lab Requirements 464
Lab Setup 464
Lab Summary 465
Initial Setup of the Nortel VPN Router 465
Lab Requirements 465
Lab Setup 466
Lab Summary 468
Enabling and Using VPN Client Logging 468
Lab Requirements 468
Lab Setup 468
Lab Summary 469
Configuring Groups 469
Lab Requirements 469
Lab Setup 469
Lab Summary 470

Configuring Users 471
Lab Requirements 471
Lab Setup 471
Lab Summary 472
Configuring Client Failover 473
Lab Requirements 473
Lab Setup 473
Lab Summary 475
Configuring IPSec Mobility 475
Lab Requirements 475
Lab Setup 476
Lab Summary 477
Configuring Automatic Backups 477
Lab Requirements 477
Lab Setup 477
Lab Summary 479
Configuring a Peer-to-Peer Branch Office Tunnel 479
Lab Requirements 479
Lab Setup 480
Lab Summary 482
Configuring RIP Routing 482
Lab Requirements 482
Lab Setup 482
Lab Summary 483
Configuring Network Time Protocol 484
Lab Requirements 484
Lab Setup 484
Lab Summary 487
Configuring DHCP Server 488
Lab Requirements 488
Lab Setup 488
DHCP Relay Lab 489
DHCP Server Lab 491
Lab Summary 492
Configuring the Nortel 100 VPN Router 492
Lab Requirements 492
Lab Setup 493
Basic Configuration Lab 493
Tunneling Lab 495
Lab Summary 502
Configuring CLIP for Management IP Address 502
Lab Requirements 503
Lab Setup 503
Lab Summary 505
Configuring Administrator User Tunnels 505
Lab Requirements 505
Lab Setup 506
Lab Summary 511

Configuring Syslog Server 512
Lab Requirements 512
Lab Setup 513
Lab Summary 515
Configuring User IP Address Pools 515
Lab Requirements 515
Lab Setup 516
Configuring User IP Address Assignment Using DHCP Lab 516
Configuring User IP Address Assignment Using Address Pool Lab 519
Lab Summary 521
Client Address Redistribution Configuration 521
Lab Requirements 522
Lab Setup 522
Lab Summary 526
Summary 527

Chapter 12 Troubleshooting Overview 529
Overview of Network Troubleshooting 530
Logical Steps 530
Make Sure You Understand the Problem 530
Diagnosing the Problem 531
Testing 531
Reaching a Resolution 532
TCP/IP Utilities 533
Ping 533
Traceroute 536
Routing Tables 538
Netstat 539
IPconfig 541
Other Troubleshooting Tools 541
Packet Sniffer 542
Cable Testing 543
Network Management Station 544
Nortel VPN Router Troubleshooting 545
Tools 546
Console Cable 546
Crossover Cable 548
System Recovery Disk 548
Laptop 549
FTP Server 551
FTP Client 552
VPN Router System Recovery 553
System Recovery for Disk-Based Versions 554
System Restore Option 555
Reformat Hard Disk Option 557
Apply New Version Option 557

Perform File Maintenance option 557
View Event Log Option 557
Restart System 558
System Recovery for Diskless Versions 558
System Restore Option 559
Reformat Hard Disk Option 559
Apply New Version Option 559
Perform File Maintenance Option 559
View Event Log Option 561
Use of the Nortel VPN Router Reporting Utilities 562
Status 563
Sessions 564
Reports 566
System 566
Health Check 568
Statistics 569
Accounting 571
Security Log 572
Config Log 574
System Log 574
Event Log 576
Admin Tools 577
Ping 578
Trace Route 579
ARP 581
Packet Capture 582
General Network Proactive Measures 584
Perform Regular Backups 585
Research 585
Always Have a System Recovery Disk Available 586
Dial Access for Support Personnel 587
Knowledge Sharing 587
Documentation 588
Upgrades and Configuration Changes 588
Research 589
Pre-Testing 590
Action Plan 590
Nortel Support 591
Summary 592

Appendix A Abbreviation and Acronym Reference Listing 593

Appendix B Command Line Interpreter Commands 613
Access via Console Connection 614
Access via Telnet Session 615
User EXEC Mode 615
help Command 616
File System Commands 616

who Command 619
terminal Command 619
verify Command 619
reset Command 620
exit Command 620
IP Connectivity Commands 620
clear Command 621
show Commands 622
show version Command 623
show flash Command 623
show admin Command 625
show file Command 625
show clock Command 625
show ip Command 626
show ip route Command 626
show ip interface Command 627
show ip traffic Command 627
show services Command 629
show switch-settings Command 630
enable Command 631
Privileged EXEC Mode 631
clear Command 632
reset Command 633
show Command 633
show all Command 635
show current-config-file Command 636
show dhcp Command 636
show health Command 636
show interface Command 638
show ip Command 639
show hosts Command 641
show ipsec Command 642
show logging Command 643
show ntp command 644
show router Command 644
show snmp Command 645
show software Command 645
show status Command 646
show system Command 647
show running Configuration Command 647
boot Command 654
capture Command 654
create Command 655
delete Command 656
forced-logoff Command 656
kill Command 656
mkdir Command 657
rmdir Command 657

more Command 657
reformat Command 658
reload Command 658
rename Command 659
retrieve Command 659
Global Configuration Mode 660
Summary 663

Appendix C Related Request for Comments Reference Guide 665

Appendix D References and Resources 687
Nortel Networks Documentation 687
RFCs 688
Internet Resources 689

Index 691

Acknowledgments

Words cannot describe the mixture of emotions that we have experienced over the past few months in trying to complete this book. From the uncertainty and the nervousness we experienced when the concept of the book was first discussed, to the excitement of penning the very last word, it is certain that we have many memories to forever replay in our minds. The challenges that were put before all of the individuals who assisted in the development and enrichment of this book were many, but everyone pulled together to ensure that this project reached completion. For this, we are very thankful.

We would first like to thank Jamie Turbyne. This book was his brainchild and would not have been written had he not had the vision to pursue it. We were sad that Jamie was eventually unable to participate in the development of the book, but life happens. We will always be grateful to Jamie and his contribution to the launch of this book.

We would also like to thank one another for being co-authors. Not only for the portions of the book that each of us individually wrote, but also for the support we gave to one another during the submission process. There is no way that this could have been completed without that teamwork.

We would also like to thank all of the people from Wiley that were involved with this book. A special thank you goes to our developmental editor, Kevin Shafer, and to the acquisitions editor, Carol Long, for all of the time they spent helping us keep this project rolling.

Finally, a special thank you goes out to our families and close friends for being patient and understanding about the amount of time that we had to spend working on this book. All of the help and sacrifices that you all made helped ensure that we had the time to work on and to complete this book. Without you all, this would have never been possible.

Introduction

This book was developed to provide an overview discussion of the Nortel VPN Router portfolio. This book is designed to not only provide real-world training examples, but also to provide a detailed reference guide for the VPN professional. Upon the completion of this book, you will have a firm foundation with the VPN Router portfolio.

Whom This Book Is For

This book is designed for both beginning and seasoned networking professionals. With that in mind, the book does provide a fair amount of general knowledge, as well as in-depth solutions and discussions. Seasoned professionals who are familiar with the Nortel VPN Router can skip the first few chapters of this book because they probably already know much of the information. Beginning networking professionals, as well as seasoned professionals new to the VPN routing solution, will probably want to read from the beginning.

What This Book Covers

The Nortel VPN Router, formally known as Contivity, functions as a VPN tunnel termination point and a stateful firewall, and does both LAN- and WAN-oriented routing. The portfolio is integrated into many of the solutions deployed in corporate LANs, including security and VoIP. The VPN Router

portfolio consists of two product lines that have been brought together as part of Nortel's rebranding strategy: the Contivity product line and the Instant Internet product line. These devices focus on security of network resources, employee mobility, access control, firewall, and both enterprise and WAN routing. Additionally, components of this portfolio of products are being integrated into several of Nortel's network solutions, including Wireless Mesh (secure and roaming wireless connections) and VoIP (securing calls being placed over the Internet). These are all growth areas within the enterprise networking environment.

The Nortel VPN Router portfolio developed out of a Nortel corporate-wide rebranding undertaken at the end of 2004. The Contivity and Instant Internet product lines are for enterprise network deployments and act as both routers and security devices. They support many different routing protocols, both WAN and LAN, including Router Information Protocol (RIP), Open Shortest Path First (OSPF), frame relay, and Border Gateway Protocol (BGP). The VPN Router portfolio also supports a suite of security features, including a stateful firewall, NAT, port forwarding, and user and Branch Office Tunnel (BOT) termination.

This book is developed with beginning to intermediate-level professionals in mind. These professionals in the networking industry should be either already involved with the products, or looking to expand the functionality of their networks with the features and services available in the VPN Router portfolio. Technicians in Network Operating Centers (NOCs), as well as IT staff involved with the VPN Router portfolio, will benefit by having this book on hand to work with devices already in their networks, or as a desktop reference to look into deploying new units into their existing topologies.

This book provides a detailed overview into the Nortel VPN Router portfolio. It contains an overview of the VPN Router, including information on the hardware supported and the software available. In addition, there are discussions about materials, examples, advice from real-world experience, as well as laboratory setups to aid networking professionals with their VPN Router products. It is impossible to provide an in-depth coverage of all of the functions and the inner workings of the VPN Router, but this book provides the information that will acquaint you with the VPN Router and will get you started on your way to mastering the technology.

This book should help all of those who are involved in VPN Router administration develop a better understanding of the VPN Router as it pertains to their individual environments. This book should also serve as a helpful reference, available when it is needed.

How This Book Is Structured

This book was developed for a beginning to intermediate-level of networking professional. It is designed to be used as a helpful reference guide, as well as an introductory manual to the Nortel VPN routing solution. The book is structured much like a training manual in that it begins by discussing basic technological ideals, and then progresses to applying and administering those ideals.

- *Chapter 1, "Networking and VPN Basics."* This chapter covers some very basic networking concepts. Providing information on both past and present standards, it is a basic overview of networking and VPN basics. To appreciate and fully understand the capabilities of the Nortel VPN Router, it is important to cover some networking basics to help in the understanding of the technology.
- *Chapter 2, "The Nortel VPN Router."* This chapter discusses the Nortel VPN Router portfolio. Nortel currently offers several VPN Router choices, each with various features and options that are designed to meet the many diverse needs of companies around the world. Not only are the hardware solutions for VPN networking introduced, but there is some discussion about the various platforms in the VPN Router family. Finally, the chapter provides an overview of some of the standard and optional features of each of the routers in the VPN Router portfolio.
- *Chapter 3, "The Nortel VPN Router Software Overview."* This chapter provides a detailed look at the software used to give the routers the instructions they need to perform the standards and optional functions they are designed to support.
- *Chapter 4, "The Nortel VPN Router in the Network."* This chapter focuses on deployment strategies for the Nortel VPN Router. There are many differing topologies for networks and because of this, there are many strategies that can be deployed to ensure maximum effectiveness and optimization of your VPN Router solution. Within the chapter, there are examples of how a VPN Router may be deployed in a network, along with a discussion of various features of the VPN Router and how it may be used within a network. Networks vary in size from the Small Office or Home Office (SOHO) to large corporate central offices, and examples of each are discussed.

- *Chapter 5*, *"Management Options and Overview."* This chapter discusses the management and the administration of the Nortel VPN Router. It provides a detailed discussion about connecting to the VPN Router to manage and administrate. Some basic commands are discussed, along with tools that are available to the VPN administrator.
- *Chapter 6*, *"Authentication."* This chapter covers authentication. Authentication is a technology that deals with the authorization process that eventually allows users and BOTs to be permitted access to the protected private network. Covering the various authentication environments and types, this chapter presents an overview of what authentication entails, along with examples and scenarios of the Nortel VPN Router with external authentication servers.
- *Chapter 7*, *"Security."* This chapter focuses on data network security. There is no absolute definition of what network security is. It is far-ranging, from a total lockdown of the network (where no data is allowed to enter or leave the protected network) to wide-open access (which exposes the network to any security breach imaginable). However, from a practical business standpoint, it is desirable to provide controlled access to and from the protected network, while maximizing security that will ensure that the network is totally protected from intrusion and/or any malicious intent. This chapter provides an overview of security protocols as they relate to the VPN Router.
- *Chapter 8*, *"Overview of Ethernet LANs and Network Routing."* This chapter discusses an overview of routing and routed protocols. Although familiar to the seasoned networking professional, the features and standards discussed in this chapter will provide a foundation of knowledge needed to administer the VPN Router. This chapter provides an overview of Ethernet LANs, as well as an overview of routing protocols.
- *Chapter 9*, *"Tunneling, VoIP, and Other Features."* This chapter provides an overview of VPN tunneling protocols, VoIP, and some other important features that are supported by the Nortel VPN Router. These standards cover the foundation of VPN routing and are very important to understand when deploying and maintaining a VPN routing solution.
- *Chapter 10*, *"The Nortel VPN Client."* This chapter takes a look at the Nortel VPN Client and some of the features that are provided within the application. The chapter not only covers the Nortel VPN Client software, but it provides additional details, including supported platforms, installation information, configuration information, and basic VPN Client concepts.

- *Chapter 11*, *"VPN Router Administration Lab Exercises."* This chapter uses all of the information that is provided in the book and provides detailed instructions on configuring some of the basic features in a lab environment. This chapter should serve as both a learning vehicle and a reference tool. The labs in this chapter provide a step-by-step configuration guide for some of the basics on the VPN Router. Upon successful completion of this chapter, you should have a much better understanding of the capabilities of your Nortel VPN Router. You should also have increased confidence in the browser-based interface and its use.
- *Chapter 12*, *"Troubleshooting Overview."* This chapter discusses troubleshooting in the VPN Router environment. An overview of troubleshooting is provided that covers not only general network data flow issues, but also troubleshooting VPN Router–specific issues. Because other problems may arise that are causing issues with the VPN Router and its performance, some basic troubleshooting strategies are discussed, as well as an overview of troubleshooting problems with the VPN Router.
- *Appendix A*, *"Abbreviation and Acronym Reference Listing."* This appendix provides a list of acronyms and abbreviations that anyone who is involved in maintaining the VPN Router should know.
- *Appendix B*, *"Command Line Interpreter Commands."* This appendix provides a Command-Line Interpreter (CLI) command reference overview that can be used as a reference guide for monitoring and configuring the VPN Router through the CLI-driven menu.
- *Appendix C*, *"Related Request for Comments Reference Guide."* This appendix is a list of RFCs that cover many of the standards and features that are discussed in this book.
- *Appendix D*, *"References and Resources."* This appendix provides a list of reference materials that were used in the development of this book.

What You Need to Use This Book

Throughout this book, multiple examples are used to help you gain a better understanding of the Nortel VPN Router. To obtain the full value from the information that is provided in this book, there are a few basic items that should be available to you. Although no special equipment is required for the reader to be able to understand the concepts presented within this book, it is helpful for the purposes of providing you with a little hands-on experience.

The majority of this book focuses on the VPN Router software release v06.00. We recommend that you have a VPN Router that is capable of running this software and that you also have the software available to use when you are testing some of the concepts and information contained within this book. Also recommended is a Windows 2000- or XP-based PC with the comparable version of VPN Client software loaded on it. Any additional items that are required are referenced within the applicable sections.

CHAPTER

1

Networking and VPN Basics

Tremendous strides in computer networking have increased the productivity of today's workers in today's workplace. The speed at which we are able to access and share data is more than was dreamed of 15 years ago. The security risk in networking today has also grown. This book is dedicated to one of the industry milestones that is quickly becoming a standard in most workplaces. This book is about Virtual Private Networks (VPNs) with the Nortel VPN routers.

VPN routing uses "virtual" connections (instead of the traditional dialed line or a leased line) to connect users in remote offices to a private network over a public network. VPN networking offers many benefits. It allows for extended geographic connectivity, improves security, and is much more cost-effective than traditional wide area network (WAN) connectivity. Most of these benefits are discussed later in this book. Never before have so many people been able to connect almost seamlessly to their corporate network from home and on the road, which instantly allows real-time communication with their corporate LAN.

This chapter is a basic overview of networking and VPN basics. It's important to cover some networking basics to understand VPN. Most of the information contained in this chapter is covered in detail in later chapters. The information presented here will provide you with a basic understanding of how VPN networking works.

Networking Basics

In its most basic form, a computer network is nothing more that two or more computers that are connected together via a medium to allow the transfer of data. Today, most businesses rely on networking to complete daily business transactions. Networks today are built to allow sharing of hardware and software services. Networking allows you to retrieve applications on remote servers, for file transfers, for print services, and so much more. Figure 1-1 shows a basic network.

Networks can be described several ways. Most often, when we think of networks, we think of either a local area network (LAN) or a wide area network (WAN). Although there are several types of "area networks," for purposes of discussion in this chapter, we will discuss these two types.

The OSI Reference Model

The Open Systems Interconnection Reference Model (also known as the OSI Reference Model, OSI seven-layer Model, or OSI Model) was developed as a tool to describe network communications and network design. The OSI Reference Model divides the functions of a network protocol into seven layers. Each layer of the OSI Reference Model utilizes the functions of the layer below it and transfers functionality to the layer above it. Figure 1-2 shows an example of the OSI Reference Model.

Typically, the lower layers of the OSI Reference Model (Physical, Data Link, Network, and Transport) are implemented in the hardware in the network, while the upper layers (Session, Presentation, and Application) are implemented in the software applications that are being used.

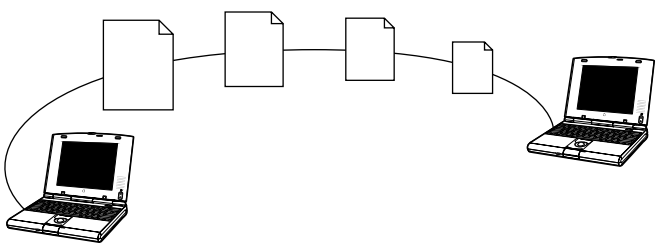


Figure 1-1: A simple network of two computers sharing data

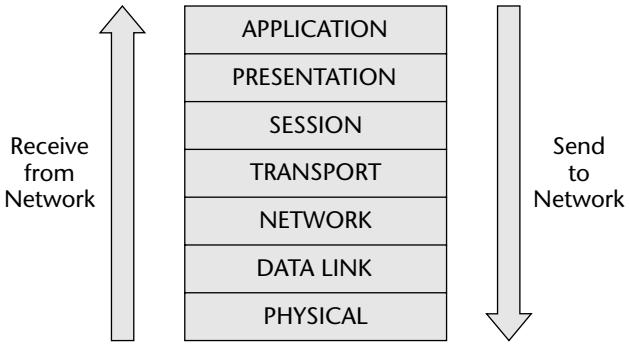


Figure 1-2: The OSI Reference Model

The OSI Reference Model is considered an abstract model because it is merely a guide and does not have to be strictly adhered to when network implementation occurs. The OSI Reference Model's layered approach is advantageous to system implementation. Because a network design can be broken into the layered pieces, it offers a lot of flexibility and reduces problems in the beginning stages of network design. A product that is implemented from one vendor at Layer 2 of the reference model should be fully interoperable with the Layer 2 and Layer 1 offerings of another vendor. This allows for more options when designing the network. Additionally, new protocols and standards are easier to implement at a layered level.

Let's take a detailed look at the OSI Reference Model, beginning with the upper layers.

The Application Layer (Layer 7)

Layer 7 of the OSI Reference Model is the Application layer. Simply put, the Application layer is used by applications on the network. The Application layer does not control all network applications; rather, it is the layer that contains services that are used by applications.

Some of the more popular applications that perform functions at this layer are File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and HyperText Transfer Protocol (HTTP), among many others. Because this layer is at the very top of the OSI Reference Model, it does not have any layers above it to interact with. Instead, it provides functions that are used by the end user. This layer represents the actual applications used on the network.

The Presentation Layer (Layer 6)

Layer 6 of the OSI Reference Model is the Presentation layer. This layer has a much more specific function than the other layers. Its function is to ensure that data is presented on the receiving end the way that the originator intended it to be.

Because there are various vendors involved in the development of devices on a network, sometimes these systems have distinct characteristics and may represent data in different ways. For example, even though a Microsoft-based PC and Macintosh personal computer are both computers, they use different applications and represent data in different ways. It is the responsibility of the Presentation layer to ensure that data is presented in a similar fashion between the two devices.

Compression and decompression of data can also be performed at the Presentation layer. Because the Presentation layer is not always needed (consider environments that are running a standard system between users), its functions are often included and described at the Application layer. It is not uncommon for Layer 7 to speak directly with Layer 5, and vice versa.

The Session Layer (Layer 5)

The fifth layer of the OSI Reference Model is the Session layer. The Session layer is the lowest of the three upper layers of the OSI Reference Model. It is concerned primarily with software application issues and not so much with the transportation of data within the network. The purpose of this layer is to allow network devices to establish and maintain extended sessions for the purpose of sharing data.

Common application protocols that are used at this layer are Transportation control Protocol/Internet Protocol (TCP/IP) sockets and Network Basic Input/Output System (NetBIOS). These protocols allow applications the ability to set up and maintain communications over the network. Simply put, this layer handles the starting, coordinating, and terminating of communication between computer applications and between a source and a destination on the network.

The Transport Layer (Layer 4)

Layer 4 of the OSI Reference Model is the Transport layer. This layer is involved with the transportation of data within a network. It is an interface layer and (unlike Layers 1, 2, and 3) it really does not concern itself with the way that data is transported between the source and the destinations. This layer relies on the lower layers to handle the actual packaging and movement of the packet, and it acts as a liaison between the lower layers and the upper layers. This layer enables communication of applications between devices on the network.

The Transport layer is responsible for keeping track of information coming from the upper layers and ensures that the data is combined into a single flow of data to the lower layers. This layer is responsible for ensuring that large amounts of data are systematically broken down into smaller blocks to be sent to the lower layers for transport. The Transport layer uses algorithms to ensure that data is transported reliably and that solid communication between devices takes place. Some of the protocols that are used at this level are the User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP).

User Datagram Protocol

The User Datagram Protocol (UDP) is a protocol that allows a source device to transfer data to a destination device without first checking to see if it is able to establish a session with the destination device. Because of this, UDP is defined as a *connectionless delivery protocol*. UDP is used by applications that do not require error checking and delivery control. Broadcast messages are an example of an application that would use UDP for a delivery protocol. There is very little overhead with UDP.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is more reliable than UDP because it does ensure that a connection can be established between a source and a destination on the network. TCP uses very strict error-detection algorithms to ensure delivery of data. TCP uses *sequence numbers* and acknowledgments to ensure data is delivered in its entirety to a destination.

Sequence numbers help ensure that all packets are received and put back into the correct order by the receiving station. The sending station will assign a sequence number to each packet that is transmitted. The receiving station keeps track of each packet. When a packet is received, the receiving station will keep track of the sequence numbers and will return an acknowledgment to the sending station as each packet is received. The sending station will resend packets when there is no acknowledgment received, and the receiving station can verify receipt by the order of sequence numbers.

The Network Layer (Layer 3)

The third layer of the OSI Reference Model is the Network layer. Here it is determined how interconnected LANs communicate with one another. This is the most important layer when transmitted data is sent onto the WAN. The layers above this layer (Layers 4 through 7) do not concern themselves with how data is sent to and received from its destination.

At the Network layer, devices on the network are given a logical address that is used for data delivery. The Internet Protocol (IP) standard is the most commonly used address for data delivery, and every device on a network has

a unique IP address. Data is transported from LAN to LAN at this level. It is the job of devices that are operating at this level to handle packets that are received from various sources and to ensure that those packets arrive at their destinations.

The Network layer is responsible for encapsulating data from higher layers and then passing the data to the Data Link layer (Layer 2). When encapsulating the data, the Network layer will place a header onto the packet. Often, the Data Link layer has a limit on the size of packets that it accepts, so the Network layer breaks the packet up into fragments and sends these fragmented packets to the Data Link layer. The Network layer is responsible for reassembling the packets once they arrive at their destination. A router is an example of a Layer 3 device.

The Data Link Layer (Layer 2)

Layer 2 of the OSI Reference Model is the Data Link layer. The Data Link layer is often divided into two sub-layers:

- *Logical Link Control (LLC):* Used to establish and control logical links between devices within a network.
- *Media Access Control (MAC):* Defines standards in which devices manage access to the network to avoid conflicting with other devices that are trying to send data.

The Data Link layer is responsible for the encapsulation of messages that are being sent from higher layers. The data is encapsulated by the Data Link layer and then it is forwarded to the Physical layer to be sent to the network destination. This layer also handles errors that occur on the network during transport. One of the ways that errors are managed is with the cyclic redundancy check (CRC), which is simply a small number of bits in a packet that is used on each end of transport to ensure data integrity. Switches and bridges are examples of Layer 2 devices.

The Physical Layer (Layer 1)

The lowest layer of the OSI Reference Model is the Physical layer. In networking, the Physical layer is important because it is the only layer in which data is physically transferred across the network interface. The physical layer details the way in which the connectors, cables, and other hardware devices operate within a network. At this layer, data is encoded and transmitted from one device to another. In general, the Physical layer is the layer that deals with the actual 0s and 1s that are transmitted through the network. Devices that operate at this level are lower-level devices, which really have no understanding of the data being transmitted. This layer simply accepts and passes data. A hub would be an example of a Layer 1 device.

Overview of a Local Area Network

A LAN is considered to be a group of computers that are in close proximity to each other (such as a school, a department in an office building, a home network, and so on). The LAN allows these users to share applications, transfer data among one another, and share hardware (such as printers). Most often, a LAN connects to other LANs or to a WAN.

Computers and devices that make up a LAN are connected with cables, network adapters, and hubs. There are also other components in LAN networking, but we are just covering the basics. Some networking protocols are also used to get these devices to communicate with one another. Many of these protocols come standard with most operating systems.

The most common type of LAN is an Ethernet LAN (see Figure 1-3). An Ethernet LAN can transfer data up to 100 megabits per second (Mbps). It is by far the most popular and widely used technology in most LANs mainly because most computer vendors provide Ethernet attachments with their equipment, making it easier to link to almost any hardware that is used in the LAN. Because it is so widely used, it works well in environments where multiple-vendor hardware is being used.

All of the Ethernet equipment in a LAN operates independent of the other Ethernet equipment. Ethernet signals are provided to all of the equipment on the LAN and the equipment "listens" for the line to be clear before transmitting its data.

A LAN can be as simple as two computers on a home network or as complicated as several thousand devices in a larger environment. Many LANs are divided into *subnetworks,* which allow you to break down larger LANs into smaller groups.

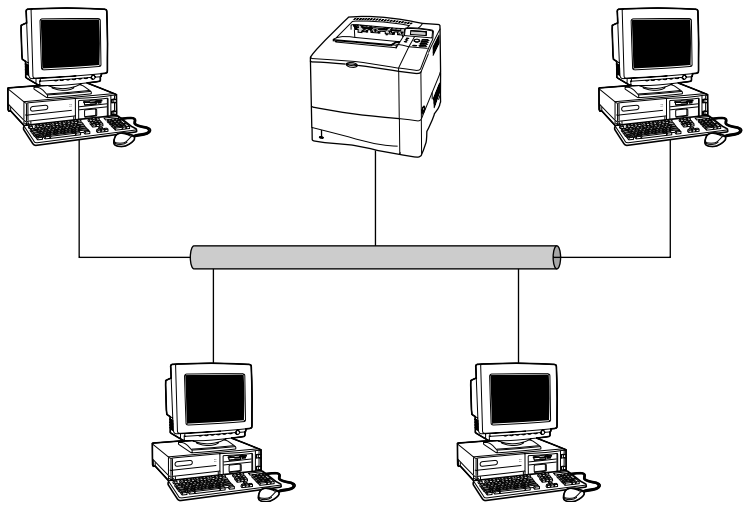


Figure 1-3: An example of an Ethernet LAN

Overview of a Wide Area Network

A WAN comprises multiple LANs and spans a large geographical distance. The most commonly known (and used) WAN is the Internet. Figure 1-4 shows an example of a WAN.

A network device known as a *router* is used to connect LANs to the WAN. The router is used to collect the address destinations of LAN and WAN devices, and it uses these addresses to deliver data between devices.

Media Access Control Addressing

Every device on a LAN contains a physical address, called the *Media Access Control (MAC) address*. The MAC address is a unique hardware address that identifies each device on the network. Most Layer 2 protocols use the MAC address to identify a device on the network. Mac addresses are written in *hexadecimal notation*, which is written in the base-16 numbering system.

Not all networking protocols will use the MAC address, but on broadcast networks, the MAC address allows all of the devices in the network to be identified and allows delivery of frames intended for a specific destination. MAC addresses are permanently attached to a device and are assigned by product manufacturers.

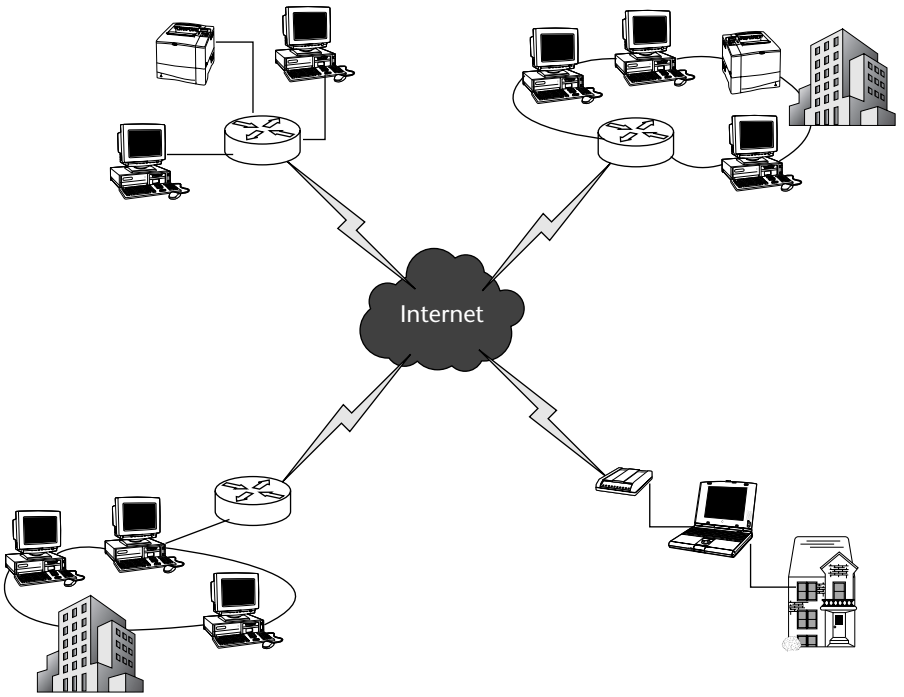


Figure 1-4: A WAN

Typically, MAC addresses are read as a group and are divided into six sets of two hexadecimal digits. Each set is separated from the remaining sets by either a colon (:) or a hyphen (-). Figure 1-5 shows an example of how MAC addressing may appear.

Internet Protocol Addressing

An *IP address* is a unique number that is used by devices to communicate with each other over a WAN. An IP address is much like a telephone number or a street address. An IP address is assigned to each host interface within a network. To communicate with any other device on a WAN, the sending and receiving device's IP address must be known. An IP address may be *static*, which means that it is permanently assigned to a device. It can also be *dynamically assigned* by a server that is within the LAN of the device.

IP addresses are broken into four *octets*. Each octet contains 8 bits. The octets are written in dotted-decimal notation. *Dotted-decimal* notation is simply a method of writing octet strings in the base-10 numeral system. Each octet is separated from the other octets with a decimal point. Figure 1-6 shows an example of binary to dotted-decimal conversion.

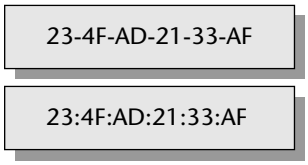


Figure 1-5: An example of a MAC address

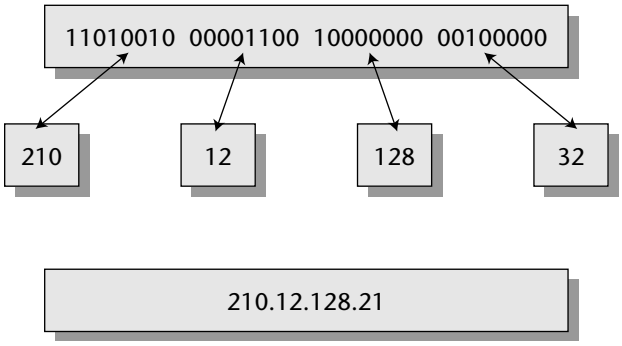


Figure 1-6: An example of binary to dotted-decimal conversion

IP Address Classes

IP addresses are broken down into different *classes*. This allows for the assignment of different classes to meet the needs of networks that have different sizes. IP addresses can be divided into two parts: One part identifies the network that the IP address is assigned to, and the other part identifies the device that has been assigned a particular IP address.

Table 1-1 shows how IP addresses are divided into classes.

IP addressing is broken down into the following five classes:

- Class A (for networks that have more than 65,536 hosts)
- Class B (for networks that have between 256 and 65,536 hosts)
- Class C (for networks that have less than 256 hosts)
- Class D (reserved for multicasting)
- Class E (reserved for future use)

Class A Addresses

Class A addresses are used for very large networks. There are only a small number of Class A addresses. The leading bit in a class A address is always a 0. The next 7 bits identify the network, and the last 24 bits belong to the device in which the IP address is assigned.

Table 1-2 shows a breakdown of the octets in a Class A address.

Table 1-1: Dividing Sections of the IP Address for Each Class

IP ADDRESS CLASS	NETWORK PORTION	HOST PORTION
Class A	Octet 1	Octets 2, 3, 4
Class B	Octets 1, 2	Octets 3, 4
Class C	Octets 1, 2, 3	Octet 4

Table 1-2: The Breakdown of the Octets in a Class A Address

FIRST BIT	OCTET 1	OCTET 2	OCTET 3	OCTET 4
0	Network ID	Host ID	Host ID	Host ID

Class B Addresses

A Class B address is assigned to medium-size networks. The first bit is always a 1 and the second bit is always a 0. The remaining 14 leading bits of the address are assigned to the network, and the last 16 bits identify the device in which the IP address is assigned.

Table 1-3 shows a breakdown of the octets in a Class B address.

Class C Addresses

Class C addresses are the most common type of addresses and are assigned to thousands of networks throughout the world. The first and second bit of an IP address is a one (1) , with the third bit always being a zero (0). The remaining 21 leading bits identify the network number, and the last 8 bits are used to identify the device that the address is assigned to.

Table 1-4 shows a breakdown of the octets in a Class C address.

Class D Addresses

Class D addresses are reserved for multicast addresses and can range from 224.0.0.0 to 239.255.255.255. The class D address identifies a group of hosts in a network that are members of a multicast group. Multicasting allows for the delivery of information to multiple devices within a group. It is a very efficient strategy to deliver messages that need to be shared with all members of the group.

Table 1-5 shows examples of well-known Class D addresses.

Table 1-3: The Breakdown of the Octets in a Class B Address

FIRST BIT	SECOND BIT	OCTET 1	OCTET 2	OCTET 3	OCTET 4
1	0	Network ID	Network ID	Host ID	Host ID

Table 1-4: The Breakdown of the Octets in a Class C Address

FIRST BIT	SECOND BIT	THIRD BIT	OCTET 1	OCTET 2	OCTET 3	OCTET 4
1	1	0	Network ID	Network ID	Network ID	Host ID

Table 1-5: Examples of Well-Known Class D Addresses

CLASS D ADDRESS	DESCRIPTION
224.0.0.0	Reserved
224.0.0.1	All devices within a network segment
224.0.0.2	All routers within a network segment
224.0.0.9	Used to send routing information in a RIP environment

Protocols and Other Standards

In data communication, a *protocol* is a convention that enables the establishment of a connection between networking devices. The protocol sets the rules by which the connection is established and the rules governing the transfer of data between the devices. A protocol can govern hardware, software, and sometimes both hardware and software.

A *technical standard* can be considered a guideline or an example of a specification. A standard is used to form a basis in which a technology or a protocol can be developed.

This section describes some of the more common protocols and technical standards.

Internet Protocol

The *Internet Protocol (IP)*, as mentioned earlier in this chapter, is a data protocol that is used by a source and a destination to communicate across a network.

In an IP network, data is transferred in blocks known as packets. The IP makes no guarantees that the information that is contained within a packet is not damaged. It is possible for data to be damaged, sometimes duplicated, and sometimes dropped completely. This is known as *best-effort delivery*.

In a data network, a *packet* is the block of information that contains the data that is being transmitted between devices. A packet comprises the following three elements:

- *Header:* Contains instructions about the data that is contained in the payload portion of the packet.
- *Payload:* Contains the data that is being transmitted.
- *Footer:* Contains end-of-packet information, as well as error-checking.

Figure 1-7 shows the packet header.

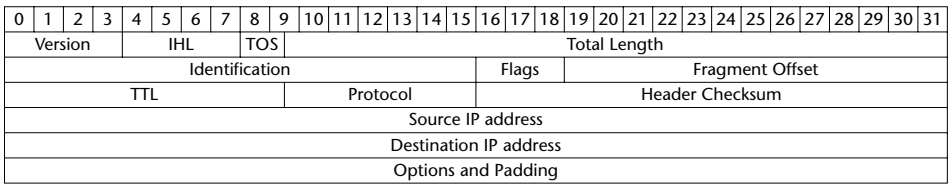


Figure 1-7: The IP packet header

As shown in Figure 1-7, the bits in the IP packet header are as follows:

- *Version:* Identifies the version number of the packet.
- *Internet Header Length (IHL):* This field identifies the length of the IP packet header.
- *Type of Service (TOS):* Identifies the type of service. Used by networks to identify the data being transported and helps determine how the packet is to be handled.
- *Identification:* Helps identify packet fragments to ensure they are kept separate from other packet fragments.
- *Flags:* Keeps information as to whether or not fragmentation is used and if there are more fragments.
- *Fragment Offset:* Directs the reassembly of packets.
- *Time to Live (TTL):* A timer that is used to keep track of a packet.
- *Protocol:* Identifies the next encapsulated protocol.
- *Header Checksum:* The checksum data of the IP header and the Options field.
- *Source IP address:* Identifies the IP address of the source device.
- *Destination IP address:* Identifies the IP address of the destination.
- *Options and Padding:* Special instruction data for the packet and may contain filler data to ensure that the data starts on a 32-bit boundary.

Interior Gateway Protocol

The *Interior Gateway Protocol (IGP)* is a protocol that is used to exchange routing information between devices within a single autonomous system. The information that is exchanged is then used by other network protocols to specify how data is transmitted to its destination.

Exterior Gateway Protocol

The *Exterior Gateway Protocol (EGP)* is used to exchange data between multiple autonomous systems. Commonly used on the Internet, it allows communications between hosts to build routing information to ensure data can be transported from source to destination.

Routing Information Protocol

The *Routing Information Protocol (RIP)* is the most commonly used IGP in networking today. RIP is used to manage information that is given to a router in a LAN (or group of LANs).

An edge device that supports RIP will send out RIP information to other edge devices. The information that each of these edge devices sends out is known as the routing table. The *routing table* contains information about all of the IP devices that the edge device knows about. Each of the neighboring devices then sends out routing information to its neighbors with the information that it has learned, along with the information of the devices that are local to it.

The route from one device to another is known as a hop. RIP determines the number of hops it takes to get from one device to another and uses that information to determine the distance it takes to get from one device to another.

RIP is a *distance-vector routing protocol*, which means that it makes routing decisions based on the distance between two communicating devices. It uses a routing table to make route decisions and it updates its routing table every 30 seconds. The routing table is reviewed each time a routing update occurs, and then it is recalculated with the best route to a destination IP address. Figure 1-8 shows a diagram of a RIP header.

As shown in Figure 1-8, the bits in the RIP packet header are as follows:

- *Command:* This field describes the action of the message.
- *Version:* Identifies the RIP version being used.
- *RIP Entry Table:* This is a variable length and contains the routing table information.

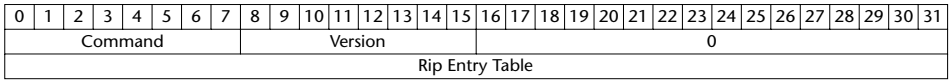


Figure 1-8: The RIP header

Open Shortest Path First

The *Open Shortest Path First (OSPF)* protocol is another often used IGP. Larger autonomous systems might prefer OSPF to RIP because OSPF does not require the 30-second updates that RIP does.

OSPF is a *link state, hierarchical routing protocol*. This means that each device in the network calculates and maintains its own routing table, and updates occur only when a change in the network occurs.

OSPF can operate securely in a network. It authenticates peers before forming an adjacency with the peers. An OSPF network consists normally of several small networks, known as *areas*. A central area, known as the *backbone area*, serves as the core of the OSPF network. All areas in an OSPF network must connect to the backbone. Figure 1-9 shows a diagram of an OSPF header.

As shown in Figure 1-9, the bits in the OSPF header are as follows:

- *Version:* Identifies the OSPF version.
- *Type:* Identifies the type of the request or reply that is contained in the message.
- *Length:* Identifies the size of the header and the message.
- *Router ID:* Identifies the packets source.
- *Area ID:* Identifies the area that the packet belongs to.
- *Checksum:* Identifies the IP checksum of the packet, excluding the authentication portion of the packet.
- *Authentication Type:* Identifies the procedure in which the packet is to be authenticated.
- *Authentication:* For use by the type of authentication that was chosen when forming the packet.

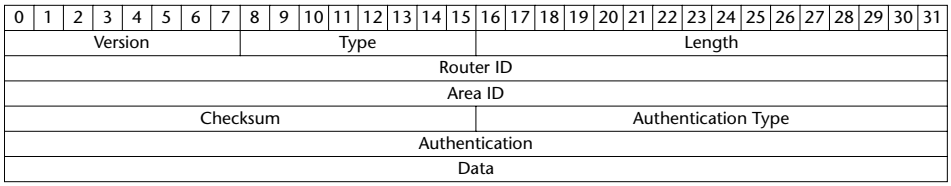


Figure 1-9: The OSPF header

Virtual Router Redundancy Protocol

The *Virtual Router Redundancy Protocol (VRRP)* assists network reliability by allowing the advertisement of a virtual router as a default route for devices in a network. This virtual router is an abstract representation of a master VRRP router and a backup VRRP router. Two (or more) physical routers are configured to serve as a virtual router, with one being the master and one the backup. The master is the one that performs all routing functions at any one time. If the master router fails, then the backup router becomes the VRRP master.

VRRP message packets are transmitted encapsulated into IP packets. Figure 1-10 shows a VRRP packet header.

As shown in Figure 1-10, the bits in the VRRP message header are as follows:

- *Version:* The VRRP version number.
- *Type:* The type of request or reply contained in the message.
- *Virtual Router ID (VRID):* This field identifies the router that the packet is reporting a status for.
- *Priority:* Identifies the priority for the sending VRRP router.
- *IP address count:* Identifies the number of IP addresses that are contained in the message.
- *Authentication type:* The authentication method that is used.
- *Authentication interval:* Defines the time interval (in seconds) that there is between advertisements.
- *Checksum:* Identifies the bit count of the entire message.
- *IP addresses:* A list of all of the IP addresses that are associated with the virtual router.
- *Authentication data:* Data used to authenticate the packet.

Digital Subscriber Line

The *Digital Subscriber Line (DSL)* technology is actually a group of technologies that allow for digital services over a copper telephone wire. DSL operates similarly to the way that the Integrated Services Digital Network (ISDN) operates, but at a much faster rate. The two most popular forms of DSL are the Asymmetric Digital Subscriber Line (ADSL) and the Symmetrical Digital Subscriber Line (SDSL).

Asymmetric Digital Subscriber Line

Asymmetric Digital Subscriber Line (ADSL) allows for faster data transmission over telephone lines than a traditional modem allows. ADSL transmits data asymmetrically, with data transmitting faster in one direction than it does in the other direction. An ADSL modem is required for the implementation of ADSL.

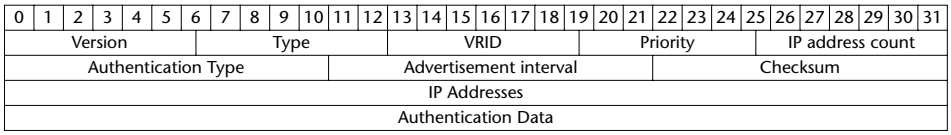


Figure 1-10: The VRRP packet header

Symmetrical Digital Subscriber Line

Symmetrical Digital Subscriber Line (*SDSL*) transmits data at a higher rate than traditional modem technology does. The main difference between ADSL and SDSL is that SDSL transmits data at the same rate in both directions. An SDLS modem is required for the implementation of SDSL.

Integrated Services Digital Network

Integrated Services Digital Network (ISDN) is a standard for transmitting data over traditional telephone lines. ISDN supports faster rates of data transfer than traditional dial-up modem technology does. In ISDN, there are two types of data transmission channels: B-channels and D-channels. Additionally, there are two types of ISDN in use: Basic Rate Interface (BRI) and Primary Rate Interface (PRI).

Bearer-Channel

The *Bearer-Channel (B-channel)* is the main data channel in an ISDN connection. The B-channels carry all of the voice and data services within the ISDN connection. In ISDN, both the BRI and the PRI will have more than one B-channel configured for their ISDN services.

Delta-Channel

The *Delta-Channel (D-channel)* is the channel in ISDN that carries the control and signaling information. In ISDN technology, only one D-channel is required with either a BRI or a PRI configuration

Basic Rate Interface

Basic Rate Interface (BRI) is an ISDN configuration that consists of two 64 kilobits per second (Kbps) B-channels and one 16 kilobits per second D-channel. The two B-channels are often joined together to support a total data rate of 128 Kbps. BRI is most often used by smaller networks, or for residential use. BRI is often referred to as 2B+D (two B-channels plus one D-channel) or 2B1D (two B-channels, one D-channel).

Primary Rate Interface

Primary Rate Interface (PRI) is an ISDN configuration that, in North America and Japan, uses 23 B-channels and 1 D-channel. Most of the rest of the world uses 30 B-channels and 1 D-channel. In PRI, the D-channel also carries data at 64 Kbps. Most large networks use PRI as their ISDN standard configuration.

Lightweight Directory Access Protocol

The *Lightweight Directory Access Protocol (LDAP)* standard was developed as a simple way to access and search directories that are running over TCP/IP. An LDAP directory consists of entries that are nothing more than a collection of attributes that identify groups and individuals assigned to the groups. Each entry in an LDAP directory defines which attributes are optional, which ones are mandatory, and what type of information the LDAP directory stores. An LDAP directory is hierarchical in nature, defining geographic and/or organizational boundaries.

Remote Authentication Dial-In User Service

Remote Authentication Dial-In User Service (RADIUS) is a protocol that allows Remote Access Servers (RAS) to communicate with a core RADIUS server to authenticate and authorize access to remote users. RADIUS is a vehicle that allows companies to store authentication on a core, central server that all remote servers can utilize. It's easy for the company to maintain because there is a central source in which access policies are established, as well as a single point to log network access activities.

Figure 1-11 shows the RADIUS header.

As shown in Figure 1-11, the bits in the IP packet header are as follows:

- *Code:* Identifies the type of RADIUS message.
- *Identifier:* Allows for the grouping of requests and replies.
- *Length:* Identifies the length of the packet.
- *Authenticator:* Partly used in the password-hiding algorithm, and it also is used to authenticate replies from the server.
- *Attributes:* Identifies the authentication details for requests and responses.

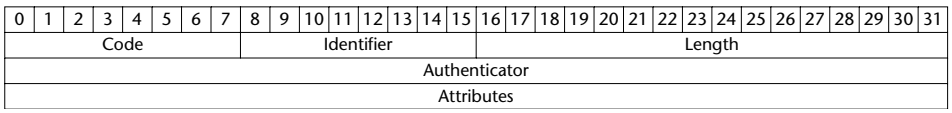


Figure 1-11: The RADIUS header

Networking Hardware

Networking hardware is defined as the hardware that is used to allow for communication on the network. This includes all of the computers, printers, interface cards, various peripherals, routers, switches, hubs, and various other devices that are needed to perform network data communication.

Random Access Memory

Random Access Memory (RAM) is a type of computer data storage. RAM is used to store active data for quick access during processing. Computers (including networking gear) use RAM to store program data and code during the execution of an application. RAM is randomly accessed and most data can be retrieved from anywhere within the RAM module instantly. Figures 1-12 and 1-13 show examples of RAM.

Modem

The *modem*'s name comes from the two main services it provides. It *modulates* an analog signal to encode digital information and then it *demodulates* the signal by decoding the data. The modem takes the 1s and 0s (the bits and the bytes) and turns them into an audio signal that is transmitted from the modem through the telephone wire to another modem.

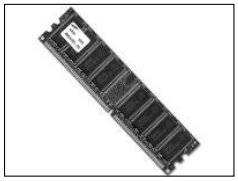


Figure 1-12: An example of a RAM module

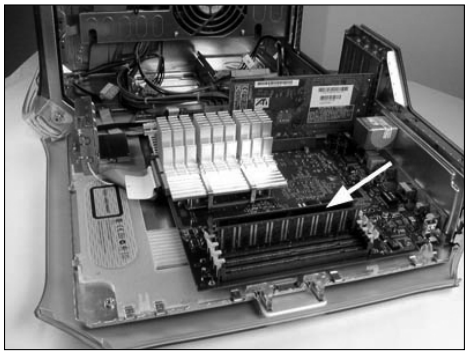


Figure 1-13: An example of RAM installed on a PC motherboard

Channel Service Unit/Data Service Unit

The *Channel Service Unit/Data Service Unit (CSU/DSU)* is an interface device that connects a router to a digital circuit. One of the primary functions of the CSU/DSU is to maintain signal timing between communication devices. The CSU/DSU is required to be used whenever a dedicated circuit is needed.

The CSU/DSU is a Layer 1 device (Physical layer in the OSI Reference Model). In addition to maintaining communication signaling, the CSU/DSU is capable of performing error checking as well.

Computer Workstations

All of the end user's computers in the network are considered *workstations*. Most workstations contain a *network interface card (NIC)*, software for networking, and cables. Some workstations have local storage, but often files are stored on a server and are not accessed or stored locally. Virtually any computer can be considered a workstation.

Servers

A *server* is one of the most important pieces of equipment in a network. It acts as a storage device, as well as controlling the flow of information in the network. A server is a computer that has a lot of RAM and ample storage space to meet the needs of the LAN it supports. For example, a file server may perform many tasks at a time, so it must be fast enough and large enough to handle and control the data that it supplies. Following are some examples of types of servers:

- *Internet server:* Provides Internet application services, such as email services and Web services.
- *Email server:* Provides storage services for emails and also provides connections for users to access their email.
- *File server:* Provides file sharing services.
- *Print server:* Provides shared access to network printers.
- *Application server:* Provides sharing services for specific applications.

Network Interface Cards

The network interface card (*NIC*) is what supplies the physical connection between a workstation and the network. Most NICs are integrated or built into the PC, although there are some that reside externally to the device that they support. The most popular types of NICs are Ethernet and Token Ring.

Switch

A *switch* provides a central location for multiple LANs to connect to the network. A switch is often called an *intelligent hub* because of its ability to sort data. Operating at the Data Link layer (Layer 2) of the OSI Reference Model, a switch can connect multiple network segments together at a central point.

When a switch receives a frame, it saves the MAC address of the originator and the port on which the frame was received. It will then use the data it collects to forward packets based on the MAC address. If it does not have the MAC address in its MAC address table, it will flood the frame out of all of its interfaces.

Figure 1-14 shows an example of using a switch to forward data in a LAN.

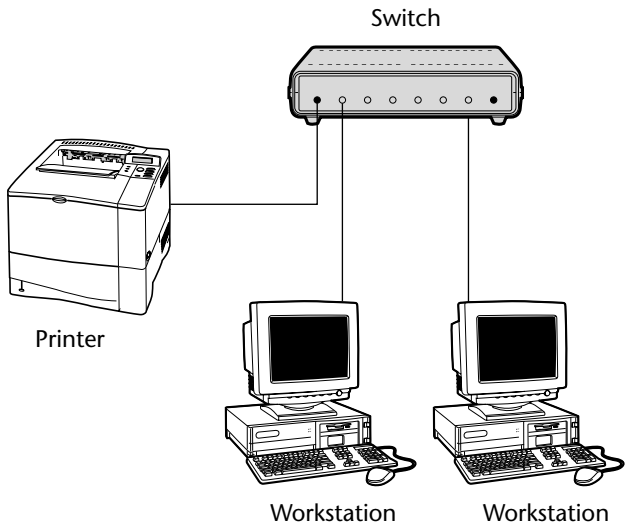


Figure 1-14: Example of a LAN for which a switch has been implemented to forward data

Hub

A *hub* (or *concentrator*) is used to connect multiple devices together in a central point. The hub operates at the Physical layer (Layer 1) of the OSI Reference Model. Unlike the switch, the hub is not intelligent enough to forward frames based on a MAC address. Instead, it simply forwards data it receives out of all of its interfaces.

Router

A *router* operates at the Network layer (Layer 3) of the OSI Reference Model and normally connects two LANs together, or a LAN to a WAN (see Figure 1-15). Routers use forwarding tables to determine what the best path is to a destination. There are multiple routing protocols used by a router that assists in making the determination on where to forward data. Chapters 8 and 9 detail routing protocols in depth.

Most computers are capable of performing routing functions, but a router is a specialized computer that has extra hardware built in to speed up routing functions.

A router creates a routing table, which lists the best routes to any particular destination. The routing tables are built with information obtained through a routing protocol, such as the Routing Information Protocol (RIP). Chapter 8 includes additional information on RIP.

Repeater

A *repeater* is a device that is used to replicate a signal in a network. In areas of the network where there is transmission loss (perhaps when distance is a factor), a repeater can be used to boost the transmission of data, to ensure it arrives at its destination (see Figure 1-16). A repeater can also be used to transmit data between subnetworks that use different protocols and/or types of cabling.

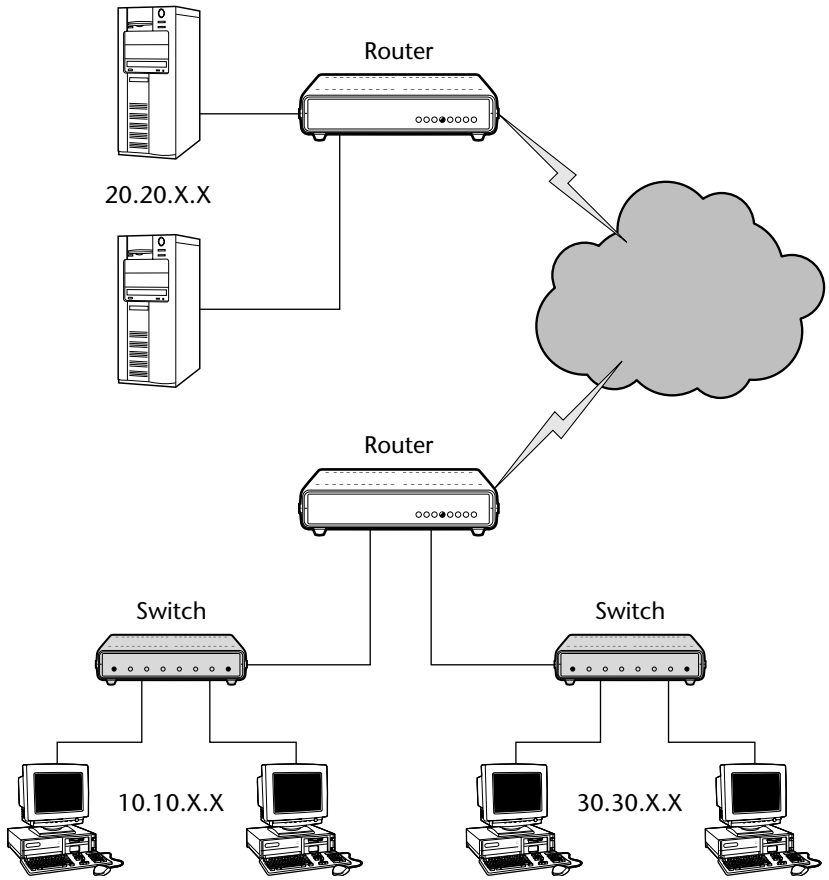


Figure 1-15: An example of LAN-to-LAN and LAN-to-WAN networking via the router

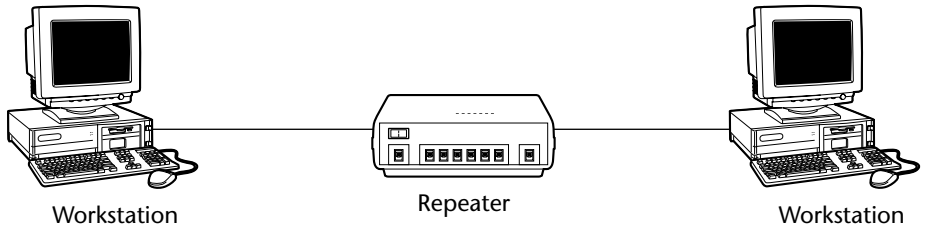


Figure 1-16: A repeater used to boost the signal of data being transferred a long distance

Remote Access

As mentioned previously, remote access is very important for users who are not local to their corporate LANs. VPNs are steadily becoming available in most of today's LANs, but there are other traditional methods covered in this section. There are many different manners in which a remote user can access a network. Following are some examples of these methods:

- Remote Access Services (RAS)
- Dial access to a single workstation
- Dedicated remote access system
- Use of a terminal server

The needs of remote users normally dictate the type of remote access that a company chooses to implement. Figure 1-17 shows an example of a topology used for remote access.

Remote Access Services

RAS is a service that is provided by a Windows NT–based computer. The remote users access the LAN via a modem interface or a WAN link, and then they log on to the LAN and are provided the same services as if they were local to the LAN. To access an NT-based LAN, the remote user must have some type of RAS client loaded on a workstation.

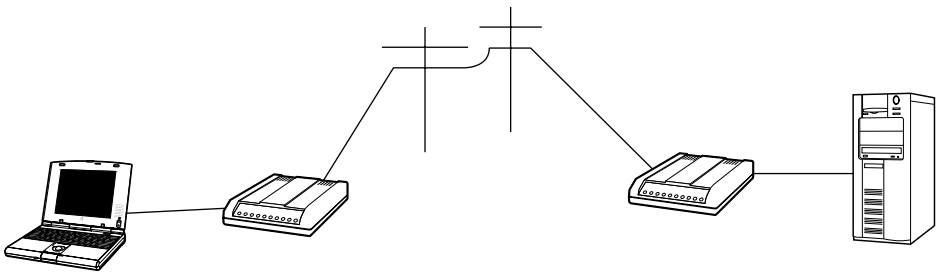


Figure 1-17: An example of a typical remote access topology

Dial Access to a Single Workstation

Many operating systems today support a variety of *remote access applications*. PCanywhere is an example of one of these. The remote access application allows a remote user to connect to a computer via a modem and control that computer from a remote location.

Remote Access System

Generally, a *remote access system* is a networking device that provides support for multiple modems that are providing remote network access, as shown in Figure 1-18.

Terminal Servers

The first *terminal servers* were placed in networks and provided services for dumb terminals. *Dumb terminals* are basically the green screen monitors and keyboards that were placed at users' desks. Terminal servers gradually grew to support *Graphical User Interface* (*GUI*) applications to clients that did not have the applications local to their workstations. Terminal servers are also very popular in providing remote access services. A Windows-based terminal server can support multiple client sessions.

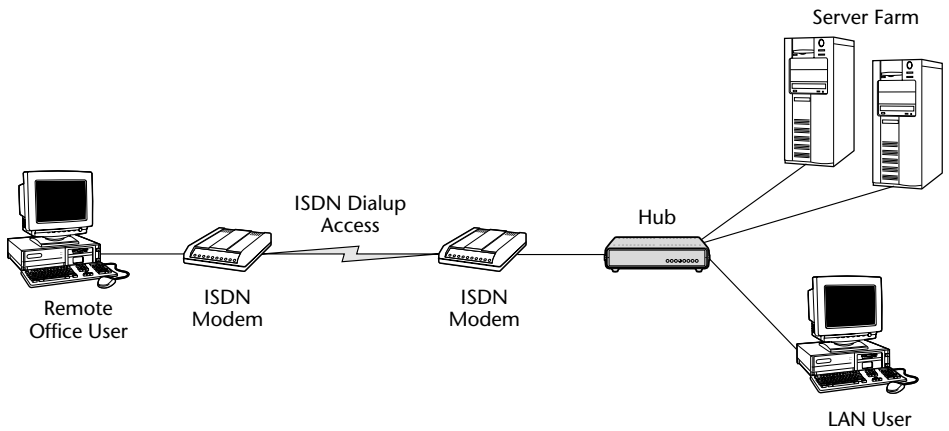


Figure 1-18: A remote office accesses the corporate LAN via an ISDN dialup configuration.

Network Security

Network traffic is a series of 1s and 0s that are transmitted between a source and a destination. Because this information is transferred over a public infrastructure, security of this data is a major concern with most companies. The ability to protect data (not only while it is in transit, but also while it is stored on the devices within your LAN) is a very important concern in today's networks. It is so important, in fact, that many companies hire professionals for the sole purpose of securing corporate data.

The Firewall

In most of today's LANs, a *firewall* is implemented to help protect the sensitive data stored on devices in the network. A firewall is either a hardware or software solution that has been implemented on the edge of the network to monitor and limit information transfers based on a set of defined rules.

The firewall protects the LAN from unauthorized access. This helps reduce the possibility of a malicious attack on the network and the devices that comprise the network. A secondary function of the firewall is to control the access of destinations that reside outside of the LAN.

It is important to recognize that most LANs contain several hundred computers and network devices and normally have multiple access points to the Internet or WAN. Without some type of firewall protection, a hacker has complete access to all of those devices and can cause a lot of headaches for not only the administrators within the network, but headaches for the company. Many companies have fallen prey to a hacker and end up spending a lot of money recovering from malicious attacks. It takes just one person in the LAN to make a mistake and open up a hole for a hacker to enter.

Firewalls are implemented at the edge of each access point in the LAN (see Figure 1-19). The firewall allows the administrator of the network to set up rules based on LAN segments down to individual users. The firewall can also control which users are allowed access outside of the local network. The firewall provides a lot of control over the users on the LAN.

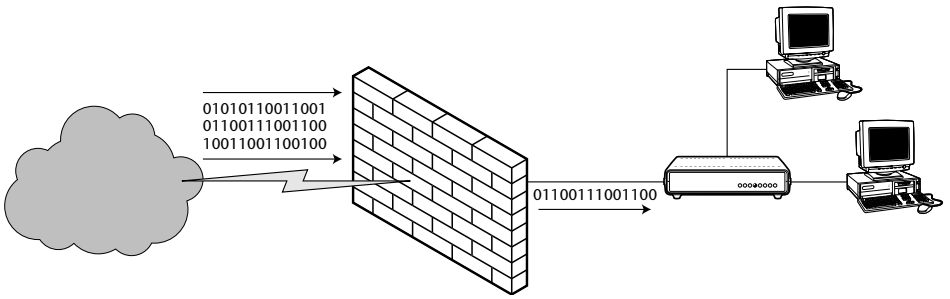


Figure 1-19: An example of a firewall implementation

Proxy services are one of the more popular methods of firewall implementations. Packet filtering and stateful packet inspection are two other methods that are used.

Proxy Server

The most common form of a firewall is the *proxy server*. The proxy server will selectively block packets of data at the edge of the network. It also provides a little more security because it will mask the addresses of devices on the LAN from devices outside of the LAN. Devices on the outside that receive data from a user within the LAN will see the address that belongs to the proxy server and all users within the LAN will appear to have the same proxy address.

A proxy server allows a client to make an indirect connection to other services in the network. The client will make a connection to the proxy server. The proxy server will then provide either access to a server that contains the data that the client wishes to access, or the proxy server will retrieve the data from cache and provide that to the client. The proxy server speeds up the retrieval of data and increases the possibility of reliable data delivery.

Many networks implement proxy servers to control what users within the LAN are able to access, as well as to provide security from potential attacks from the outside.

Packet Filtering

A network administrator can implement a set of filters on the firewall. When the firewall receives a packet, it will compare that packet with the established filter rules and will make a forwarding decision based on the filter rules that are set on the firewall.

Stateful Packet Inspection

In a *stateful packet inspection* implementation (also referred to as *stateful firewall*), the firewall keeps a record of the state of network connections. It can recognize what are considered legitimate packets for these network connections. The firewall will then forward packets that match the established criteria for these connections and refuse packets that do not match.

Demilitarized Zone

A *DMZ* is an area between the Internet and the firewall where a network device resides to help intercept Internet traffic and control requests from the LAN (see Figure 1-20). In this configuration, an extra layer of security is added. In most DMZ configurations, the computers in the DMZ will act as proxy servers for requests coming from the LAN. The equipment in the DMZ can be servers, computers, routers, and so on.

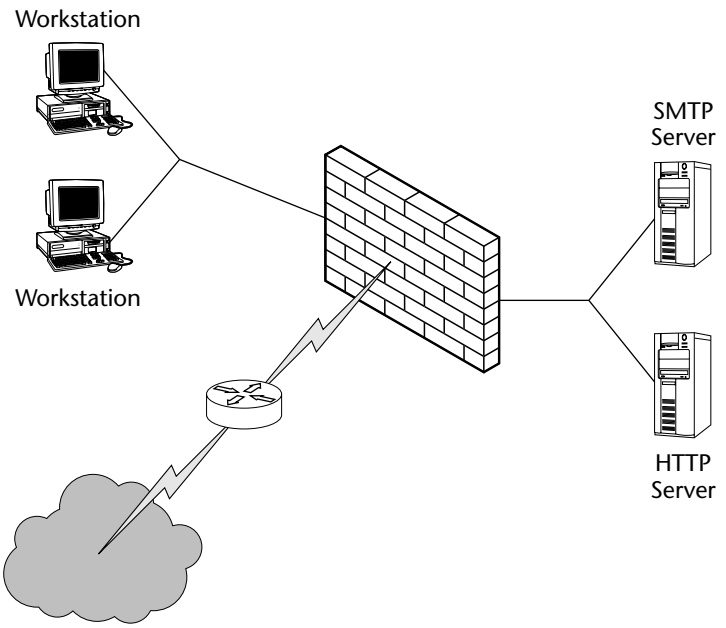


Figure 1-20: An example of a firewall solution that includes a DMZ

Hackers

In the world of data security, the term "hacker" describes an individual (or group of individuals) who is able to gain access to a system to perform some action that can be extremely detrimental to the stability of the network and the data contained within the network. Following are some of the methods that a hacker can use to corrupt the integrity of the network:

- *Backdoors:* Sometimes applications may contain a bug allowing for back-door access that may provide a hacker with a certain degree of control to that application and to other applications.
- *Remote access:* Occasionally, a hacker may access the LAN through some form of remote access. If a hacker is able to access a workstation remotely, he or she is often able to gain access to files on that workstation, if not access to information within the LAN.
- *Operating system vulnerabilities:* Like any other software application, a computing operating system can contain bugs that allow a hacker to access computers and other devices.

- *Email:* Email messages are one of the easiest ways for hackers to cause problems. Often, hackers exploit backdoors in email programs that allow them to generate thousands of repeat messages that cause email servers to slow greatly, or even shut down.
- *Spam:* Usually just annoying, spam may contain links to Web sites that will install cookies on a computer. Some of these cookies exploit a backdoor that allows a hacker in.
- *Macros:* Many applications contain macros that are user-defined scripts used to enhance the application. Hackers can use the applications to create macros that could crash your computer.
- *Viruses:* Anyone who uses a computer has heard of a virus. A *virus* is a program that is created to copy itself onto computers and spread itself through shared data. A lot of viruses are harmless, but there are some that could erase data and even cause your system to crash.
- *Denial of Service (DoS):* A DoS attack is generated when a hacker sends a request to join to a server. The server, in turn, will try to send an acknowledgment to the user and attempt to create a session. When it is unable to find the user that sent the request, the server becomes bogged down with these repeated requests. This causes the server to slow down or even crash.

VPN Basics

Understanding basic networking is a good first step to understanding VPNs, which are private networks, used by a company over an existing WAN infrastructure.

A *secure VPN* uses tunneling protocols to provide security, authentication, and integrity to VPN users.

VPN Overview

Business needs are constantly evolving and, with that evolution, the need to access information from a central location is even more prevalent. The VPN is highly sought after by companies interested in expanding the capabilities of their networks.

VPNs are prevalent in most business and homes where users are able to securely log in to the corporate LANs. VPN technology is very beneficial to people who travel often. They find that VPN allows them the flexibility of checking corporate applications virtually anywhere in the world. Because the access of data is instantaneous, information is shared in real time.

A VPN is very cost-effective as well. Unlike traditional private leased lines, VPN technology utilizes existing cabling and routers to connect one site to another in a virtual manner, over a public network (most often the Internet).

VPN Tunneling Protocols and Standards

A few protocols have been introduced to accommodate VPN technology, including the following:

- Secure Sockets Layer (SSL)
- Public Key Infrastructure (PKI)
- SecurID
- Internet Protocol Security (IPSec)
- Layer 2 Forwarding (L2F)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Generic Routing Encapsulation (GRE)

In this section, we discuss these protocols and get an understanding of what each does.

Secure Sockets Layer

Secure Sockets Layer (*SSL*) is a networking standard that is used to improve safety and security of network communications, through the use of encryption. SSL utilizes several security standards, including certificates, private keys, and public keys.

An SSL session starts with the handshake that first establishes a TCP/IP session. Once the TCP/IP session has been established, then a client is authenticated with a public key. After the authentication is complete, the server determines the level of security that is required for the client by choosing the strongest algorithm that is supported by the client and the server. The last step that is taken is the establishment of a shared secret that is used to encrypt data being passed between the server and the client. Finally, the SSL session is established.

Encryption services are very CPU-intensive and, therefore, an SSL session is established only when the transfer of sensitive data occurs. You can often determine if SSL has been employed by looking at a URL address field in a Web browser and seeing an "s" following the "http" (that is, "https").

SSL uses several components to verify the digital identity of an inquiring node. To establish an SSL session, these components are used for the purposes of performing checks and verifications made between the end nodes. These components are as follows:

- Certificates
- Certificate Authority
- Keys
- Shared Secret

Certificates

SSL uses certificates, which are digital records that identify a person, group, or organization. Certificates are personal digital identification used for a variety of security reasons (see Figure 1-21). Certificates are used in conjunction with public keys to identify the owner of the key and provide a way to pass sensitive data.

Certificate Authority

Certificates are assigned by a *Certificate Authority (CA).* Once the certificate is issued, it is then made available to the public. The certificate basically is confirmation that the CA verifies information to be true and secure, and that the public key attached to the certificate is valid.

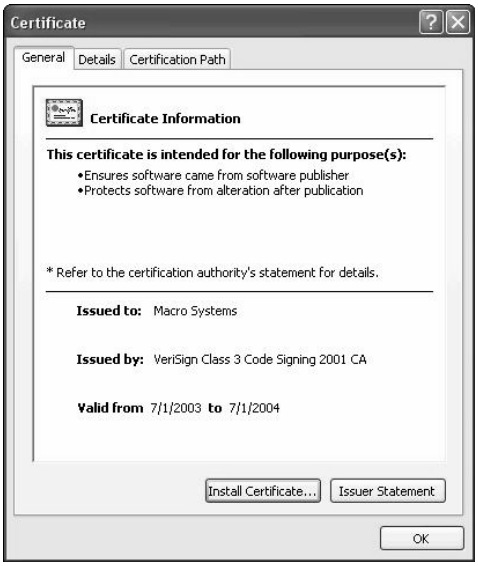


Figure 1-21: An example of a certificate

Keys

A *key* is a series of bits used by algorithms to encrypt and decrypt data messages. An encryption algorithm will take a message and a key. Based on the keys bits, a new, encrypted message is generated and sent to the destination. Sometimes the same key is used to decrypt the data, but most often the destination has a key (which will be the only key that can decrypt the data and restore it back to the original message). Keys are used to provide the necessary encryption and decryption methods used to protect and secure data transmissions.

When a sending station wants to send encrypted data, a pair of keys is assigned: One of the keys is given to the sender and one to the destination. Data is then encrypted by one key and decrypted by the other. No other key can decrypt this information.

Shared Secret

A *shared secret* is widely used because it is one password that is shared between users. The problem with a shared secret is that it stands a chance of being compromised because it is shared. Shared secrets are pre-shared keys that are allocated to source and destination devices prior to the transfer of data.

Public Key Infrastructure

Public Key Infrastructure (PKI) is a way of verifying identities. It allows the users to be united with a public key. PKI allows users to be known to each other through authentication. It allows the sharing of data by establishing the relationship and then sharing certificates to decrypt and encrypt information.

PKI encompasses the hardware, software, and the procedures that are needed to provide these services. It ensures that all users use a private key to provide a digital signal to one another, which allows users to establish secrecy and integrity in the data they are sharing.

SecurID

Developed by RSA Security, *SecurID* is a technology that provides user authentication to network resources. The SecurID mechanism contains hardware (known as a *token*) that is assigned to an individual user (see Figure 1-22). The token generates authentication codes that regenerate periodically, using a built-in clocking device. The authentication codes are also set and are generated by the token's corresponding SecurID server.



Figure 1-22: Examples of two different SecurID tokens

Internet Protocol Security

Internet Protocol Security (*IPSec*) is the standard that has been established for Internet Protocol communication. IPSec provides authentication and encryption for IP packets.

IPSec is a collection of several related protocols. It can be used on its own or can work with other tunnel protocols to provide an encryption scheme within them. IPSec operates at Layer 3 of the OSI Reference Model. It is capable of protecting both UDP and TCP traffic.

IPSec is designed to provide for key exchange and for securing the flow of packets. Securing packet flow is accomplished by using an *Authentication Header (AH)* and *Encapsulating Security Payload (ESP*). Currently, key exchanges are handled with the Internet *Key Exchange (IKE)* protocol.

Figure 1-23 shows an AH packet.

As shown in Figure 1-23, the bits in the AH packet are as follows:

- *Next Header:* Refers to the protocol of the data that is transferred.
- *Payload Length:* Refers to the size of the packet.
- *Reserved:* Not used.
- *Security Parameters Index:* Refers to the security parameters.
- *Sequence Number:* Refers to an incrementing number that is used to prevent replay attacks. A *replay attack* is data that is captured and repeated or delayed.
- *Authentication Data:* The data necessary to authenticate the packet.

Figure 1-24 shows an ESP packet.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Next Header								Length								0															
Security Parameters Index (SPI)																															
Sequence Number																															
Authentication Data (variable)																															

Figure 1-23: Diagram of an Authentication Header (AH) packet

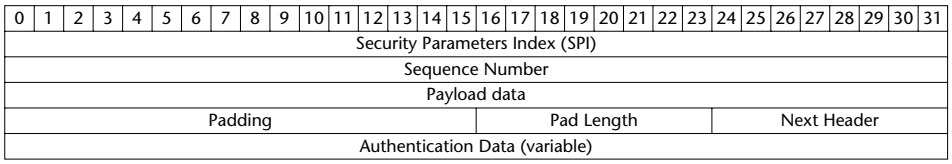


Figure 1-24: Diagram of an Encapsulating Security Payload (ESP) packet

As shown in Figure 1-24, the bits in the ESP packet are as follows:

- *Security Parameters Index:* The security parameters.
- *Sequence Number:* Refers to an incrementing number that is used to prevent replay attacks.
- *Payload:* The data that is being transferred.
- *Padding:* Used to pad the data the full length of the block.
- *Pad Length:* Size of the padding used.
- *Next Header:* Refers to the protocol of the data that is transferred.
- *Authentication Data:* The data necessary to authenticate the packet.

Layer 2 Forwarding

The *Layer 2 Forwarding* (L2F) protocol is used to create a secure tunnel between a LAN and a remote user. L2F permits the tunneling of information at the Data Link layer (Layer 2) of the OSI Reference Model. L2F allows the encapsulation of Point-to-Point Protocol (PPP) packets within the tunnel. This protocol was later merged with the Point-to-Point Tunneling Protocol (PPTP) to make L2TP. RFC 241 covers the L2F protocol.

Figure 1-25 shows the L2F header.

As shown in Figure 1-25, the bits in the L2F packet header are as follows:

- *F:* This bit is either on or off, and it identifies whether or not an offset bit is set.
- *K:* This bit is either on or off, and it identifies whether or not a Key field is present.
- *P:* This bit is either on or off, and it identifies if the packet is a priority packet or not.
- *S:* This bit is either on or off, and it identifies if there is any data in the sequence field.
- *Reserved:* Reserved for future use. Always 0.

- *C:* Identifies if the packet contains a checksum or not. This bit is either on or off.
- *Version:* Identifies the protocol version.
- *Protocol:* Identifies the protocol that is encapsulated in the L2F packet.
- *Sequence:* Identifies the sequence number.
- *Multiplex ID:* Identifies the particular connection that is used in the tunnel.
- *Client ID:* This field is used to assist endpoints in ensuring data is directed to the correct users.
- *Length:* Identifies the size of the packet.
- *Offset:* Identifies the number of bytes past the header that the payload data begins.
- *Key:* The Public Key data.
- *Data:* The payload.
- *Checksum:* Used to ensure data is received intact.

Point-to-Point Tunneling Protocol

The Point-to-Point Tunneling Protocol (*PPTP*) is a standard that supports multiple protocol VPN tunnels. PPTP allows remote users the ability to connect to their corporate network over the Internet in a secure manner. PPTP is not considered as secure as IPSec. PPTP authentication is normally handled by Microsoft Challenge Handshake Authentication Protocol (MSCHAP). PPTP is not a pure TCP protocol because it uses two channels for communication. One of the channels is a TCP channel on port 1723, and the other is a packet channel that is called the Generic Routing Encapsulation (GRE) protocol (which is discussed later in this section).

Figure 1-26 shows the PPTP header.

<table>
<tr><td colspan="1">0</td><td colspan="1">1</td><td colspan="1">2</td><td colspan="1">3</td><td colspan="1">4</td><td colspan="1">5</td><td colspan="1">6</td><td colspan="1">7</td><td colspan="1">8</td><td colspan="1">9</td><td colspan="1">10</td><td colspan="1">11</td><td colspan="1">12</td><td colspan="1">13</td><td colspan="1">14</td><td colspan="1">15</td><td colspan="1">16</td><td colspan="1">17</td><td colspan="1">18</td><td colspan="1">19</td><td colspan="1">20</td><td colspan="1">21</td><td colspan="1">22</td><td colspan="1">23</td><td colspan="1">24</td><td colspan="1">25</td><td colspan="1">26</td><td colspan="1">27</td><td colspan="1">28</td><td colspan="1">29</td><td colspan="1">30</td><td colspan="1">31</td></tr>
<tr><td>F</td><td>K</td><td>P</td><td>S</td><td colspan="8">Reserved</td><td>C</td><td colspan="3">Version</td><td colspan="8">Protocol</td><td colspan="8">Sequence</td></tr>
<tr><td colspan="16">Multiplex ID</td><td colspan="16">Client ID</td></tr>
<tr><td colspan="16">Length</td><td colspan="16">Offset</td></tr>
<tr><td colspan="32">Key</td></tr>
<tr><td colspan="16">Data</td><td colspan="16">Checksum</td></tr>
</table>

Figure 1-25: The L2F header



Figure 1-26: The PPTP Header

As shown in Figure 1-26, the bits in the PPTP header are as follows:

- *Length:* Identifies the length of the message.
- *Message Type:* Identifies the type of data contained within the message.
- *Magic Cookie:* Ensures data synchronization. This field is always set to hexadecimal `0x1A2B3C4D`.
- *Data:* The payload.

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (*L2TP*) operates at the Data Link layer (Layer 2) of the OSI Reference Model. It is a protocol standard for tunneling traffic between two peers over a public network. L2TP does not provide authentication services or security, so IPSec is often used to tunnel L2TP packets.

L2TP supports multiple protocols and supports providing private IP addresses over the Internet. L2TP offers the same functions as L2F, as well as supporting Flow Control and Attribute Value Pair (AVP) Hiding.

Flow control is used to control the flow of data in a network under controlled conditions.

AVP hiding prevents hackers from eavesdropping by encrypting L2TP messages. An AVP represents a variable and a value used for comparison when trying to authenticate a user network access request. AVP hiding is used by the L2TP tunneling protocol, and it shows the status of AVPs that are considered sensitive. When AVP hiding is implemented, then the attribute pairs are encrypted. An example of an attribute is a username or a password; the value could be the subnetwork or a group that the user should belong to.

L2TP was developed by combining two well-known tunneling protocols: PPTP and L2F.

Figure 1-27 shows the L2TP header.

As shown in Figure 1-27, the bits in the L2TP packet header are as follows:

- *T:* This refers to the message type. This bit is either on or off and it identifies if this is a data message or a control message.
- *L*: This bit is either on or off and it identifies if there is anything set in the Length field.
- *S*: This bit is either on or off and it identifies if there is anything set in the Ns or the Nr field.

- *O:* This bit is either on or off, and it identifies if there is any data in the Offset field.
- *P:* This bit is either on or off, and it identifies if the data message is a priority message or not.
- *Version:* Identifies the L2TP version.
- *Length:* Identifies the total length of the message.
- *Tunnel ID:* Identifies the connection.
- *Session ID:* Identifies the session inside the tunnel.
- *Ns:* Identifies the sequence number for this message.
- *Nr:* Identifies the sequence number that is expected in the next message.
- *Offset:* Identifies the number of bytes past the header that the payload begins.
- *Offset pad:* This is the padding field, if used.
- *Data:* The payload.

Generic Routing Encapsulation

The Generic Routing Encapsulation (*GRE*) protocol is established as a way to encapsulate a large variety of protocol packet types in a tunnel. GRE tunnels are connectionless, which means that each end of the tunnel does not keep any information about the status of the other end. A GRE tunnel interface is active as soon as it is implemented, and it remains up as long as the interface is up. GRE interfaces do not keep track of the opposite end, so data can be transmitted through a tunnel when the destination is unavailable.

Figure 1-28 shows the GRE header.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>T</td><td>L</td><td colspan="2">0</td><td>S</td><td>0</td><td>O</td><td>P</td><td colspan="4">0</td><td colspan="4">Version</td><td colspan="16">Length</td></tr>
<tr><td colspan="16">Tunnel ID</td><td colspan="16">Session ID</td></tr>
<tr><td colspan="16">Ns</td><td colspan="16">Nr</td></tr>
<tr><td colspan="16">Offset</td><td colspan="16">Offset Padding</td></tr>
<tr><td colspan="32">Data</td></tr>
</table>

Figure 1-27: The L2TP header

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>C</td><td>R</td><td>K</td><td>S</td><td>s</td><td colspan="3">Recur</td><td colspan="6">Flags</td><td colspan="4">Version</td><td colspan="16">Protocol</td></tr>
<tr><td colspan="16">Checksum</td><td colspan="16">Offset</td></tr>
<tr><td colspan="32">Key</td></tr>
<tr><td colspan="32">Sequence Number</td></tr>
<tr><td colspan="32">Routing</td></tr>
</table>

Figure 1-28: The GRE header

As shown in Figure 1-28, the bits in the GRE header are as follows:

- *C:* The first bit is the Checksum Present bit. This identifies if a checksum field is set or not.
- *R:* This bit is the Routing Present bit, and it identifies if the routing field is set or not.
- *K:* This bit is the Key Present bit, and it identifies if the key field is set or not.
- *S:* This bit is the Sequence Number Present bit, and it identifies if the sequence number field is set.
- *s:* This is the Strict Source Route bit. This bit is set only if the routing information contains strict source routes.
- *Recur:* This is a 3-bit field used for recursion control. This identifies the number of additional encapsulations that are permitted.
- *Flags:* This represents five reserved bits that are always 0.
- *Version:* The GRE version number.
- *Protocol:* Identifies the protocol type of the payload.
- *Checksum:* The IP checksum of the GRE header and the payload. If a destination compares data it receives with the checksum and the data does not match, the receiver knows that the data was corrupted in transit.
- *Offset:* Indicates the byte offset between the routing field and the Source Route Entry.
- *Key:* Used by the receiver to authenticate the source of the packet received.
- *Sequence Number:* Used by the receiver to determine the order of the packets received.
- *Routing:* This is a list of the source route entries.

Summary

This chapter has reviewed networking and VPN basics. The information that was covered in this chapter should establish an understanding for information presented in other chapters of this book. Many of the concepts that were presented in this chapter are covered later in the book.

CHAPTER 2

The Nortel VPN Router

Chapter 1 discussed some basic networking strategies and terminologies, as well as some security concerns with today's Internet and some of the protocols that have been established to help battle those potential security problems. Finally, Chapter 1 addressed the ever-growing need for VPN routing.

VPN networking is becoming a standard option for most corporate networks. To participate in VPN networking, the following questions should be discussed:

- What special hardware is required for VPN networking?
- What protocols are supported on that hardware?
- Is there room for future growth?

This chapter discusses the Nortel VPN Router portfolio. Nortel has several router options to meet the many diverse needs of companies around the world. Often, the Nortel VPN routing solution can be implemented into a network without too many changes to the current infrastructure.

How do you determine the Nortel VPN Router that is right for you? This chapter discusses some of the standards and the optional equipment that is supported. Additionally, we briefly discuss deployment strategies to assist you in understanding the versatility of the Nortel VPN Router portfolio.

The Nortel VPN Router Portfolio

Formerly known as the Nortel Contivity Secure IP Services Gateway, the Nortel VPN Router family provides secure network access and IP services. The Nortel VPN Router provides a huge cash advantage over traditional remote access networking because it utilizes the public Internet for connectivity to an enterprise network. Public access to a private LAN could, in itself, promote multiple security concerns, but the Nortel VPN Router alleviates these concerns by providing data security services.

Nortel has many VPN Router solutions to meet the needs of networks throughout the world. Following is a list of the routers discussed in this chapter. Figure 2-1 shows a graphical comparison of these routers.

- *Nortel VPN Router Model 100:* Intended for use within smaller branch offices and home offices.
- *Nortel VPN Router Model 221:* Intended for use within smaller branch offices and home offices.
- *Nortel VPN Router Model 251:* Intended for use within smaller branch offices and home offices.
- *Nortel VPN Router Model 600:* Intended to support multiple branch office-to-branch office connections, as well as being able to support small corporate LANs that require less than 50 IPSec tunnels.
- *Nortel VPN Router Model 1010:* Intended to support multiple branch office-to-branch office connections, as well as being able to support small corporate LANs that require less than 30 IPSec tunnels.
- *Nortel VPN Router Model 1050:* Intended to support multiple branch office-to-branch office connections, as well as being able to support small corporate LANs that require less than 30 IPSec tunnels.
- *Nortel VPN Router Model 1100:* Intended to support multiple branch office-to-branch office connections, as well as being able to support small corporate LANs that require less than 30 IPSec tunnels.
- *The Nortel VPN Router Model 1700:* Intended to support small to medium corporate LANs that require less than 500 IPSec tunnels.
- *Nortel VPN Router Model 1740:* Intended to support small to medium corporate LANs that require less than 500 IPSec tunnels.
- *Nortel VPN Router Model 1750:* Intended to support small to medium corporate LANs that require less than 500 IPSec tunnels.
- *Nortel VPN Router Model 2700:* Intended to support medium corporate LANs that require less than 2,000 IPSec tunnels.
- *Nortel VPN Router Model 5000:* Intended to support large corporate LANs that require less than 5,000 IPSec tunnels.

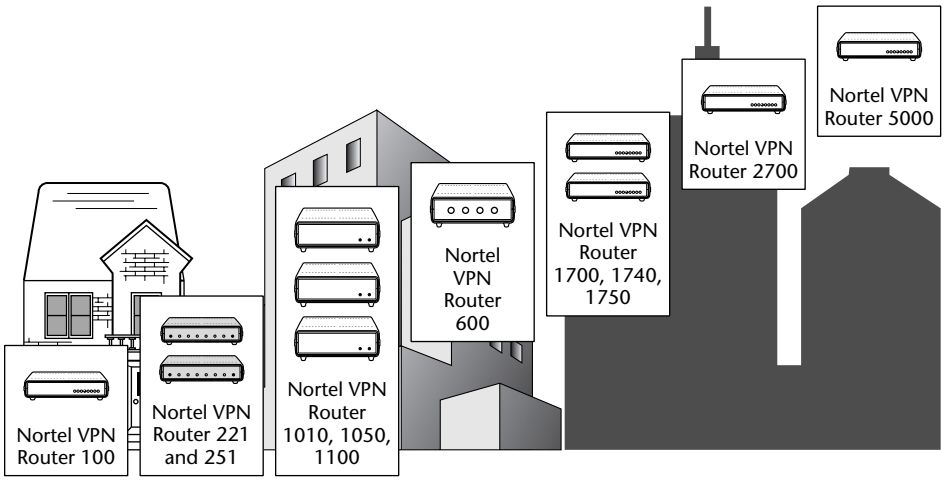


Figure 2-1: Nortel VPN Router solutions—a graphical comprehensive review

Modules and Interfaces

Many standard and optional hardware interfaces are supported on the Nortel VPN Router portfolio. This section discusses these and introduces some of the technologies that are supported.

SSL VPN Module 1000

The Nortel SSL VPN Module 1000 can be inserted into any available PCI expansion slot on any of the following supported Nortel VPN Routers:

- VPN Router 1740
- VPN Router 1750
- VPN Router 2700
- VPN Router 5000

The Nortel SSL VPN Module 1000 provides network SSL access to existing VPN configurations, thus enhancing the security standards of the network. It is an upgrade that is cost-effective because it does not require any additional equipment to introduce into the network. The SSL VPN module 1000 provides support for up to 1,000 SSL VPN users. It is an ideal solution for networks in that it allows for concurrent support for both SSL and IPSec access, without requiring additional equipment.

Hardware Interface Options

Many of the Nortel VPN Routers discussed so far have optional equipment that can be supported. This section discusses some of these optional modules and what each one can offer.

Peripheral Component Interconnect Expansion Slots

The Peripheral Component Interconnect (PCI) is a computer-based standard that specifies the subsystem that provides for the transfer of data between multiple computer components. PCI devices can be the circuits that are installed on a computer motherboard, as well as expansion modules that fit into expansion slots on a computer motherboard. By providing these expansion slots and developing the separate expansion modules, users gain more flexibility in choosing the functions that are (and will be) available to them.

10/100Base-T Ethernet

The Ethernet standard is a networking technology that was developed to define wiring and signaling required in a LAN to transfer data. Ethernet became popular in the 1990s and has become the most widely used networking technology in most LANs today.

The 10/100Base-T Ethernet module's name can be broken down as follows:

- *10/100:* Refers to the transmission speed that is supported by the module. The "10" refers to a transmission speed of 10 Mbps and the "100" refers to a transmission speed of 100 Mbps. This is a configurable option, supporting either 10 or 100 Mbps.
- *Base:* Refers to the baseband signaling. A *signal* is a flow of electronic information, usually modulated as a time or position function. Because many lower signals are normally sent to higher signal frequencies for transmission, the lower signals are considered the base, hence baseband signaling.
- *T:* Refers to the twisted-pair cabling that is used for this standard.

1000Base-SX/1000Base-T Ethernet

1000Base-SX and 1000Base-T are Gigabit Ethernet (GbE) standards. 1000Base-T is a GbE standard for implementing Ethernet at a speed of 1 gigabit per second. While it is not a standard for most small LAN configurations, it is slowly becoming a standard in many medium to large LANs.

The 1000Base-SX and 1000Base-T Ethernet module's name can be broken down as follows:

- *1000:* Refers to the transmission of 1,000 Mbps, or 1 gigabit/second (Gbps).
- *Base:* Refers to the baseband signaling.
- *T:* Refers to the twisted-pair cabling that is used for this standard.
- *SX:* Refers to the simplex multimode fiber cabling that is supported.

1000Base-T is one of the GbE standards that is supported on the Nortel VPN Routers. At a minimum, the 100Base-T standard requires Category 5 enhanced twisted-pair cabling.

1000Base-SX is one of the GbE standards that is supported on the Nortel VPN Routers. 1000Base-SX requires multimode fiber-optic cabling. Multimode fiber is used for shorter distances (normally within a building).

CSU/DSU

The Channel Service Unit (CSU)/Data Service Unit (DSU) is a device that is used to connect a router to a digital circuit for the purpose of data transmission over a high-speed network. The CSU/DSU works exactly like a modem does for dial-access lines.

The CSU/DSU provides signal timing between the router and the end device, typically a Telco switch. It also is the termination device between the physical connections.

T1/E1

The T1 carrier is a digital communication service in use today in the United States and in Japan. It is part of the T-carrier telecommunications system, which was introduced by Bell Labs in the 1960s.

The T1 carrier system line supports twenty-four 64 Kbps channels for the transmission of digital data. The T1 line incorporates *Pulse Code Modulation (PCM)*, which is a standard for digitizing analog data, and *Time Division Multiplexing (TDM)*, which is a standard for transmitting multiple streams of data into a single signal.

The T1 line can transmit data at an overall rate of 1.54 Mbps. In today's Internet, most Internet providers connect to the Internet over a T1 line. In the business world, most major corporations use T1 to connect to the Internet providers, ensuring the fast data rate through the entire communications process.

The E1 carrier is a European digital communication service that is in use by pretty much the rest of the world. It is part of the E-carrier telecommunications system. The E1 signal carries data at a rate of 2.048 Mbps and comprises thirty-two 64 Kbps channels.

ADSL

As mentioned in Chapter 1, the Asymmetrical Digital Subscriber Line (ADSL) is a Digital Subscriber Line (DSL) standard that utilizes the traditional telephone cable and expands the bandwidth usage of that cable. ADSL is asymmetric in that it can transfer data faster in one direction than it can in the other direction. This is very desirable to users who have traditionally connected to the Internet over a standard modem. ADSL provides rapid download speeds (256 Kbps to 8 Mbps). The upload speeds are typically 64 Kbps to 1,024 Kbps.

Another benefit of ADSL over a traditional modem is that you can use the same line for a phone call and for Internet access. Traditional dialup modems cannot run the two simultaneously.

Serial Interfaces (V.35, X.21, RS-232)

A *serial interface* (or *serial port*) is one where only 1 bit of information is transmitted at a time, sent 1 bit after the other in a serial stream. In *full-duplex operation*, the serial line will receive data over one line and will transmit over another. In *half-duplex operations*, only one line is used.

The *V.35 interface* is a standard used by most routers in the United States today to connect to T1 carriers for the purpose of synchronous data exchange. An International Telecommunication Unit-Telecommunications sector (ITU-T) standard, the V.35 standard supports data transmission speeds up to 48 Kbps.

The *X.21 interface* supports the X.21 standard that is governed by the ITU-T. X.21 is a standard for data communication between user devices and a circuit switch network supporting speeds up to 2 Mbps, although data transfer at 64 Kbps is the most commonly used speed.

RS-232 is the most commonly used serial line standard. The RS stands for "Recommended Standard" and it is a standard defining communications between a *Data Terminal Equipment (DTE)* interface (such as a computer) and a *Data Circuit Equipment (DCE)* interface (such as a modem). The RS-232 standard does not establish transmission speeds like the X.21 and the V.35 do. The RS-232 standard is maintained by the Electronic Industries Alliance (EIA) and the Telecommunications Industry Association (TIA).

V.90 Dial Access Modem

Sometimes referred to as the *V.Last modem standard*, the *V.90* is a standard approved by the International Telecommunication Union (ITU) for the 56 Kbps modem. The introduction of the V.90 standard merged some proprietary modem standards into a standard that most modem manufacturers now conform to.

Modems that were produced prior to the V.90 standard can, for the most part, be upgraded with software to make them V.90-compliant. The V.90 standard communicates at a download speed of 56 Kbps and an upload speed of 33.6 Kbps. The V.90 standard is referred to as V.Last because, at the time it became a standard, it was thought that it would be the last standard for a traditional modem. Interestingly enough, other standards have been introduced since.

High Speed Serial Interface

The *High Speed Serial Interface (HSSI)* standard is a serial interface that can support data transmission as fast as 52 Mbps. HSSI is used to connect a DTE device to a DCE device and is normally supported over a T3 line.

HSSI is supported over short distances (up to 50 feet) and can interconnect the slower LAN speeds with the high speed afforded on the Internet. It uses shielded twisted-pair (STP) cabling.

HSSI operates at Layer 1 of the OSI Reference Model. It controls both the physical and the electrical interfaces on the DCE and the DTE equipment, and utilizes a standard called "gapped timing," which allows a DTE device to control the timing of data from the DCE device by adjusting the clock speed.

Encryption Accelerator Modules

The *Encryption Accelerator Module* is used to encrypt and compress IPSec data that is forwarded to the VPN Router. The module supports AES-128 cryptography with SHA-1 authentication, as well as 3DES with either SHA-1 or MD5 authentication. The module comes with 64MB of RAM. This allows the module to handle most of the IPSec encryption and, therefore, frees the router's CPU cycles to process other data.

Console Port (DB-9)

The *console port* is a standard user interface that allows direct access to the router for management of the router. This is very useful when first configuring the router, as well as allowing access when a Telnet session is not available.

The *DB-9 interface* is a standard interface that identifies the shape and the number of pins contained in the interface. It consists of two rows of parallel pins, four pins on the top and five on the bottom. The interface itself is shaped like a "D." Most network devices have this type of a console connection that allows access to the device.

Nortel VPN Router Solutions

The Nortel VPN Router family has a VPN Router model that will serve the needs of anyone who utilizes VPN for data security and remote access. From remote office to remote office communications, to retail store remote access to a corporate LAN, the Nortel VPN Router portfolio can meet the needs of any VPN solution.

There are thousands of network configurations out in the world today. Each of these networks maintains different topology configurations. Networks utilize different protocols for data communication, and each of them supports different business needs. Because there is such a diverse set of needs, Nortel has provided a solution that can support these needs.

For the employee who works from home and needs reliable, secure access to the corporate network, Nortel offers various solutions. Figure 2-2 shows a couple of Nortel VPN Routers that would support a home-based tunnel.

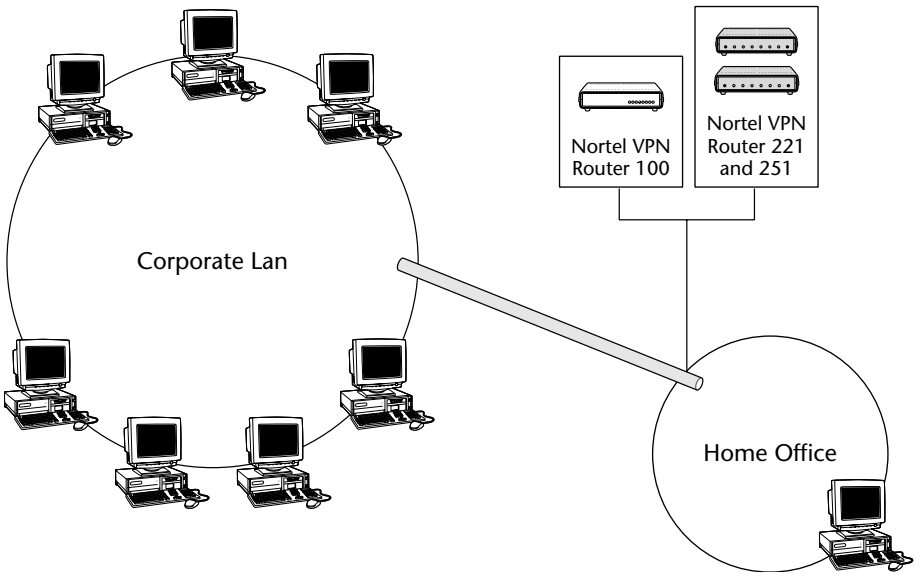


Figure 2-2: The VPN Router 100, 221, and 251 are all good home office VPN solutions

Nortel also has a solution for companies having remote offices that share data. Figure 2-3 shows an example of a remote office-to-remote office tunnel.

For the remote offices that need to connect to the corporate office to share data and utilize corporate resources, Nortel offers several routers that can support this type of configuration. Figure 2-4 shows an example of remote Branch office connectivity.

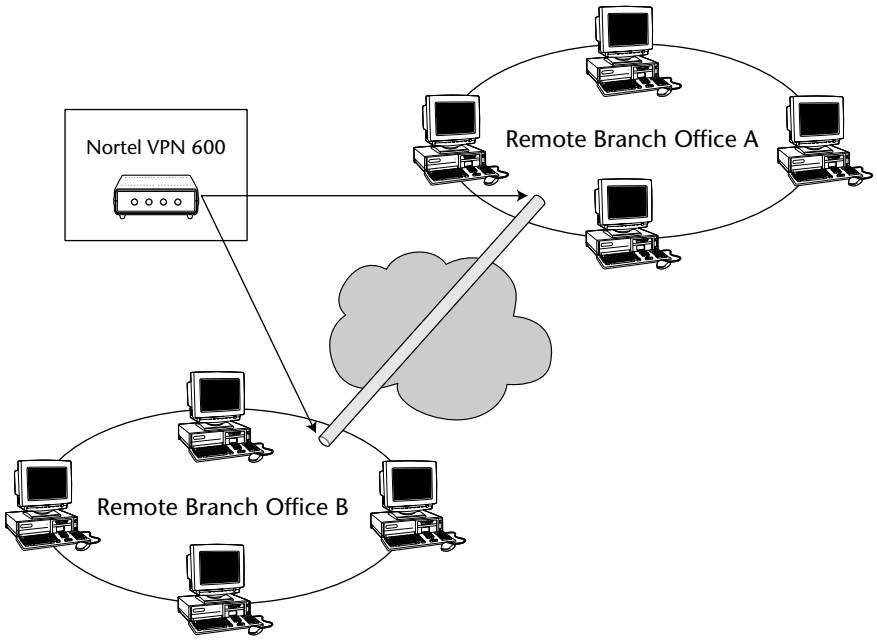


Figure 2-3: The VPN Router 600 is a great branch office–to–branch office solution.

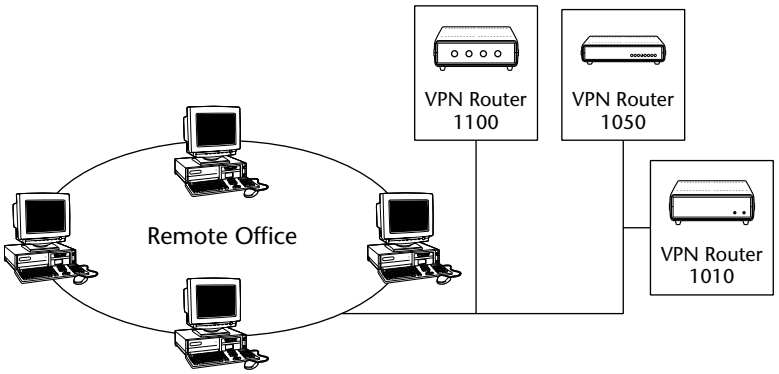


Figure 2-4: Nortel VPN Router 1010, 1050, and 1100 are all excellent solutions for remote branch offices.

Nortel also offers several VPN Routers that can serve as a core edge VPN Router for small (see Figure 2-5), medium (see Figure 2-6), and large (see Figure 2-7) LAN campuses.

VPN Router 100

The VPN Router 100 is designed with smaller branch offices and telecommuters in mind. The VPN Router 100 allows for one WAN connection and up to five active tunnels.

The VPN Router 100 is a very cost effective model. It supports home-based users, as well as small branch offices. The VPN Router 100 can be implemented into a current network design without causing changes to the current configuration of the devices on the network.

The VPN Router 100 also supports proxy firewall solutions, which allows for all traffic destined for the Internet to be forwarded to a firewall server. This helps control the data that can be accessed on the Internet, as well as control access to the private network.

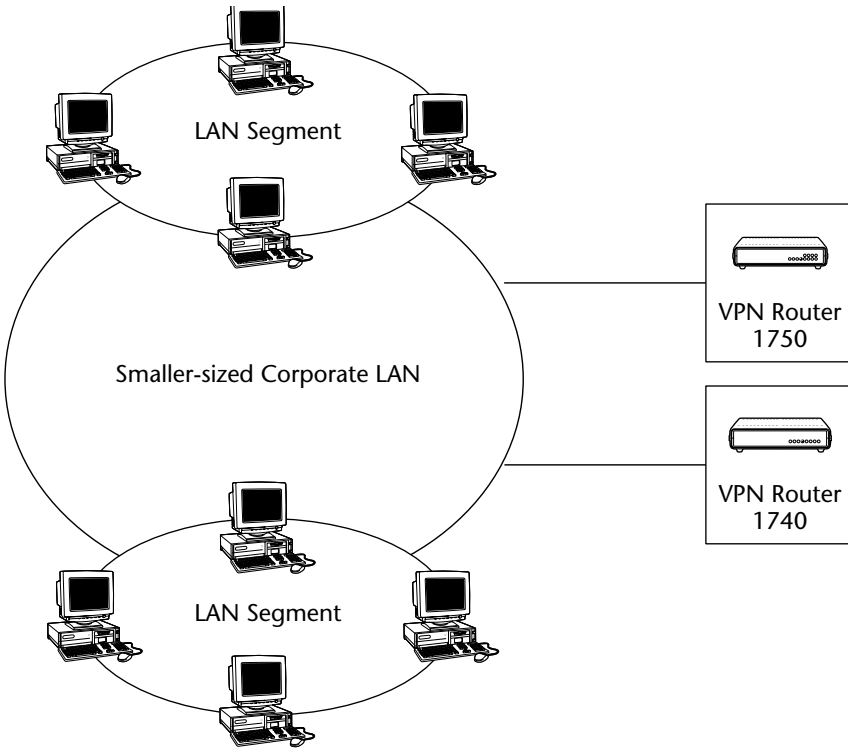


Figure 2-5: The Nortel VPN Router 1740 and 1750 are made to support smaller corporate LANs.

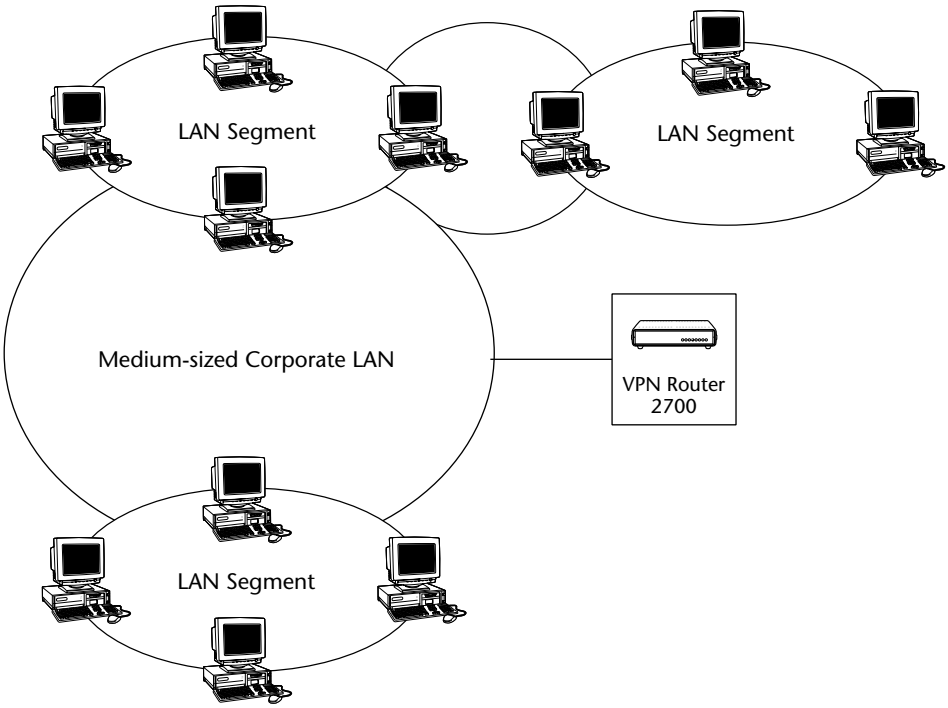


Figure 2-6: The Nortel VPN Router 2700 is a great solution for medium-sized corporate LANs.

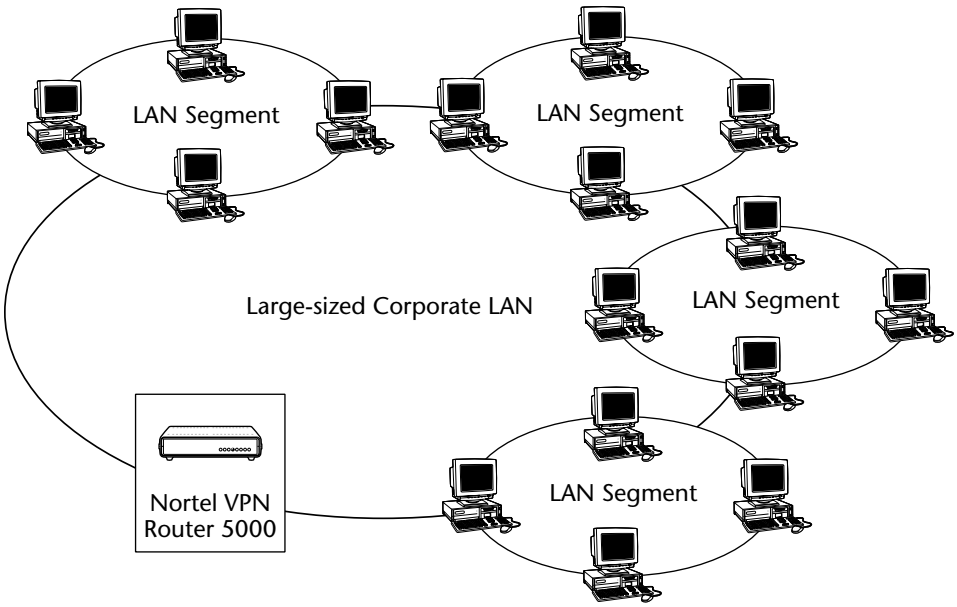


Figure 2-7: The Nortel VPN Router 5000 is designed with large corporate LANs in mind.

Overview

The VPN Router 100 provides and supports connectivity over the Internet to a LAN. It supports IPSec tunneling, encryption, authentication, and firewall protection.

The VPN Router 100 is great for smaller remote users, especially when cost is a major consideration. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment.

Remote management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices. User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

Technical Specifications

The VPN Router 100 contains 16MB of RAM and has 8MB on-board flash memory. It comes with standard User and Network Interfaces. There is one 10/100 Ethernet LAN port, along with a seven-port 10/100 Ethernet switch for users. Finally, as a standard interface, there is a serial port for out-of-band management. There are several optional interfaces for the VPN Router 100 as well. The router will support an additional 10/100 Ethernet interface, an ISDN interface, and a single or a dual analog modem. Figure 2-8 shows the VPN Router 100.

VPN Router 200 Series

The VPN Router 200 series is designed with smaller branch offices and telecommuters in mind. It is available in two models: the VPN Router 221 and the VPN Router 251.

The VPN Router 200 series provides advanced IPSec capabilities and supports up to five VPN tunnels. The VPN Router 200 series supports stateful firewall and URL/content filtering. The VPN Router 200 series also contains an integrated ADSL option.

VPN Router 221

The Nortel VPN Router 221 is designed for home-based employees and branch offices. It is a cost-effective solution that supports stateful firewall inspection, as well as Denial of Service (DoS) protection. In addition to stateful firewall and VPN services, the VPN Router 221 supports IP routing and content filtering. It is an all-in-one solution. Encryption standards that are supported on the VPN 221 are Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES).



Figure 2-8: The Nortel VPN Router 100

Overview

The VPN Router 221 provides and supports connectivity over the Internet to a LAN. It supports IPSec tunneling, encryption, authentication, and firewall protection.

The VPN Router 221 is great for smaller remote use, especially when cost is a major consideration. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment.

Remote-management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices. User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

Technical Specifications

The VPN Router 221 comes with standard user and network interfaces. There is one 10/100 Ethernet LAN port, along with a four-port 10/100 Ethernet switch for users. As a standard interface, there is a console port for out-of-band management. Figure 2-9 shows the VPN Router 221.



Figure 2-9: The Nortel VPN Router 221

VPN Router 251

The Nortel VPN Router 251 is designed for home-based employees and branch offices. It is a cost-effective solution that supports stateful firewall inspection, as well as DOS protection. In addition to stateful firewall and VPN services, the VPN Router 251 supports IP routing and content filtering. It is an all-in-one solution. Encryption standards that are supported on the VPN 251 are DES, 3DES, and AES.

Overview

The VPN Router 251 provides and supports connectivity over the Internet to a LAN. It supports IPSec tunneling, encryption, authentication, and firewall protection.

The VPN Router 251 is great for smaller remote use, especially when cost is a major consideration. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment.

Remote management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices.

User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

Technical Specifications

The VPN Router 251 comes with standard user and network interfaces. There is a four-port 10/100 Ethernet switch for users. The VPN Router 251 also has the integrated ADSL interface. As a standard interface, there is a console port for out-of-band management. Figure 2-10 shows the VPN Router 251.

VPN Router 600

The VPN Router 600 is designed to support multiple branch office-to-branch office connections, as well as being able to support LANs that require up to 50 IPSec tunnels and several WAN connections.

Overview

The VPN Router 600 provides and supports connectivity over the Internet to a LAN. It supports IPSec tunneling, encryption, authentication, and firewall protection.

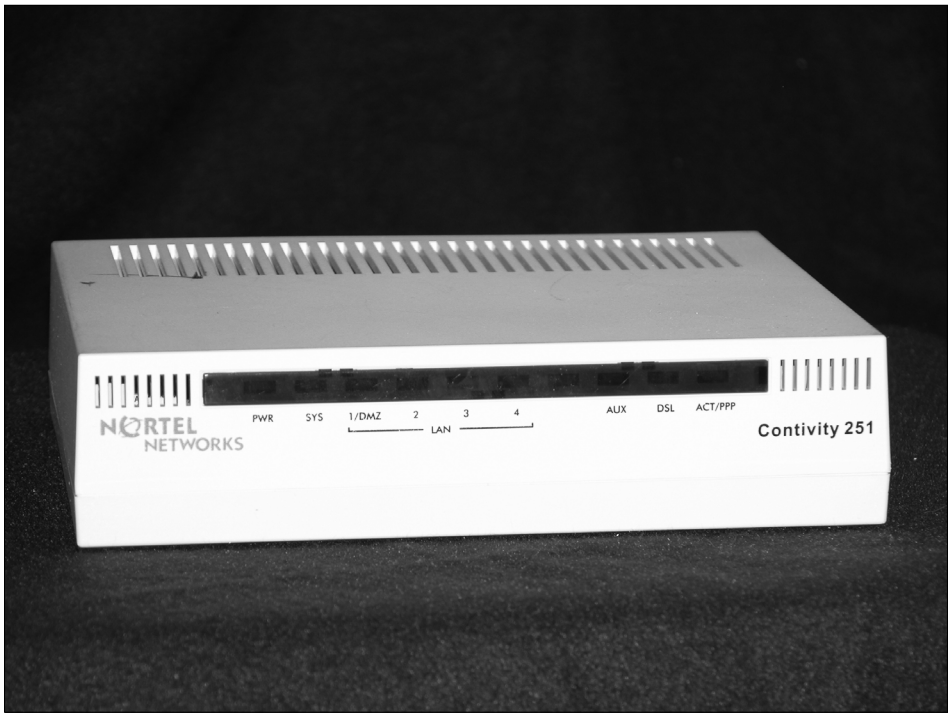


Figure 2-10: The Nortel VPN Router 251

The VPN Router 600 is great not only for branch offices, but also as either a hub or a spoke, depending on your network requirements. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment.

Remote-management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices. User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

Technical Specifications

The VPN Router 600 comes with standard user and network interfaces. There are two 10/100 Ethernet LAN ports, as well as a console port for out-of-band management. Optional interfaces include another 10/100Base-T Ethernet port, a T1/E1, V.90 Dial Modem, ADSL, and 56/64K CSU/DSU. With 128MB RAM and a PCI expansion slot, the VPN Router 600 can handle the needs of smaller VPNs. Figure 2-11 shows the VPN Router 600.



Figure 2-11: The Nortel VPN Router 600

VPN Router 1000 Series

The VPN Router 1000 series provides IPSec for branch offices that require up to 30 active tunnels. It provides advanced IPSec capabilities, as well as firewall capabilities. Advanced licensing ensures that the VPN Router 1000 series can grow to meet the needs of your network security as these needs arise. This series supports IPSec, L2TP, PPTP, and L2F tunnels. Advanced logging capabilities ensure that all traffic is logged for auditing. The VPN Router 1000 supports multiple authentication protocols, including LDAP, RADIUS, SecureID, X.509 certificates, and smart cards.

VPN Router 1010

The VPN Router is a compact solution ideal for remote offices. It can support up to five concurrent tunnels. The VPN Router 1010 comes with standard dual 10/100Base-T Ethernet ports. One of the Ethernet ports is for the private LAN and it is labeled LAN0 on the front of the VPN Router. The other Ethernet port is for the public LAN and it is labeled LAN1 on the front of the chassis.

Overview

The VPN Router 1010 provides and supports connectivity over the Internet to a LAN. It supports IPSec tunneling, encryption, authentication, and firewall protection. This router supports IP routing with load-balancing, ensuring that network traffic continues even when a problem arises. This capability supports both tunneled and non-tunneled traffic.

The VPN Router 1010 is great not only for branch offices, but also as either a hub or a spoke, depending on your network requirements. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment.

Remote-management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices. User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

Technical Specifications

The VPN Router 1010 contains 128MB of RAM and has 64MB on-board flash memory. It comes with standard user and network interfaces. There are two 10/100Base-T Ethernet LAN ports, as well as a console port for out-of-band management.

Standard software options allow for up to five VPN tunnels and RIPv2 IP routing support. Also standard is the Nortel VPN Client software with unlimited license. Optionally, there are license upgrades available to support the following:

- Advanced routing
  - OSPF
  - VRRP
  - Bandwidth management
- Data Link Switching (DLSW)
- VPN tunnel upgrade (up to 30 tunnels)
- Stateful firewall

Figure 2-12 shows the VPN Router 1010.

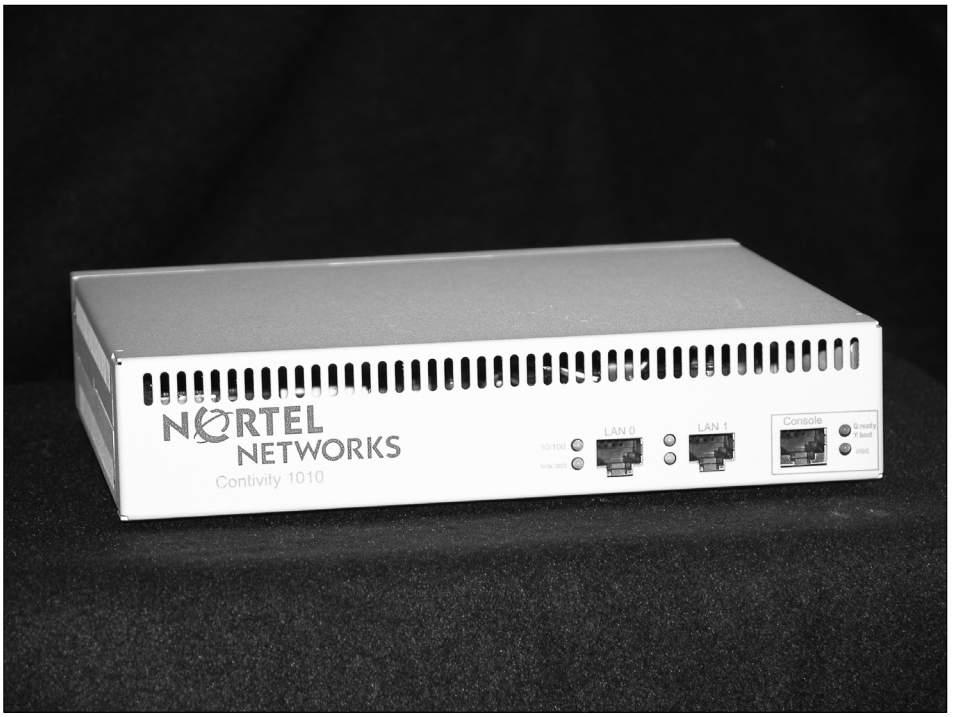


Figure 2-12: The Nortel VPN Router 1010

VPN Router 1050

The VPN Router is a compact solution ideal for remote offices. It can support up to five concurrent tunnels. The VPN Router 1050 comes with a standard single 10/100Base-T Ethernet port. In addition to the single Ethernet port, the 1050 also includes an internal auto-negotiating 10/100 four-port Ethernet switch. The four-port switch is the private-side LAN0 interface, and the single port is the public-side interface.

Overview

The VPN Router 1050 provides and supports connectivity over the Internet to a LAN. It supports IPSec tunneling, encryption, authentication, and firewall protection. This router supports IP routing with load-balancing, ensuring that network traffic continues even when a problem arises. This capability supports both tunneled and non-tunneled traffic.

The VPN Router 1050 is great not only for branch offices, but also as either a hub or a spoke, depending on your network requirements. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment.

Remote-management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices. User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

Technical Specifications

The VPN Router 1050 contains 128MB of RAM and has 64MB on-board flash memory. It comes with standard user and network interfaces. There is one 10/100Base-T Ethernet LAN port, a four-port 10/100 Ethernet switch, as well as a console port for out-of-band management.

Standard software options allow for up to five VPN tunnels and RIPv2 IP routing support. Also standard is the Nortel VPN Client software with unlimited license. Optionally, there are license upgrades available to support the following:

- Advanced routing
  - OSPF
  - VRRP
  - Bandwidth management
- DLSW
- VPN tunnel upgrade (up to 30 tunnels)
- Stateful firewall

Figure 2-13 shows the VPN Router 1050.



Figure 2-13: The Nortel VPN Router 1050

VPN Router 1100

Just like the VPN Router 1050, the VPN Router 1100 is a compact solution ideal for remote offices. It can support up to five concurrent tunnels. The VPN Router 1100 comes with a standard single 10/100Base-T Ethernet port. In addition to the single Ethernet port, the 1050 also includes an internal auto-negotiating 10/100 four-port Ethernet switch. Finally, the VPN Router 1100 includes two PCI slots to accommodate optional solutions. The four-port switch is the private-side LAN0 interface, and the single port is the public-side interface.

Overview

The VPN Router 1100 provides and supports connectivity over the Internet to a LAN. It supports IPSec tunneling, encryption, authentication, and firewall protection. This router supports IP routing with load-balancing, ensuring that network traffic continues even when a problem arises. This capability supports both tunneled and non-tunneled traffic.

The VPN Router 1100 is great not only for branch offices, but also as either a hub or a spoke, depending on your network requirements. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment.

Remote-management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices. User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

Technical Specifications

In addition to 228MB of RAM and 64MB on-board flash memory, the VPN Router 1100 also has two PCI expansion slots. It supports one 10/100Base-T Ethernet LAN port, and has a four-port 10/100 Ethernet switch, as well as a console port for out-of-band management. Optional interfaces include another 10/100Base-T Ethernet port, T1/E1, ADSL, and 56/64K CSU/DSU.

Standard software options allow for up to five VPN tunnels and RIPv2 IP routing support. Also standard is the Nortel VPN Client software with unlimited license. Optionally, license upgrades are available to support the following:

- Advanced routing
  - OSPF
  - VRRP
  - Bandwidth management
- DLSW
- VPN tunnel upgrade (up to 30 tunnels)
- Stateful firewall

Figure 2-14 shows the VPN Router 1100.

VPN Router 1700 Series

The VPN Router 1700 series supports up to 500 tunnels and is designed with larger branch offices and campuses in mind. Advanced licensing ensures that the VPN Router 1700 series can support current network configurations and can grow to meet the needs of your network security as these needs arise. Like the VPN Router 1000 Series, this series supports IPSec, L2TP, PPTP, and L2F tunnels. Advanced logging capabilities ensure that all traffic is logged for auditing. The VPN Router 1700 supports multiple authentication protocols, including LDAP, RADIUS, SecureID, X.509 certificates, and smart cards.

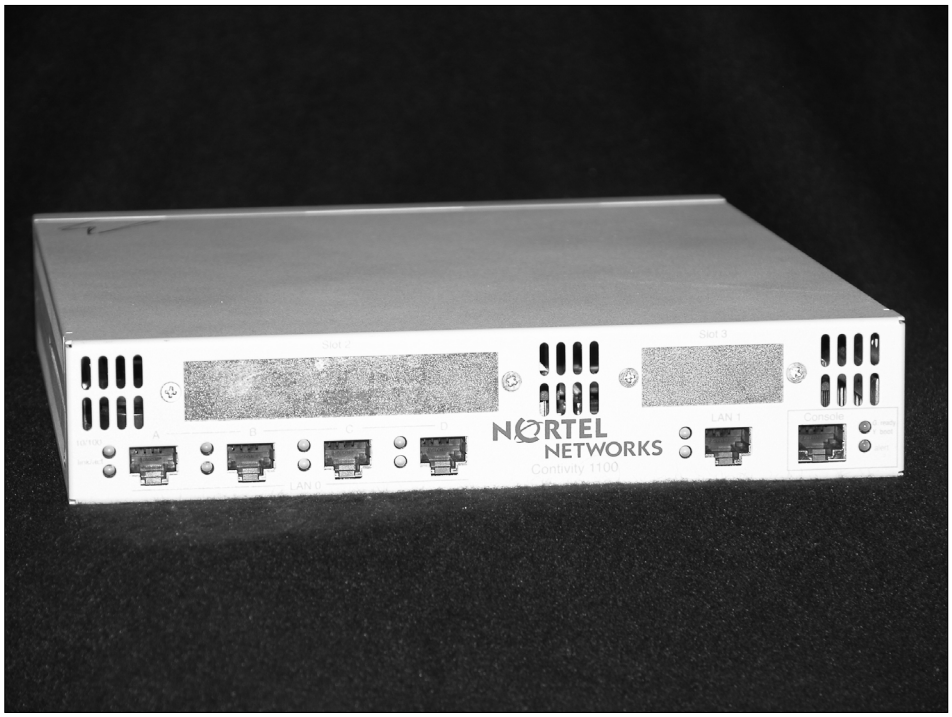


Figure 2-14: The Nortel VPN Router 1100

VPN Router 1700

The VPN Router 1700 supports up to 500 tunnels. It supports IPSec, PPtP, L2TP, and L2F tunneling, encryption, authentication, and firewall protection. This router supports IP Routing with load-balancing, ensuring that network traffic continues even when a problem arises. This capability supports both tunneled and non-tunneled traffic.

The VPN Router 1700 is great for campuses that require up to 500 tunnels. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment. It supports secure IP access, full VPN services, and stateful firewall.

Remote-management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices. User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

VPN Router 1740

The VPN Router 1740 is a compact solution ideal for large remote offices and small LAN campuses. It comes in two models: the VPN Bundle and the Secure Router Bundle. The VPN Bundle can support up to five concurrent tunnels and the Secure Router Bundle can support up to 500 concurrent tunnels. The VPN bundle also comes with two 10/100Base-T Ethernet ports and three PCI expansion slots for optional standards. The Secure Router Bundle comes standard with one 10/100Base-T Ethernet port and four expansion slots.

Overview

The VPN Router 1740 can support up to 500 tunnels. It supports IPSec, PPtP, L2TP, and L2F tunneling, encryption, authentication, and firewall protection. This router supports IP routing with load-balancing, ensuring that network traffic continues even when a problem arises. This capability supports both tunneled and non-tunneled traffic.

The VPN Router 1740 is great for campuses that require up to 500 tunnels. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment. It supports secure IP access, full VPN services, and stateful firewall.

Remote-management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices. User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

Technical Specifications

In addition to 128MB of RAM (upgradeable to 256MB), the VPN Router 1740 also has two 10/100Base-T Ethernet ports (VPN Bundle) or one 10/100Base-T Ethernet port (Secure Router Bundle). It has three expansion slots (VPN Bundle) and four expansion slots (Secure Router Bundle), as well as a console port for out-of-band management. Optional interfaces include another 10/100Base-T Ethernet port, T1/E1, ADSL, 56/64K CSU/DSU, V.90 dial modem, and 100Base-T or 100Base-SX Ethernet.

Standard software options are the Secure Router Bundle, which allows for up to 5 VPN tunnels and RIPv2 IP Routing support. Also standard is the Nortel VPN Client software with unlimited license. The other software standard option is the VPN Bundle, which supports up to 500 VPN tunnels and RIPv2 support, as well as the VPN Client software package.

Optionally, there are license upgrades available to support the following:

- Advanced routing
  - OSPF
  - VRRP
  - Bandwidth management
- DLSW
- VPN tunnel upgrade (up to 500 tunnels)
- Stateful firewall

Figure 2-15 shows the VPN Router 1740.

VPN Router 1750

The VPN Router 1750 is a solution ideal for large remote offices and small LAN campuses. The VPN Router 1750 comes with two 10/100Base-T Ethernet ports and four PCI expansion slots for optional standards.



Figure 2-15: The Nortel VPN Router 1740

Overview

The VPN Router 1750 supports up to 500 tunnels. It supports IPSec, PPtP, L2TP, and L2F tunneling, encryption, authentication, and firewall protection. This router supports IP routing with load-balancing, ensuring that network traffic continues even when a problem arises. This capability supports both tunneled and non-tunneled traffic.

The VPN Router 1750 is great for campuses that require up to 500 tunnels. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment. It supports secure IP access, full VPN services, and stateful firewall.

Remote-management access is supported on this router, which is a huge benefit, especially when the corporate LAN supports multiple remote offices. User access through an Internet Branch Office Tunnel is made available without any changes to current remote LAN applications and configurations.

Technical Specifications

In addition to 128MB of RAM (upgradable to 256MB), the VPN Router 1750 also has two 10/100Base-T Ethernet ports, has four expansion slots, and a console port for out-of-band management. Optional interfaces include another 10/100Base-T Ethernet port, T1/E1, ADSL, 56/64K CSU/DSU, V.90 dial modem, and 100Base-T or 100Base-SX Ethernet.

Standard software options allow for up to five VPN tunnels and RIPv2 IP routing support. Also standard is the Nortel VPN Client software with unlimited license.

Optionally, there are license upgrades available to support the following:

- Advanced routing
  - OSPF
  - VRRP
  - Bandwidth management
- DLSW
- VPN tunnel upgrade (up to 500 tunnels)
- Stateful firewall

Figure 2-16 shows the VPN Router 1750.

VPN Router 2700

The VPN Router 2700 is a VPN solution ideal for medium- to large-sized LAN campuses. The VPN Router 2700 can support up to 2,000 concurrent tunnels. Optional software licensing can ensure that the VPN Router 2700 can support your network as an IP router, a dedicated VPN switch, a firewall solution, or any combination of these.



Figure 2-16: The Nortel VPN Router 1750

Overview

The VPN Router 2700 supports up to 2,000 tunnels. It supports IPSec, PPTP, L2TP, and L2F tunneling, encryption, authentication, and firewall protection. This router supports IP routing with load-balancing, ensuring that network traffic continues even when a problem arises. This capability supports both tunneled and non-tunneled traffic.

The VPN Router 2700 is designed with large organizations in mind. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment. It supports secure IP access, full VPN services, and stateful firewall.

Technical Specifications

In addition to 256MB of RAM (upgradable to 512MB) the VPN Router 2700 also has a 1.33 GHz processor, three PCI slots, and an optional SSL VPN module. The router has two standard 10/100Base-T Ethernet ports and a console port for out-of-band management. Optional interfaces include another 10/100Base-T Ethernet port, T1/E1 w CSU/DSU, ADSL, 56/64K CSU/DSU, V.90 dial modem, and a HighSpeed Serial Interface (HSSI).

Standard software options include the Secure Router Bundle (which allows for up to five VPN tunnels and RIPv2 IP routing support) and the VPN Bundle (which includes support for 2,000 VPN Tunnels with RIPv2 support). Standard with each package is the Nortel VPN Client software with unlimited license.

Optionally, there are license upgrades available to support the following:

- Advanced routing
  - OSPF
  - VRRP
  - Bandwidth management
- DLSW
- VPN tunnel upgrade (up to 2000 tunnels)
- Stateful firewall

Figure 2-17 shows the VPN Router 2700.



Figure 2-17: The Nortel VPN Router 2700

VPN Router 5000

Optional software licenses ensure that the VPN Router 5000 can support numerous functions in an enterprise LAN. It can serve as an IP router, a VPN solution, a firewall solution, and any combination of these. The VPN 5000 can support 5,000 concurrent tunnels, and it does include hardware redundancy. The VPN Router 5000 includes standard an 10/100Base-T Ethernet port, as well as a 10/100/1000Base-T (GigE) Ethernet port.

Overview

The VPN Router 5000 supports up to 5,000 tunnels. It supports IPSec, PPTP, L2TP, and L2F tunneling, encryption, authentication, and firewall protection. This router supports IP routing with load-balancing, ensuring that network traffic continues even when a problem arises. This capability supports both tunneled and non-tunneled traffic.

The VPN Router 5000 is designed with large organizations in mind. It gives the security and encryption necessary to maintain security without requiring any additional external networking equipment. It supports secure IP access, full VPN services, and stateful firewall.

Technical Specifications

In addition to 512MB of RAM (upgradable to 1.5GB) the VPN Router 5000 also has dual 2.2 GHz processors, five PCI slots, an optional SSL VPN module, one standard Encryption Accelerator Module (with an optional second Accelerator Module), dual power supplies (hot-swappable), and dual hard disk drives. The router has a standard 10/100/1000Base-T Ethernet port, one 10/100Base-T Ethernet port, and a console port for out-of-band management. Optional interfaces include another 10/100Base-T Ethernet port, T1/E1 w CSU/DSU, ADSL, 56/64K CSU/DSU, V.90 dial modem, and a High-Speed Serial Interface (HSSI).

Standard software options include support for 5,000 VPN Tunnels with RIPv2 support. Standard with each package is the Nortel VPN Client software with unlimited license.

Optionally, there are license upgrades available to support the following:

- Advanced routing
  - OSPF
  - VRRP
  - Bandwidth management
- DLSW
- Windows Mobile
- Stateful firewall

Figure 2-18 shows the VPN Router 5000.



Figure 2-18: The Nortel VPN Router 5000

VPN Router Features Comparison

Tables 2-1 through 2-3 are three comparison charts for the VPN Router family. This section is to serve as a quick reference for the standard and optional solutions that are offered within the VPN Router family.

Table 2-1: Comparison Chart of Standard Options

PLATFORM	MEMORY	PCI EXPANSION SLOTS	PROCESSOR TYPE	10/100BASE-T STANDARD PORTS	CONSOLE PORT	NUMBER OF TUNNELS	REDUNDANT SLOTS
VPN Router 1005	16MB RAM, 8MB Flash	None	300 MHz Pentium	1	Yes		None
VPN Router 221	16MB RAM, 4MB Flash	None	100 MHz MIPS	None	Yes	5	None
VPN Router 251	16MB RAM, 4MB Flash	None	166 MHz ARM	None	Yes	5	None
VPN Router 600	128MB RAM	1	300 MHz Celeron	2	Yes	50	None
VPN Router 1010	128MB RAM, 64MB Flash	None	300 MHz Celeron	2	Yes	30	None
VPN Router 1050	128MB RAM, 64MB Flash	None	300 MHz Celeron	2	Yes	30	None
VPN Router 1100	128MB RAM, 64MB Flash	2	300 MHz Celeron	2	Yes	30	No
VPN Router 1700	128–256MB RAM	1	850 MHz Pentium III	2	Yes	500	No
VPN Router 1740	128–256MB RAM	3–4	850 MHz Pentium III	2 – 1	Yes	500	No
VPN Router 1750	128–256MB RAM	4	850 MHz Pentium III	2	Yes	500	No
VPN Router 2700	256–512MB RAM	3	1.33 GHz Pentium III	2	Yes	2000	No
VPN Router 5000	512MB–1.5GB RAM	5	Dual 2.2 GHz Intel	1	Yes	5000	Yes

Table 2-2: Comparison Chart of Supported, Optional Equipment (Part 1)

PLATFORM	OPTIONAL 10/100BASE-T PORTS?	GIG ETHERNET?	T1/E1 CSU/DSU?	56K/64K CSU/DSU?	HSSI?
VPN Router 100	Yes	No	No	No	No
VPN Router 221	No	No	No	No	No
VPN Router 251	No	No	No	No	No
VPN Router 600	Yes	No	Yes	Yes	No
VPN Router 1010	No	No	No	No	No
VPN Router 1050	No	No	No	No	No
VPN Router 1100	Yes	No	Yes	Yes	No
VPN Router 1700	Yes	No	Yes	Yes	Yes
VPN Router 1740	Yes	Yes	Yes	Yes	Yes
VPN Router 1750	Yes	Yes	Yes	Yes	Yes
VPN Router 2700	Yes	Yes	Yes	Yes	Yes
VPN Router 5000	Yes	Yes	Yes	Yes	Yes

Table 2-3: Comparison Chart of Supported, Optional Equipment (Part 2)

PLATFORM	ADSL?	SSL?	ACCELERATOR?	V.90 MODEM?	ISDN BRI?
VPN Router 100	No	No	No	Yes	Yes
VPN Router 221	No	No	No	No	No
VPN Router 251	Yes	No	No	No	No
VPN Router 600	Yes	No	No	Yes	Yes

(continued)

Table 2-3: *(continued)*

PLATFORM	ADSL?	SSL?	ACCELERATOR?	V.90 MODEM?	ISDN BRI?
VPN Router 1010	No	No	No	No	No
VPN Router 1050	No	No	No	No	No
VPN Router 1100	Yes	No	No	Yes	Yes
VPN Router 1700	Yes	No	Yes	Yes	Yes
VPN Router 1740	Yes	Yes	Yes	Yes	Yes
VPN Router 1750	Yes	Yes	Yes	Yes	Yes
VPN Router 2700	Yes	Yes	Yes	Yes	Yes
VPN Router 5000	Yes	Yes	Yes	Yes	Yes

Deployment Examples

Nortel VPN Routers can be deployed in three different configurations. This section discusses the following three deployment strategies:

- The Branch Office Tunnel (BOT) VPN Solution
- The Extranet VPN Solution
- The Remote Access VPN Solution

Branch Office Tunnel VPN Solution

Many companies have offices located across the world. The need to provide real-time data to all of these offices, while guaranteeing data security and data integrity, is paramount. The Nortel VPN Routers can do the job.

Remote offices must be able to connect to each other and to the corporate LAN in a secure manner. Corporate data must remain secure, and a VPN Router can provide the necessary security. To be able to provide the data to the remote office and keep it hidden from the rest of the Internet is important.

The Branch Office Tunnel (BOT) VPN solution allows for the transfer of data communication over the Branch Office Tunnel instead of relying on traditional dial access and leased line configurations. This means that the Branch Office Tunneling solution is a high-speed, very cost effective model. Figure 2-19 shows an example of a Branch Office Tunnel implementation.

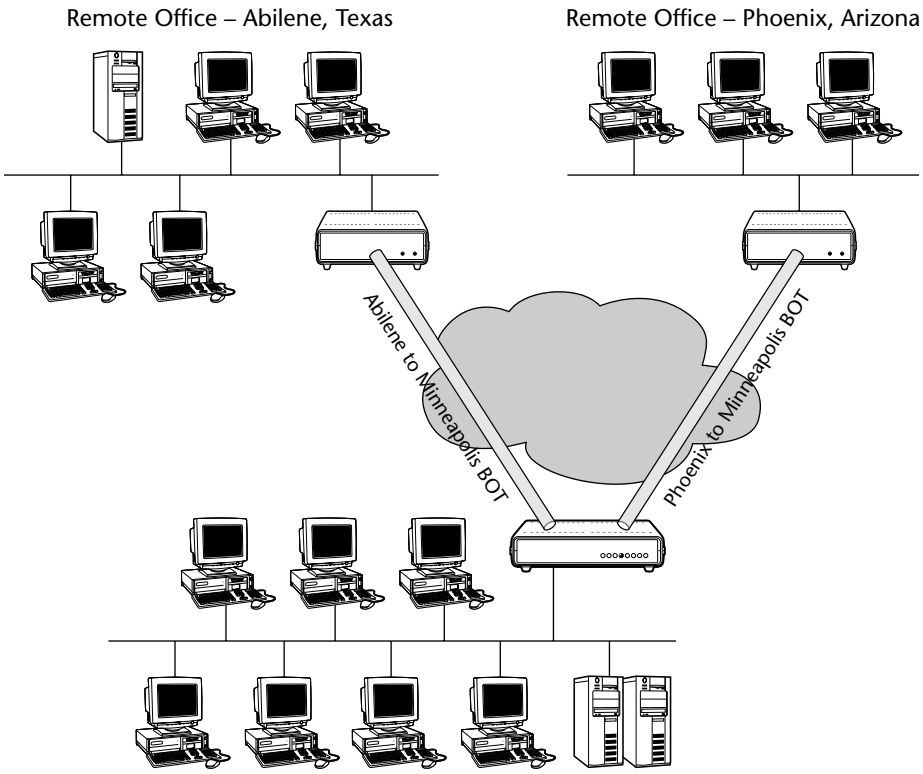


Figure 2-19: An example of a Branch Office Tunnel VPN solution

Extranet VPN Solution

In LANs today, the term "intranet" describes the standards that are implemented that make up the corporate LAN. It is a privately owned and maintained data network that is accessible only by authorized individuals, usually employees of the company. An "extranet" is an extension of the traditional intranet. It allows access over a WAN to the LAN. An extranet is mainly used by individuals that deal with the company daily. It allows access to specific network services on the intranet, while blocking access to other services.

Companies that need to share data or process business transactions can easily do so through their own intranet by implementing an Extranet VPN solution. This can cut down on the amount of time it takes to process these transactions, as well as providing security in the process.

Extranet solutions typically implement firewalls to protect the internal resources. Certificates and security keys can be exchanged to ensure that the data is accessed by the correct individuals and that other data cannot be accessed.

To implement an Extranet solution, both companies must coordinate the setup. Firewalls must be established on both sides to ensure that internal data remains secure and shared data can be accessed. Figure 2-20 shows an example of two Extranet solutions. One extranet connects Widgets, Inc., to the Wget Supply Company (a supplier). The other extranet connects Widgets, Inc., to Wid4ever, a business partner.

Remote Access VPN Solution

The Remote Access VPN Solution is implemented to allow users who work remotely (a home-based office) and those that are traveling a secure method to access network services over the Internet. This is a very cost-effective, safe, and secure solution.

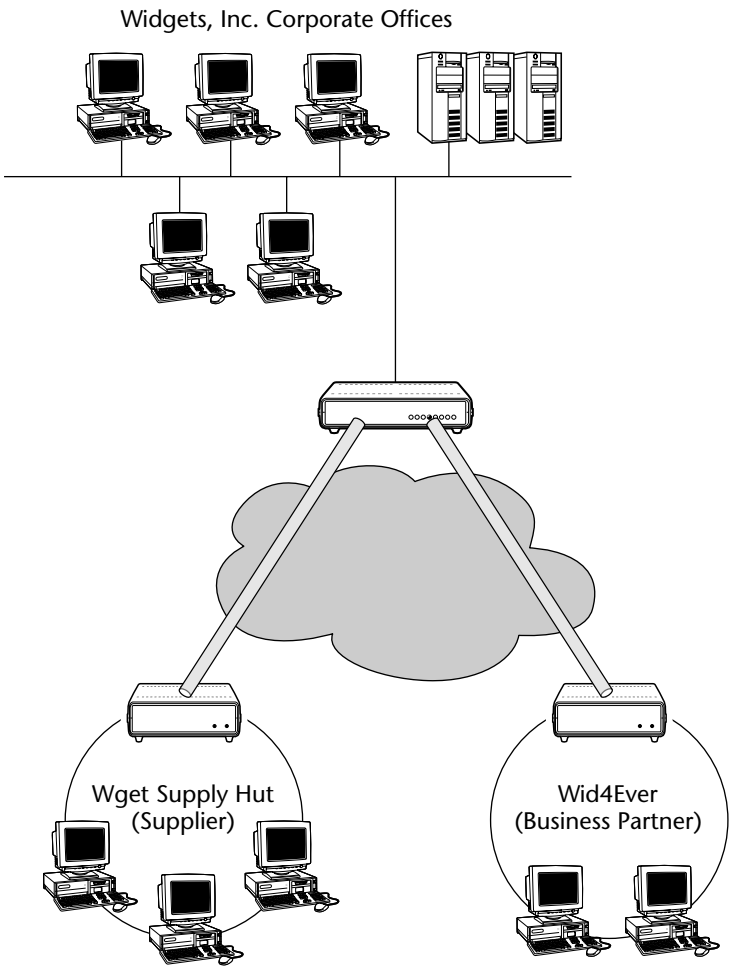


Figure 2-20: An example of an Extranet VPN solution

Remote users access the Internet through their service provider and then establish a secure tunnel to the corporate network. The session is encrypted and authentication is performed to ensure data integrity and security. This allows the remote user access to all network services without jeopardizing data security.

An example of a company that could find a need for a Remote Access solution is one that has a large field sales base. Imagine how much productivity can be gained by enabling employees to access their network 24/7 from almost anywhere in the world. Figure 2-21 shows an example of a Remote Access VPN solution.

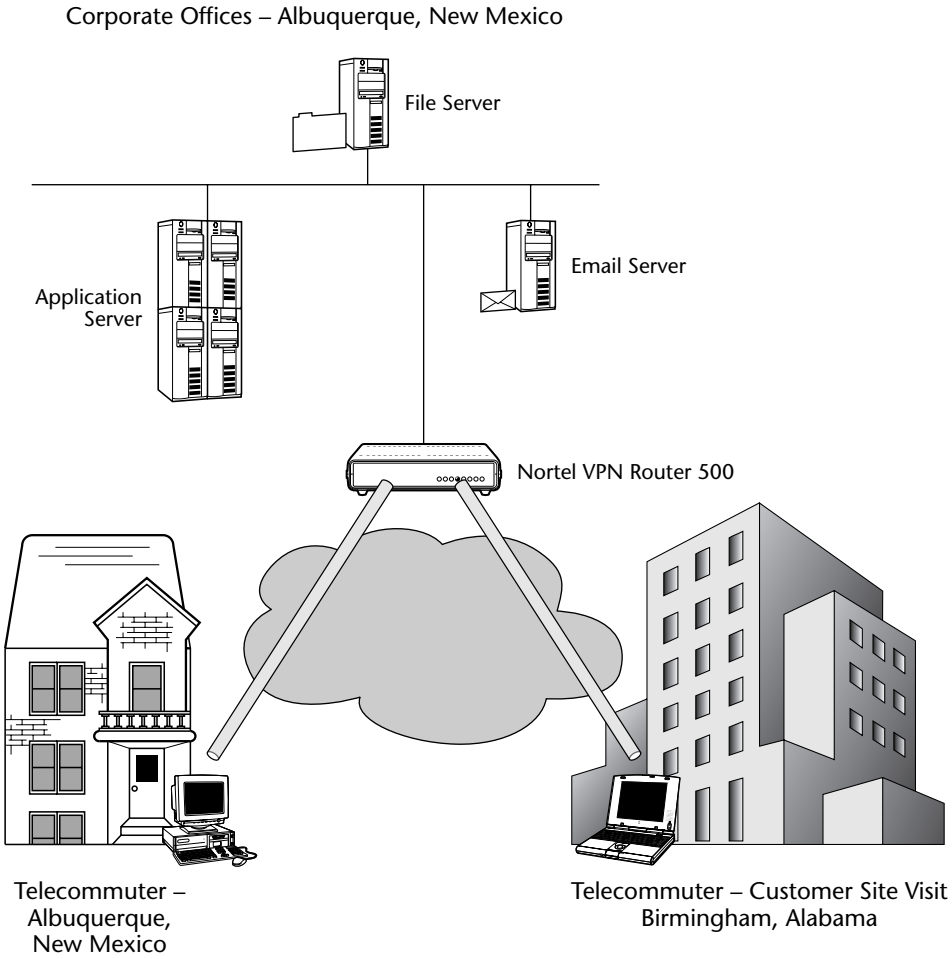


Figure 2-21: An example of a Remote Access VPN solution

Summary

This chapter discussed the Nortel VPN Router portfolio. The options and standards that are available to each of the routers in this portfolio were discussed as well.

Whether you are looking for a VPN solution or are considering taking the Nortel certification exams, this chapter provided you with all you need to understand the VPN routing solutions that are offered by Nortel.

This chapter also built the foundation that you will need to firmly grasp some of the other concepts that are introduced in the remaining chapters of this book.

CHAPTER

3

The Nortel VPN Router Software Overview

In data communications, the hardware that is used for interfacing with other hardware to allow information to be developed and shared between end users is a very important part of the equation. Without a keyboard, it would be very diffucult for us (as end users) to be able to enter our information into the computer. Without a monitor, it would be virtually impossible to determine what application we are accessing and what field the computer is waiting for us to fill out. Also essential is a computer that is fundamental in data communication, as well as the router, the switch, the hub, cables, and so on.

An equally important (if not more important) piece of the data communications equation is the software that is used to allow for data communications. *Software* is a set of written programs and instructions that control the functioning of the hardware and its associated operations. Without software, the hardware would be nothing more than expensive space fillers.

Chapter 2 discussed the Nortel VPN Router hardware solutions for VPN networking. We have discussed the various platforms in the VPN Router family, and we also discussed some of the standard and optional features of each of the routers in the VPN Router portfolio. This chapter discusses the software used to give the routers the instructions they need to perform the standards and optional functions they are designed to support.

Nortel VPN Software

Nortel VPN Software solutions are used to facilitate the functionality of the Nortel VPN Routers (Contivity Secure IP Services Gateway), as well as the Nortel VPN Client that is loaded on end user PCs. This software is necessary to complete your VPN solution.

When purchasing a Nortel VPN Router, the router will come preloaded with the latest version of code. The Nortel VPN Client software is included on a CD, as well as other important documentation. Nortel also offers software and documentation downloads on its main Web site, `www.nortel.com`.

Occasionally software functionality does not meet the needs of the environment in which it is being used. There are also times when a new protocol or a standard is introduced that must be supported. Because of this, Nortel does produce upgrades on occasion to meet the needs of the networks it supports. This chapter discusses some of the features of software for both the client and the router.

NOTE **In this chapter, the Contivity Secure IP Services Gateway is referred to as the VPN Router software.**

The Nortel VPN Router software supports a number of features to meet the growing demands of networks today. As new features are introduced in data communications worldwide, Nortel adjusts to meet these needs. The Nortel VPN software supports some basic features, as well as some advanced features that require a license key to access and utilize.

Accounting Services

The router software provides detailed accounting features that enable network administrators to monitor and obtain historical records vital to the safety and security of the VPN Router. It allows administrators to set up automatic logging to external devices, support for internal and external Radius logging, and system event logging services.

Bandwidth Management Services

The Nortel VPN Router software supports all facets of bandwidth management and Quality of Service (QoS) to ensure reliable delivery of data traffic. Minimum bandwidth requirements can be configured based on individual as well as group settings. This allows network administrators a lot of flexibility in determining the traffic flows that are supported by the VPN Router, ensuring

that the bandwidth is allocated to those that need it most. Other supported services include the following:

- Differentiated Services (DiffServ)
- Multi-Level Random Early Detection (MRED)
- Resource Reservation Protocol (RSVP)

Certifications

The following security certifications are supported by the Nortel VPN Router software:

- Federal Information Processing Standard (FIPS) 140-2
- International Computer Security Association (ICSA) 1.0d
- Virtual Private Network Consortium (VPNC)

Encryption Services

Encryption in data communications is the way in which information is altered to hide the original data in an unreadable format. Used in conjunction with other standards, it assists in securing data transmissions. The following encryption standards are supported by the Nortel VPN Router software:

- Advanced Encryption Standard (AES); 128-bit
- Advanced Encryption Standard (AES); 256-bit
- ARCFOUR (RC4)
- Data Encryption Standard (DES)
- Triple Data Encryption Standard (3DES)

IP Routing Services

Routing services are a very important part of internetwork communications. Following are the routing protocols that are supported by the Nortel VPN Routers:

- Border Gateway Protocol (BGP) version 4
- Data Link Switching (DLSw)
- Dynamic Routing over IPSec
- Open Shortest Path First (OSPF) version 2

- Routing Information Protocol (RIP) version 1
- Routing Information Protocol (RIP) version 2
- Virtual Locate Area Network (VLAN) 802.1Q
- Virtual Router Redundancy Protocol (VRRP)

Management Services

Access to the VPN Router and the management of the VPN Router is available through multiple modes. Management of the VPN Router can be performed whether you are local to the VPN Router or not. Management of the VPN Router includes access for configuration and monitoring, as well as tools supported to verify the VPN Router integrity. Following are the various ways of managing the VPN Router:

- Command Line Interface (CLI)
- Easy Install utility
- Multi-Element Manager
- Simple Network Management Protocol (SNMP) monitoring
- Web browser GUI

Stateful Firewall

A *stateful firewall* is a firewall that keeps track of the state of the network and its associated connections. It compares packets with one another and is able to recognize packets with a known connection state. More than 100 network application protocols are recognized and supported by the stateful firewall.

User Authentication

The Nortel VPN Router software supports a number of user-authentication protocols and standards. Among these are the following:

- External Lightweight Directory Access Protocol (LDAP)
- Hard Token Support
- Internal LDAP
- Remote Authentication Dial-In User Services (RADIUS)
- Soft Token Support
- X.509 Digital Certificates

VPN Tunneling Protocols

The following VPN tunneling protocols are supported:

- Internet Protocol Security (IPSec)
- Layer 2 Tunneling Protocol (L2TP)
- Point to Point Tunneling Protocol (PPTP)
- Secure Sockets Layer (SSL) Services

Secure Sockets Layer Services

With the appropriate hardware and licensing, the Nortel VPN Router software will support the SSL standard. SSL is a cryptographic protocol that provides secure communications over the Internet.

WAN Services

Several wide area network (WAN) protocols and standards are supported by the Nortel VPN Router software. These network protocols and standards are a must for communication with Internet devices. Following are the supported protocols and standards:

- Asymmetric Digital Subscriber Line (ADSL)
- Dial Backup
- Dial on Demand
- Frame Relay
- Point to Point Protocol (PPP)
- Point to Point Protocol over Ethernet (PPPoE)

VPN Router Software Version 6.00

As with the previous versions of software, the Nortel VPN Router software is also known as the Contivity Secure IP Services Gateway. The VPN Router software provides the instructions necessary for the VPN Router to perform its functions.

The latest version of VPN Router software is version 6.00. The following VPN Routers are supported by this version of software:

- Nortel VPN Router 1010
- Nortel VPN Router 1050

- Nortel VPN Router 1100
- Nortel VPN Router 600
- Nortel VPN Router 1700
- Nortel VPN Router 1740
- Nortel VPN Router 1750
- Nortel VPN Router 2700
- Nortel VPN Router 5000

Memory Requirements

The Nortel VPN Router software version 6.00 requires at least 128MB of memory to operate. This amount is determined based on the features that are being supported in the environment in which the VPN Router is being used. The more functions the VPN Router is required to perform, the more memory that will be used. Nortel provides tools that assist in determining the memory requirements for the services the VPN Routers support.

Optional Software Licenses

Nortel VPN Routers are shipped ready to support the basic features of the VPN Router. Nortel also provides optional licensing for advanced features. The optional licensing helps keep the costs down on advanced services that not all users will have the need for. License keys may be purchased to allow support for the following:

- Advanced router features
- Contivity stateful firewall features
- Additional VPN tunnel features

Nortel VPN Router software contains basic features that provide support to meet the needs of most networks that it supports. On occasion, network administrators have requirements for support of some of these advanced features. The advanced feature support is not included in the basic software release because not every network has the need for the optional services and therefore should not have to pay for those services.

Advanced Router License Key

The Advanced Router License key is required for environments where advanced routing features are required. These features include the following:

- OSPF
- VRRP
- IP multicasting
- Bandwidth management

Contivity Stateful Firewall License Key

If you want to utilize the Contivity Stateful Firewall solution on your VPN Router, the stateful firewall key is required.

Additional VPN Tunnel Support License Key

If you have the need to support additional tunnels, you can purchase a license key that will support the maximum number of tunnels for the VPN Router that you are using. The additional tunnels are part of the VPN bundle software.

Features Introduced in VPN Router Version 6.00

The Nortel VPN Router software version 6.00 introduces support for many routing, safety, and security protocols and standards. The features supported ensure that the Nortel VPN Router is capable of supporting all data and voice communication needs of the LANs that it supports. All of these features are discussed in detail in upcoming chapters. Following is a brief overview of some of these new features:

- *Advanced Encryption Standard (AES):* The Advanced Encryptions Standard (AES) is an encryption standard that is used in many networks. It is a very fast standard and is easy to implement. AES has a fixed block size of 128 bits and it comes in three key sizes. The supported key sizes are 128 bits, 192 bits, and 256 bits. VPN Router software version 6.00 includes support for a key size of 256 for branch office tunnels.
- *Cone Network Address Translation (NAT):* Network Address Translation (NAT) is a protocol that is used to rewrite the source/destination addresses of IP packets as the packet passes through a router. NAT is commonly used to allow multiple hosts on a private LAN access to the Internet using a single public IP address. Cone NAT is used by the Voice over IP (VOIP) protocol to fix potential address and port discovery transversal issues.
- *Border Gateway Protocol (BGP) version 4:* The Border Gateway Protocol (BGP) is a routing protocol that is used over the Internet to ensure network communications can be routed between *Autonomous Systems (AS).*

BGP makes routing decisions based on network policies and/or rules. BGP version 4 supports classless routing between domains, as well as supporting route aggregation.

- *Demand Services:* Demand Services is a feature that supports both backup interfaces and dial-on-demand services. These are backup services that will bring up an alternate interface in case the main interface fails. When using backup interfaces, the backup interface will come up as soon as the primary connection fails. Dial-on-demand services will activate a dial interface when the primary connection fails.
- *Institute of Electrical and Electronics Engineers (IEEE) 802.1Q Phase 2:* Nortel VPN Router software version 6.00 enables support for several features within the Institute of Electrical and Electronics Engineers (IEEE) standard 802.1Q. VRRP support on a VLAN basis is now supported. Also, firewall and stateful firewall policies are now configurable on a per-VLAN basis. Finally, Asymmetric Branch Office Tunnels (ABOT) is now a configurable service on a per-VLAN basis.
- *Management Virtual Address (MVA):* A Management Virtual Address (MVA) is a *Circuitless IP (CLIP)* address that is used for management of the VPN Router. This ensures that management to the VPN Router can be obtained through any physical interface on the VPN Router and removes the possibility of losing remote management should the management subnet interface fail.
- *Multinetting:* Multinetting provides the network administrator with the ability to assign up to eight IP addresses on a single Ethernet interface. The first address is the primary subnet address, and all of the other configured addresses are secondary addresses. All of the security rules that are applied to the interfaces are shared and are configured for the primary subnet.

Loading, Verifying, and Upgrading the VPN Router Software

When operating the Nortel VPN Router within your LAN, it is important that you understand the code version that you are running. Understanding the features that are supported in a version of code is very important. It is also important to understand any potential limitations in the code version that you are running.

This section covers how to verify the code version that you are running, how to push new versions to your VPN Router, and how to upgrade to a new version.

Release Notes

Contained on the CD-ROM that comes with the VPN Router software are the release notes for the client that you will be loading. You can also download the release notes from the Nortel Web site (`www.nortel.com`). It is always important to review the release notes to assist you in determining what code version is suitable for your needs. The client release notes will inform you of important information that is necessary for you to understand. Following is some of the information included within the VPN client software release notes:

- Copyright information
- Trademark information
- Software licensing agreement
- Table of contents
- The Personal Computer (PC) operating systems that are supported
- The enhancements that are included in the version of code
- Known issues (commonly referred to as "bugs") with the code version
- Important considerations that must be taken into account with that particular version of code

On minor code revisions, the release notes will normally include only any enhancements and known issues. The release notes are typically in PDF format, but are occasionally provided in a Microsoft Word or text document.

Loading a New Version of VPN Router Software

The Nortel VPN Router comes preloaded with the most current version of code. Periodically, a new version of code comes out. The new release will most likely have bug fixes, as well as new enhancements and new functionality. If you are administrating a Nortel VPN Router, then most likely you will be involved in a code upgrade at some point. This section examines the necessary steps that must be taken to successfully upgrade your VPN Router.

The first thing that you must do is set up an interface and a management IP so that you can access the VPN Router via the Graphical User Interface (GUI). In Chapter 5, we discuss the GUI in depth, but for the purposes of the software installation, it is important to understand the portions of the GUI that are used for the initial setup of the router.

NOTE The examples used here provide the instructions for a Windows-based PC operating system.

You will need to attach a console cable between the serial port on your VPN Router and your PC. That is all it takes for the physical connection between the PC and the VPN Router. Next, you must set up and establish a connection between the PC and the VPN Router. Locate HyperTerminal by selecting the following path: `Start` → `Programs` → `Accessories` → `Communications` → `HyperTerminal` (see Figure 3-1).

Once you have located your HyperTerminal application shortcut, you simply click on it and HyperTerminal starts. The next window you will see is the Main HyperTerminal Startup window. In this window, you will see the HyperTerminal name, development information, and copyright information. The Upgrade Info button can be selected during this phase, and it provides you with additional information about the HyperTerminal application as well as upgrade information. Figure 3-2 shows an example of this window.

Once the application has loaded, you will now see the Connection Description dialog box come up. In this phase, the steps that are necessary to establish a new HyperTerminal connection are initiated.

NOTE **If you opted to review the Upgrade information in the previous step, then this next window will be available to you when you close the Upgrade window.**



Figure 3-1: Locating the HyperTerminal application



Figure 3-2: The HyperTerminal start window

In the Connection Description phase, you must set a name for your connection. You should select a name that will assist you in locating this session in the future, should you decide to save the connection profile.

In the next phase, you enter a name for the connection. The name you choose for the connection should be a name that helps you remember what the connection is for. It can be any name you want and can be renamed and/or deleted in the future. As shown in Figure 3-3, the new connection has been assigned the name New VPN Router. You can also select from a group of default icons for this connection as well. Again, select an icon that will help you identify the connection.

Two buttons are available in this window: OK and Cancel. To continue establishing the new connection, click OK. To stop the process, click Cancel.

The next window you see prompts you to enter information pertaining to the physical connection you will need to utilize in order to make a connection to the destination you want to reach. Four sections are in this window, as well as two buttons.

The first section of this window is a drop-down menu that allows you to select the country in which you are originating the connection from. Because we will not be establishing a dial-access connection, nothing needs to be done to this section.

In the second and third sections, you enter an area code and a phone number. Again, this is used only when setting up a dial-access connection, so nothing needs to be entered in these two sections.

The final section of this window is another drop-down menu that asks you what physical connection type you will be using on your PC to establish this connection. The menu options that are normally contained in this area are the hardware options (modems, serial ports, and so on) that HyperTerminal recognizes, based on your device profiles. Figure 3-4 shows an example of this window.

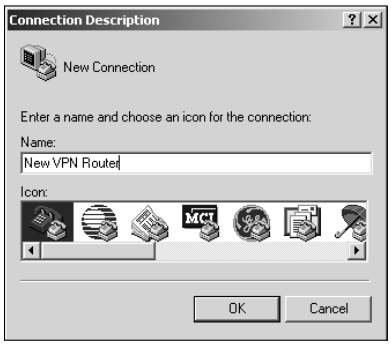


Figure 3-3: Assigning the name New VPN Router to the new connection

Select the physical interface that you will be using to establish a connection to the destination. Because we are using the serial port on the PC to establish a connection to the serial port on the VPN Router, select COM1 (see Figure 3-5). Once COM1 is selected, you are presented with two buttons: OK and Cancel. You can select OK to continue establishing the new connection. Select Cancel to cancel the process.

In the next phase of the new connection setup, the COM1 port settings must be identified. It is very important to set these up correctly because if they are incorrect, you will not be able to establish a connection to your VPN Router. There are five sections that you will need to set during this phase (see Figure 3-6).

The first section is the data rate section. This is a drop-down menu that provides multiple supported data rates. To establish a connection to our VPN Router, select a data rate of 9600 bits per second.



Figure 3-4: The HyperTerminal access instructions window

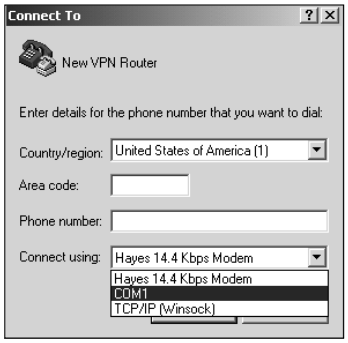


Figure 3-5: Selecting COM1 for our connection

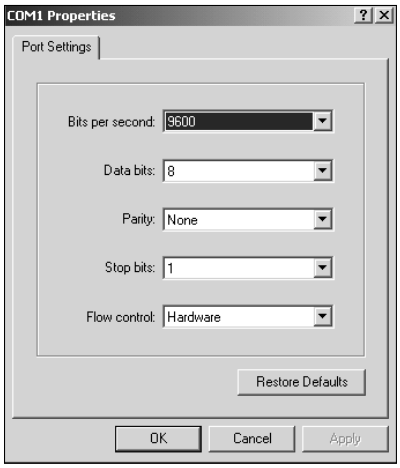


Figure 3-6: Configuring the port settings for the connection

The next section, the data bits section, is a drop-down menu that allows you to select the number of data bits that you want to use for each character that is transmitted over this connection. Most often this will either be a 7 or an 8, depending on what the destination device is set to use. During this phase you will want to select 8 data bits.

The next section of this phase allows you to set the error-checking data parity bits used for this connection. Five options are presented during this phase. To establish a console connection to your VPN Router, you will want to select "none" from the drop-down menu.

The fourth section is another drop-down menu that allows you to select the number of stop bits that need to be used for this connection. The stop bits are a timing mechanism that determines the time period between each character being transmitted. When setting up the connection to the VPN Router, you will select 1 stop bit.

The final section of the Port Settings phase is the flow control section. This is a drop-down menu that allows you to select the method by which data flow is controlled. Whenever establishing a connection to a serial device, you will always select Hardware. Because we are setting up a connection to a serial port on the VPN Router, we will want to select Hardware for the flow control option.

Finally, four buttons are available to you during this phase. The first is the Restore Defaults button. If you want to change all of your selections back to the HyperTerminal port setting defaults, you can click this button at any time and it returns you to factory default settings.

NOTE **If you choose to select the Restore Defaults button, your changes are removed immediately. You are not prompted to verify whether you are sure that you want to return to factory defaults.**

The remaining three buttons are OK, Cancel, and Apply (not used). If you are okay with your changes and are ready to proceed with your connection setup, then click OK. Otherwise, select the Cancel button to cancel the connection setup process.

You have completed the connection establishment phase and should now have a connection to the console port of your VPN Router. At this point, you will need to turn on the VPN Router and let it boot up.

The HyperTerminal window provides access to the VPN Router. It takes a few minutes for the router to come up, but once it has booted, you will see information about the VPN Router in your HyperTerminal screen. At the bottom of the HyperTerminal window is a clock that keeps track of the connection duration, and you can also see the port settings that were established in the last phase of the connection setup.

In the HyperTerminal session window, you see copyright information, Version ID information, access date, and the serial number of the VPN Router. Finally, you will see the login prompt. You are asked for the administrator's user name. This can be changed during the VPN Router configuration. During the initial setup of the device, you need to enter the default administrator user name, which is "admin."

Once you have entered the administrator's user name, you are prompted for a password. The password can be changed during the configuration of the VPN Router. The router will be set to the default password for the initial setup phase, which is "setup." Figure 3-7 shows an example of this window.

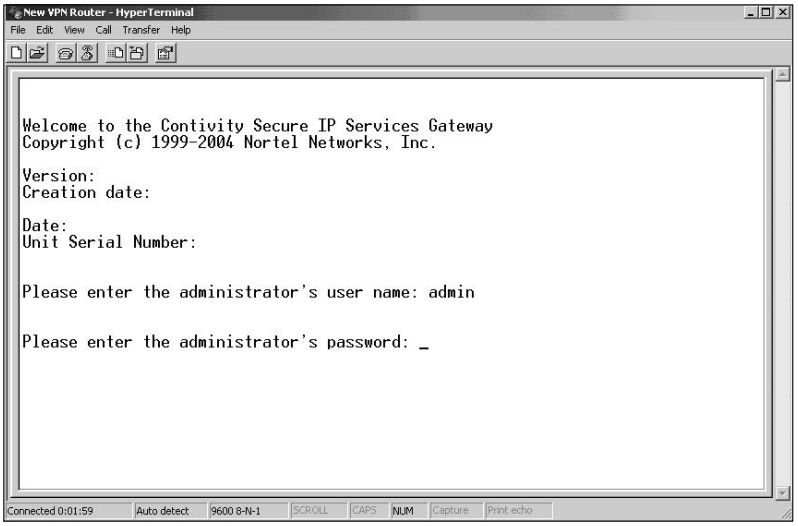


Figure 3-7: The HyperTerminal initial session—entering the administrator's password

Once you have entered the correct user name and password, you will be given access to the VPN Router Main Menu (see Figure 3-8). The Main Menu is where you can go to begin the initial setup of your VPN Router. The first thing that you must do is assign a Private IP address so that you can access the VPN Router for configuration purposes.

From the Main Menu, you will want to access the first menu item (option number 0). This section of the Main Menu provides access to the management address configuration section. Select the number zero (0) on your keyboard and press Enter. Figure 3-9 shows an example of the Management Address configuration menu.

You will be prompted to enter the new management IP address. The management IP address is the address that you use to connect to the VPN Router for management and configuration options.

NOTE **Prior to VPN Router code version 6.00, the management IP address had to be part of the same subnet as the private interface. VPN Router software version 6.00 makes it possible to use a Circuitless IP (CLIP) address as the management IP address. This allows you to access the management of the device from any physical interface.**

If there is a management IP address assigned to the VPN Router, you must enter **0.0.0.0** and press Enter to remove it. Otherwise, enter the management IP address that you want to assign to the VPN Router and press Enter. In Figure 3-10, the IP address 10.10.10.2 has been assigned as the management IP address for the VPN Router.

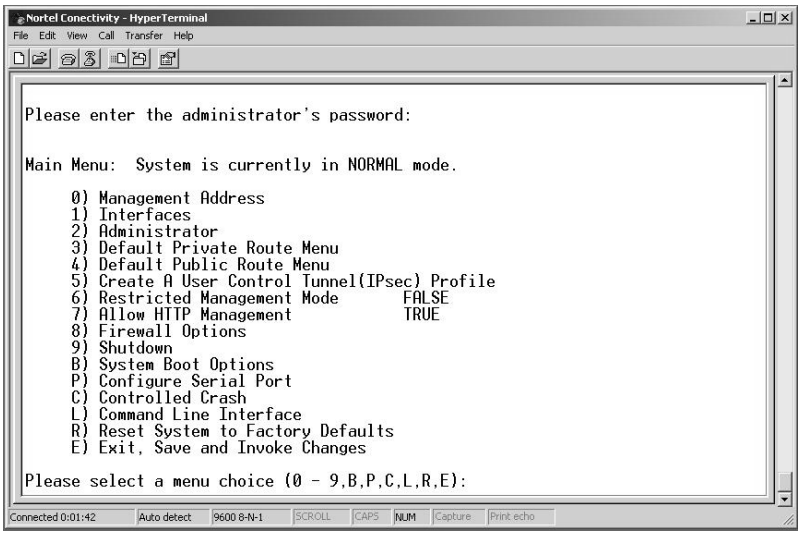


Figure 3-8: The HyperTerminal VPN Router main menu

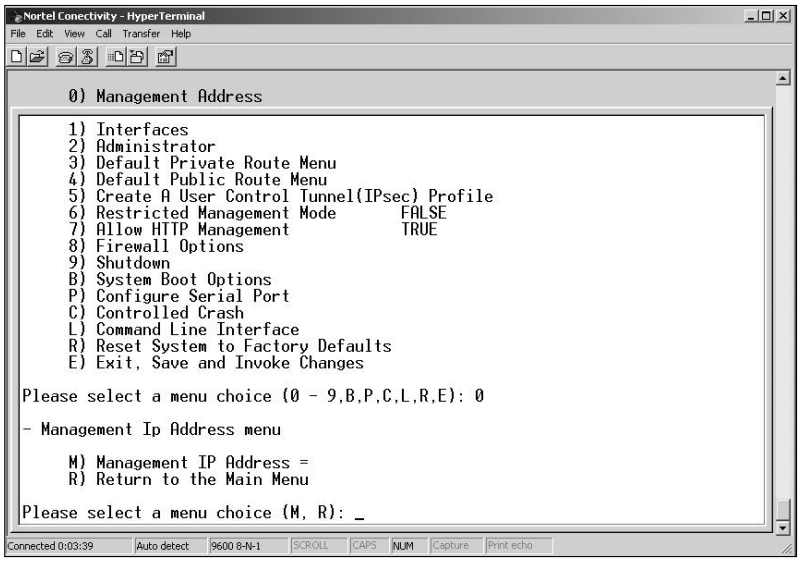


Figure 3-9: The Management Address configuration screen

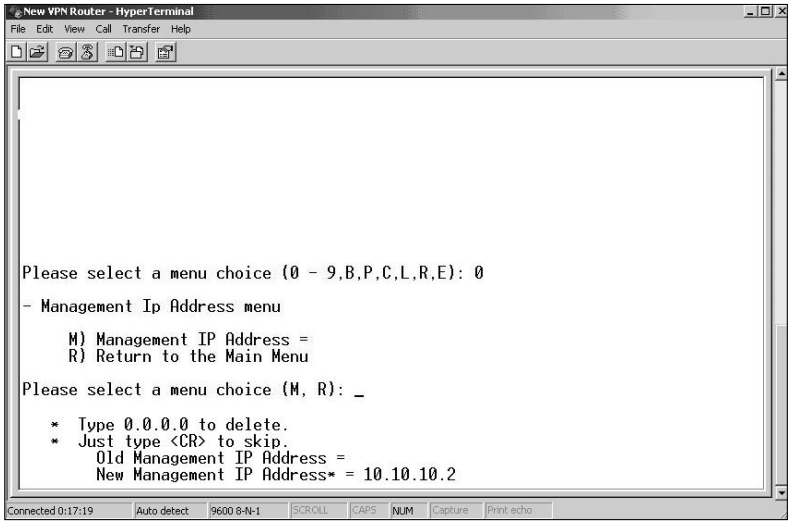


Figure 3-10: Assigning a management IP address

Once you have assigned a Management IP address, you are prompted to enter an IP address for the Private LAN interface. The IP address that you assign to this interface must be on the same subnet as your management station (most likely the PC you are currently using).

The next phase of the initial VPN Router setup is to assign an IP address to your private interface to establish a connection to that private interface. You

will have the option of configuring a *private IP* and a *public IP* interface. If the VPN Router that you are configuring has multiple private LAN interfaces, you will have to configure only the interface that you will be accessing to continue the GUI configuration.

From the Main Menu, you will want to access the second menu item (option number 1). This section of the Main Menu provides access to the interface address configuration section. Figure 3-11 shows an example of the Interface configuration menu screen.

Because we are configuring an IP address on the private LAN interface, the option that is selected from the Interface menu is option zero (0). Select option 0 and press Enter.

Once you have assigned the IP address to the Private LAN interface, you need to hit Enter to apply it. In Figure 3-12, the IP address 10.10.10.3 has been assigned as the Private LAN interface IP address.

You will now be asked to enter the subnet mask for the interface IP address (see Figure 3-13). The subnet mask 255.255.255.0 has been assigned to the interface IP address.

After you have assigned the management IP address and the private LAN IP interface IP address and subnet mask, you will have to choose your connection speed. We recommend that you leave this set to auto-detect, unless your local network requires a port to be set to a particular speed. This setting needs to match the setting of the connected device. Figure 3-14 shows an example of the port speed setting menu.

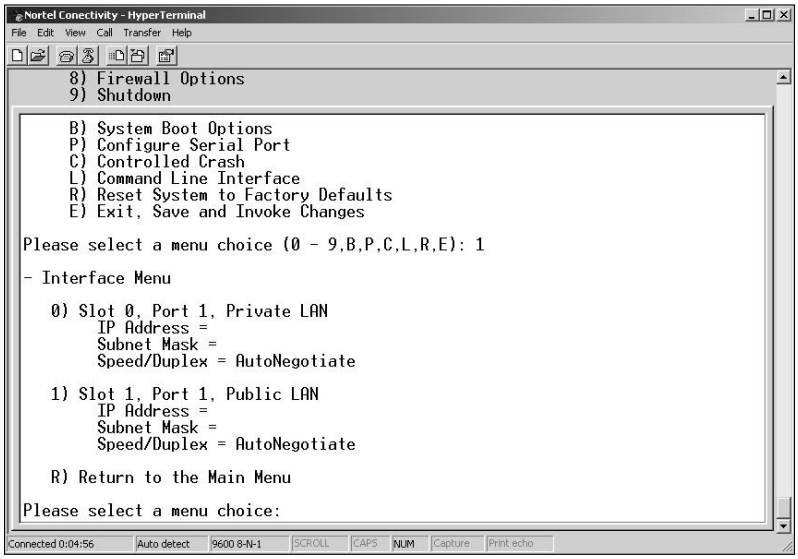


Figure 3-11: The Interface configuration menu

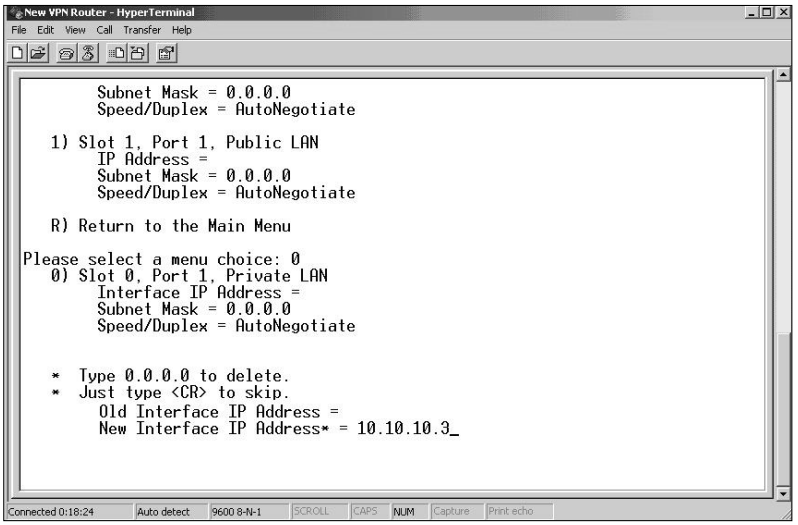


Figure 3-12: Assigning an IP address to the Private LAN interface

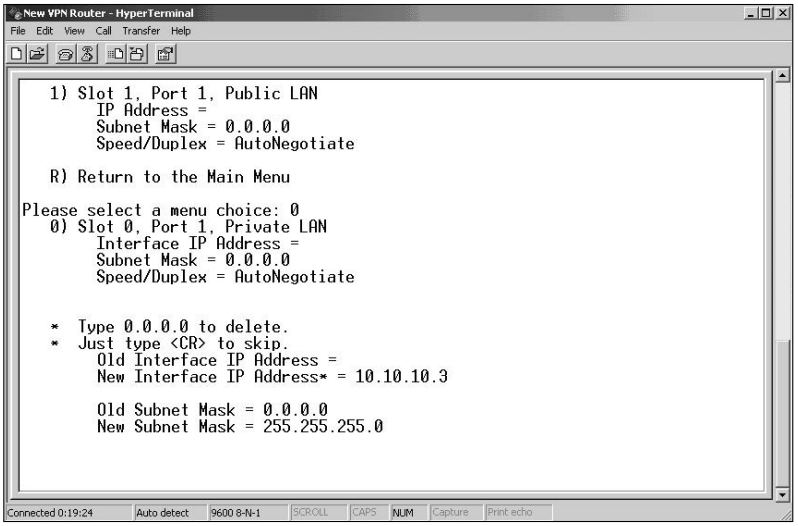


Figure 3-13: Assigning a subnet mask to the Private LAN interface

After you have set the port speed and pressed Enter, you will be directed back to the interface configuration main menu. The initial settings that are required for GUI access to the VPN Router are complete.

Take a look at the Interface configuration menu (see Figure 3-15) and verify that your parameters are correct for the interface that you have just configured. If everything looks correct and you are ready to proceed, then you will need to select R and press Enter. You will then be directed to the VPN Router HyperTerminal Main Menu.

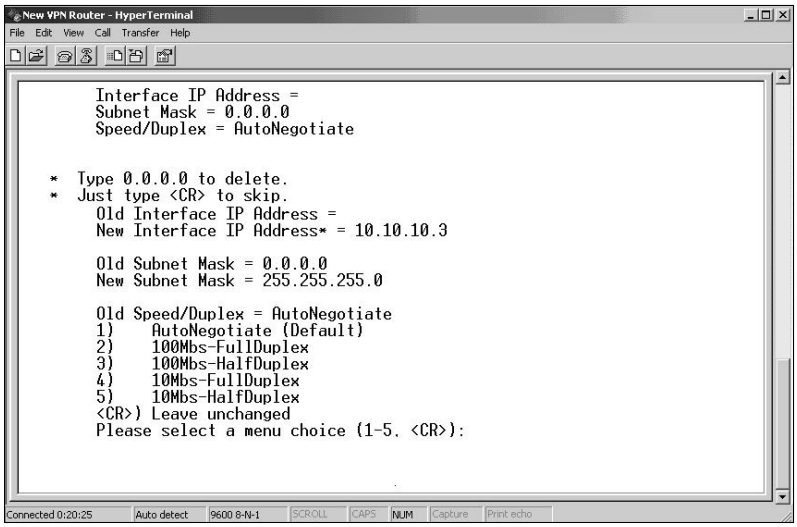


Figure 3-14: Setting the port speed

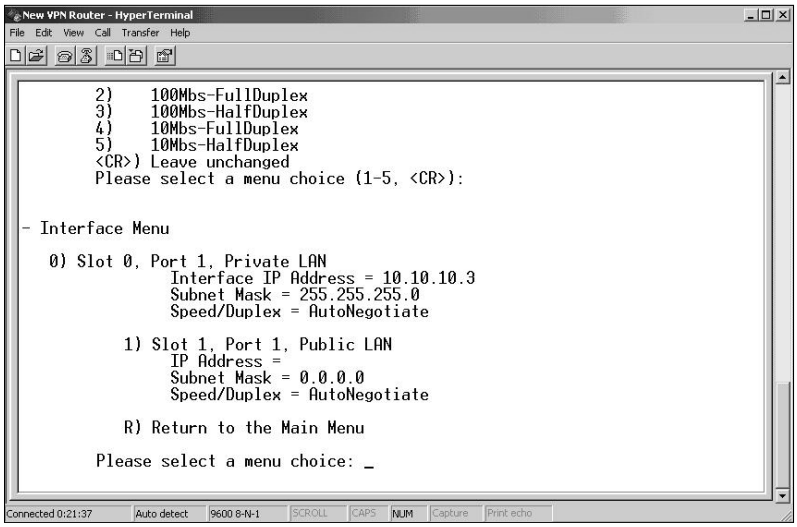


Figure 3-15: The configured Interface menu

From the VPN Router HyperTerminal Main Menu, you will want to save your settings. The menu pick that you will select is option E (Exit, Save, and Invoke Changes). Select E and press Enter. The changes will be applied. Figure 3-16 shows an example of the Main Menu.

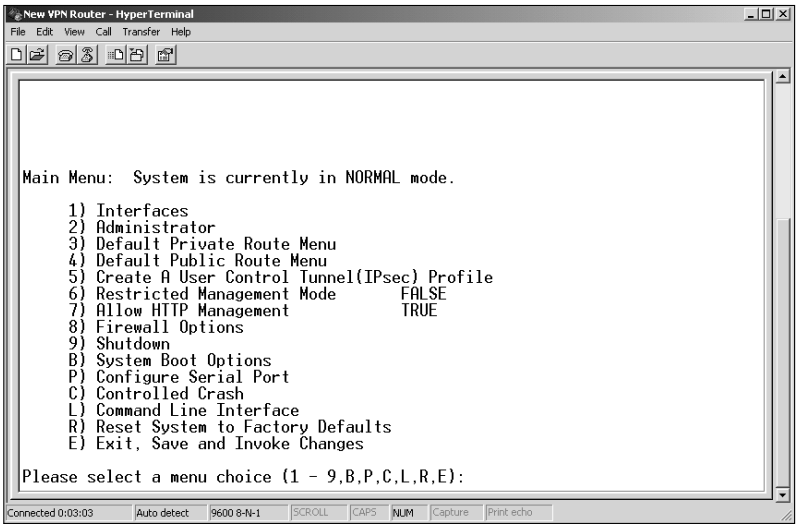


Figure 3-16: VPN Router HyperTerminal Main Menu

The VPN Router is now configured with an interface IP address and a management IP address. This provides you with access to the VPN Router to configure it with the GUI.

You can now disconnect from your HyperTerminal session and select your Internet browser icon. The Internet browser is the Windows-based application that you use to connect to the Internet. For the examples that follow in this book, we will be using Microsoft Internet Explorer.

Double-click the Internet Explorer icon which, by default, is located on your Windows desktop. The Internet Explorer window launches. Once the Internet Explorer window has launched, you will need to tell it that you want to connect to the management IP of the VPN Router.

In the Address field of Internet Explorer, you enter the management IP address that you have configured on your VPN Router. In Figure 3-17, the IP address 10.10.10.2 has been entered in the IP address field. Next, select Go (or press Enter on your keyboard) and Internet Explorer connects to the management IP address on the VPN Router.

When Internet Explorer completes the connection to the management IP address of your VPN Router, you will see the VPN Router GUI main introduction screen (see Figure 3-18).

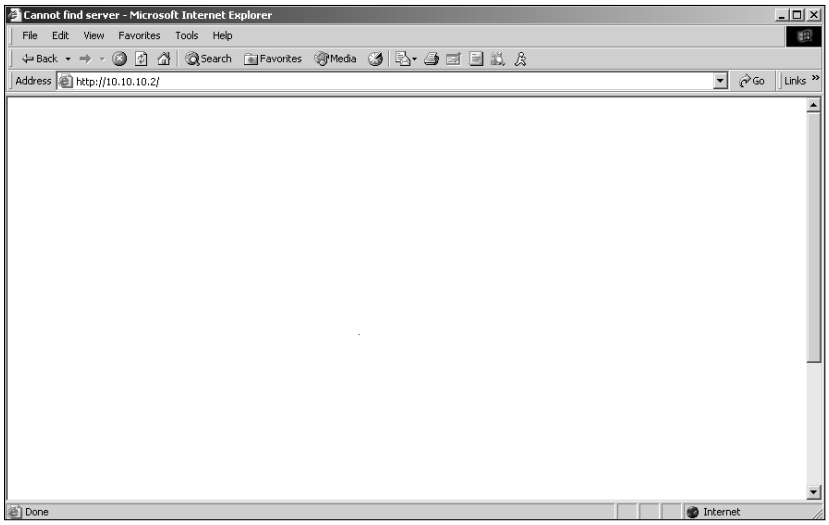


Figure 3-17: Connecting to the management IP address of the VPN Router

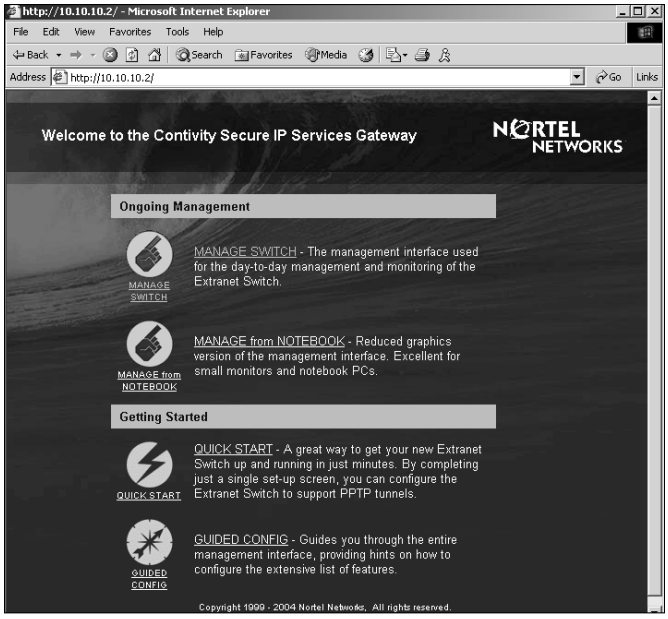


Figure 3-18: The GUI introduction window

From this screen you have four options from which to pick. Each of these options has a brief description on what that particular option is for. The options are:

- *MANAGE SWITCH:* The main management GUI interface used for the day to day management of the VPN Router.
- *MANAGE from NOTEBOOK:* Similar to the MANAGE SWITCH option, but less graphics-intensive.
- *QUICK START:* Used to quickly configure the VPN Router.
- *GUIDED CONFIG:* Provides hints to assist in the configuration of the VPN Router.

Now we are ready to prepare for a software upgrade to the VPN Router. For the purposes of this section, the Manage Switch option was chosen.

Once you have selected a management option from the introduction window, you are prompted for a username and a password (see Figure 3-19). By default, the user ID is "admin" and the password is "setup." Enter your user ID and your password, and click OK.

If you have successfully logged on to the GUI, you will be directed to the main menu window (see Figure 3-20). The main menu window consists of the menu options that are located on the left side of the window. The main screen section of the window is in the lighted, shaded area. There is also a button to log off and a link to the help screen, which are both located in the top-right corner.

Because we want to upgrade code on our VPN Router, we need to select the appropriate menu items for the menu list. The main category menu item that we select is ADMIN, and then we need to select the sub-category UPGRADES (see Figure 3-21). Note how the picks that are being selected are represented by a connecting line. This is a very helpful directory tree model to use when selecting configuration and management options on the VPN Router.

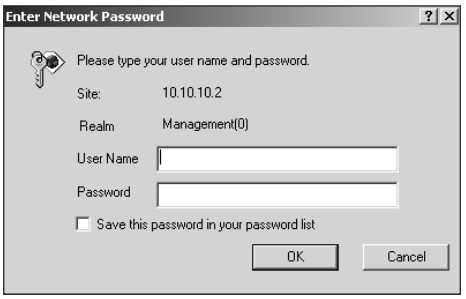


Figure 3-19: The VPN Router login window

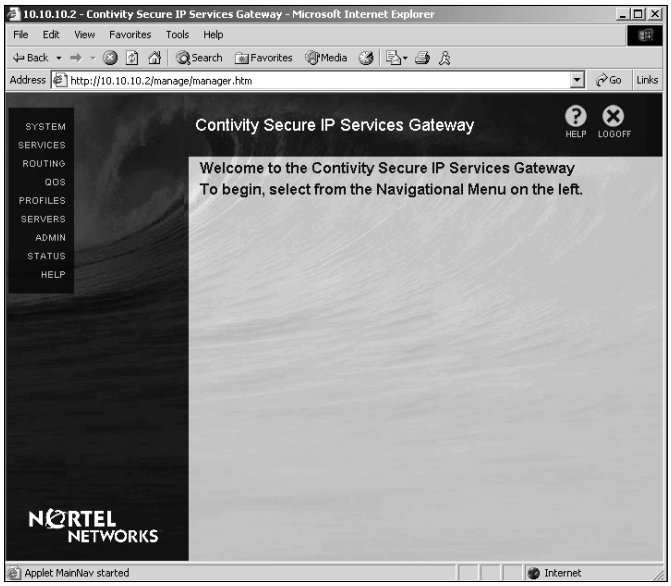


Figure 3-20: The GUI main menu

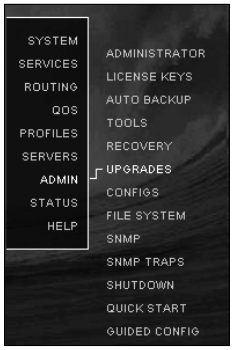


Figure 3-21: Selecting the configuration menu options

Clicking the subcategory UPGRADES opens the software upgrades configuration screen (see Figure 3-22). In this screen, you can see the main menu categories and the subcategories for the main menu selection at the top of the directory tree.

In the main configuration section of the window, you will see a section that contains information on the software that is currently running on the VPN Router. The middle section of the window contains sections that need to be filled out with FTP information that will instruct the VPN Router where to obtain the software that you want to load onto the VPN Router. The final section of the window is a drop-down menu that lists all versions of software that are currently loaded on the VPN Router. There is also a Refresh button at the bottom of the window that allows you to refresh the current window.

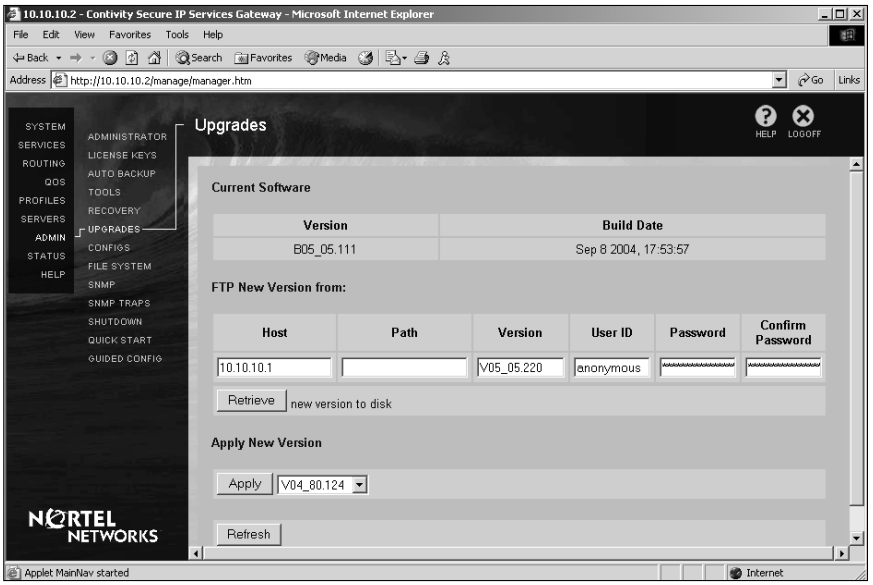


Figure 3-22: The Software upgrade configuration screen

To obtain the correct software that you want to load onto the VPN Router, you must have the software loaded on an FTP server and must provide the VPN Router with the instruction it needs to obtain the software.

The first section that needs to be filled out is the IP address of the STP server host that you have loaded the software onto. The next section is the directory path of the software that is loaded on the server. The version section is the version number of the software. The last three fields are for the FTP server login credentials.

After you have entered all of the required FTP information, you will be prompted with a menu, as shown in Figure 3-23. This screen informs you that the retrieval process may take several minutes and asks you if you want to continue. To continue, select OK.

In the next phase of the software retrieval process, you are presented with a status window. Initially, the status window starts up and informs you that the process is beginning.

Once the FTP process has begun, the File retrieval status window keeps you informed of the progress of the file transfer. It informs you of the total number of files that will be retrieved and the number transferred so far. This process takes several minutes. Figure 3-24 shows an example of this window.

When the file transfer process has completed, the file retrieval progress window informs you that the file transfer has completed successfully. The only option that you have is to close this window.

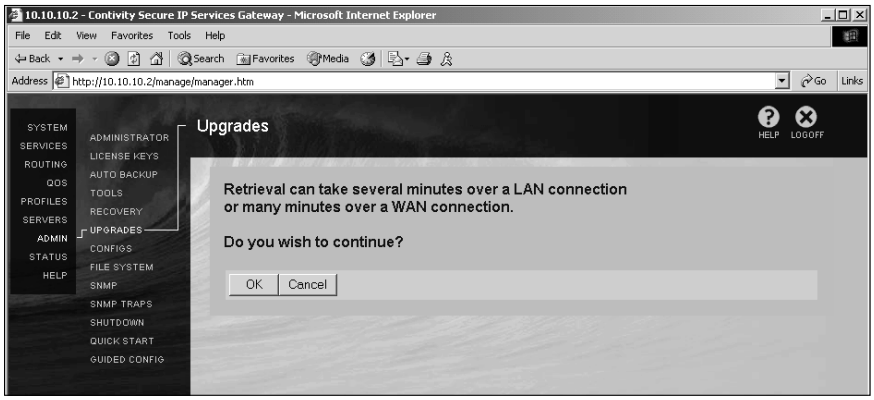


Figure 3-23: The FTP process verification screen

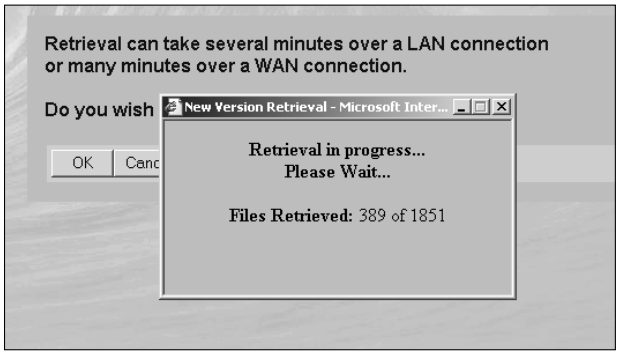


Figure 3-24: The File status progress window

In the next phase of the upgrade process you will be directed back to the software upgrade configuration window. Notice in the example shown in Figure 3-25 that the Current Software version on the VPN Router is B05_05.111. The software version that we have retrieved is V05_05.220.

To complete the software upgrade, the VPN Router must be instructed to load the new version. This is completed by selecting the correct version from the Apply New Version drop-down menu. Highlight the version that is being loaded onto the VPN Router and click Apply.

Once you have selected the new software code version, you are presented with an information verification screen (see Figure 3-26). This screen informs you that the system is updating to the version of code that you have selected. You have the option of selecting OK or Cancel from this screen. If you select OK, the VPN Router updates and reboots with the new version of code.

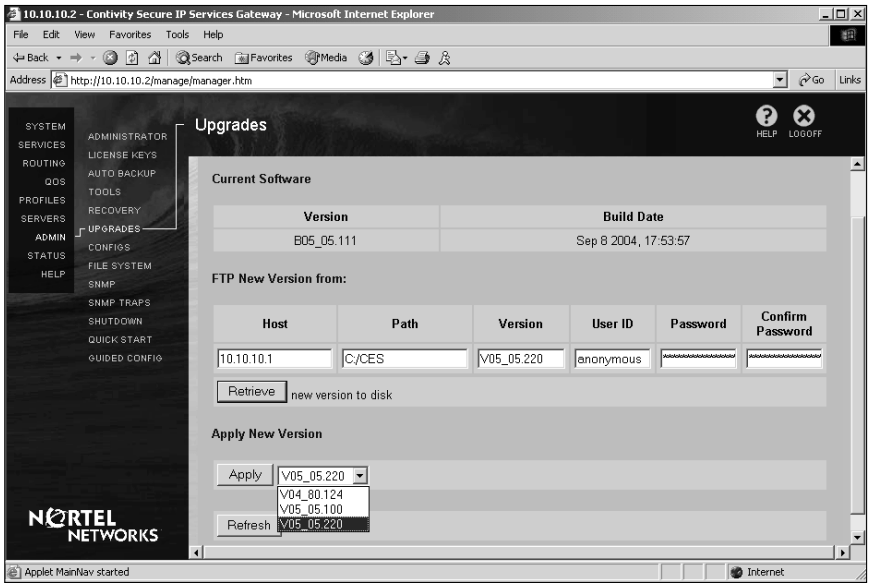


Figure 3-25: Selecting the version of code that is being installed

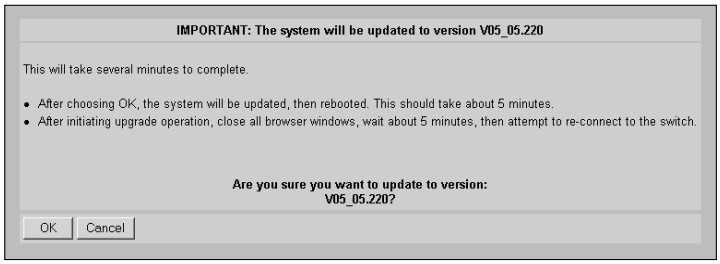


Figure 3-26: The update verification screen

At this point, you can cancel your GUI session and begin a constant ping to the private LAN interface IP address. The syntax for this in a DOS session is as follows:

```
Ping (IP address) -t
```

For example, as shown in Figure 3-27, you could enter the following:

```
Ping 10.10.10.3 -t
```

Monitor the constant ping until you receive a response from the interface IP address (see Figure 3-28). When a reply is received, you can connect back to the management IP address via your Internet browser and continue the configuration of the VPN Router.

Once you have connected back to the management IP address via the Internet browser, you will want to verify the code version on the VPN Router is the version that you want to be running. The simplest way to do this is by selecting HELP → ABOUT. In Figure 3-29, you can see that the current software version is the version that we selected the VPN Router to be upgraded to.

The VPN Router software upgrade is now complete. The VPN Router will now support all of the features and the functionality listed in the release notes for the version of software that you have loaded.

Because the VPN Router can store multiple versions of code, the backout process is very simple and user-friendly. Picking the version that you want to return to is only a click away.

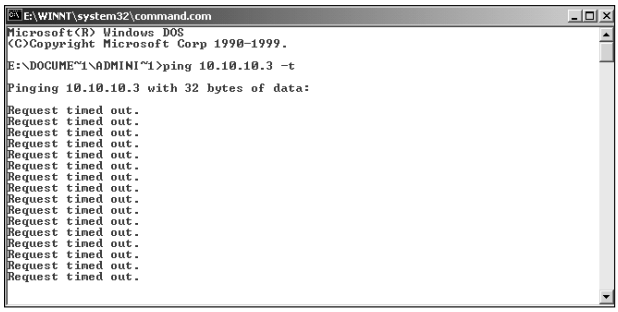


Figure 3-27: Pinging the Interface IP address

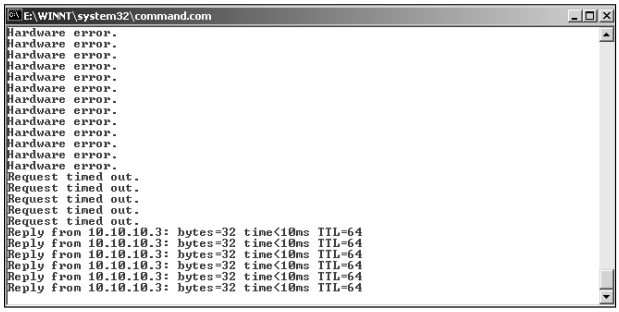


Figure 3-28: Receiving a Reply from the private LAN interface

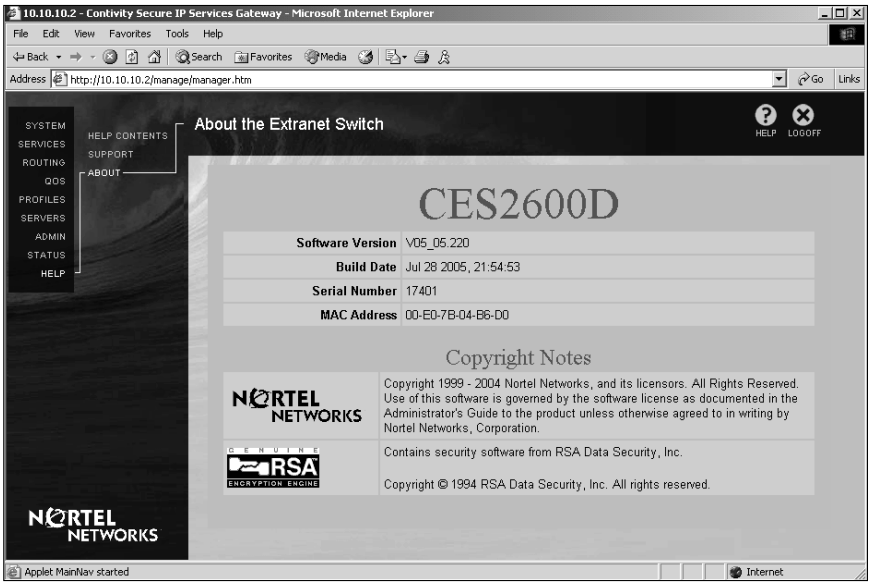


Figure 3-29: Verifying the software version that is running on the VPN Router

Removing Unused Versions

Sometimes it may be helpful to return to a previous version of software, especially when you realize that a version of code does not fit the needs of your company. We recommend that you continue to store a previous version of code in case you want to revert back to that code for any reason.

A drawback to storing multiple versions of software on your VPN Router is that they do take up disk space that may be needed in the future for any number of reasons. Once you are comfortable with a version of code, you may want to remove any unused versions from the stored section of the hard disk on your VPN Router.

Removing unused versions of software is an easy process through the VPN Router management GUI interface. Connect to the GUI via your Internet browser and log in to the management GUI. From the main menu, select ADMIN → FILE SYSTEM, as shown in Figure 3-30.

The File System Maintenance window initially displays the storage devices on the VPN Router that you are managing. In Figure 3-31, you can see that the only storage device is the main hard drive, which is identified as ide0.

Highlight the storage device where you have stored your VPN Router software that you want to remove. Once you have highlighted the storage device, you click the Display button.

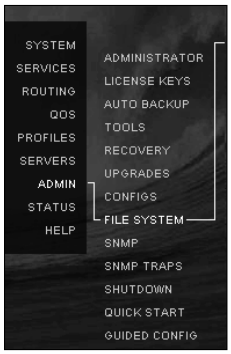


Figure 3-30: Accessing the file system to remove unwanted files

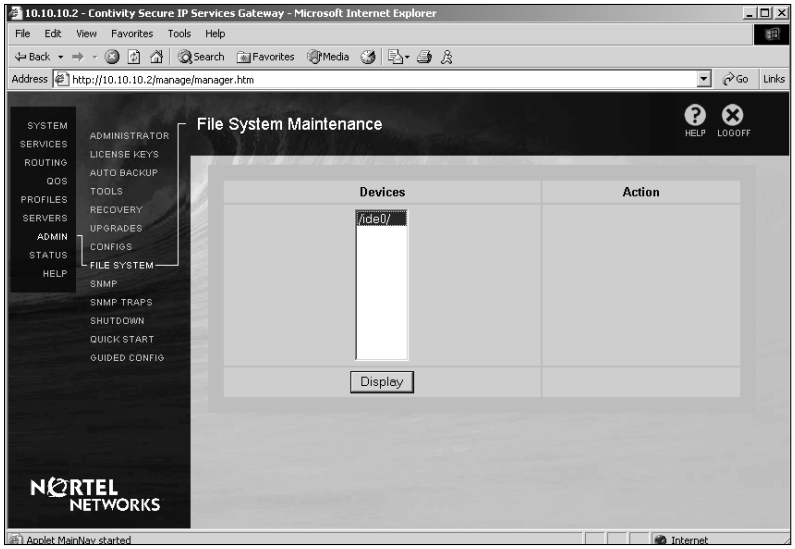


Figure 3-31: File System Maintenance main menu screen

The next screen displays a list of the file systems on the storage device that was selected. As shown in Figure 3-32, two columns are listed in the window. In the left column, you see the main directory structure on the storage device. In the right column, all of the files are listed. You will see a directory for the system files. The VPN Router software is located within the directories and is labeled by version number.

As shown in Figure 3-33, you can view the details of a particular directory. Highlight the directory in the left column and then click the Details button at the bottom of the window. To select the software version that is being removed, simply select the directory that is named for the software version and click Display.

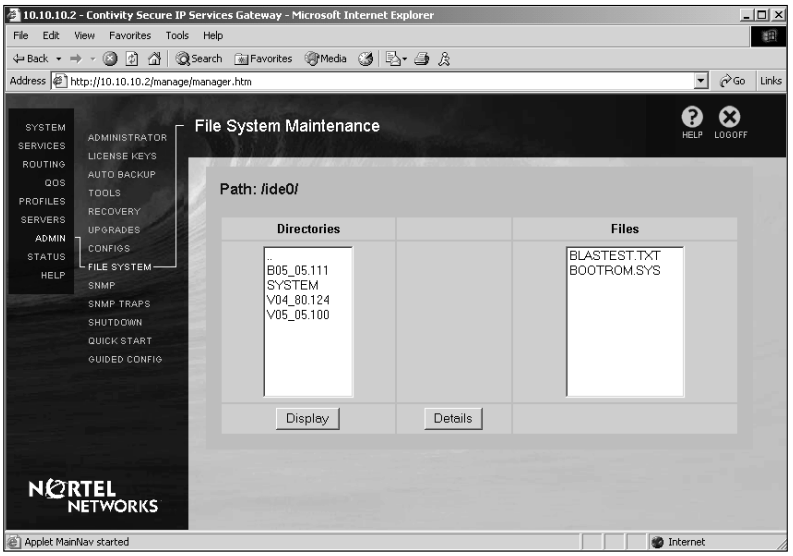


Figure 3-32: The File System Maintenance directory structure

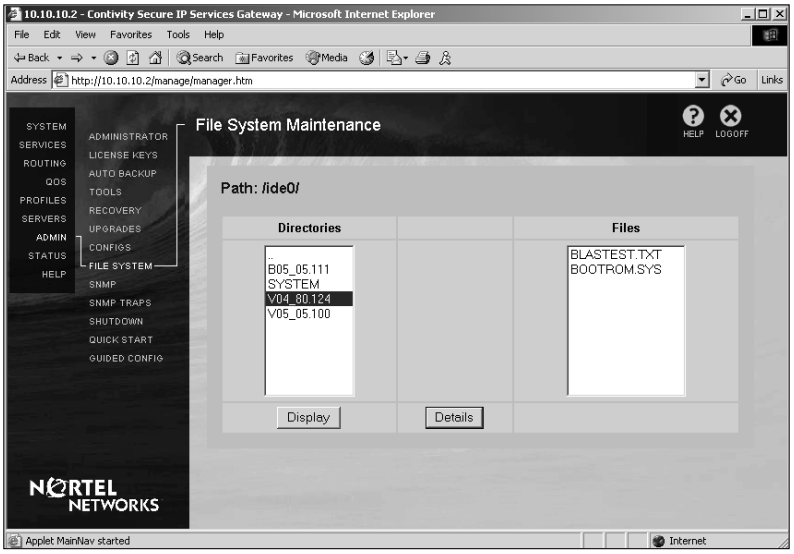


Figure 3-33: Selecting the software version that is being removed

After you have selected a directory to display, the directory is listed in a new section of the File system Maintenance window. This window lists the name of the directory and information about the type, and has a button option instructing the file system to remove the selected directory. To remove the software from your storage device, click the button. Figure 3-34 shows an example of this phase of the uninstall process.

In the next phase, you are asked to confirm the removal of the software/file system. During this phase, you are able to cancel the removal of the software if you want to. To proceed with the removal of the software, click OK.

The final window you receive will be the File System Maintenance window shown in Figure 3-35. You can see that the directory that contained your software version has been removed. The uninstall process is now complete.

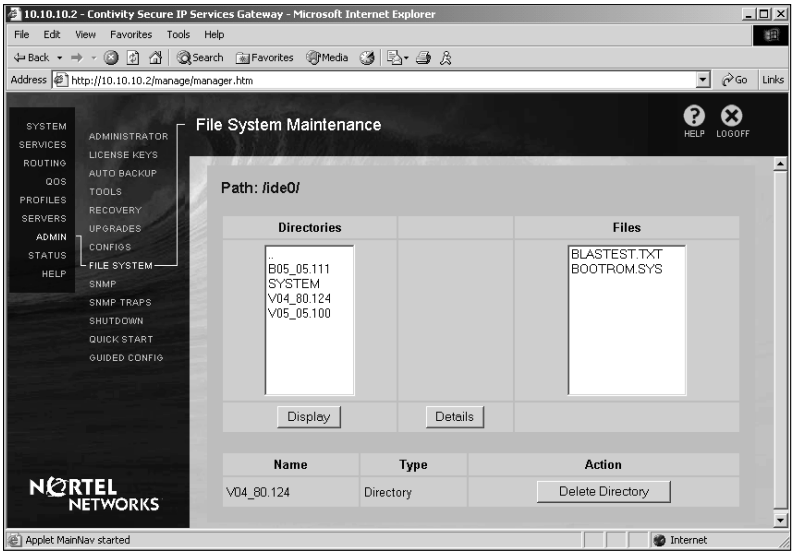


Figure 3-34: Selecting and removing unused software

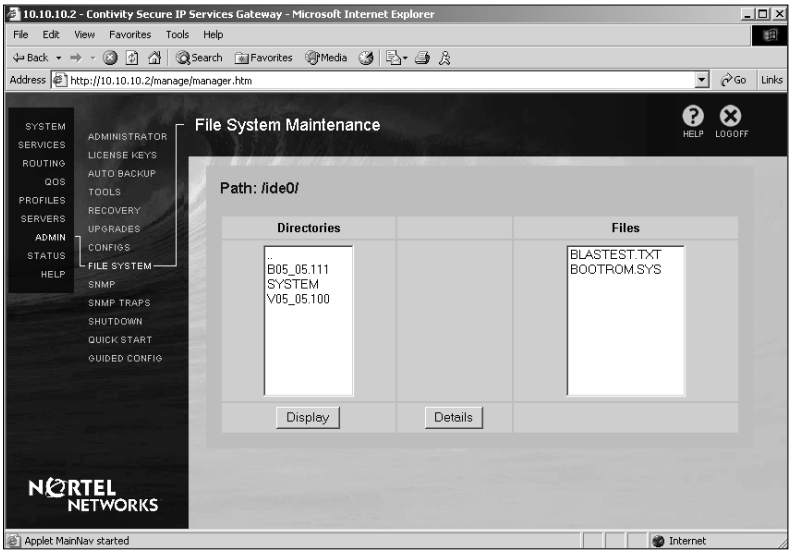


Figure 3-35: The File System Maintenance window

VPN Client Software

The Nortel VPN Client, also known as the Contivity VPN Client (CVC) and the Contivity Multiple-OS Client, is used to allow users (the clients) the ability to connect remotely over a WAN to the corporate LAN. It provides for secure access and is developed to support a multiple range of user potential PC operating systems, including the following:

- IBM-AIX
- Linux
- Macintosh OS
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows 2000
- Microsoft Windows ME
- Microsoft Windows NT
- Microsoft Windows XP
- Pocket PC
- Sun-Solaris
- UNIX

The Nortel VPN Client provides support for end users to connect to their remote LAN through a fully encrypted and authenticated connection. The VPN client can be centrally administrated with the LAN administrator determining the allocation of bandwidth, control of access, methods of authentication, and encryption parameters. Administrators are also able to customize the client to meet the needs of the networks without any end-user support. The VPN client interoperates with other Remote Access applications on the end user's PC, so the configuration of the client should not disrupt the ability to utilize the other applications that may be used.

Installing the VPN Client Software

The Nortel VPN Client software is included with the CD-ROM version of the Nortel VPN Router software. The VPN client software is also available to registered users on the Nortel Web site (`www.nortel.com`). Also included on the CD-ROM (as well as on the Nortel Web site) are the code version release notes.

To load the VPN client software, you can run the file from disk. If you downloaded it, you will run it from the directory in which you have stored the application. The VPN client software installation application is a self-extracting executable that, once clicked, will guide you through the installation process.

Release Notes

Contained on the CD-ROM that comes with the VPN Router software are the release notes for the client that you will be loading. It is always important to review the release notes to assist you in determining what code version is suitable for your needs. The client release notes will inform you of important information that is necessary for you to understand. Following is some of the information included within the VPN client software Release notes:

- Copyright information
- Trademark information
- Software licensing agreement
- Table of contents
- The PC operating systems that are supported
- The enhancements included in the version of code
- Known bugs in the code version
- Important considerations that must be taken into account with that particular version of code

On minor code revisions, the release notes will normally include only enhancements and known issues. The release notes are normally in PDF format, but occasionally are included in a Microsoft Word or a text document.

Installing the VPN Client

This section takes a step-by-step look at the installation process. The code version that is being installed for this example is VPN client version 5.01.

NOTE Provided here are examples of installing the VPN client onto a Windows 2000 platform.

Installing the VPN client onto your PC is a very simple process. Simply locate the VPN client self-extracting executable icon and double-click it. The VPN client installation executable normally will be named `eac [versionnumber].exe`. For example, the VPN client installation executable for the version 5.01 VPN client software is `eac501d.exe`.

Once you have double-clicked the VPN client software installation icon, the installation process begins. In Windows 2000, a window informs you that the executable is extracting the files needed to perform the install of the client (see Figure 3-36). The window also contains a status bar informing you of the current status of the extraction in percentages.

After all of the necessary files have been extracted, two more windows will appear. The larger window will have the Nortel name and will have the code version number of the VPN client that you are installing. The second window is a Windows 2000 status window informing you that the VPN client setup program is preparing the InstallShield Wizard, which will assist you in the installation of the VPN client. Figure 3-37 shows an example of this second phase of the installation process.

NOTE The InstallShield Wizard is part of the InstallShield technology, which is utilized by several thousand software vendors to assist in the distribution of software. The InstallShield Wizard utility guides the user through the installation process, making it simpler and more uniform for all.

Once the InstallShield Wizard has been prepared, the installation of the client software begins. The window that appears next is a Welcome window informing you that the installation is ready to begin. You have an option at this window to continue (by clicking Next) or to cancel.

The next phase of the VPN client installation process is the licensing agreement. It is important that you read through and understand this agreement. The licensing agreement will explain to you what the intention of the software is. It also explains to you what you can and cannot do with the software.

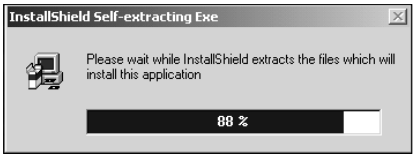


Figure 3-36: Extraction of necessary files

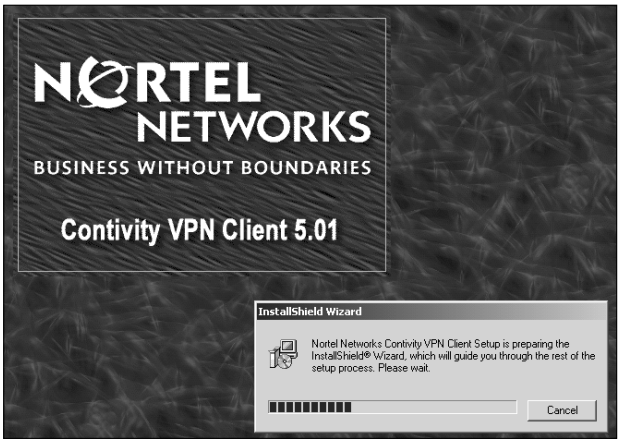


Figure 3-37: Window with version number and status

Once you have read through the agreement, you have the option of clicking one of three buttons. The first is the Back button, which returns you to the previous step of the installation process. The second is the Yes button, and by clicking it, you agree that you have read and will conform to the licensing agreement. Clicking Yes installs the VPN client. The final button is the No button. By clicking the No button you are stating that, for whatever reason, you do not agree to the licensing agreement. Clicking the No button cancels the installation process.

The next phase of the VPN client installation process is the Destination selection dialog box. In this phase, you instruct the InstallShield Wizard where to load the VPN client onto your PC. Normally, you will want to select the default destination that is already selected for you. If you have reasons to place the installation into another destination, you need to direct the installation to the path where you want the VPN client application to reside on your PC.

The window informs you that the InstallShield Wizard is prepared to install your VPN client software in the following destination. In Figure 3-38, you can see that the InstallShield Wizard is installing the VPN client software in the `E:\Program Files\Nortel Networks` directory.

There are three buttons for you to select at this phase: Back, Next, and Cancel. Click Back to return to the previous phase of the installation. Click Next to direct the InstallShield Wizard to install the VPN client into the directory that is specified in the dialog box. Click Cancel to cancel the installation process.

The next phase of the VPN client installation process is the Select Program Folder phase (see Figure 3-39). In this phase, you can accept the default folder name or assign one of your own. If you want to accept the default folder name, you can select the button. Otherwise, you need to type in a folder name.

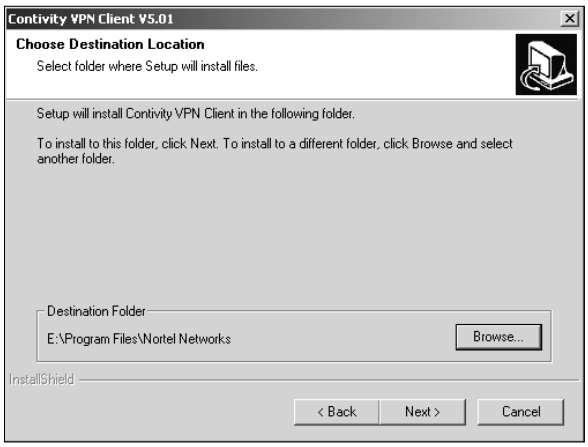


Figure 3-38: Choosing the destination location

Click the Back button to return to the previous phase of the installation. Click Next to direct the InstallShield Wizard to accept the folder name that was specified and to continue the installation process. Click Cancel to cancel the installation process. Figure 3-40 shows an example of this phase of the VPN client installation.

The next phase of the VPN client installation is the install and run phase. As shown in Figure 3-40, you are presented with the following three options. You must determine which option would be applicable for the needs of the end users.

- Application (default)
- Windows service (Two-step Domain Logon)
- Windows GINA (Connect before Logon)

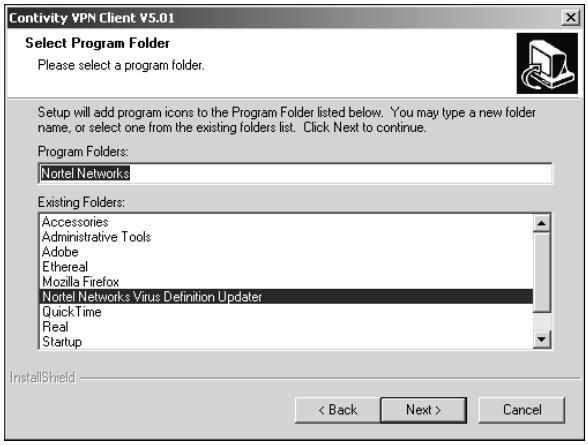


Figure 3-39: The Select Program Folder window

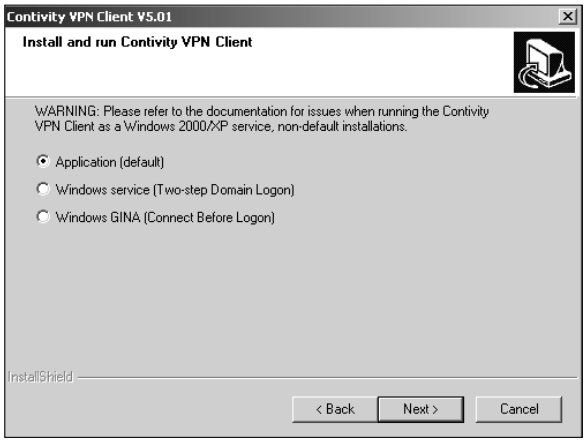


Figure 3-40: The Install and run Contivity VPN Client window

The Application option is the most commonly used method of VPN client installation. Using this option, the end user has only to specify user identification and password in the client session initialization in order to connect to the VPN Router and access LAN resources.

The Windows service option allows end users to connect to a VPN Router, and then they need to log in to their Windows domain to access LAN resources.

The Windows GINA option is supported on Windows 2000 and Windows XP operating systems. GINA is an acronym for Graphical Identification and Authentication. It allows for an automatic Windows domain login service through a VPN tunnel. When using the GINA option, the user is not required to launch a client and log out of a local system to authenticate on the Windows domain. Once you have established a tunnel with the VPN client, the Windows domain login is established for the user via the tunnel.

Click the Back button to return to the previous phase of the installation. Click the Next button to direct the InstallShield Wizard to accept the installation option that you have selected and to continue the installation process. Click the Cancel button to cancel the installation process.

The next phase of the VPN client installation is the confirmation window. This is the final window that you will review prior to the installation of the VPN client. It contains details such as the program and the driver(s) that are being installed. If you need to review any of the options that you have selected, this window instructs you to click Back.

Click the Back button to return to the previous phase of the installation. Click the Next button to direct the InstallShield Wizard to begin copying the installation files. Click the Cancel button to cancel the installation process.

The next phase of the installation process is the Setup Status window. There is a percentage status bar that will keep you informed of the installation progress. Only one button is available during this phase: Cancel. If you select this button during the installation, the installation is aborted.

Once the VPN Client program has been installed, the next phase of the installation process is engaged. This phase is where the necessary drivers are loaded onto your PC. A *driver* is a software application that works with another software application to teach that application how to communicate and work with the hardware that it is designed to work with. There are no buttons to select during this phase of the VPN client installation process.

The next phase of the VPN client installation is a simple window that informs you that your program folders and icons are being created. There is no user dialog option button during this phase.

The next phase of the VPN client installation process is a window that will display the location that you specified you wanted the VPN client software to be loaded into, as well as the associated icons that are available. The icons you will see are the VPN client icon, the Readme.txt icon, and the VPN client uninstall icon. In Windows 2000, you can access these icons from your Start menu as well. Figure 3-41 shows an example of the program window that you will see.

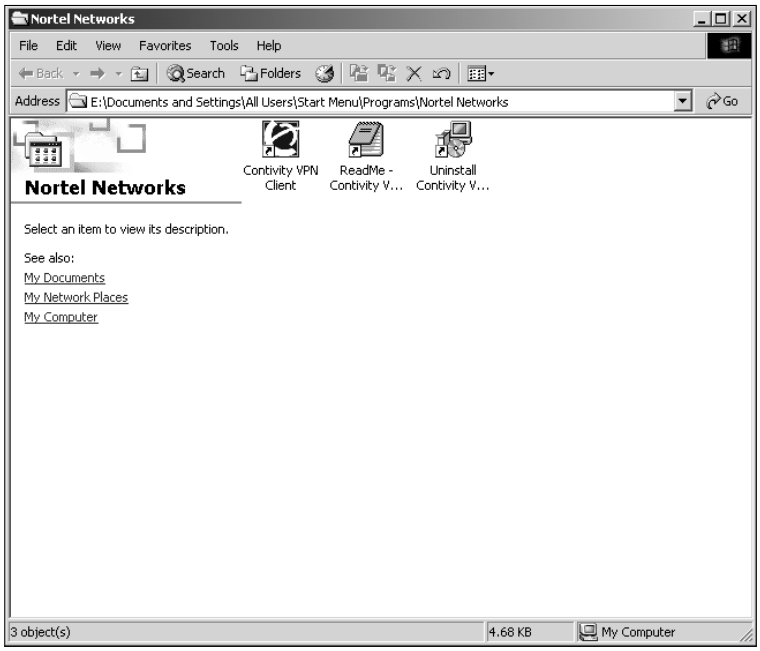


Figure 3-41: The twelfth phase of the installation process

The next window that you will see is a display window of the `readme.txt` file. You should read through this file because it details information about your VPN client software version. The `readme.txt` file displays Windows-specific information that may be important to you, depending on other applications you may be using. Although three buttons are displayed, only one is available (not grayed out). Once you have completed reading this information contained in this window, you will select the Next button to continue the installation process. Figure 3-42 shows an example of the `readme.txt` phase of the VPN client installation process.

NOTE **If you choose not to read the information in the `readme.txt` window phase, you can always refer to the Readme.txt icon shown in Figure 3-41. It is the same information.**

The next phase of the installation process is the final phase. In this phase, you will be prompted to reboot your PC. You can select from one of the following:

- Yes, I want to restart my computer now.
- No, I will restart my computer later.

The only button that is available to you during this phase is the Next button. Select either Yes or No and then click Next. If you select Yes, your PC reboots and you are able to use your VPN client. If you choose No, your PC does not reboot and you need to reboot manually to be able to use your client.

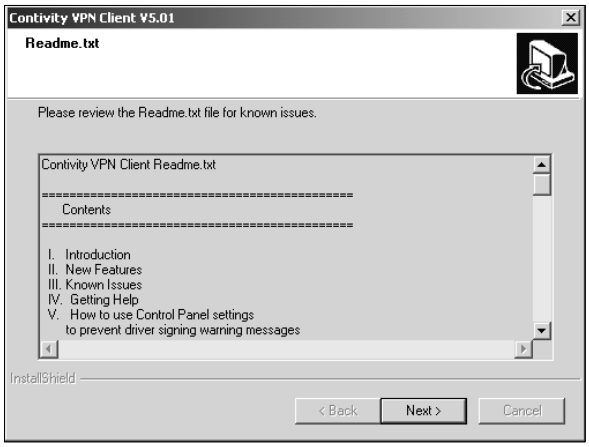


Figure 3-42: The readme.txt file window

Upgrading the VPN Client Software

There are times when you (or your network administrator) will determine that the current version of VPN client is no longer suitable for your VPN needs. There are many reasons why one might want to consider upgrading a client. You may find a need to upgrade VPN Router software and may find that another client is required to support that router software. A new feature enhancement may have been introduced. Whatever the reason is for upgrading VPN client software, the process itself is very simple.

You can upgrade your VPN client software simply by running the installation program of your new VPN client. This is a fairly simple process if performing the steps discussed previously in this chapter. Another option is to remove the current version of VPN software and to install the version that you want to run.

Uninstalling the Existing Version of VPN Client Software

Removing the version of VPN client that you currently have installed on your PC is a simple process. The first step is to locate the executable file for the uninstall program that was included with your VPN client. The icon can be selected through your Windows Start menu by selecting the path Start → Programs → Nortel Networks → Uninstall Contivity VPN Client (see Figure 3-43). Locate this path and click the Uninstall icon. The InstallShield Wizard walks you through the process of removing your VPN client.

Another way you can select to uninstall your VPN client version is to locate the Start menu directory window and double-click the Uninstall icon. Figure 3-44 shows an example of this.

Once you have begun the process of removing your VPN client, you will receive a Windows prompt that the InstallShield Wizard is starting up to assist you with the process. This window has a status bar that informs you of the percentage of install that has been performed. There is an Option button that allows you to cancel this process at any time.

The next phase of the uninstall process is the Confirm File Deletion dialog box. This window asks if you want to remove the VPN client and all associated components. There are two selection buttons in this window. If you select OK, your process of removing the client begins. If you select the Cancel button, then the removal process is terminated.

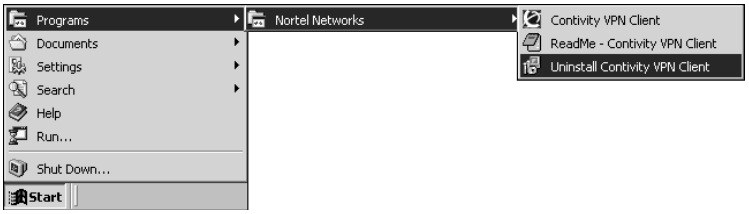


Figure 3-43: The Start menu uninstall process

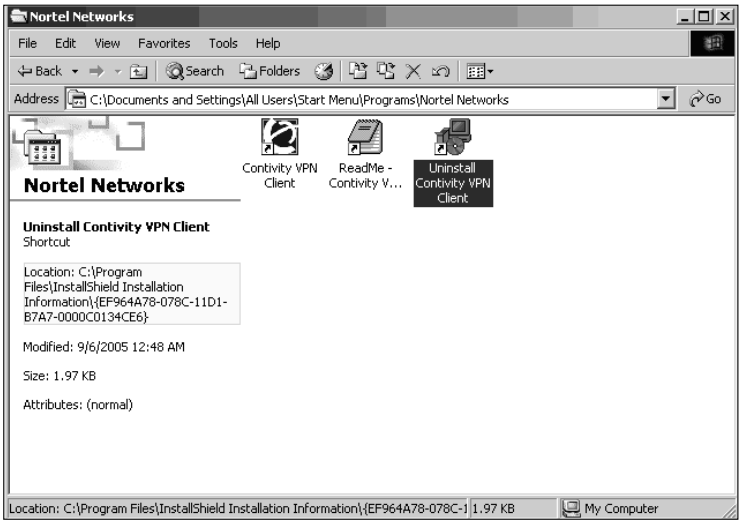


Figure 3-44: Double-clicking the Uninstall icon

The next phase of the uninstall process is the Setup Status window. The Setup Status window keeps you informed on the InstallShield uninstall process. A smaller window appears at the beginning of this process. It is informing you that the device drivers are currently being removed from your system. The removal of the device drivers is the longest portion of the uninstall process. You can halt the uninstall process by clicking the Cancel button.

NOTE While the option does exist to cancel the uninstall process during this phase of the uninstall process, we don't recommend that you do so. Some necessary drivers and/or files may have already been removed, making the VPN client unusable until you reload the application.

The next phase of the uninstall process is the uninstall phase. All applications associated with the VPN client are now removed. There is a status bar that keeps you informed of the percentage of the uninstall process that has been completed. A cancel button is available to you during this phase. You can halt the uninstall process by clicking the Cancel button.

The final phase of the uninstall process is the InstallShield Wizard Complete dialog box. This window informs that the uninstall process is complete and that you will need to reboot your PC to complete the process. There are two options for you to select from. You can either opt to reboot now or reboot at a later time. The only button that is available to you is the option to Finish. If you choose to reboot later, the uninstall process is not complete until the reboot is performed.

NOTE Beginning with Nortel VPN client version 6.01, the reboot is no longer necessary for the uninstall changes to take effect.

Installing the Upgrade

This section provides a step-by-step look at the installation process for the new version of code that we will be installing on our PC. The code version that is being installed for this example is VPN client version 6.01.

NOTE As of this writing, the most current version of VPN client that is available is VPN client 6.01

Installing the VPN client onto your PC is a very simple process. Simply locate the VPN client self-extracting executable icon and double-click it. The VPN client installation executable normally will be named `eac [versionnumber].exe`. For example, the VPN client installation executable for the version 6.01 VPN client software is `eac601d.exe`. Figure 3-45 shows an example of the VPN client software version 6.01 executable icon.

Once you have double-clicked the VPN client software installation icon, the installation process begins. In Windows 2000, a window informs you that the executable is extracting the files needed to perform the install of the client. The window also contains a status bar informing you of the current status of the extraction in percentages.

After all of the necessary files have been extracted, two more windows appear. The larger window will have the Nortel name and will have the code version number of the VPN client that you are installing. The second window is a Windows 2000 status window informing you that the VPN client setup program is preparing the InstallShield Wizard, which will assist you in the installation of the VPN client. Figure 3-46 shows an example of this second phase of the installation process.

Once the InstallShield Wizard has been prepared, the installation of the client software begins. The window that appears next is a Welcome window informing you that the installation is ready to begin. You have an option at this window to continue (by clicking Next) or to cancel.



Figure 3-45: The VPN client software (version 6.01) installation executable icon

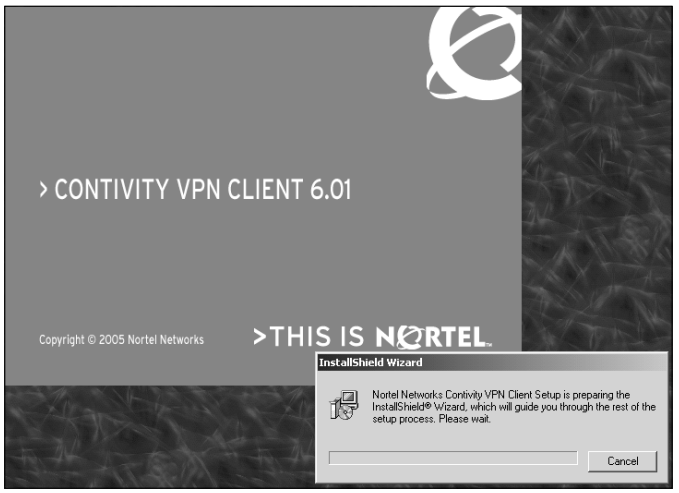


Figure 3-46: Window with version number and status

NOTE **If you are installing a VPN client version over an existing VPN client installation, you will see a different window in the third phase of the upgrade installation process informing you that a current version of VPN client is installed and asking you if you want to re-install the VPN client. If you have opted not to uninstall the previous version, you would confirm that you want to re-install the VPN client. Figure 3-47 shows an example of the third phase window if you are installing *over* an existing VPN client.**

The next phase of the VPN client installation process is the licensing agreement. It is important that you read through and understand this agreement. The licensing agreement will explain to you what the intention of the software is. It also explains to you what you can and cannot do with the software.

Once you have read through the agreement, you have the option of clicking one of three buttons. The first is the Back button, and it returns you to the previous step of the installation process. The second is the Yes button and by clicking it, you agree that you have read and will conform to the licensing agreement. Clicking the Yes button installs the VPN client. The final button is No. By clicking the No button you are stating that, for whatever reason, you do not agree to the licensing agreement. Clicking the No button cancels the installation process.

The next phase of the VPN client installation process is the Destination selection dialog box (see Figure 3-48). In this phase, you instruct the InstallShield Wizard where to load the VPN client onto your PC. Normally, you will want to select the default destination that is already selected for you. If you have reasons to place the installation into another destination, you will need to direct the installation to the path where you want the VPN client application to reside on your PC.

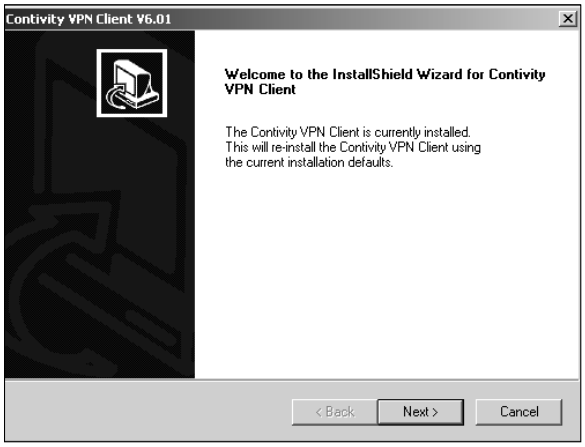


Figure 3-47: Welcome window of the upgrade installation process if you are installing over an existing VPN client.

The window instructs you that the InstallShield Wizard is prepared to install your VPN client software in the following destination. In Figure 3-48, you can see an example of this dialog box and can see that the InstallShield Wizard is installing the VPN client software in the `E:\Program Files\Nortel Networks` directory.

Click the Back button to return to the previous phase of the installation. Click Next to direct the InstallShield Wizard to install the VPN client into the directory that is specified in the dialog box. Click the Cancel button to cancel the installation process.

The next phase of the VPN client installation process is the Select Program Folder phase (see Figure 3-49). In this phase, you can accept the default folder name or assign one of your own. If you want to accept the default folder name, you can choose the Next button. Otherwise, you will need to type in a folder name.

Click the Back button to return to the previous phase of the installation. Click Next to direct the InstallShield Wizard to accept the folder name that was specified and to continue the installation process. Click the Cancel button to cancel the installation process.

The next phase of the VPN client installation is the install and run phase. As shown in Figure 3-50, you are presented with the following three options. You must determine which option would be applicable for the end users' needs.

- Application (default)
- Windows service (Two-step Domain Logon)
- Windows GINA (Connect Before Logon)

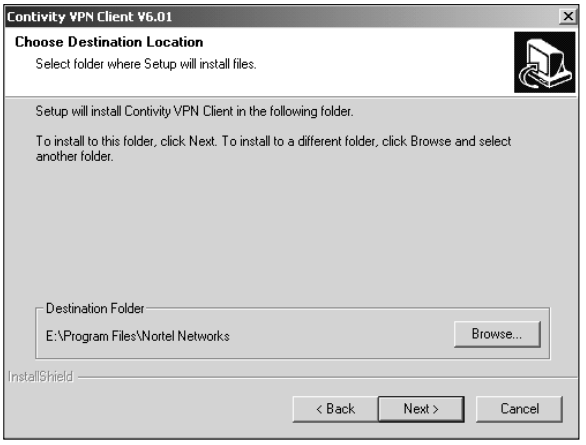


Figure 3-48: Choosing the destination location during the upgrade installation process

The Application option is the most commonly used method of VPN client installation. Using this option, the end user will only have to specify user identification and password in the client session initialization in order to connect to the VPN Router and access LAN resources.

The Windows service option allows end users to connect to a VPN Router, and then they will need to log in to their Windows domain in order to access LAN resources.

The Windows GINA option is supported on Windows 2000 and Windows XP operating systems. GINA allows for an automatic Windows domain login service through a VPN tunnel. When using the GINA option, the user is not required to launch a client and log out of a local system in order to authenticate on the Windows domain. Once you have established a tunnel with the VPN client, the Windows domain login is established for the user via the tunnel.

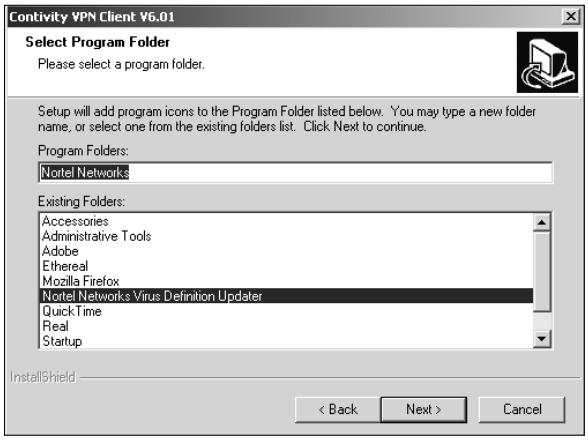


Figure 3-49: The Select Program Folder phase of the upgrade installation process

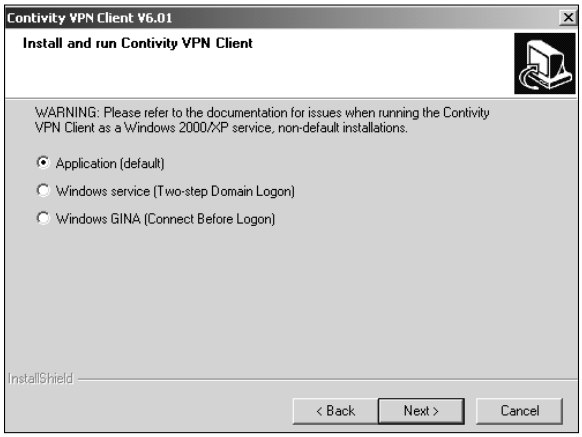


Figure 3-50: The install and run phase of the upgrade installation process

Click the Back button to return to the previous phase of the installation. Click Next to direct the InstallShield Wizard to accept the installation option that you have selected and to continue the installation process. Click Cancel to cancel the installation process.

The next phase of the VPN client installation is the confirmation window. This is the final window that you will review prior to the installation of the VPN client. It contains details such as the program and the driver(s) that are being installed. If you need to review any of the options that you have selected, this window instructs you to click the Back button.

Click the Back button to return to the previous phase of the installation. Click the Next button to direct the InstallShield Wizard to begin copying the installation files. Click the Cancel button to cancel the installation process.

The next phase of the installation process is the Setup Status window. There is a percentage status bar that will keep you informed of the installation progress. Only one button is available during this phase: Cancel. If you select this button during the installation, the installation will be aborted.

Once the VPN Client program has been installed, the next phase of the installation process is engaged. This phase is where the necessary drivers are loaded onto your PC. There are no buttons to select during this phase of the VPN client installation process.

The next phase of the VPN client installation is simply a window that informs you that your program folders and icons are being created. There are no buttons to select during this phase.

The next phase of the VPN client installation process is a window that will display the location that you specified you wanted the VPN client software to be loaded into, as well as the associated icons that are available. The icons you will see are the VPN client icon, the Readme.txt icon, and the VPN client uninstall icon. In Windows 2000, you can access these icons from your Start menu as well. Figure 3-51 shows an example of the program window that you will see.

The next window that you will see is a display window of the `readme.txt` file. You should read through this file as it details information about your VPN client software version. The `readme.txt` file displays Windows-specific information that may be important to you, depending on other applications you may be using. Although three buttons are displayed, only one is available (not grayed out). Once you have completed reading the information contained in this window, you will select the Next button to continue the installation process. Figure 3-52 shows an example of the `readme.txt` phase of the VPN client installation process.

NOTE **If you choose not to read the information in the readme.txt during the upgrade process, you can always refer to the `readme.txt` icon in Figure 3-51. It is the same information.**

Next is the final phase of the installation process. With VPN Client code version 6.01 and later, you are no longer required to reboot your PC for the application to work. You can optionally reboot, but it is no longer a requirement.

The only button that is available to you during this phase is the Finish button. Clicking Finish returns you to Windows. You are now ready to use your VPN client. Figure 3-53 shows an example of this window.

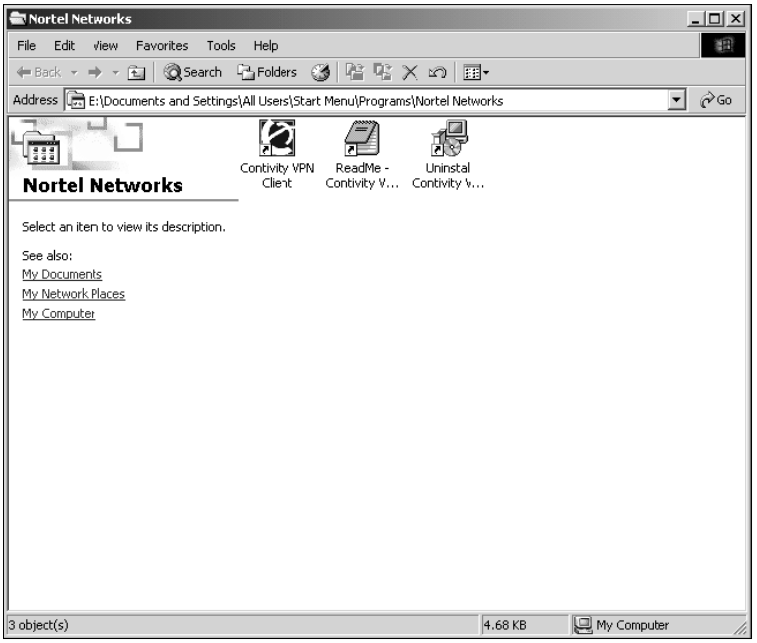


Figure 3-51: The location specified for the upgrade installation process

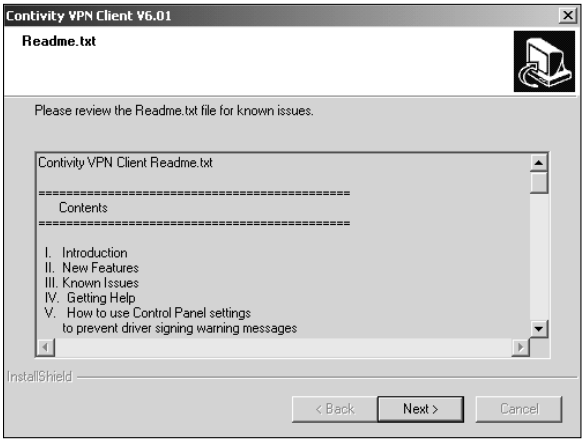


Figure 3-52: The readme.txt file phase of the upgrade installation process

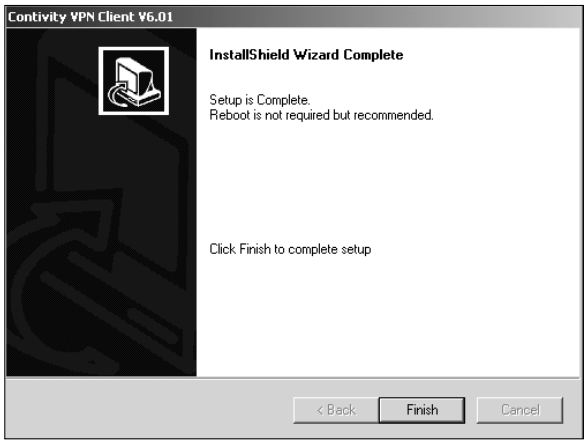


Figure 3-53: The "Installation complete" window of the upgrade installation process

NOTE **If you are installing over an existing VPN client, you will have to reboot your computer in order for the changes to take effect.**

Starting the VPN Client

Once you have loaded the VPN client onto your PC, you are ready to start it for the first time. There are a few options that you will need in order to set up connection parameters within your VPN client. Most of the time, your network administrator will provide the necessary parameters to you, but there may be times where you need to ensure the correct parameters before you are able to use your client to create a user tunnel to a remote LAN.

To start the VPN client for the first time if you are using a Window OS, select Start → Programs → Nortel Networks → Contivity VPN client. Figure 3-54 has an example of starting your client in this manner.

NOTE **The Start menu path may be different if you have chosen values other than default values when initially loading the VPN client.**

Another method in a Windows-based operating system environment to run your VPN client is to access the Start menu directory and to double-click the Contivity VPN Client icon. Figure 3-55 shows an example of running the VPN client from the directory in which is it located.

After the initial configuration of your first connection profile, you will no longer be prompted with the Connection Wizard window when you start your VPN client. If you want to use the services of the Connection Wizard when setting up additional profiles, you can access the wizard by selecting File → Connection Wizard from the VPN client main window (see Figure 3-57).

The Nortel VPN client contains a Connection Wizard that will assist you in setting up a connection. The Connection Wizard runs automatically when you start the Nortel VPN client application for the first time. If you are not an advanced user of the Nortel VPN client, we recommend that you allow the wizard to assist in setting up your first connection. Figure 3-56 shows an example of the Connection Wizard window.

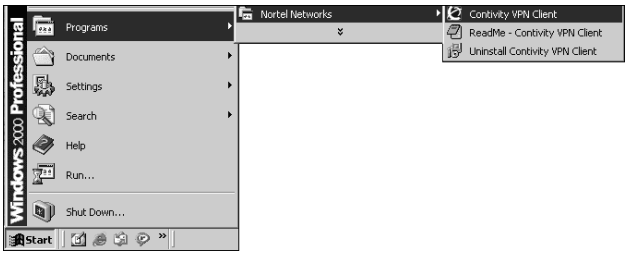


Figure 3-54: Starting the VPN client from the Start menu

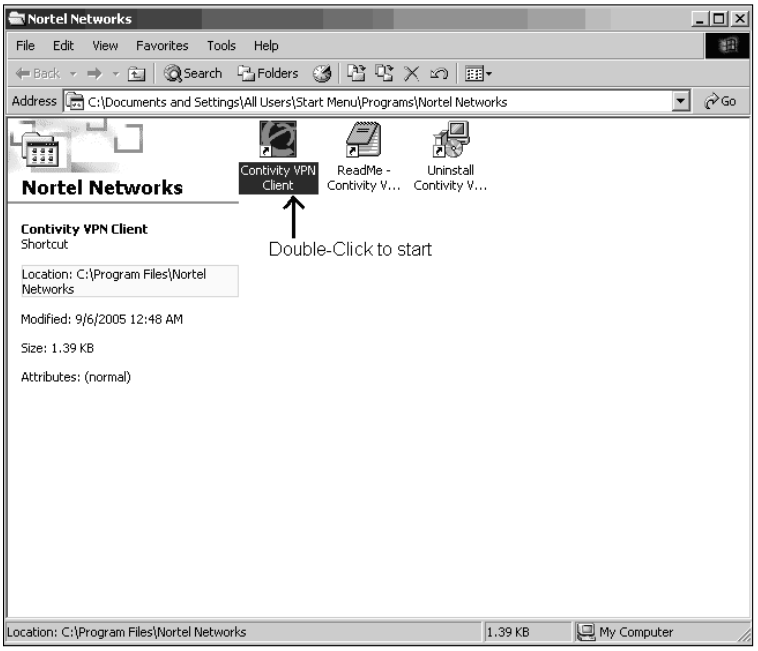


Figure 3-55: Starting the VPN client from a directory

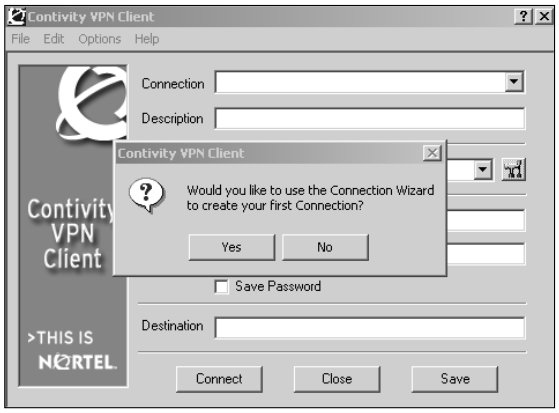


Figure 3-56: When starting the VPN client for the first time, you will see the Connection Wizard window.

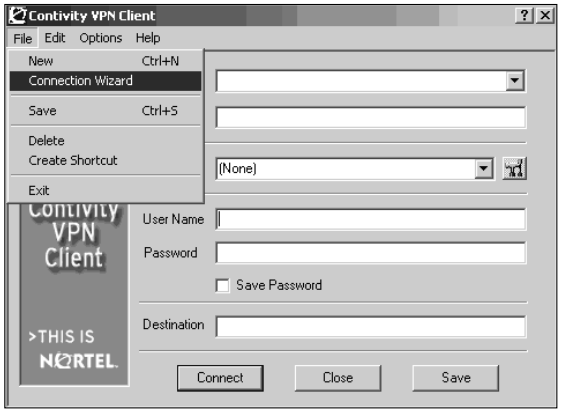


Figure 3-57: Accessing the Connection Wizard from the VPN client main window

After you have been prompted about whether or not you want to run the Connection Wizard to establish your first connection, you will move on to the remainder of the initial start process.

If you selected that you did not want to run the wizard, you will be directed immediately to the VPN client main window shown in Figure 3-58.

NOTE **If you opted not to run the Connection Wizard, you will have to establish your connection parameters manually. You can also run the Connection Wizard at any time by selecting File → Connection Wizard.**

The VPN Client Connection Wizard Process

If you selected the option to run the Connection Wizard (either by initial setup, or selecting the Connection Wizard menu), you will be prompted with a series of setup options. The options that you are prompted for are required and must be filled out completely to establish your connection.

The first phase of the Connection Wizard setup is the New Connection Profile (see Figure 3-59). The new connection profile will be the profile that is used by you (the end user) to identify the connection profile on your PC.

There are two fields of information in the connection profile window. The first is required and it identifies the name of the connection profile. For example, if you want to set up a connection profile to your corporate LAN, you may want to name the connection profile "Work." If you are setting up a connection profile to a remote office for a business partner named "Pal-partners," you may want to name the connection profile "Pal."



Figure 3-58: If you opted to not run the Connection Wizard, you will receive this window.

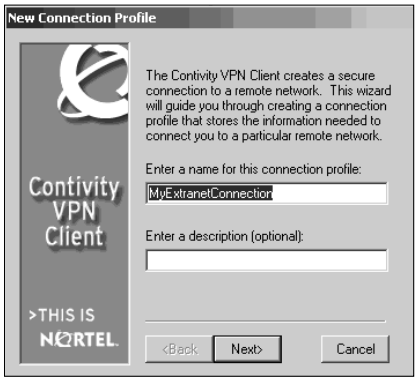


Figure 3-59: The New Connection Profile dialog box

The second field that is available in the New Connection Profile dialog box is a description of the profile. This is an optional field and it can assist you in defining the connection profile. For example, if you are setting up a connection profile to your corporate LAN, you may want to describe the connection profile as "Main corporate LAN." If you are setting up a connection profile to a remote office for a business partner named "Pal-partners," you may want to enter the description "Invoice checking."

No matter what names you use to identify the connection in the New Connection Profile dialog box, these names are there to assist you (the end user) in locating and utilizing a connection.

In the next dialog box, you choose the authentication type for the connection that you are creating (see Figure 3-60). You have three different options to select, and the one you choose depends on the type that has been configured by the network administrator.

The first option is for username and password authentication. The second option is for either hardware or software token card authentication. The final option is for a digital certificate or smart card.

Select the authentication type and click Next. The other button options are Back (to return to the previous menu) and Cancel (which cancels the connection setup).

The remaining steps of the connection setup depend upon the authentication type that is being used. In the following section, we discuss the remaining steps of the connection setup based upon the chosen authentication type.

Selecting Username and Password Authentication Type

If you chose username and password authentication, you will now receive a window asking you to identify the username and password that is to be used for you to be authenticated upon connection to the VPN Router (see Figure 3-61). You will enter the username and password that were provided to you by you network administrator. All characters are case sensitive, so it is important that you enter this information correctly. A "Save the Password" button is available to save the password so you do not have to enter it each time.

NOTE **If this is a custom install provided by your network administrator, then the administrator may have removed the option to save the password. This is done for security reasons and will require that you enter the password each time you connect to the VPN Router.**

Once you have entered the username and password, you have an option to continue (Next), cancel (Cancel), or to return to the previous menu (Back).

In the ensuing window shown in Figure 3-62, you are asked if you have group ID and password authentication information or not. This information

is provided by the network administrator and is determined by the needs of the LAN.



Figure 3-60: The Authentication Type dialog box



Figure 3-61: The User Identification dialog box



Figure 3-62: The Group Authentication Information dialog box

Select whether or not you have the Group ID and password authentication information and then click Next. The other button options are Back (to return to the previous menu) and Cancel (which cancels the connection setup).

No Group ID and Group Password

If you are not using Group ID and password authentication, you are now asked to provide the IP address or host name that you will be connecting to (see Figure 3-63). This is the public interface of your VPN Router. Enter the IP address or the host name and then click Next. The other button options are Back (to return to the previous menu) and Cancel, which cancels the connection setup.

With Group ID and Group Password

If you are using Group ID and password authentication, you are now asked to provide the Group ID and the Group password (see Figure 3-64). Enter the Group ID and the Group Password and then click Next. The other button options are Back (to return to the previous menu) and Cancel (which cancels the connection setup).

In the next window (see Figure 3-65), enter the IP address or the host name and then click Next. The other button options are Back (to return to the previous menu) and Cancel, which cancels the connection setup.

Finally, you choose whether or not you want to create a dial-up connection that will be used to initiate your VPN connection (see Figure 3-66). Choose whether or not you need to dialup (to an access provider) prior to initiating your VPN connection. Choose either Back, Next, or Cancel.

The setup of the connection is now complete. You will receive a window informing you of this, and then you can select one of the option buttons to complete the configuration of your VPN connection. In Figure 3-67, you can see that by clicking Finish you are now be able to test your connection.

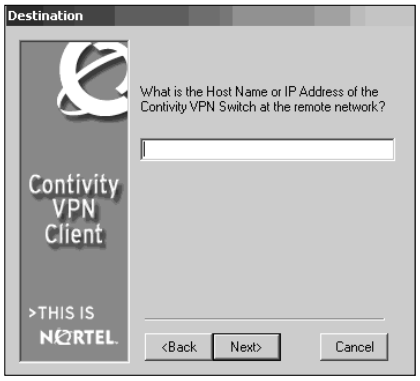


Figure 3-63: The Destination dialog box



Figure 3-64: The Group Authentication Information dialog box



Figure 3-65: The Destination dialog box



Figure 3-66: The Dial-up Connection dialog box

Selecting Hardware or Software Token Card Authentication Type

If you are selecting Token Card Authentication, you are prompted with a window where you select the Token card type you are using (see Figure 3-68). Select the appropriate Token card type and click the appropriate option button at the bottom of the window.

Next, you are prompted to enter the token card User ID, as well as Token group logon information (see Figure 3-69). Enter the correct logon information and then select one of the buttons at the bottom of the window.

In the next window (see Figure 3-70), enter the IP address or the host name and then click Next. The other button options are Back (to return to the previous menu) and Cancel (which cancels the connection setup).

Finally, you choose whether or not you want to create a dialup connection that will be used to initiate your VPN connection (see Figure 3-71). Choose whether or not you need to dialup (to an access provider) prior to initiating your VPN connection. Choose either Back, Next, or Cancel.



Figure 3-67: The Connection Profile Complete notification window



Figure 3-68: The Use Token Card dialog box

The setup of the connection is now complete. You will receive a window informing you of this and then you can select one of the buttons to complete the configuration of your VPN connection. In Figure 3-72, you can see that by clicking Finish, you will now be able to test your connection.



Figure 3-69: The Token Group Information dialog box

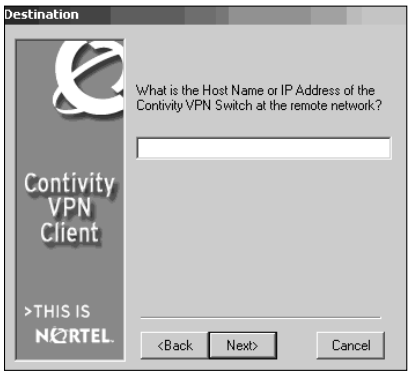


Figure 3-70: The Destination dialog box



Figure 3-71: The Dial-up Connection dialog box



Figure 3-72: The Connection Profile Complete notification window

Summary

Networking hardware is only as good as the software that it is running. Ensuring that the needs of a LAN are supported is fundamental in future operations and potential growth.

In this chapter, we have reviewed the Nortel VPN Router software and the Nortel VPN client software. The chapter also offered an overview of the features that are provided with this software.

We also covered how to establish an initial connection to the VPN Router for the purpose of software verification and upgrades. The examples used throughout this chapter should assist the reader in establishing initial connection on both the VPN Router and the end-user work stations.

Now that we have discussed the software for the VPN Router, we will be discussing the technologies supported by this software. In Chapter 4, we discuss VPN networking, including VPN tunneling protocols and technologies. Nortel VPN routing deployment strategies are also discussed.

CHAPTER

4

The Nortel VPN Router in the Network

This chapter discusses how a VPN Router is deployed in the network. There are many differing topologies for networks, and it is beyond the scope of this chapter to cover each and every topology. However, the chapter provides examples of how a VPN Router may be deployed in a network, along with a discussion of various features of the VPN Router and how it may be used within a network. Networks vary in size from the Small Office or Home Office (SOHO) to large corporate Central Offices, and examples of each will be discussed within the scope of this chapter.

Before getting into the discussion of how a VPN Router may be utilized in a network environment, it may be useful to review what VPN tunneling provides and some basic VPN tunneling principles.

What Is a Virtual Private Network?

The Internet is a large, meshed network that allows people and entities to communicate with one another on a global scale. This network for the most part is insecure with much of the information passed over it being in easily readable, clear text format. Prior to the availability of VPN technology, government agencies, companies, and only a select few individuals could afford secured,

dedicated point-to-point communication because of the high cost of implementation and maintenance. These dedicated communication links were extremely rigid and could not be easily moved or reconfigured.

With the emergence of VPN technology, secure transmittal of information can be accomplished by using the large, meshed, global network of the Internet at lower costs, with a higher degree of flexibility and ease of configuration.

The Internet is not secure for the transmission of confidential information, so how can this be accomplished? The answer is a rigorous form of encryption that, even if the information is intercepted, has a high improbability of being deciphered. The implementation of VPN Routers connected to the Internet allows for the creation of a virtually private and secure network between them. This can be visualized in Figure 4-1 as a tunnel through the Internet, allowing two endpoints to communicate with each other with total security.

The visualization of the VPN tunnel as a conduit passing secure data between two publicly accessible IP addresses through the Internet is simply for the ease of illustration. In reality, data from the private IP space behind VPN Device A destined for the private network space behind VPN Device B is encrypted by VPN Device A using encryption techniques that are difficult to decipher. Data from behind VPN Router A is encrypted and sent over the Internet to VPN Router B, where it is deciphered and directed to the device on its private IP network that the data is intended for.

The types of encryption used on Nortel VPN Routers are *Data Encryption Standard* (*DES*), which is also referred to as *56-bit encryption*, and *Triple Data Encryption Standard* (*3DES*), which may also be referred to as *128-bit encryption*. After encrypting the packet received on its private IP space interface, VPN Device A passes it out on its public IP space interface as an *Encapsulating Security Packet* (*ESP*) with a destination address of the public IP space address of VPN Device B.

VPN Devices A and B have created a tunnel that allows them to send and receive packets with encrypted payloads, which may only be deciphered by them. This tunnel has been established prior to the sending and receiving of secure ESP packets with parameters that both devices have been configured for in this particular tunnel.

These parameters include a *Pre Shared Key* (*PSK*) encryption being used to encrypt data packets, networks accessible on both secured private networks, and the public IP addresses assigned to each public interface. Both devices have negotiated these parameters during the initial creation of the tunnel. Once these parameters have been accepted and agreed to by both devices, the tunnel is established and secure ESP packets are passed between them.

You can find further discussion of tunnel creation in Chapters 6 and 7.

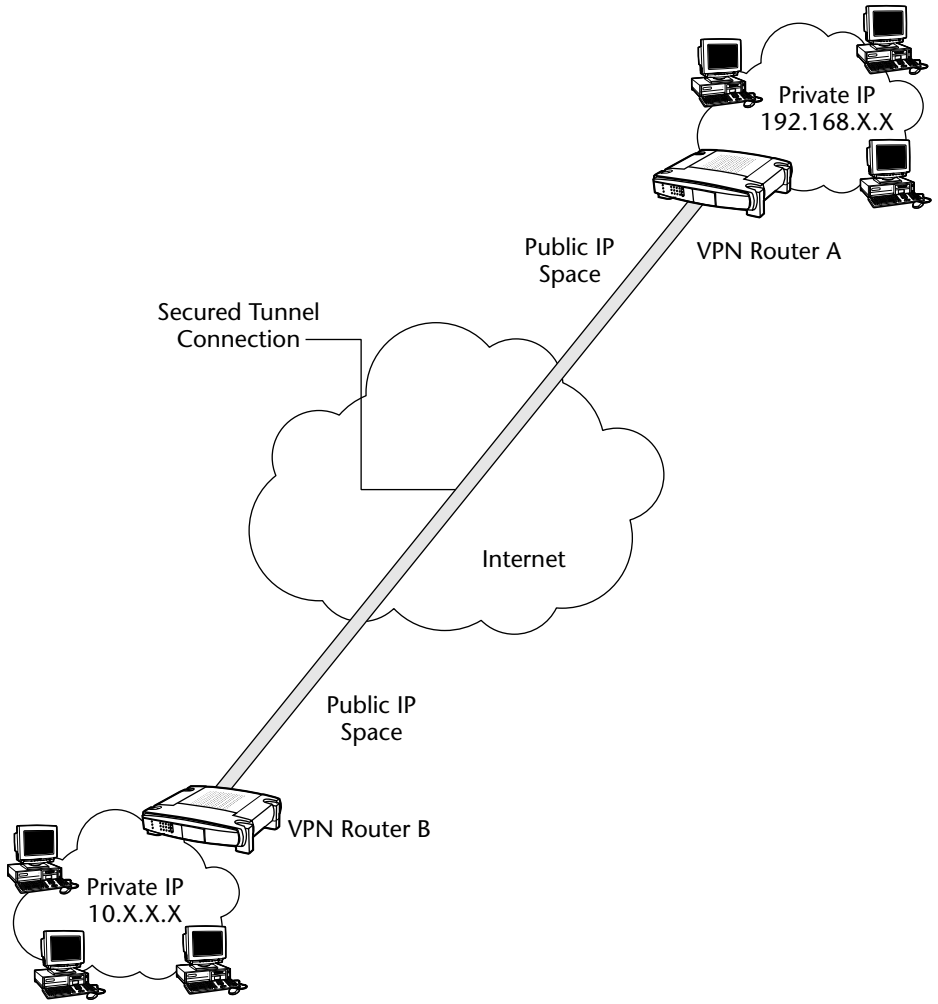


Figure 4-1: VPN secure tunnel through the Internet

Tunneling Basics

The major tunnels in use in VPN technology today are Branch Office Tunnel (BOT), Aggressive mode Branch Office Tunnel (ABOT), and User/Client tunnel. These tunnels all use the same encryption techniques, but differ in implementation because of environment and other various configuration factors.

A brief description of each will be discussed in this chapter, along with further discussion in subsequent chapters.

Branch Office Tunnel

BOTs are formed between two VPN-enabled devices with known Internet (IP) addresses. These are usually formed between larger, fixed installations that do not require any degree of mobility. Installations of this type are usually used between Central Offices and Regional Offices, which often used dedicated links. However, with VPN technology, they are using the Internet to provide the required connectivity. (Central Offices and Regional Offices are discussed in more detail later in this chapter.)

Because the endpoint address of each endpoint is fixed, those addresses are used as part of the overall tunnel definition. These types of tunnels are also sometimes referred to as *peer-to-peer tunnels*, and tunnel initiation can be started by devices on either end of the tunnel.

Local area network (LAN) subnet addresses that are to be permitted to participate in the tunnel are defined and fixed by the definition of accessible networks using this tunnel behind each endpoint VPN-enabled device. Devices residing on subnet addresses that are not defined within the accessible network definition are not permitted to send data over the tunnel. Data packets from these not-permitted subnet addresses destined for a subnet defined on the other endpoint are dropped by the receiving VPN-enabled device.

BOTs may be configured in a manner to force all IP data from a remote endpoint though the tunnel to the Central Office. This type of tunnel is usually referred to as *mandatory tunneling*, where all traffic must be passed though the Central Office's network no matter what its ultimate destination IP address is. Reasons for this type of tunneling include the enforcement of corporate policies with regard to Internet access, as well as providing the capability to perform an accounting of Internet usage. This places an increased burden on the Central Office as far as using the capacity of its networks to pass data, which eventually finds its way to an IP address that may reside out on the Internet.

An alternative to mandatory BOTs is using split tunneling. *Split tunneling* occurs when a BOT configuration is such that traffic destined for IP addresses not defined in the accessible network definitions is permitted to be passed out the public interface to the Internet. The main advantage to this tunnel configuration is that it reduces the bandwidth demand on the Central Office networks by not having it route data that is ultimately destined for an address out on the Internet. Internet access policies can be instituted locally on the remote office's VPN device. The main drawback is that it adds another layer of required configuration and maintenance of policies for that device. Figure 4-2 shows a representative BOT.

In Figure 4-2, a BOT is established between two VPN Routers—one located in New York City and the other in Los Angeles—over the Internet. The accessible network on the private side of the New York City VPN Router is 192.168.X.X. This IP notation is used to designate a class B IP address space.

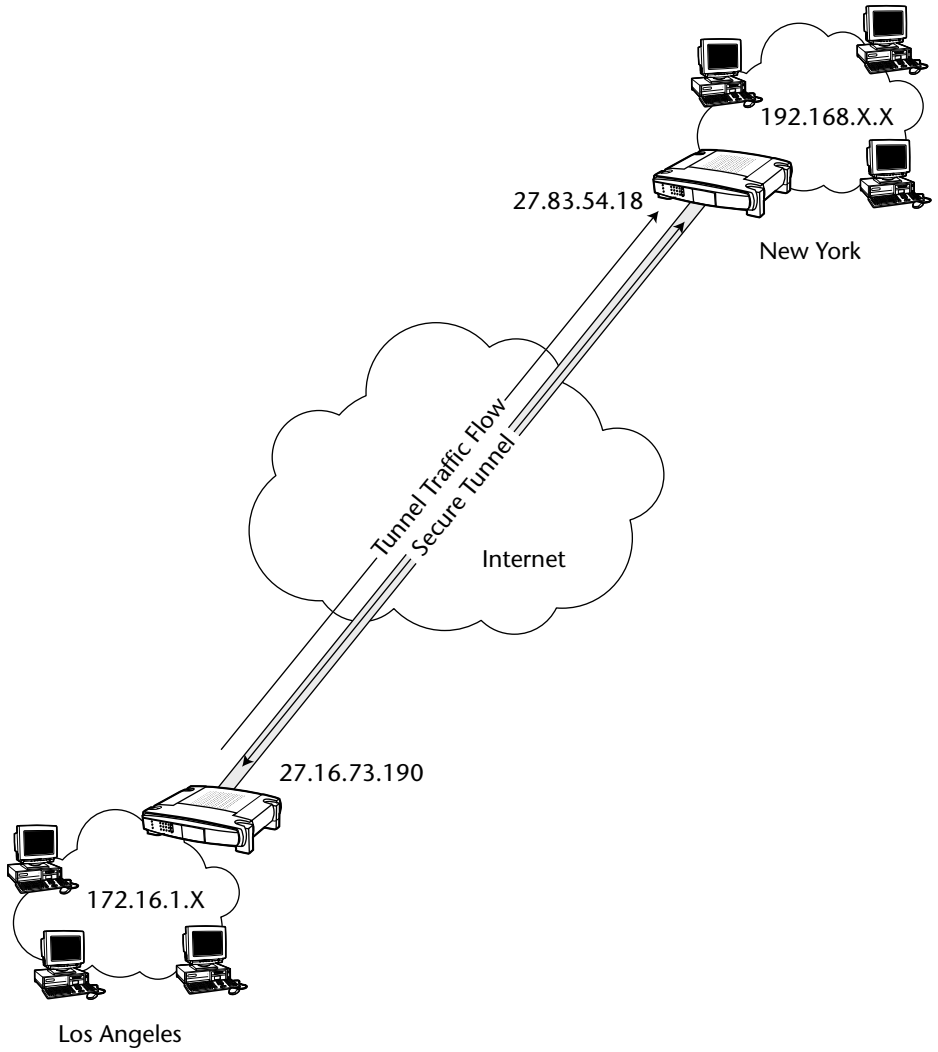


Figure 4-2: Typical BOT installation

This means all addresses in the range of 192.168.0.1 to 192.168.255.254 are located on the New York City private LAN. So, when a packet arrives from the private LAN on the Los Angeles VPN Router with a destination address that is within the private IP address space located on the New York private LAN, then the Los Angeles VPN Router encapsulates the packet and passes it out to the public IP address space interface with a source address of 27.16.73.190 as a secure ESP packet with a destination address of 27.83.54.18.

When the packet is received on the public IP interface of the New York VPN Router, it determines it is a packet from a secure VPN tunnel, which it has established with the Los Angeles VPN Router. The packet is deciphered by the

New York City VPN Router and placed on its private IP space interface located on the local LAN. The packet is routed over the LAN to its target destination.

The example in Figure 4-2 is a typical BOT where split tunneling may be enabled. As mentioned previously, split tunneling refers to allowing traffic that is not destined for the other end of the tunnel to be passed out the public IP interface to its default gateway on the Internet. To allow this type of IP traffic flow, a firewall must be enabled on the VPN Routers. (Chapter 7 provides further discussion on the firewall feature.)

When a packet arrives at the New York City VPN Router private IP interface, and has a destination address other than the private IP address space located behind the Los Angeles VPN Router of 172.16.1.X, it is passed out to the Internet from the public IP interface to its default gateway. There the packet appears as a normal unencrypted packet and is routed over the Internet to the address it was intended to be delivered to.

With the firewall enabled, the traffic from the 192.168.X.X private IP address space (which is normally non-routable over the Internet) is sent out through Network Address Translation (NAT) with a packet showing the source address as being from the public IP address of the New York City VPN Router (which allows it to be routed over the Internet to its destination).

Figure 4-3 shows an example of a mandatory tunnel configuration. In the example, the Syracuse office has an accessible remote network defined as 0.0.0.0/0, which takes all the traffic destined for an address that is not located on the local LAN of 172.16.2.X and sends all of that traffic to the other end of the tunnel to the New York City private LAN.

The New York City VPN Router will decipher the packet and send it to the address for which it is intended. If the packet has a destination other than the local LAN address, the VPN Router sends it to its Private LAN default gateway, which will assist in routing it to the destination address in the original packet.

Aggressive Mode Branch Office Tunnel

An Aggressive mode Branch Office Tunnel (ABOT) is very similar to a BOT, but is used when one tunnel endpoint is unable to have a fixed endpoint Internet (IP) address for various reasons. The reasons may be wide and varied but could include the following factors:

- Unavailability of a dedicated IP address at the access point to the Internet
- The types of service provided by the local Internet service provider (ISP)
- Flexibility in being able to relocate quickly
- Cost savings

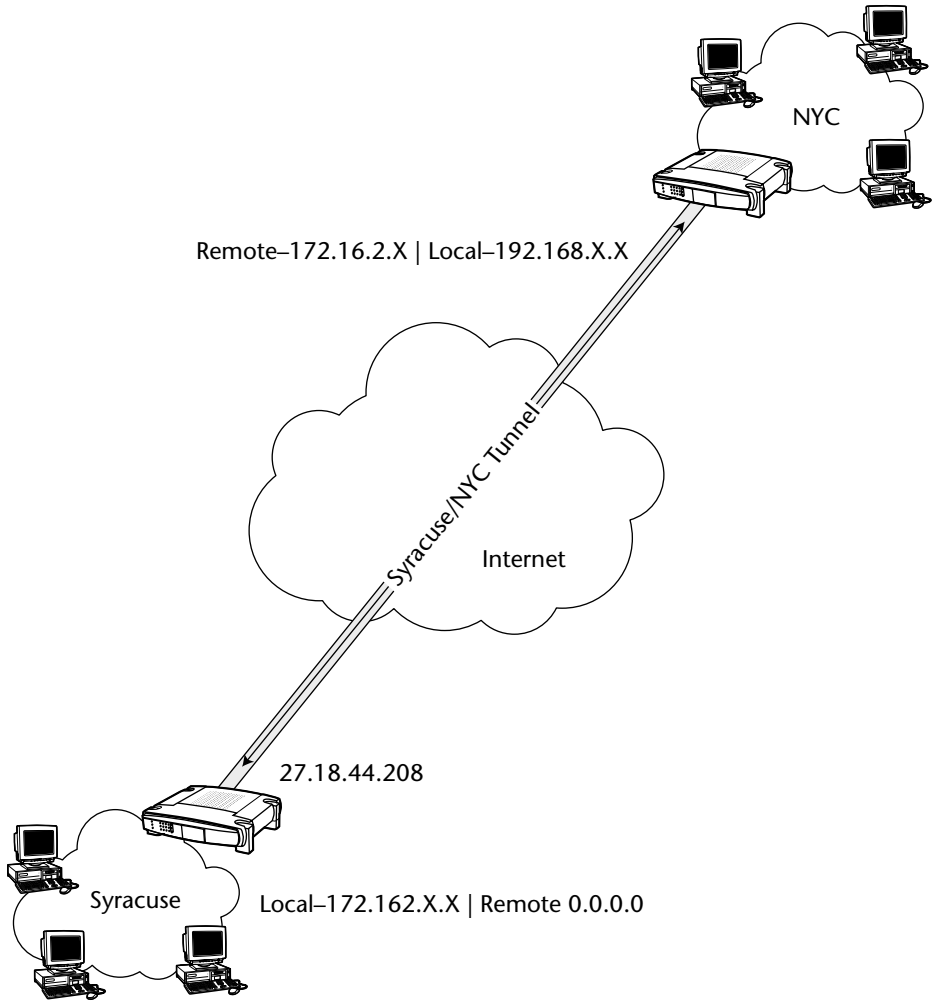


Figure 4-3: Example of mandatory tunneling BOT

The Internet has a fixed number of addresses and, at times, a dedicated address is not available from a provider because allocated address space has been exhausted. Some providers have set portions of their assigned address space to be used for dynamic address allocation. This type of IP address assignment is usually used with dialup services, which may include analog telephone access via modem, Integrated Services Digital Network (ISDN), or Digital Subscriber Line (DSL) telephone services.

Other types of Internet access that are currently being provided are Point-to-Point Protocol over Ethernet (PPPoE) and cable Internet access. Both of these services are most commonly set up to use dynamic address allocation. However some providers of these services are able to provide dedicated IP

addresses. In the areas where the population is small and spread out they are usually serviced by smaller independent Internet service providers (ISPs) who can provide only dynamic IP address assignment.

Generally, using dynamically allocated IP addresses results in a lower subscription cost service with ISPs who charge a higher monthly rate on accounts that require a dedicated IP address.

An advantage to using an ABOT is a certain degree of mobility that it provides. ABOT requires only a minimal amount of configuration changes on the VPN-enabled device that is initiating the tunnel, and only deals with the changes it requires to obtain local Internet access. The Main VPN device on the other end of the tunnel with a fixed IP address will require no configuration changes at all.

The disadvantage to using an ABOT configuration is that the tunnel can only be initiated from the VPN-enabled device with the dynamically assigned IP address because the main VPN device with the statically assigned IP address is unaware of that device's endpoint address.

Some vendors of VPN-enabled devices utilize keep-alive signaling to nail up a tunnel once it is initiated so that it is in a constant enabled-tunnel state, allowing IP traffic to flow from the Central Office site even if the remote end of the tunnel is in an unmanned office.

Another term used in the description of an ABOT is *Initiator/Responder Tunnel*. The advantage of this type of tunnel configuration is that it does offer a degree of mobility and is suitable for use in the setting up of a temporary office, or in areas where dedicated IP addresses are not available. Figure 4-4 shows an example of an ABOT.

In Figure 4-4, a remote office located in White Plains, New York, is configured to have an Aggressive mode tunnel to the New York City main office. Its connection to the Internet is through a service such as DSL or PPPoE where there is no dedicated IP address at that location. Because this is an ABOT, the tunnel negotiation and establishment needs to be initiated from this office to the New York City office, thus the alternative name of an Initiator/Responder Tunnel.

The tunnel always must be initiated from this side because there is no dedicated public IP address for the tunnel to have it initiated from the main office in New York City. This may be a problem at times because if the tunnel is not established, then resources at the White Plains office are not accessible from the New York City main office.

The tunnel nailed-up feature on the Nortel VPN Routers allows for the tunnel to remain up after it is established so that traffic can flow over the tunnel and it will not time-out in periods of inactivity, as it would normally if this feature were not utilized.

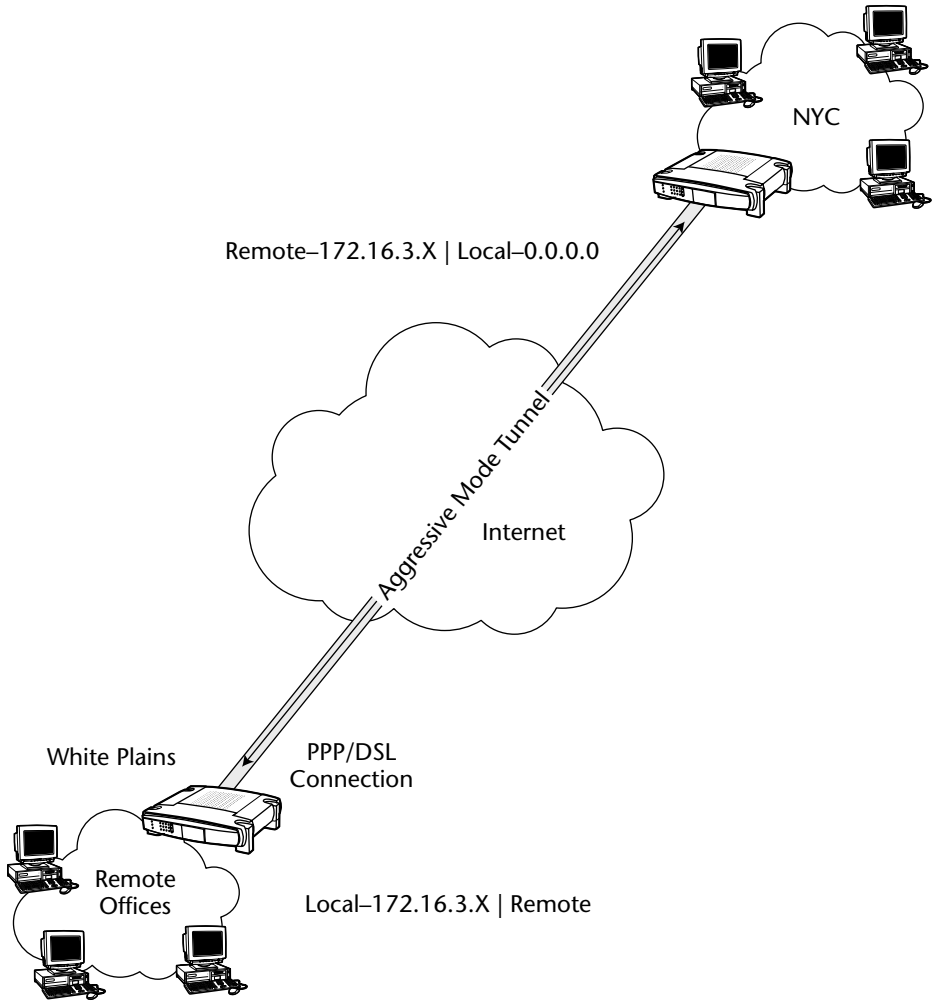


Figure 4-4: ABOT configuration

User/Client Tunnel

User or Client Tunnels may be originated directly from a user PC or a VPN-enabled device acting as a client. If originating from a user's PC, software will be required to allow for a secure tunnel connection to the VPN Router. Following are the most widely used secure connection types:

- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunnel Protocol (PPTP)
- Layer 2 Forwarding protocol (L2F)
- IP Security (IPSec)

PC-Based VPN Tunnels

PCs running VPN tunneling software can make secure connections directly to VPN Routers. These users must be authorized for use of that VPN Router by being on the approved access list of the device or the network to which they are attempting to attach.

Various methods of authentication are in use, and they will be discussed further in Chapter 6. A user is either permitted or denied access to resources on the network behind the VPN Router by the level of permissions that has been granted to the user directly or by inherited rights from a group association that the user is a member of. Users can be restricted in what resources are available to them utilizing the authentication process to set their permission level upon access.

The Nortel VPN Routers support the mentioned tunneling protocols. However, Nortel provides a proprietary IPSec VPN Client Software for users connecting using this tunneling protocol to connect to Nortel VPN Routers. This client software is supported on the following operating systems:

- Microsoft Windows
- McIntosh
- Linux
- Palm handheld platforms

Figure 4-5 shows an example of user tunnel connections.

Figure 4-5 contains examples of how PC-based clients are able to connect to a VPN Router over the Internet. For the purpose of this example, it is assumed that all the PCs are using the Nortel VPN Client Software and using the IPSec tunneling protocol to connect to the main office VPN Router.

The users in Auburn are using a NAT-enabled router that may connect to the Internet over DSL, PPPoE, or cable Internet access. Routers with this capability are readily available in many computer retail outlets and are intended for the Small Office or Home Office (SOHO) environment to allow multiple computers to connect to the Internet from a single connection to an ISP. This is accomplished by using the NAT protocol. This means the LAN behind the router is an address space that is in the private or non-routable category. Table 4-1 shows the standard for these non-routable addresses over the Internet.

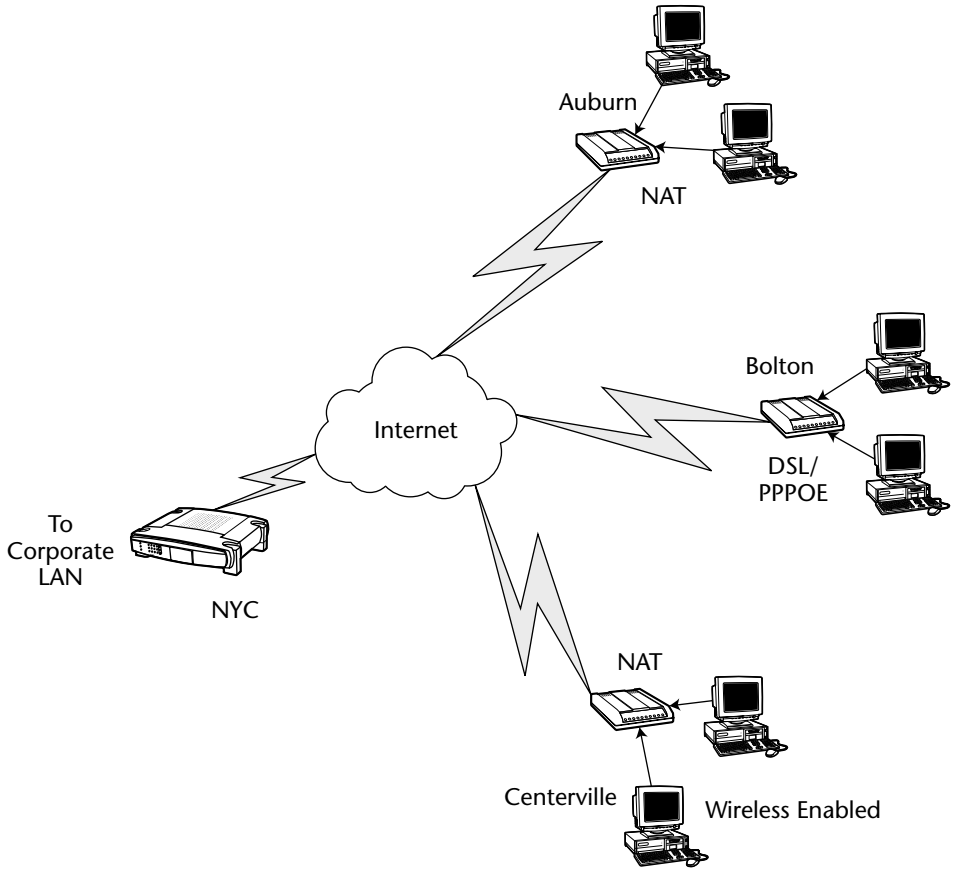


Figure 4-5: User VPN tunnels

Table 4-1: Non-Routable IP Address Standard

ADDRESS	CLASS	RANGE
10.X.X.X	Class A	10.0.0.0–10.255.255.255
172.16.X.X	Class B	172.16.0.0–172.16.255.255
192.168.X.X	Class B	192.168.0.0–192.168.255.255

If a packet contains one of these non-routable addresses, the first router on the Internet that receives it will not forward it to its next hop router. The packet will simply be dropped. So, how does a PC on a private IP space with non-routable addresses access the Internet? It is with the use of NAT, which is at times referred to as *port NAT*. The NAT-enabled router connects to the Internet and allows for multiple PCs to access the Internet through it. This is accomplished using a port-mapping NAT table to keep track of the sessions it has established. So, it permits PCs behind it to be able to connect to servers that are out on the Internet, even though their addresses are considered to be non-routable addresses.

An example of this would be that both PC-A and PC-B at the Auburn office will like to access two different HTTP Web servers on the Internet. The Web browser on both PCs use port 80 for HTTP services. Although they are on different private IP addresses, when the request is sent out from a NAT-enabled router, the router sends both requests to their respective Web servers using its public IP address as the source address along with port 80. This is accomplished by using a port address table to keep track of the sessions from the PCs to the differing servers on the Internet. Figure 4-6 shows an example of how port NAT is accomplished.

The true reason for the discussion on NAT is that VPN security is usually established and maintained by the knowledge of both endpoint addresses along with the use of port 500 to establish a VPN tunnel. If NAT is in use between a VPN client PC and the VPN Router it is attempting to construct a VPN Tunnel with, then the client PC IP address is masked by the NAT process. To overcome this, VPN Routers use a function called *NAT Traversal*. When enabled on a VPN Router, this function negotiates the port being used to establish and maintain a VPN tunnel connection.

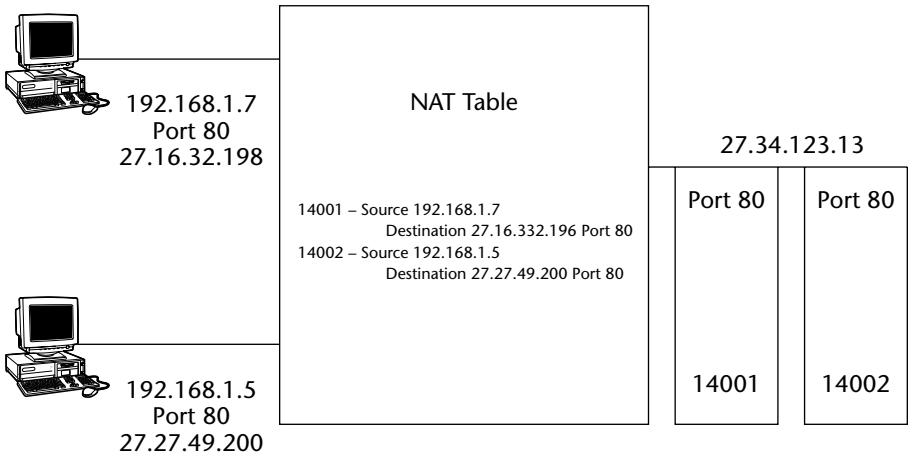


Figure 4-6: Port NAT-enabled router

NAT Traversal works well, but at times there are difficulties with this functionality over the Internet because of ports being blocked by ISPs or firewalls in use in front of the VPN Routers. The different aspects of NAT are discussed in the subsequent chapters of this book, and extensively in Chapter 10.

In Figure 4-6, both PCs make a Web page call to two different Web servers on the Internet. The NAT-enabled router receives this request on its private side interface. It takes the request packet from each PC and adds it to a NAT table.

The table uses a port address that is not in the normal port address range to construct a table to keep track of session requests and responses. To follow a transition through the router (refer to Figure 4-6), we will use the Web request of PC-A to see how this is done.

PC-A is requesting a Web page on port 80 from Internet Web server 27.16.32.198. The NAT-enabled router accepts this request packet and adds it to its port NAT table using port address 14001. (These port addresses are purely arbitrary and are being used only for example purposes.) The assignment of port 14001 in the NAT table has the true source address of the requesting PC—in this case, 192.169.1.7 using a port 80 call. The NAT-enabled router then modifies the request packet, inserting its own public IP address 27.34.123.13 and port 14001 in place of the PC-A source address and requesting port. The modified packet is then placed on the wire to the Internet, where it is routed to the destination address.

The Web server at that address accepts this request and then sends a response packet addressed to the NAT-enabled router's public IP address using port 14001. The Nat-enabled router accepts this response packet and, noting it is a call for port 14001, uses its NAT table and forwards the packet onto the private LAN with a destination address of 192.168.1.7 using port 80. When PC-A receives this packet, it has completed the request/response session between itself and the Web server that the page is being requested from.

This example is a bit of an over-simplification, but it is intended for those who are unfamiliar with NAT and its uses between hosts (client/servers) over the Internet.

VPN-Enabled Device Acting in Client Mode

Earlier, this chapter discussed the creation of BOTs and ABOTs. There is a major difference between these types of tunnels when a VPN device acts in client mode. For the different BOT modes we discussed the use of routing between accessible networks on both sides of the VPN tunnel. However, when a VPN-enabled device connects in client mode, it is treated as if it were a single user tunnel, like that created using a PC and a VPN tunneling software application.

Just as the single-user tunnel is assigned an IP address that is routable on the private side network, so also is a VPN-enabled device assigned such an address. However, a VPN-enabled device that creates a VPN tunnel can be used to allow many users access to the same network resources without the need for VPN tunneling software to be loaded on their PCs. This is accomplished by a feature of the VPN device being able to perform a many-to-one NAT using the assigned IP address as the gateway to access the network resources at the other end of the VPN tunnel.

There will be more discussion of NAT later in this chapter. Figure 4-7 shows an example of a VPN-enabled device acting in client mode.

In Figure 4-7, The Needham VPN-enabled router connects to the Internet over a DSL PPPoE connection. The public IP address it receives from the ISP is dynamically assigned, so the tunnel type in this particular case is an Aggressive mode type tunnel. Although the Client mode tunnel is a form of an ABOT, it differs from an ABOT because it is assigned an IP address that is routable on the private LAN behind the VPN Router with which the tunnel is established.

In this particular example, there is a Boston-based VPN Router with a public IP address of 27.139.48.206 with which the Needham VPN-enabled router has established a Client mode tunnel. The public IP address of the Needham VPN-enabled router is dynamically assigned, so it may be any IP address that is able to be routed over the Internet.

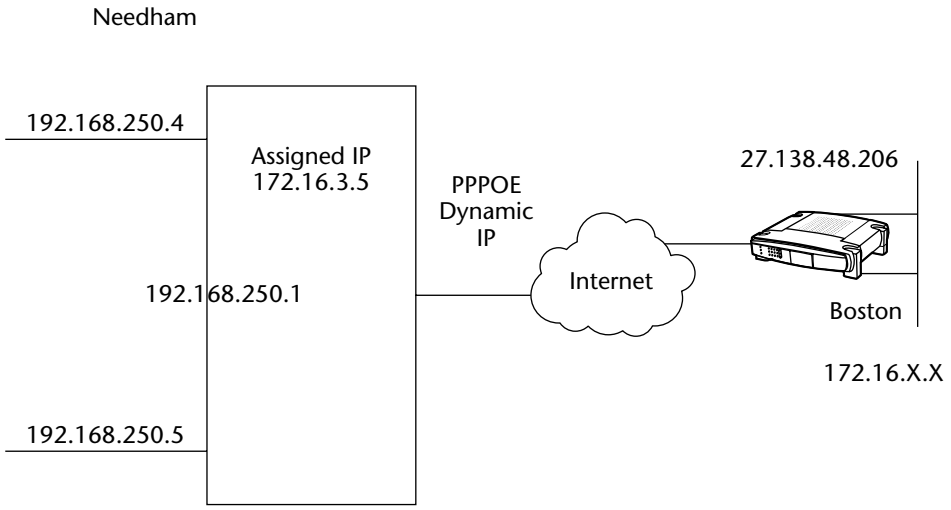


Figure 4-7: VPN-enabled device acting in client mode

The private LAN IP address that is behind the Boston VPN Router is 172.16.X.X. The Needham VPN-enabled router with the Client mode tunnel has been assigned a client address of 172.16.3.5, which is used to route traffic from its private LAN with an IP address of 192.168.250.X. The Needham client IP address of 172.16.3.5 is a routable address over the Boston private LAN. The Needham PCs have addresses of 192.168.250.4 and 192.168.250.5, which use the IP address of 192.168.250.1 assigned to the private LAN interface as their default gateway address. This means that traffic destined for an IP address not on the local network is routed to that address to be processed and routed over the Internet.

In this example, the Needham VPN-enabled router has *split tunneling* enabled. This allows traffic that is not destined for the Boston private LAN of 172.16.X.X to be routed to its public default gateway assigned by the ISP unencrypted so that it may be routed to its destination over the Internet. The Internet-destined traffic that is unencrypted is able to be routed over the Internet because the packet source IP address is the public interface IP address. This is accomplished with the use of NAT, which translates the private LAN IP addresses of 192.168.250.X as the source address to that of the public interface. This address becomes the source address assigned to the packet before it is sent out over the public interface to the Internet.

Traffic destined for the Boston private LAN of 172.16.X.X is processed by the Needham VPN-enabled router. The packet is modified using NAT to translate the source address from the private LAN IP address of 192.168.250.X to that of the address assigned as the client address of 172.16.3.5. After the translation is completed, the packet is encapsulated in an Encapsulated Security Packet (ESP), which uses as its source address the IP address of the public interface of the Needham VPN-enabled router before being sent out to be routed over the Internet. The use of the client address allows the Needham private LAN address devices with the use of NAT to access resources on the private LAN behind the Boston VPN Router.

An advantage to using a VPN-enabled router in client mode is that the private IP space behind it is hidden or shielded from devices on the Boston private LAN by using the client IP address for NAT translation.

A disadvantage is that the Boston private LAN devices are not able to establish connections directly to devices on the Needham private LAN. This type of tunneling is best used when there is a need for client/server applications, where the clients reside at a remote office and must access servers at a centralized site such as the Boston office in this example. This allows for the applications to be used without allowing the Boston private LAN devices access to any of the devices located on the Needham private LAN.

Small Office or Home Office

The *small office* may range from one to a few users, while a *home office* is normally a single-user environment. A VPN Router in this environment would be used as an Internet gateway to access resources available on the Internet, along with the capability to form a VPN tunnel to either a Regional Office or a corporate Central Office to take advantage of the resource available at those locations.

The normal corporate services would consist of email and access to corporate databases, where information may be accessed and shared. Users may also run client/server applications with their local PC acting as a client to an application server located on the private network at either a corporate Central Office or Regional Office.

The VPN tunnel may also be used to carry Voice over IP (VoIP) between a central phone switch located at either the corporate central or Regional Office. To have corporate telephone services available to them, users may either use a soft telephone or an IP-enabled telephone handset.

A *soft telephone* is software on a user's PC that utilizes the voice and sound capabilities of the computer to digitize and form packets of the voice data, as well as receiving VoIP packets and converting them to analog signals to allow the user to hear the sound signal received from the central phone switch.

An *IP-enabled telephone handset* has the appearance of an ordinary telephone. However, it is very different electrically from the conventional telephone most people are familiar with. It receives and sends voice information digitally over an Ethernet connection. The electronics within the handset replace the need for a local computer to perform the conversion of voice and sound into and from the digital information that is passed over the local Ethernet link.

Let's explore a few scenarios with an example of SOHO typical setups. Figure 4-8 shows three SOHO installations.

One of the examples shown is a single user using a PC connected to a DSL modem that is directly connected to the Internet. This user has full access to the Internet using a DSL modem using a PPPoE account from a local Internet provider. All the resources of the Internet are available to the user directly from the PC. However, to gain access to the resources behind the Central Office VPN Router, this user must use VPN client software. The VPN client that is to be used is normally dictated by company policy and is administered through the company Information Services (IS) department.

Many installations using the Nortel VPN Router make use of the Nortel VPN client to permit access to the company private LAN infrastructure with use of this client. The client is capable of using various forms of authentication from simple username/password to more rigorous forms of authentication using tokens and certificates. Chapter 10 covers the client in further depth.

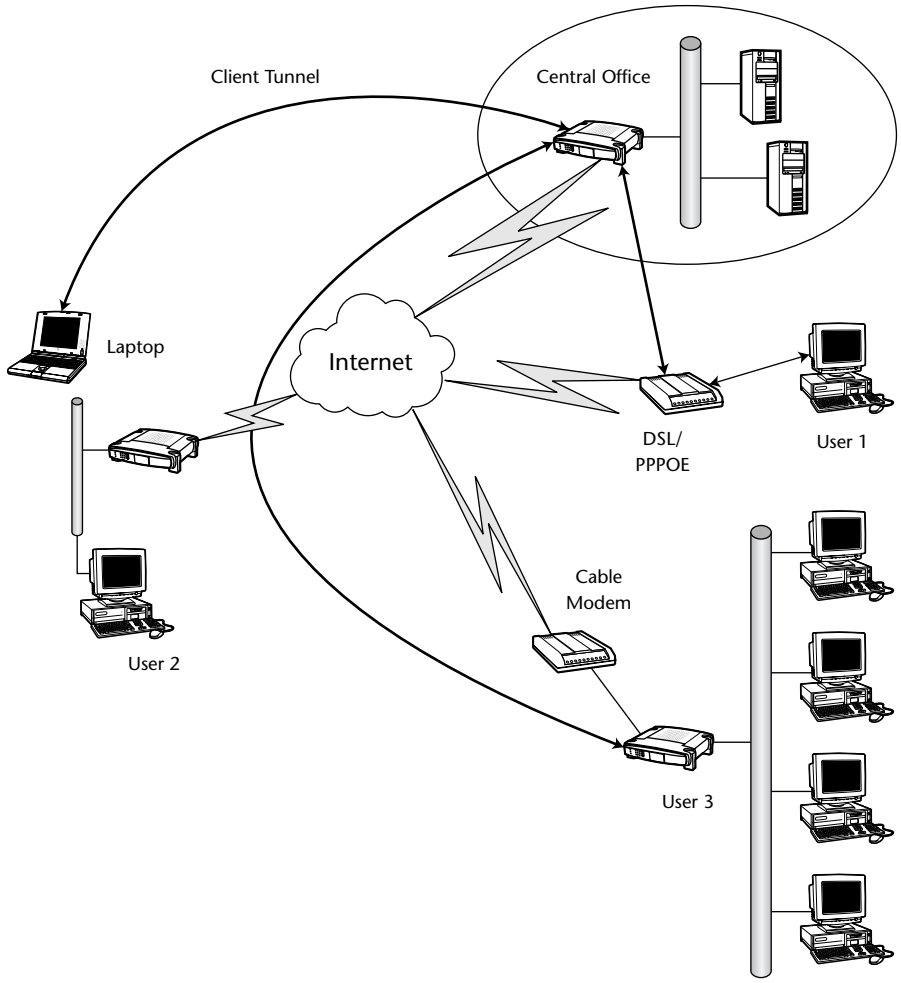


Figure 4-8: An example of typical SOHO installations

Depending on company policy, this user may be required to use mandatory tunneling. This usually is the case when the user equipment is provided by the company (such as a company laptop with a company standard boot-up image). In those cases, the computer launches the VPN client on power-up and all user activity (no matter which application is used) travels down the tunnel to the Central Office. This traffic will include packets with destinations for the private company LAN, as well as traffic with destinations that are available on the Internet. The policy of using mandatory tunneling allows the company to control and monitor the use of company resources, whether they are located physically on company premises or elsewhere.

The company also has the capability to apply its policies not only to the physical devices used throughout its infrastructure, but also to the traffic it allows to travel over its network infrastructure. The use of mandatory tunneling for all traffic puts greater demands on the company network because of the need for more bandwidth to handle traffic destined for devices on its own network and additional traffic destined to devices available over the Internet. However, a scenario such as this example allows for ease of instituting and regulating company policies regarding company devices, and the uses of its network infrastructure.

The second user also is using a similar PPPoE connection to the Internet as the previous user. However, this user is using a Nortel 251 VPN Router, which can connect directly to a DSL line. In this particular instance, the Nortel 251 VPN Router is being used primarily as a NAT device, providing firewall protection while allowing multiple computers to have access to the Internet.

In this environment, there is a fixed installation of a desktop computer with provision of one of the four Ethernet ports being used for a laptop computer. The desktop is solely used for access to the Internet, while the laptop is a company-provided computer for use for non-office traveling users requiring mobile computing or telecommuters who work between the office and home.

The laptop of User 2 is configured the same as the laptop being used by User 1. It has a standard company software image using the same applications including use of the Nortel VPN client to access the company VPN Router using mandatory tunneling. So, while the user of the desktop computer has full access to the Internet without company policies either regulating or monitoring that user's ability to use the Internet freely, the laptop user remains in full compliance of company policy because all traffic from the laptop travels over the client tunnel through the company's network infrastructure.

The third scenario is a small office. In this example, a two-user office is using a cable modem with a Nortel 221 VPN Router to provide VPN tunneling with a main mode tunnel (BOT) or an ABOT to tunnel to the Central Office. Whether BOT or ABOT tunnel mode is to be used is primarily determined by services offered by the local cable provider, whether the installation has a static public IP address assigned to it or an address that is being dynamically assigned by the provider.

If ABOT is used, then the nailed-up tunnel feature may be utilized to maintain the tunnel in an up state so that it will not timeout because of user inactivity. This will allow devices on the Central Office private LAN to access the devices on the private LAN of the small office even while it may be unmanned.

In the User 3 scenario shown in Figure 4-6, a Nortel 221 VPN Router is being used to connect to the cable modem's Ethernet port. Because this is a mandatory tunnel, all IP traffic from this office is sent down the tunnel to the Central Office's VPN Router. The four private LAN Ethernet interfaces in

this particular case are being used to connect two desktop computers and two IP-enabled telephone handsets.

The IP-enabled handsets communicate with a VoIP telephone switch located on the private LAN at the Central Office. Using the nailed-up feature in an ABOT tunnel situation allows the tunnel to be maintained in an up state, even when there is no IP traffic being generated from the small office to the Central Office. Thus, if an incoming telephone call is destined for one of the IP-enabled telephone handsets, the VoIP-enabled telephone switch at the Central Office is able to communicate to that handset through the tunnel, even when there is no IP traffic being generated at the User 3 office.

If a main mode peer-to-peer BOT tunnel is utilized, then the nailed-up feature is unnecessary because a tunnel can be initiated from the Central Office to the User 3 office when the tunnel has been downed for lack of IP traffic being generated.

For security purposes, tunnels are torn down for two main reasons. The first is the lack of IP traffic traversing the tunnel in a given period of time. This is also referred to as *idle timeout.* The second is when a tunnel rekey occurs. A *tunnel rekey* is set to a particular interval of time when the two VPN-enabled routers exchange tunnel-related credentials to validate that they are the two devices that are to participate in a particular tunnel. More discussion of idle timeout and tunnel rekey can be found in Chapter 7.

Figure 4-9 shows another small office configuration. This particular installation is using a Nortel 100 VPN Router to tunnel to the Central Office. In this configuration, the tunneling is not mandatory and split tunneling is enabled. The Nortel 100 VPN Router has three Ethernet interfaces and they are referenced by their physical location on the unit.

Ethernet 1 is the seven-port interface located on the front of the unit. These seven ports are one logical interface with one assigned IP address. These Ethernet ports are an auto-sensing auto-negotiating switching hub. Only on this particular interface can users be connected with cables that may either be straight through or crossover Ethernet cables. This interface's switching hub senses the signals between itself and the other device and configures itself electrically to communicate properly as far as send/receive, speed, and duplex mode that is used. The Ethernet 1 interface is usually used for the private LAN interface in a typical installation.

Ethernet 2 is located at the rear of the unit located to the lower left on the unit's back plate. This interface is normally used at the public LAN interface and, in this example, is used to connect to a DSL modem for access to the Internet.

The Ethernet 3 interface is located in the expansion slot of the unit and in this particular example is used for a Demilitarized Zone (DMZ) to allow access from the Internet to devices located on its LAN. The DMZ is discussed in more detail later in this chapter.

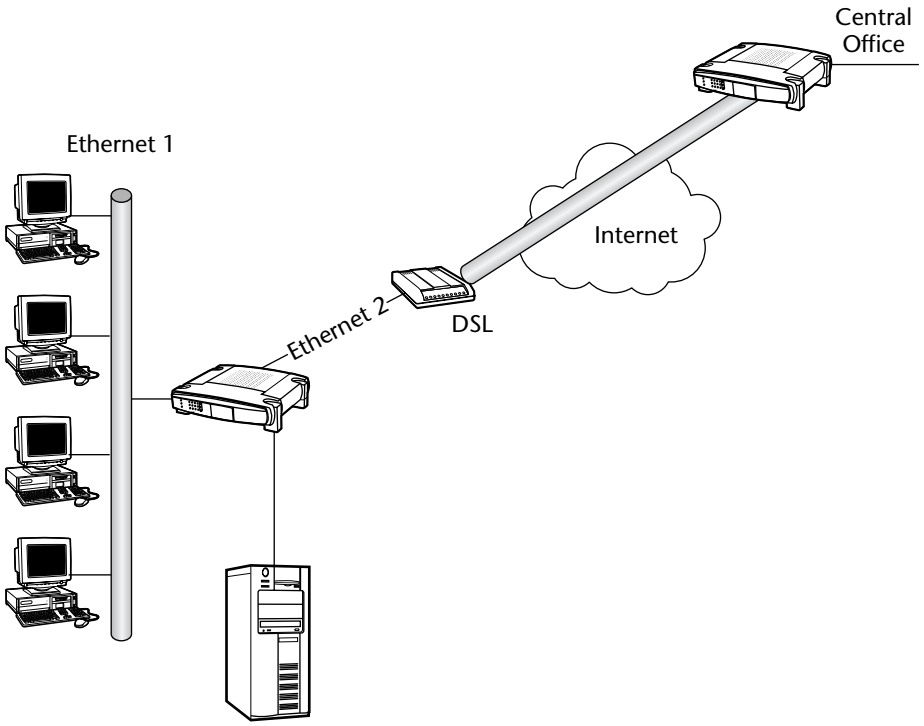


Figure 4-9: SOHO installation using a Nortel 100 VPN Router

For purposes of this example, interface Ethernet 1 (ETH1) is used as the private LAN interface. The amount of devices connected to this interface is not necessarily limited to the number of ports on the unit. These ports may be connected either to a passive hub or a switch to connect a greater number of devices than the seven Ethernet ports would allow. This is also true for the previous examples shown for the SOHO environment. However, there are design issues that must be considered (such as bandwidth) when deciding how many devices are to be used in such a computing environment.

Care in planning and sizing would yield better performance with an increase in overall user satisfaction. So, this interface may have a number of computers, network printers, IP-enabled telephone handsets, and other IP-enabled network devices connected to it with access to both the Internet and the resources available on the Central Office's private LAN.

The Ethernet 3 (ETH3) interface in this example is used to form a DMZ where the devices on its LAN are available to the Internet. It does not necessarily need to be used for this purpose exclusively. There are some scenarios where this interface has been used to form another private LAN segment that may be either accessible from the other private LAN or not, depending on the requirements the designers of that network segment are attempting to fulfill.

As discussed in the next section, a DMZ in networking terms is used to define a network segment that has some isolation from the private LAN, but may be accessed from the public interface and the Internet. Using the Nortel 100 VPN Router, this can be accomplished in various ways using private and publicly accessible network IP addresses. If private address space is used, then NAT may be used to allow Internet traffic to access those devices on that LAN segment. This type of NAT is called *server publication,* where specified ports may be available on the public IP interface from anywhere over the Internet.

The users connected to the ETH1 interface in Figure 4-9 are able to utilize resources located on the Central Office's private LAN and to reach resources that are available over the Internet since split tunneling is enabled. When the Nortel 100 VPN Router receives a packet from one of these users on the ETH1 interface, it examines it for the destination address.

If the destination address is a device located on the private LAN at the Central Office, the packet is not modified as far as source and destination addresses, but is encapsulated in an ESP packet with a source address as the public IP address of the Nortel 100 VPN Router, and the destination address as the public IP address of the VPN-enabled router located at the Central Office. When the packet arrives at the Central Office VPN-enabled router, it is de-encapsulated (decrypted) and placed on the private LAN interface to be routed over its local LAN to its destination. Return packets destined for the private LAN behind the Nortel 100 VPN Router are also handled in the same manner.

When the Nortel 100 VPN Router receives a packet not destined for the private LAN behind the Central Office VPN-enabled router, it uses NAT to modify the packet by inserting its public IP address to be used as the source address and the return port as the translation entry in its NAT table. Once modified, the packet is sent out the public interface to its local default router to be routed over the Internet. A packet returned from an established session is compared to its NAT translation table and then is modified with the destination and port address of the device located on the private LAN that initiated the session.

The devices discussed so far in this chapter are able to perform VPN tunneling and provide general Internet access via the use of NAT. However, they are firewall devices in that packets received are examined to determine their source and whether they should be allowed to traverse the firewall and be placed on the local private LAN.

A device that is configured to allow only mandatory tunneling examines each packet for type and source address. If the packet is not from its trusted endpoint address, then it is simply dropped. If the packet fails to decrypt properly it is also discarded. So, the only packets accepted are those that meet the criteria of the tunnel as far as destination and source address, along with the

proper encryption. These are permitted to be fully decrypted and placed on the private LAN of the device. So, with mandatory tunneling, only packets that meet all the criteria with the establishment of the tunnel are allowed to be placed on the private LAN of the device.

With split tunneling being allowed, the VPN device must perform a bit more processing to make sure it meets with its criteria before being accepted for placement on the private LAN. So, only the packets that meet either the tunnel criteria or that have an established NAT session from a device on the private LAN are allowed to be passed through the VPN device and onto the private LAN. All other packets received at the VPN device's public interface are dropped.

DMZ Creation and Usages

As mentioned, a DMZ in networking terms is a section of network under the control of an organization, which may be accessed from the Internet either directly through normal routing or using NAT server publication from a private IP address space LAN. Let's first discuss the use of publicly routable addresses, as shown in Figure 4-10.

In Figure 4-10, a Nortel 100 VPN Router is used to connect to the Internet via its ETH2 interface public interface. It has been given a publicly routable address of 27.65.210.184. The ETH3 interface is being used to form a DMZ to allow devices connected to this interface to communicate directly to the Internet.

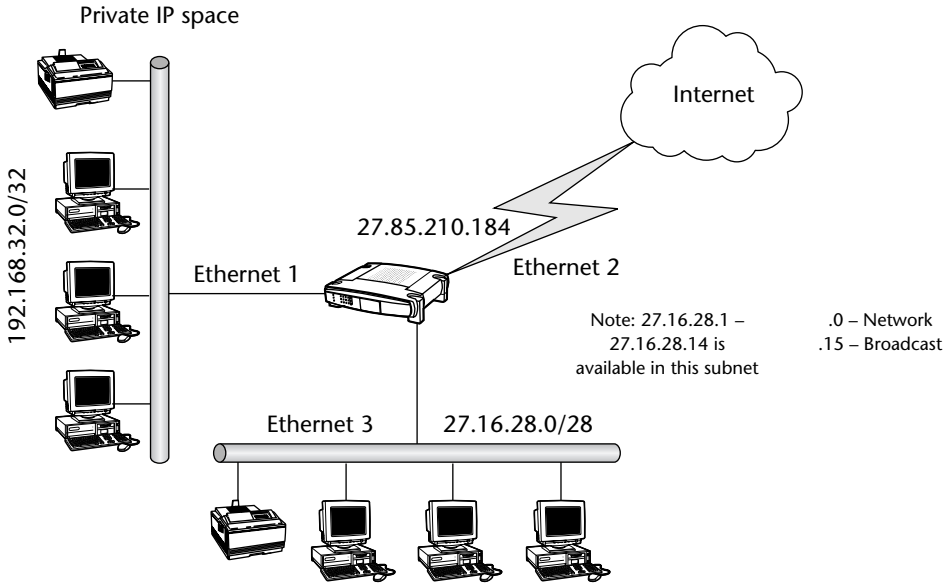


Figure 4-10: DMZ with publicly routed IP addresses

This can be wide open, and broad levels of communication or filters and policies can be configured to limit the types of Internet traffic that are allowed. Further discussion on policies and filters appears in Chapter 7. This example considers only the movement of data to and from the Internet.

In this configuration, a 28-bit subnet has been set aside to form the DMZ. In this case, the subnet with network address of 27.16.28.0 is being used, with 28 bits of subnet mask being used. Another numerical representation of this 28-bit subnet mask is 255.255.255.240. When a subnet is subdivided in this manner, it allows for 14 addresses to be used for device assignments. These addresses range from 27.16.28.1 through 27.16.28.14, with addresses 27.16.28.0 (Network Address) and 27.16.28.15 (Network Broadcast Address) reserved for network operation.

The ETH3 interface has been assigned the address of 27.16.28.1, allowing the other 13 remaining addresses to be assigned to other devices. These devices are directly accessible from the Internet using normal routing. The devices on this DMZ network segment use the ETH3 interface as their default gateway to communicate with devices not located on their local LAN. The Nortel 100 VPN Router has IP Forwarding enabled to allow for the normal routing to occur. By default, the firewall is enabled, and these packets otherwise would just be dropped for security purposes.

When a packet is received on the ETH2 interface destined for the 27.16.28.0 network, it is passed through the unit without modification and is placed on the wire of the LAN from its ETH3 interface. In reverse, if the ETH3 interface receives a packet that is not destined for the local LAN but the Internet, it passes it through the unit to the ETH2 interface without modification. The packet will contain the actual address of the sending device as its source address. The ETH2 interface will just forward this packet to its default gateway, which may or not be local to it, or is only accessible over a link to a distant Internet router.

Communication between the private IP address space on the ETH1 interface of the Nortel 100 VPN Router with the ETH3 public IP address space may be permitted or may be restricted by the use of filters and policies. The overall design intent of a particular installation will determine what configuration is necessary for the unit to comply with the needs that must be met for this network.

In Figure 4-11, a DMZ is formed using private non-routable private space IP addresses. The servers located on the 172.16.254.X IP-addressed LAN are available with the use of server publication. For example, a Web server would be able to advertise its service via NAT on the public interface of the Nortel 100 VPN Router.

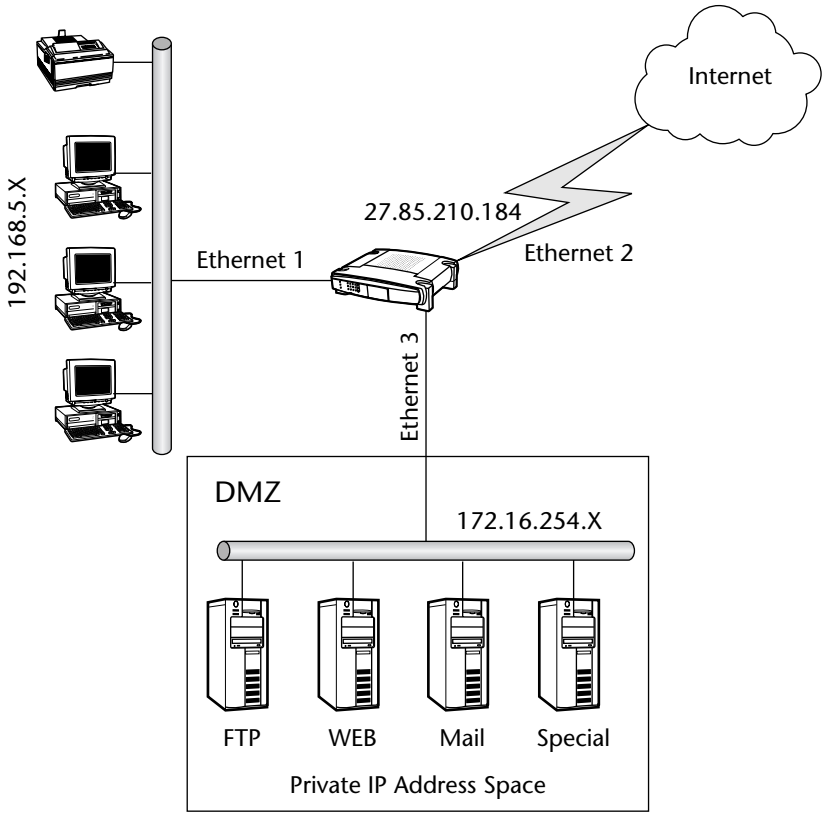


Figure 4-11: DMZ using private IP space addresses

The Web server at 172.16.254.16 accepts Web requests at port 80. A port forwarding or server publication NAT rule can be set up on the ETH2 public address that would allow for Web requests received on the public interface at IP address 27.85.210.184 to be accepted by the unit and forwarded on to the Web server located on the private LAN. All responses from the Web server would be via NAT, which means the packet will be modified showing a source address of the public IP address for ETH2 (which is sent to the requesting device over the Internet).

However, in this configuration, only one server may be advertised for any particular service. So, in this particular example only one Web server, FTP server, mail server, or other application server may advertise their services. However, there is a method that would allow for multiple servers of one type to advertise their services using the public interface as the portal to those services. Using the public subnet in Figure 4-10 in conjunction with the NAT rules, you can have multiple Web servers. Figure 4-12 shows an example of this.

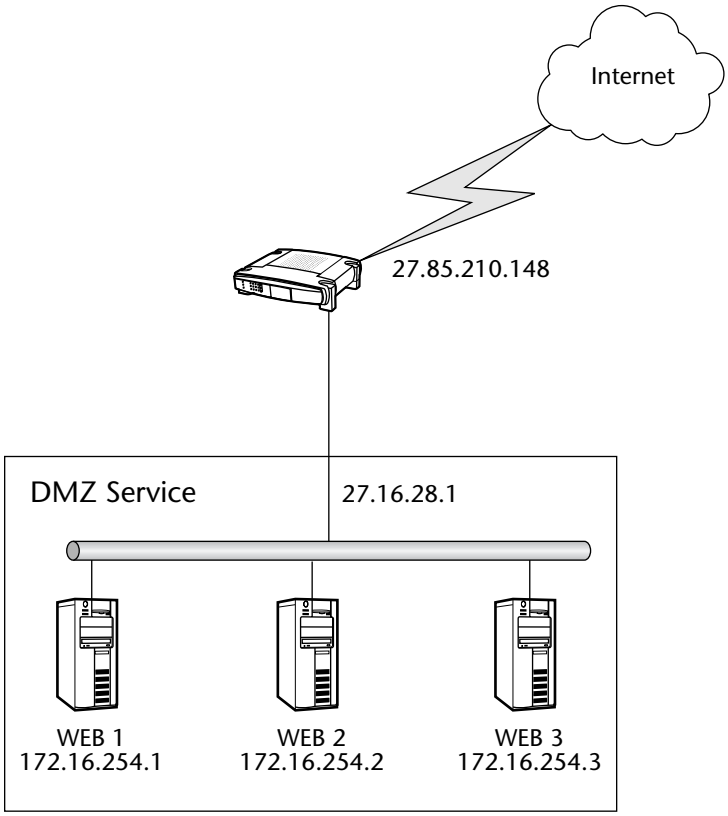


Figure 4-12: DMZ with multiple servers of a given type

In Figure 4-12, the NAT table shown in Table 4-2 is in use.

This example is simplified to show like ports, but in reality, the addresses need not be sequential. However, they must all exist within the advertised subnet that is routable over the Internet using the public IP address assigned to ETH2 as the gateway address to reach that subnet. The ports are shown as matching, but in reality, these can be different as long as the server that is being reached responds for a service advertised on that port. For the Internet side, these ports remain fixed for the service that is being advertised. So, Web services (HTTP) are always advertised on port 80 for that service.

Table 4-2: NAT Table

PUBLIC IP ADDRESS	PORT	PRIVATE IP ADDRESS	PORT
47.16.28.1	80	172.16.254.1	80
47.16.28.2	80	172.16.254.2	80
47.16.28.3	80	172.16.254.3	80

When a packet is received on the ETH2 interface for a Web page request for a server located at 27.16.28.2, the unit compares it with its NAT table and modifies the packet with a destination address of 172.16.254.2. It tracks the sessions with the use of source port addresses so it will ensure that the response is returned to the requestor. When the response packet is received on the ETH3 interface, it uses the destination port address to compare it to the sessions being tracked via the NAT table. The unit then modifies the packet to have a source address of 27.16.28.2 and forwards it out to the Internet with the destination address of the device that made the original Web page request. Using this configuration for a DMZ allows for multiple devices to be serving the same services to devices out on the Internet.

There are many uses for a DMZ, and the previous example is just a small demonstration of its use and configuration. Further discussion on using a DMZ follows in Chapter 7.

The Regional Office

Figure 4-13 shows an example of a typical Regional Office configuration. The Regional Office is a centralized corporate remote office providing services regionally to members of the corporation. Those members may consist of small offices, home offices, or users who are mobile. Regional offices may offer a wide range of services to the users that it serves, but determination of those services is part of the overall corporate strategy dealing with networks and computing. Factors that go into the decision-making for the services are ease of access, types of services offered, required bandwidth, fault tolerance, ease of implementation, and costs. These factors are not completely inclusive, but would be part of the corporate strategy planning of its network infrastructure.

The Regional Office may consist of one VPN Router or, if the size warrants, it may include several VPN Routers. The VPN Routers are primarily used as edge devices on the edge of the Regional Office network. These devices are used to link the Regional Office to the corporate Central Office and to provide network access to remote local users. In Figure 4-13, there is a peer-to-peer branch office to the corporate Central Office. This allows for secure communications between the private networks at the corporate Central Office and that of the Regional Office. Devices on either private LAN may communicate directly on the private LAN segment of the other.

SOHO users, as well as client PC users, also are able to terminate tunnels on the VPN Router. The office users may either be BOT or ABOT branch office tunnels depending on the types of services provided them by their local ISP. The PC-based users may have a wide range of Internet connectivity ranging from dialup services to broadband services available using DSL or cable

access. These branch office and user tunnels may be restricted to allowing access only to the private LAN behind the Regional Office VPN Router, or may be permitted to participate in the tunnel that connects the private LAN of the Regional Office to that of the Central Office.

The illustration in Figure 4-13 shows a single VPN Router, and, depending on the Regional Office requirements, it can be any of the Nortel VPN Routers currently available. Although each of the VPN Routers is capable of terminating branch office type tunnels, only the Nortel 100 VPN Router does not support user tunnel connections using the Nortel Multi OS VPN Client. So, dependent on the Regional Office requirements, whether or not to allow user tunnels to be terminated on that VPN Router will determine if a Nortel 100 VPN Router would be suitable for that installation. The Nortel 100 VPN Router supports only tunnels using the IPSec tunneling protocol. These tunnel types may be one of the following:

- Peer-to-peer (main mode) BOTs
- Initiator/responder ABOTs
- Client mode tunnels (treated as an IPSec user tunnel)

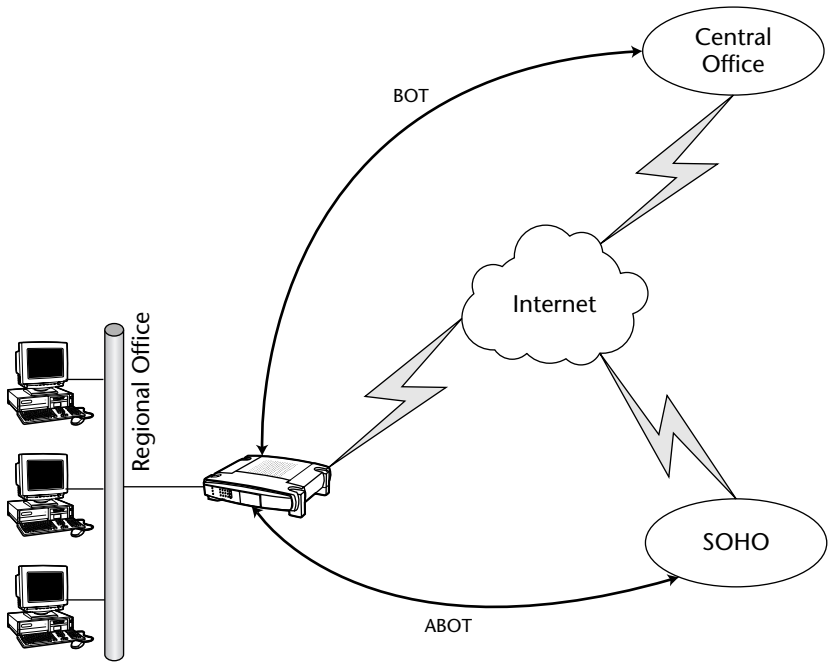


Figure 4-13: An example of a typical Regional Office configuration

In summary, the determination of which Nortel VPN Router is suitable for the Regional Office is dependent upon many factors, but careful planning can ensure that the selected VPN Router will meet all the immediate needs of the Regional Office and allow for any future expansion in the near future.

Because corporate networking infrastructure is at times fluid and evolutionary, the Nortel VPN Router offerings cover a wide range of devices that will meet these needs. They are flexible in configuration to allow for future changes that may be mandated by growth and expansion of the corporate network.

Nortel 100 VPN Router Added to Existing Regional Office Network

Figure 4-14 illustrates a network expansion at a Regional Office. The existing networking infrastructure consisted of a router with a T1 PPP link to the corporate Central Office. The scenario calls for the Regional Office to support smaller offices being added locally to that Regional Office, so the plan is to provide corporate computing services to those small remote offices through the Regional Office.

In Figure 4-14, the plan is to add two small sales offices and provide them with corporate computer and networking services through the Regional Office in their local area. The Nortel 100 VPN Router has been selected for each location.

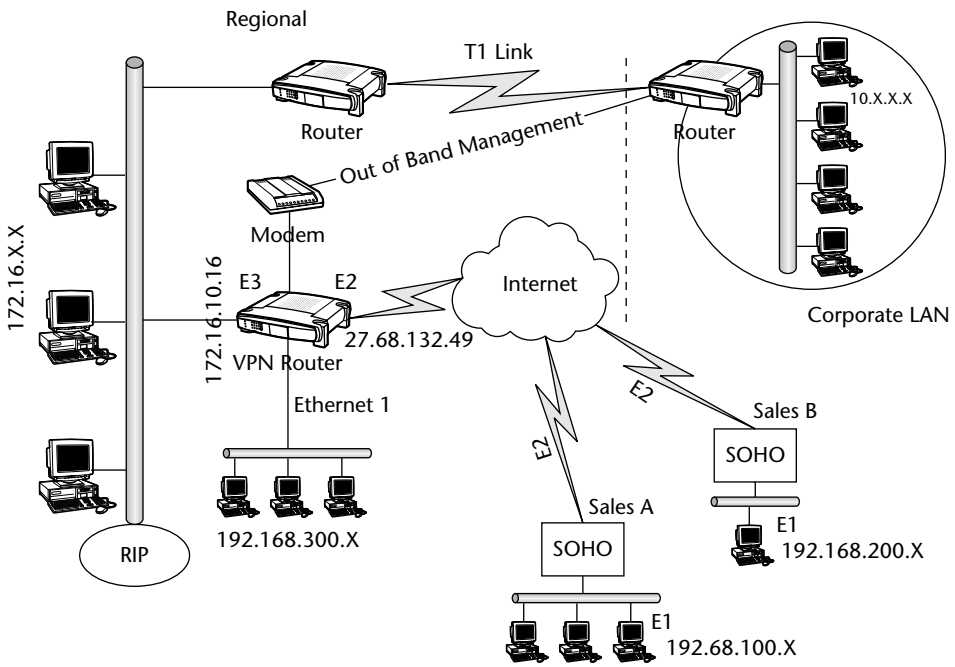


Figure 4-14: Nortel 100 VPN Router added to existing network

The two remote sales offices will be configured for mandatory tunneling, so all IP traffic from those offices is sent through the tunnel to a Regional Office Nortel 100 VPN Router. Because these offices may possibly be relocated at a future date it has been decided to configure these devices using the ABOT type of tunneling, where the Nortel 100 VPN Routers will be configured as tunnel initiators and the Regional Office Nortel 100 VPN Router will be configured as a responder for each tunnel.

The public interface (ETH2) of the Nortel 100 VPN Router has been given a dedicated IP address of 27.68.132.49. Its ETH3 interface is connected to the Regional Office LAN and has been given a dedicated address on that network of 172.16.10.16. However, the Regional Office has other routers and subnets, all within the 172.16.X.X IP address subnet, and routes are learned using Routing Information Protocol (RIP). So, the Regional Office Nortel 100 VPN Router has been configured to advertise and accept RIP route updates using its ETH3 interface.

By using RIP, the Nortel 100 VPN Router will advertise the routes it has that are the routes to the 192.168.100.X network subnet at Sales Office A and the 192.168.200.X network subnet at Sales Office B along with the 192.168.300.X network it has connected to its ETH1 interface. The routes to these subnets will be advertised with ETH3 IP address of 172.16.10.16 as the gateway address to these subnets.

These routes will be given in the RIP update broadcasted from the Nortel 100 VPN Router at the Regional Office out its ETH3 interface to the devices on its local LAN, as well as devices on the corporate LAN (if RIP updates are being passed between the routers over the T1 link between the Regional Office and the corporate Central Office). So, all devices on the local LAN of the Sales Offices, Regional Office, and the corporate Central Office are able to have access to each other from the RIP routes they receive.

As mentioned, the Sales Office's Nortel 100 VPN Routers have been configured with mandatory tunneling that sends all IP traffic up the tunnel to the Nortel 100 VPN Router at the Regional Office. If the users at the Sales Office are to be permitted to have general access to the Internet, this can be accomplished by either permitting split tunneling on the Regional Office Nortel 100 VPN Router, or (if it is not allowed) routing to the corporate Central Office, where it may be monitored and filtered using corporate guidelines for Internet usage.

If split tunneling is permitted, filters still may be applied to the Regional Office Nortel 100 VPN Router, but these filters will be required to be administered locally at the Regional Office. The Corporate Information Services Department will need to make the determination whether this is a feasible option, or ease of centralized control and uniformity of corporate Internet usage policy is preferable. The advantage of using split tunneling and applying local filters if needed is that it reduces the bandwidth usage on the T1 link between the Regional Office and corporate Central Office.

The network subnet of 192.168.300.X connected to the ETH1 interface would be useful as a DMZ or other isolated network segment from the remainder of the LAN network located at both the Regional Office and corporate Central Office. Filter policies may be added to accomplish this. Also, this segment could contain servers such as Web or FTP servers on that segment that have a server publication to the Internet. This would permit users to use those services without jeopardizing the overall network being secured by the Nortel 100 VPN Router. The use of this segment is totally arbitrary, and will be determined by the needs of the services the corporation deems necessary to have at that location. It could remain unused initially and left for the possibility of future network growth.

Each of the Nortel VPN Routers is equipped with a Serial RS-232 console port. The primary use of the port is for initial configuration and diagnostic purposes, but it may be connected to a modem to allow for out-of-band management of the unit. The modem is set to auto-answer and when dialed into with a PC using a dialup modem and running a terminal session, the administrator may make configuration changes to the unit or monitor the activity of the unit via Command Line Interface (CLI) commands.

With the use of VPN technology, it is now feasible for corporations to supply corporate computer and networking services to even a single-person office (whether it is in an office park or a home office) at fairly low cost. As data and voice information converge, these services will include all the services required for an office to run efficiently. With VoIP, voice information has merged with computer-based data so that both are transmitted over a single data link using VPN technology to secure that data. So, a single user, although distantly removed from the corporate Central Office, can communicate using voice as an extension of the existing Central Office telephone infrastructure. This eliminates the need for having separate carriers for each service and, thus, reducing the overall costs of providing these services to the SOHO.

Upgrading a Regional Office to VPN Technology

Let's examine a scenario of upgrading an existing Regional Office network to a total VPN technology solution. As shown in Figure 4-14, the Regional Office had a dedicated direct T1 link between itself and the corporate Central Office. These high-speed lines are expensive and cost is dependent on the distance between the offices. The farther apart they are, the more expensive it is to maintain these lines. The overall corporate strategy is to replace the router and the line to add VPN technology, and thus reduce the overall cost of maintaining the network to the Regional Office.

Figure 4-15 illustrates the replacement of the Regional Office router with a VPN Router that has a built-in WAN card for the interface with the T1 line.

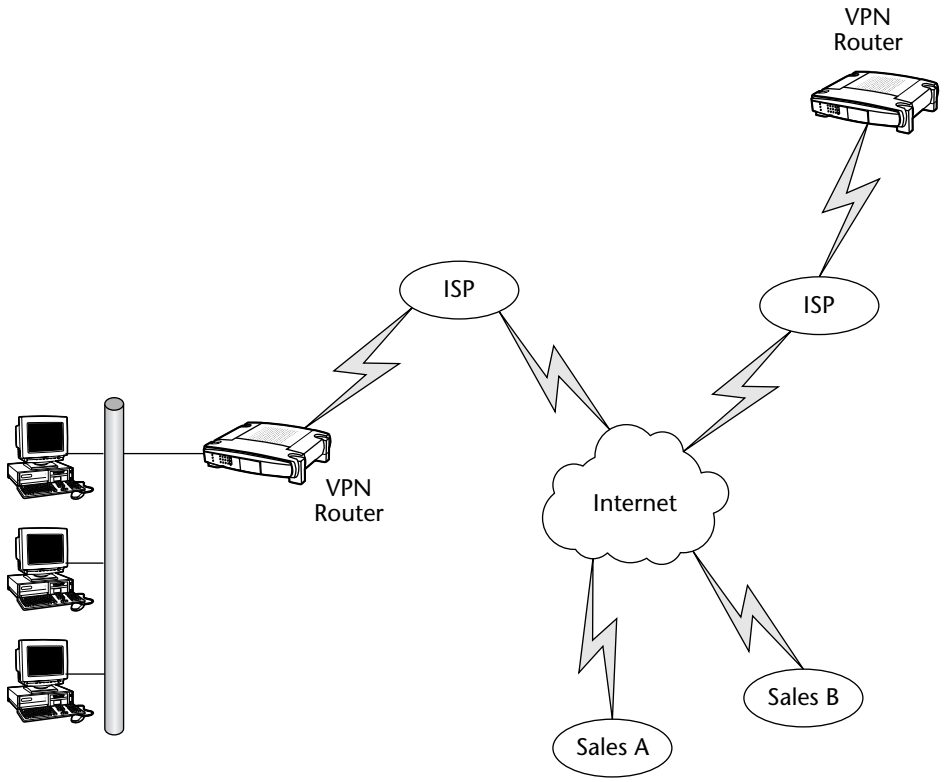


Figure 4-15: Regional Office upgrade to total VPN solution

In Figure 4-15, a VPN Router with a built-in wide area network (WAN) card is being used to replace the existing router at the Regional Office. The VPN Router has an internal Channel Service Unit/Data Service Unit (CSU/DSU) allowing it to be connected directly to the T1 digital communications line. The direct T1 line between the Regional Office and the corporate Central Office is being replaced by an Internet service provider (ISP) that offers T1 services and is local to the Regional Office. This will cut costs dramatically on the subscription rate of the line because now the overall distance of the line is much shorter. The corporate Central Office has also converted to a similar situation for its T1 services.

Communications between the corporate Central Office and the Regional Office now will utilize the Internet to establish secure data transfer between offices with the use of encryption available with VPN technology to form a tunnel between the offices to pass sensitive data through.

The dedicated T1 line has been replaced with a lower-cost solution with increased security because, even though the T1 line was a direct dedicated link between the offices, the possibility of snooping the line remained and data could be easily compromised if it were being transmitted in clear text modes.

With the VPN Router solution, tunnel traffic data packets are rigorously encrypted before being placed on the T1 wire, so, if the line was snooped, the probability of data being compromised is unlikely.

As in the previous scenario illustrated in Figure 4-14, the local sales offices would communicate with the Regional Office in the same manner. Because this VPN Router is capable of supporting Nortel VPN Client users, it may be used as a local entry point for mobile computer users to obtain corporate computing services.

So there are many advantages to upgrading to VPN technology, including the following:

- Cost savings
- Ease of expansion
- Added functionality
- Secure data communications

The solutions presented in this section for the Regional Office have been of the single VPN Router variety. However, the computing and networking needs that a particular Regional Office may require can warrant the use of multiple VPN Routers. The following section provides a discussion of scenarios using multiple VPN Routers.

The flexibility and ease of configuration of the VPN Routers allows for various scenarios to be applied to offices of any size if there is a need or requirement that the use of multiple routers can address. So, the scenarios presented here are for informational purposes and are not to be construed as a "must" type of configuration for offices of a particular size. The determination of what VPN Router configurations would be required at any one location is purely dependent on the VPN routing needs for that office, and not on the physical size of an office.

Following are office requirements that would affect the VPN Routing needs, no matter the size of the office:

- Bandwidth requirements
- Number of tunnels to be terminated on the VPN Router
- Redundancy
- Failover

The Central Office

The corporate Central Office has a vast amount of computing and networking needs. It is the center of the corporate intranet and provides essential informational services to all of its offices, no matter where they are located. When

speaking of an intranet, the first thought that comes to mind to most is a network located within a specific locale. However, with VPN technology, a corporate intranet has come to include many of the corporate office locations, if not each and every office location supporting the corporation's activities.

In certain cases, even third-party entities such as suppliers and distributors with close relationships with the corporation are permitted access for the ease of information transfer between companies. With VPN technology, access can be controlled and limited by the use of policies and filters on any particular network connection that is allowed access to the corporate intranet. Figure 4-16 illustrates what a corporate intranet may entail with the use of VPN technology.

This simplistic representation of the corporate intranet is for ease of illustration. The corporate central site or the overall corporate intranet is a mesh of computing services with servers, clients, and voice all vying for access over its networked infrastructure.

There is no one scenario that would be all-inclusive of a typical Central Office configuration, and attempting to illustrate it would not be beneficial for purposes of explanation. So, the discussion of the services available at a corporate central site location will be broken down into functional blocks and discussed as separate entities, even though they are all combined to offer a unified computer and network service to the corporation at large.

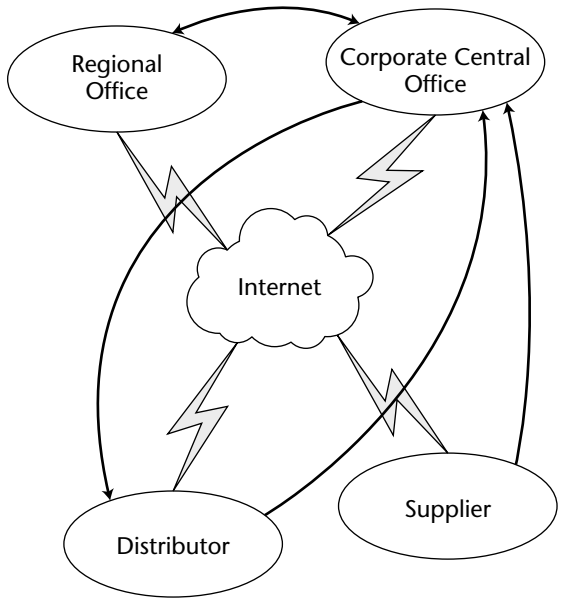


Figure 4-16: Corporate intranet using VPN technology

All the corporate computing and networking services do not necessarily reside in a single location. These services may appear to be single location–based but, in reality, may be located geographically over many different locations. For large corporations, this allows for possible redundancy and for fail-safe purposes (that is, if, for any reason, a particular location is not operational, that the corporate computing and networking infrastructure will not be totally com promised).

The planning for a corporation's overall computing and networking strategy should not just consist of the services being offered, but also how those services can still be delivered in the event a particular corporate locale has been impacted and is no longer operational. The ease of configuration for relocating tunnels on a VPN Router ensures that the corporate intranet can be redefined if such an event should occur. For larger installations with redundant devices, this can be configured to occur automatically, so that there is no impact on the services being offered by the corporate intranet. However, for smaller installations that cannot afford redundant devices, there is still a comfort level that if things must be changed for any reason, they could be done quickly and with very little cost.

The VPN Router as an Access Point

As mentioned previously, VPN Routers are normally found at the edge of a network. Although that is not the only location where they may be found within a network, a primary use of the device is to allow secured access into the corporate intranet. Figure 4-17 shows examples of VPN Routers at the edge of a corporate intranet.

In Figure 4-17, a corporate Central Office is shown with multiple VPN Routers. One VPN Router is supporting a BOT to the Toledo Regional Office, while another is supporting a BOT to the Los Angeles Regional Office. A third VPN Router is used for remote user access using VPN tunneling client software. A fourth VPN Router is for use as a firewall to allow internal intranet users to have access to the Internet.

It is possible to allow all the traffic flowing between the corporate intranet network and the external public network to pass through a single VPN Router because it would be able to perform each of the functions just described. However, this would result in a single point of failure. Also, heavy usage may affect the bandwidth the unit is able to provide. For busy corporate Central Offices, multiple VPN Routers make provisions for possible failures and a backup that will allow continued operation in the case of such an event.

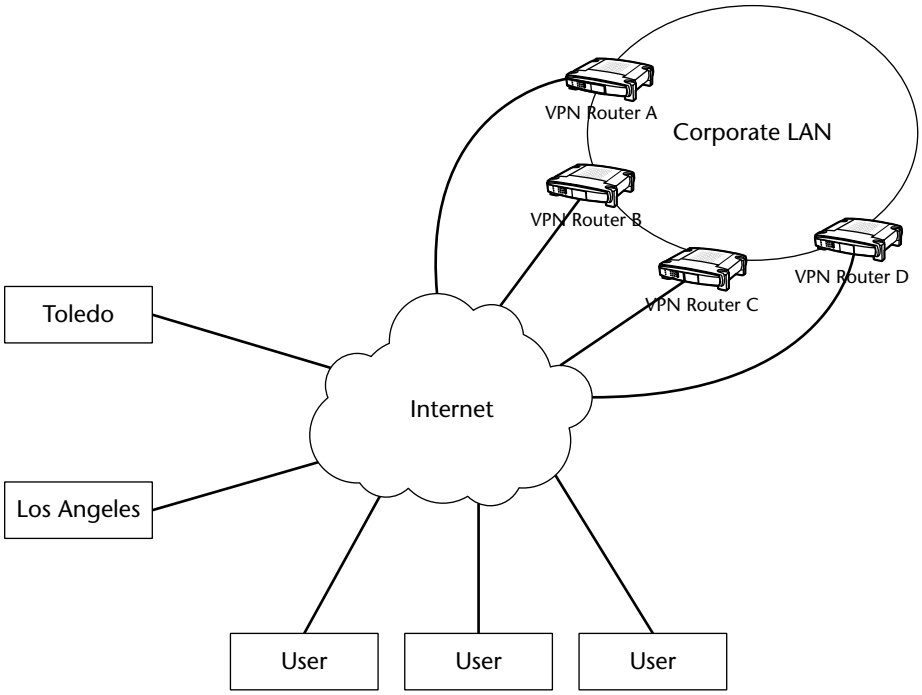


Figure 4-17: VPN Routers used as intranet Access Points

In Figure 4-17, VPN Router C is being used to permit external users to have access to the corporate intranet. In the event that VPN Router C experienced a failure, these users will lose their primary access to that network. This may be handled by utilizing other VPN Routers for access to the corporate intranet. VPN Router D at the corporate Central Office may be used to gain access to that network, as well as the VPN Routers located in the Toledo and Los Angeles offices. This requires that clients be pointed to those units to connect to those VPN Routers to gain access to the corporate network.

Similarly, depending on which links are down, BOTs may be redirected to allow for continued service. For example, if the Central Office VPN Router linking the Toledo office has its link go down between itself and the local ISP, then the Toledo VPN Router can be configured to redirect the tunnel to the Central Office VPN Router B. Therefore, redundancy for a large corporate entity is essential to reduce the possibility that a failure would severely affect normal day-to-day operations.

Later in this chapter, we will discuss further how redundancy and failover may be used to automatically redirect IP traffic in the case of a device failure or communications link failure.

Client Access to the Corporate Network

The PCs accessing the corporate network require client software to do so. Nortel VPN Client Software is an IPSec client that will allow that user to access the corporate network by connecting to a Nortel VPN Router running that software on a PC. More discussion on the client itself is covered in Chapters 6, 7, and 9.

This section discusses the VPN Router and its relationship to other devices on the corporate network in support of the corporation's users. Although this section discusses the corporate Central Office, these features may be utilized in any office of a corporation or a smaller single-location company. The solutions discussed are scalable over a wide range of office and company sizes. The strategy and planning of what requirements must be addressed are unique to the company and what is needed to ensure the success of their business.

Figure 4-18 shows a number of VPN Client users accessing the VPN Router located at the corporate Central Office. Although the VPN Router has an internal Lightweight Directory Access Protocol (LDAP) server in this scenario, an external authentication server is being used. A small office having only one VPN Router and no other devices requiring user authentication may use the internal LDAP server for that purpose. However, in larger installations with either multiple VPN Routers or other servers requiring user authentication it is easier to administer one single server dedicated to user authentication on the network. The authentication server may be one of the following:

- LDAP server
- RADIUS server
- Certificate server

Remote Authentication Dial-In User Service (RADIUS) has accounting functionality, as well as being used for user-authentication purposes. The type of authentication being used is determined by the size of the user base and the number of access points that require authentication. Because user authentication databases in large installations are fairly dynamic with new users being added and other users leaving the corporation, a single authentication service is much easier to administer.

On gaining access to the corporate network, users get access to Domain Name System (DNS), Windows Internet Naming Service (WINS), Dynamic Host Configuration Protocol (DHCP), and other dedicated application servers. DHCP is primarily used for IP address assignment. This is an essential service in many installations because it allows for the dynamic assignment of IP addresses to users as they connect to the corporate network.

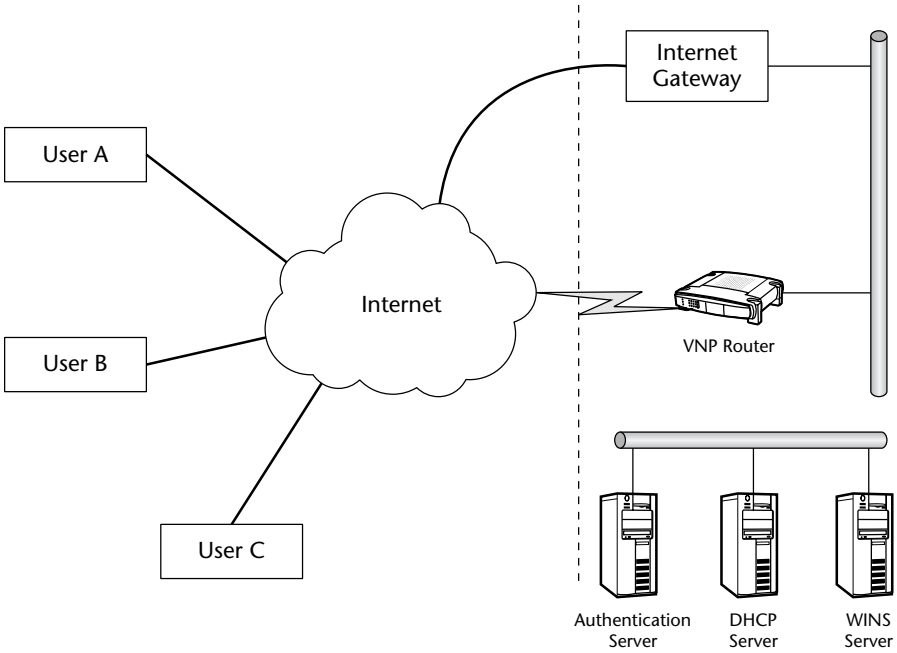


Figure 4-18: Corporate client services

The VPN Router is capable of providing DHCP services. However, it would need to be administered separately on each unit and the IP address space would need to be divided so that each device only allocates addresses in the address range it is assigned. If this is not done carefully, then it is possible that units may assign the same IP address to two different users, and this can cause major complications on a network that is dependent on each device having its own unique address. When multiple devices are allocating IP addresses to users and other devices accessing the corporate network, it is much easier to administer and control this function from a single server.

DHCP servers not only allocate IP addresses to users, but may also provide the default gateway, Domain Name System (DNS) server addresses, and WINS server addresses. When a client or device issues a DHCP address request, the response will not only include the IP address that is to be assigned to the user or device, but might also assign a default gateway address, along with one or more IP addresses for DNS and WINS servers.

A default gateway is used when a client or device is attempting to communicate with a device whose address is not within its own subnet. Those requests are directed to the device whose address is contained within the default gateway portion of the DHCP response provided by the DHCP server. It is the responsibility of the default gateway device to route the packet according to its destination address and to either return the response from the requested device, or return an error to the client or device that made the initial request if the communication of the request was unsuccessful.

Packets destined for the local network that the VPN Router is directly connected to are handled by Address Resolution Protocol (ARP), which is a broadcast on the local LAN requesting the Media Access Control (MAC) address of the device residing at the requested IP address. The device with the requested IP address responds by giving its MAC address, which is then loaded into the ARP cache of the requesting device. ARP cache addresses are updated at varying rates, dependent on the parameters of that device. However, the device looks into its cache first to see if there is an address that has an ARP entry before broadcasting a request on the LAN. Once an IP address has a successful MAC response, communication between devices is accomplished directly between the two devices.

A DNS server is used to provide name resolution for the requesting client or device. Uniform Resource Locater (URL) addresses are text-based names given to servers. These must be resolved to an IP address for routing over the Internet to occur. A name of a host is easier to remember and also has other advantages over just using numeric IP addresses. However, for the purpose of this discussion, it is not necessary to go into what those advantages are. So, when a client makes a request of the form `www.mywebpage.net`, the PC sends a DNS lookup to its assigned DNS server requesting the address at which the named server resides.

Clients and devices are usually configured with multiple DNS server addresses to be used in host name resolution. The reason for this is a particular DNS server may not be available or responding to the host name resolution request. After a timeout period, the client or requesting device will attempt host name resolution using the addresses of its secondary DNS servers. If host name resolution cannot be completed, then a "host not found" error is reported back to the client or requesting device. DNS host name resolution is accomplished over the Internet by DNS servers communicating with their DNS authority servers, which, in turn, communicate with each other. So, once a registered host name is presented to a DNS authority server, all DNS servers will be able to resolve that host name to a particular IP address on the Internet.

The use of a WINS server is essential for the Microsoft Windows networking environment. Corporations using Windows-based clients and servers may communicate with each other through the use of assigned host names. WINS allows for the Windows-based host name request to be resolved to an IP address so that devices may communicate with each other. This is similar to the DNS host name resolution as described earlier, but it differs in name convention in that WINS is required to resolve hosts named using Microsoft Windows. Again, multiple WINS servers may be assigned to a client or a device as primary and secondary servers to facilitate the host name lookup process similarly to that of DNS.

Corporations may have many other servers that are dedicated to specific applications to which the users may have access. The primary service that many users rely on is email. However, depending on the nature of the business the corporation is involved in, there may be databases, accounting systems, file services, and other dedicated applications that the user may utilize in performing their jobs. Client access to the network and the services it is allowed to use can be controlled with access privileges at the time authentication is performed. However, that topic is beyond the scope of this chapter and further discussion can be found in Chapter 6.

Depending on corporate policies dealing with Internet access, clients and branch offices may be permitted to do split tunneling to gain local access to the Internet. However, if mandatory tunneling is being enforced then all traffic must travel up the tunnel. In those cases, Internet traffic may be routed through the corporate network where Internet access may be monitored and controlled. In Figure 4-18, this is shown as an Internet gateway device. It may be a router or another VPN Router with firewall enabled so that access policies may be applied to that traffic. Further discussion of the internal stateful firewall of the Nortel VPN Router can be found in Chapter 7.

Client Load Balancing and Failover

In installations where there are a large number of remote users requiring access to the corporate network, the use of multiple VPN Routers can provide for load balancing and failover if one of the VPN Routers becomes unavailable. Figure 4-19 illustrates the use of two VPN Routers to accomplish this.

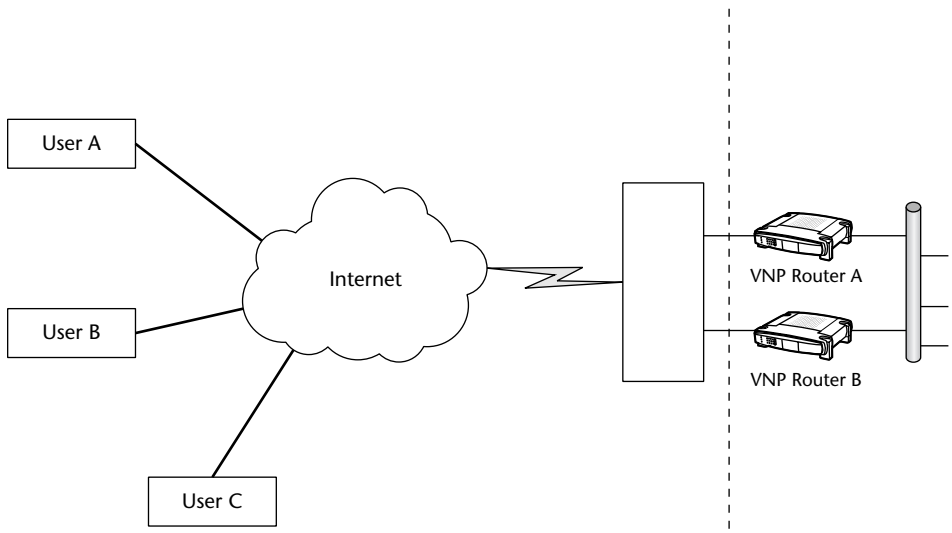


Figure 4-19: VPN Routers for load balancing and failover

The two VPN Routers A and B are being used to provide load balancing and failover. With load balancing and failover, clients are configured to connect with VPN Router A as the primary server and with VPN Router B as the secondary server. In the situation of access not being available via VPN Router A, then the client will *failover* to VPN Router B because it is the next failover server it has configured within its settings. While VPN Router A remains unavailable, clients will continue to attempt to connect to it first, and then fail over to VPN Router B. Those clients connected to VPN Router B will remain connected to it as long as they maintain their tunnel sessions, even if VPN Router A has again become available during that time. However, if they drop off of VPN Router B and then try to re-establish a tunnel session, they would once again attempt a tunnel connection to VPN Router A. If VPN Router A accepts the connection, they will gain access to the corporate network using that connection.

With *load balancing*, both VPN Routers must reside on the same network because the two devices must communicate with each using their management ports on the private LAN. The two devices use a protocol to determine which connections they will accept on their public interfaces. So, with all clients configured to first attempt to create a tunnel session with VPN Router A on the attempt, VPN Routers A and B use the given protocol to determine if VPN A should accept that connection or reject it. If it is to be accepted, then VPN Router A (upon proper authentication of that client) will grant access to that user. If the connection attempt is to be rejected, then VPN Router A refuses the connection, whereupon the client then will attempt to connect to its configured secondary VPN Router (in this scenario, that is VPN Router B).

VPN Routers A and B may be configured to both be the failover router of the other, as well as serve in a load balancing of clients between them. Because there are two independent VPN Routers working in unison to provide client access to the corporate network, this is a good demonstration of the use of an external authentication server to provide user authentication to both VPN Routers using a common user database. Using an external authentication server eases the burden of maintaining user databases on each separate device. This is more reliable because revision of a single database ensures that user access permissions are uniform across all devices utilizing that server for authentication purposes.

Corporate User Access to the Internet

Previous examples have discussed private LAN users being allowed Internet access through the VPN Router. As mentioned, both filters and polices may be used to regulate that access. However, in large installations where a large number of internal users require Internet access as part of their job functions, then a method of providing redundant access to the Internet may be a requirement. Figure 4-20 illustrates VPN Routers A and B being used to provide redundant access to the Internet.

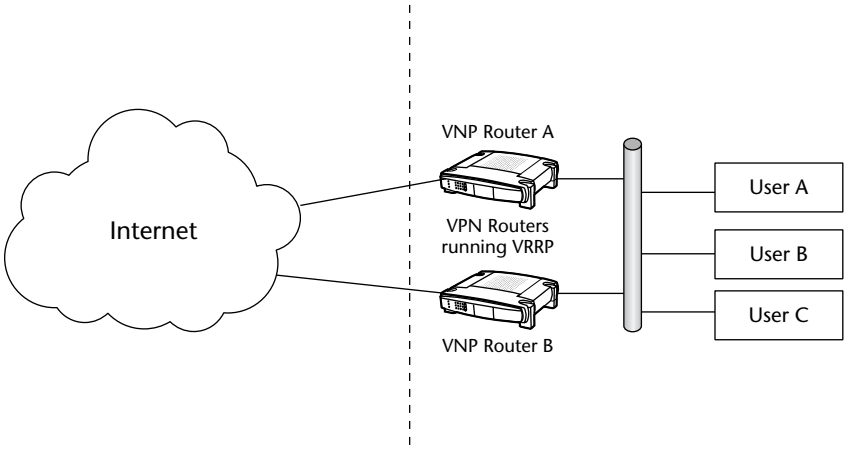


Figure 4-20: Internet access using redundant VPN routers

Internal user redundant Internet access is accomplished by using the Virtual Router Redundancy Protocol (VRRP). There are a number of Request For Comments (RFC) that you can research for further information on this topic.

Both VPN Routers need to reside on the same network because they will communicate on their management ports over the private LAN. The users on the internal corporate network use one IP address as the gateway to the Internet. VPN Routers A and B have been configured to back up the interface of the other. The two VPN Routers create a virtual interface that is used as the gateway to the Internet for the devices on the private LAN.

In this scenario, VPN Router A is master and VPN Router B is the backup. So, VPN Router A reports the status of its private interface to VPN Router B. All IP traffic that is directed to the virtual gateway interface is handled and processed by VPN Router A. If, for any reason, the private interface of VPN Router A is not functioning, VPN Router B (upon detection of VPN Router A's private interface being in a failed state) will assume responsibility of handling and processing all the IP traffic that is directed to the virtual interface.

VPN Routers A and B should be configured exactly the same so that they will use the same policies and filters no matter which VPN Router is assuming the responsibilities of handling and processing the IP traffic directed to the virtual gateway interface. So, with the use of VRRP and redundant VPN Routers, corporate users on the local corporate network have a fault-tolerant gateway to the Internet.

Backup Interface Services

This chapter has discussed redundancy for clients creating tunnels to the VPN Router and for devices on the corporate private LAN getting out to the Internet.

This section discusses redundancy that allows for backing up an interface link that can be used to perform BOT backup. Backup Interface Services (BIS) is a function to automatically enable a backup interface when a primary connection fails. The primary connection may be an interface group, a specific route, or a connection to a specific destination. Any VPN Router interface may be configured as a backup interface. Following are the types of interfaces that may be used to back up the primary interface:

- Ethernet interface
- Dialup interface
- ISDN interface
- WAN interface

Figure 4-21 illustrates the use of BIS to back up a primary link that connects a VPN Router in New York with one in San Francisco. If, for any reason, the primary link fails, then the backup interface will be enabled and a backup link between New York and San Francisco will be brought up to enable traffic that once traveled over the primary link between those two VPN Routers to be routed over the backup link.

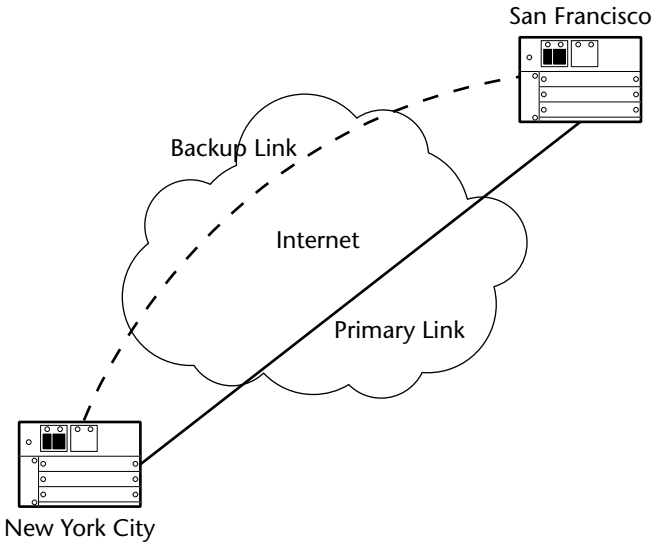


Figure 4-21: Backup Interface Services (BIS)

BIS is configured on the VPN Routers as a BIS profile. A *BIS profile* specifies the primary connection, the backup connection, the failover criteria, and the actions to be initiated upon failover. When the primary link fails, BIS enables the backup interface to come up running the same protocols that were configured on the primary link. The backup interface remains operational as long as the primary interface remains in a failed state. When the primary interface is restored to operational status, the backup interface is no longer enabled and full communications travels over the primary link.

BIS can be configured so that the backup interface takes the place of the primary link when the following events occur:

- Interface group fails
- Route unreachable
- Ping failure
- Time of day or day of the week

Interface Group Fails

An interface group may consist of BOTs, physical interfaces, or a combination of BOTs and interfaces. With an interface group configured as a BIS trigger, the backup interface is not enabled until all components of the interface group are in a down state.

Route Unreachable

When a route unreachable is used as a BIS trigger, the backup interface is enabled when routing has determined that the primary route no longer exists. If your network is running routing protocols such as RIP or OSPF, and redundant routing paths have not been configured, then it may take several minutes for routing to determine that a path no longer exists. Routing protocols may take a period of time to age out a route when it no longer is available.

Ping Failure

Ping failure to a specific destination can be used as a BIS trigger. However, the target address must be a device that is always available such as a primary server, gateway router, and so on. When the target device fails to respond to ping requests, the backup interface is enabled.

Time of Day or Day of the Week

A BIS trigger can be configured to trigger a backup interface to be enabled at a specific time during the day, or a particular day of the week. The time-of-day trigger may be combined with other trigger types (such as interface group, ping, or route unreachable) to enable a backup interface.

The major function of using BIS is to provide redundancy of a primary path in the event of a connection failure. However, the time-of-day trigger may be used as an operational configuration to reduce the cost of the subscription rate on certain types of communication links. In Figure 4-22, a Boston Regional Office has an ISDN connection to the internet. The bandwidth demand is heaviest from 7 A.M. through 6 P.M., Monday through Friday. However, during after hours and weekends the bandwidth requirement is very low and the cost of maintaining an ISDN connection during those periods is unnecessary. It was determined that during those off-peak hours, a dialup line would be more than adequate to handle the off-hours communications.

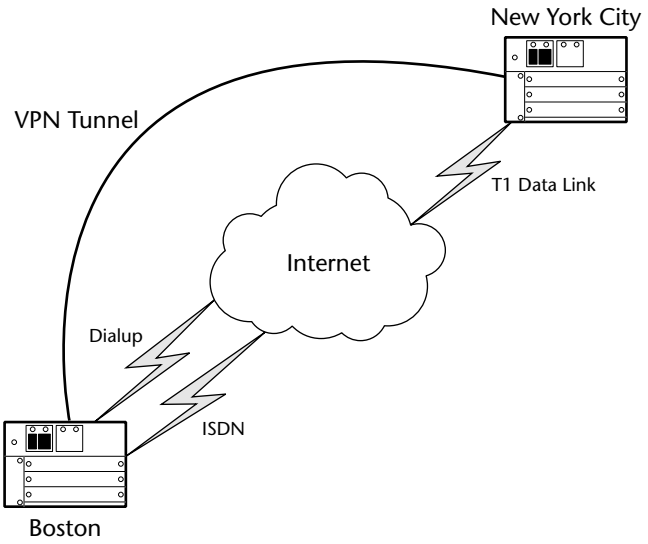


Figure 4-22: BIS configured using time-of-day trigger

In this example, the Boston office has been configured using BIS with the primary interface being the ISDN connection and a backup connection being the dialup interface. Both of these interfaces connect to the Internet to provide a communications path to the home office located in New York City. The dialup service and the ISDN service may use the same ISP, but it is not necessary. In this case, the time-of-day trigger may be combined with either interface group, route unreachable, or ping triggers to enable the dialup backup interface. So, with normal operation, the ISDN interface is the primary connection from 7 A.M. through 6 P.M., Monday through Friday, with the dialup interface assuming the connection responsibility for all off-hour operation. Also, if for any reason the ISDN connection is not available during the days and hours it is to be used as the primary connection, the dialup backup interface will be enabled to allow for secure VPN tunnel operation to continue between the two offices.

Placement in the Network

So far, this chapter has discussed scenarios where the VPN Router has been at the edge of the networks it is supporting. By the "edge," we mean it is placed between the private LAN network and the Internet or public switched network. However, this may or may not necessarily always be the case. There are instances where the VPN Router is placed behind routers or firewalls in larger installations. In those instances, provision must be made to permit the flow of ESP packets so that VPN tunnels may be established and terminated. In the case of firewalls in the path between VPN Routers, provision must be made to allow for endpoint-to-endpoint communications allowing for port 500 and protocols 50 and 51 to not be interfered with. Figure 4-23 shows a large corporate installation.

In Figure 4-23, the corporate Central Office has heavy bandwidth requirements that require that its connection to the Internet be carried over a fiber-optic link. The link connects to a router with a fiber-optic interface, along with high-speed Ethernet interfaces for the LAN side. To maintain control over the traffic permitted into its network, the corporation has installed a firewall. Because BOT requires that ESP endpoint-to-endpoint traffic be allowed to successfully terminate a VPN tunnel, the policies and filters on the firewall must be adjusted to permit this. It may seem that punching holes in a firewall would allow for undesired traffic to traverse the firewall. However, this is not the case because the rules and policies may be such that only specific endpoint IP addresses using port 500 and protocols 50 and 51 be permitted to pass through the firewall.

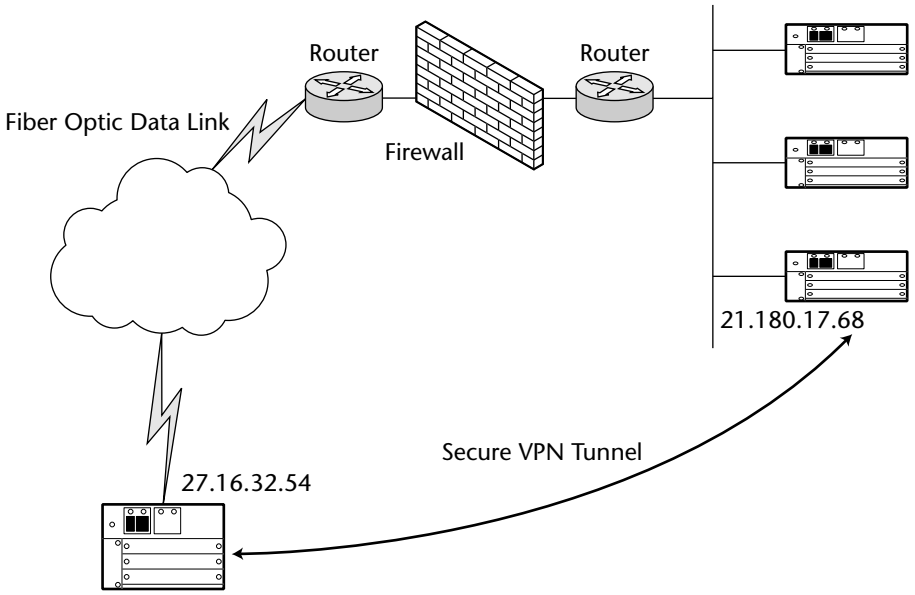


Figure 4-23: An example of a corporate installation

In this figure, the remote office with a public IP address of 27.16.32.54 is permitted to communicate with address 27.180.17.68 using port 500 and protocols 50 and 51. The firewall will drop all other traffic from those addresses. So, this prevents all other traffic from traversing the firewall. Once the tunnel between the two devices is established, open communications between the two endpoint VPN Routers from the private LAN behind each VPN Router is allowed to flow within the tunnel. If needed, further policies and filters may be applied to the tunnel traffic itself, allowing for further control over the traffic permitted to enter or leave from the corporate LAN.

All of the previous examples in this chapter have illustrated the building of corporate intranets using the Internet and other public switched communication networks with the use of VPN Routers. These networks or intranets covered large geographical areas. However, the VPN Router may be used within a particular location to secure sensitive areas of an intranet. Figure 4-24 shows an example of this.

In this example, VPN Routers have been added internally to isolate and protect portions of the corporate intranet from within the organization. Functions such as accounting, payroll, and the office of the corporate executive may contain data that is strictly confidential and not to be shared with the remainder of the corporation. A centralized VPN Router is used to form secure BOTs with each VPN Router protecting those sensitive areas.

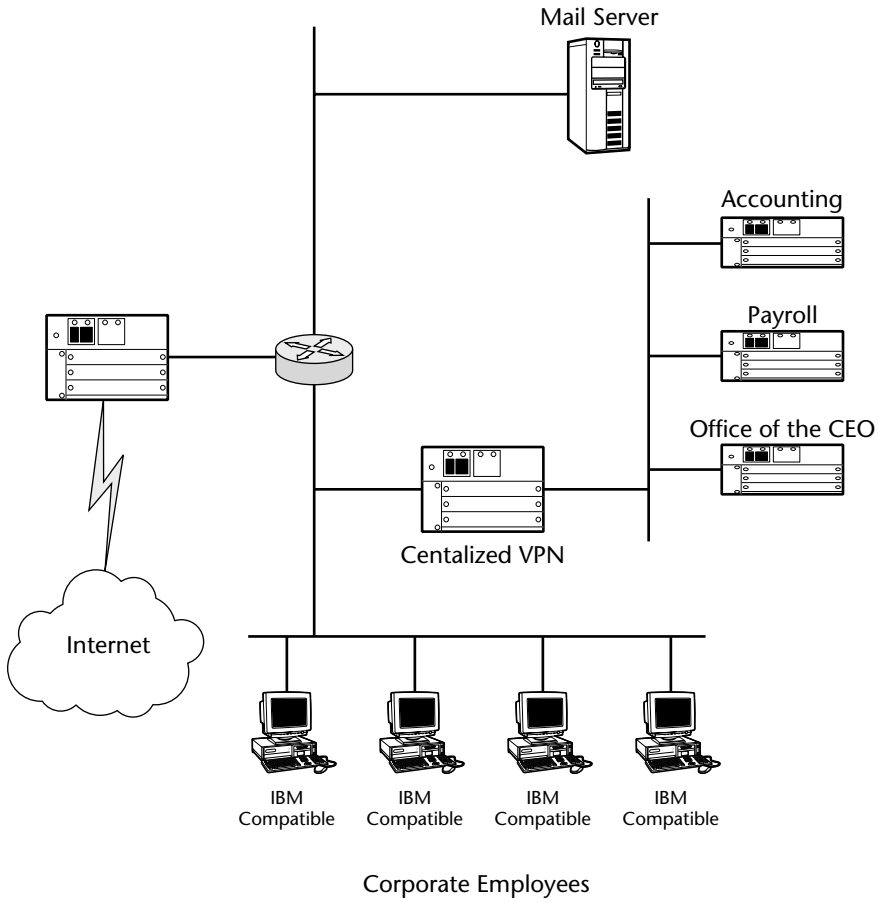


Figure 4-24: Internal intranet VPN Routers

In this simple example, the centralized VPN Router's private LAN is the remainder of the general corporate private LAN. Users in the accounting department using their local VPN Router are able to get to necessary resources on the corporate LAN and from the Internet. However, general users on the corporate LAN are restricted from participating in the tunnel allowing access to the accounting department. This can be accomplished by restricting the addresses permitted to participate in the tunnel via the accessible network definition and the use of policies and filters on the tunnel and interfaces. Also, control of the data that flows between the other offices connected to the centralized VPN Router may be controlled and restricted with the use of the same parameters that control access to the overall general corporate private LAN.

Network Administration of VPN Routers

There are many considerations for the administration of VPN Routers on the corporate intranet. Location of the VPN Router largely determines how it may be administrated. Large installations usually have a centralized *Network Operations Center* (*NOC*) whose responsibility it is to monitor and control all aspects of the corporate network infrastructure. The VPN Router has multiple methods of being monitored and administered. These include the following:

- Direct access via console cable, Graphical User Interface (GUI), telnet command line
- Control tunnels
- Out-of-band management
- Logging
- Simple Network Management Protocol (SNMP)

Figure 4-25 illustrates an NOC office.

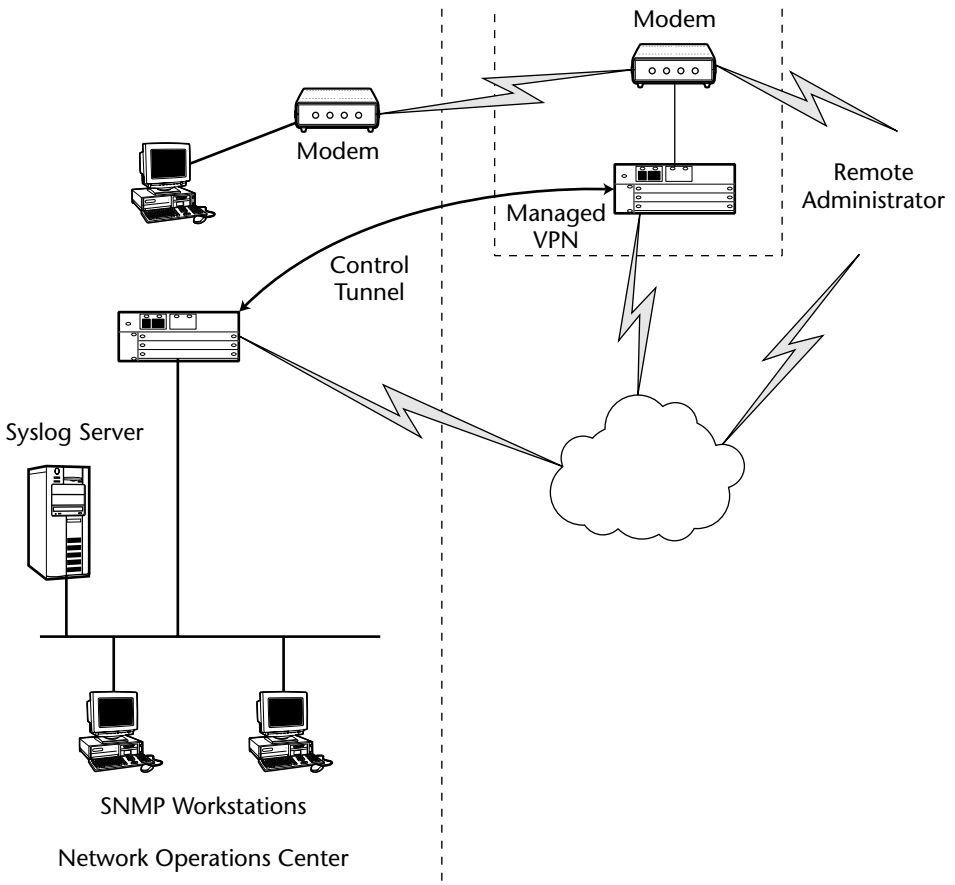


Figure 4-25: NOC administration of VPN Routers

Direct Access

In Figure 4-25, an NOC staff employee with VPN Router administration rights to the unit is able to monitor, control, and administer the unit. This can be accomplished remotely in a variety of ways. The most basic method is using the Nortel VPN Client to connect to the VPN Router's public interface, and then administering it either using the Web-enabled GUI or CLI commands using telnet. NOC staff employees would need a user's IDs and passwords to first allow them to tunnel to the VPN Router, and then they must have the administrator user ID and password to log directly into the VPN Router for its administration. Use of the Nortel VPN Client allows for the VPN Router to be administered from anywhere over the Internet. Other methods of administering the VPN Router would be the use of a control tunnel or out-of-band management.

Control Tunnels

A *control tunnel* is a tunnel that is created for the sole purpose of administering a VPN Router remotely over a tunnel connection. This would require the NOC staff employee to have access to the VPN Router that has the control tunnel to the VPN Router to be administered. This may be done by the user being either on the private LAN behind the VPN Router being used to form the control tunnel, or being able to use the Nortel VPN Client to connect to that VPN Router. The use of control tunnels is desirable in situations where the NOC users have only the responsibility of administrating the VPN Router, but not other network devices on the private LAN behind that VPN Router. Control tunnels allow only for the administration of the VPN Router and will not permit access to the private LAN located behind that VPN Router or for a user accessing the unit over a control tunnel to participate in any of the other tunnels connected to the VPN Router.

Out-of-Band Management

Out-of-band management utilizes dialup modems connected to the console ports of the VPN Routers so that an NOC employee can access and gain control of the VPN Router if it should either become unresponsive over the Internet with a control tunnel or allow access with use of the Nortel VPN Client software. When a user dials into that modem and has the administrator user ID and password, the user would be able to administer the unit. After gaining access, the user would be presented with the same console menu that a local user would obtain using a console cable and a PC running a terminal session such as HyperTerminal. From that menu, a user may enter into CLI mode, whereupon the user would be able to use a wide range of commands to monitor and control the VPN Router. Further discussion of managing the VPN Router can be found in Chapter 5 and Appendix B.

Logging

Nortel VPN Routers have a number of logs that may be viewed by using the Web-based GUI. Other reports and a display of current status and statistical information may be reported either using the GUI or CLI query commands. Further information on logs and reporting appears in Chapter 5. However, for the purpose of discussing NOC operations in support of the VPN Router, only the Syslog server will be discussed here.

Log messages from VPN Routers may be directed to a Syslog server where log messages may be collected and reviewed. In Figure 4-25, the Syslog server is shown as residing at the NOC, but that doesn't need to be the case. The VPN Router is configured with an IP and UDP port that are to be used to communicate with the Syslog server. As long as the server is able to have packets routed to it from the VPN Router, the data on that device will be collected. Logs can be collected and reviewed by NOC staff to monitor the current status of a VPN Router, as well as to review historical data to ensure the proper operation of the device.

SNMP

The Simple Network Management Protocol (SNMP) is a network protocol that also establishes a structure that allows for managing the applications and devices within the network.

SNMP became a very popular network-management tool from the onset. There were not a whole lot of frills with SNMP, which made it easy to implement and use in the network. SNMP provided a lot of assistance for users to manage their network because it provided a way to access and manage the configuration of the devices on the network. SNMP also allowed for the management of devices from multiple vendors with very little effort to implement and maintain. In SNMP, there are three important fundamental components:

- SNMP managers
- SNMP agents
- Management Information Base (MIB)

In all network SNMP configurations, at least one manager is required. Often referred to as the *SNMP network management station*, it is the network device that is used to run the SNMP management software. The SNMP management station monitors the network devices and reports when something is not acting appropriately.

The devices on the network run the SNMP agent software, which allows them to communicate with the SNMP management station. It is the function of the SNMP agent to provide the SNMP manager access to the agent's Management Information Base (MIB). The agent responds to commands sent from the manager and, in turn, retrieves and sets values within the MIB of the device. Figure 4-26 shows how this works.

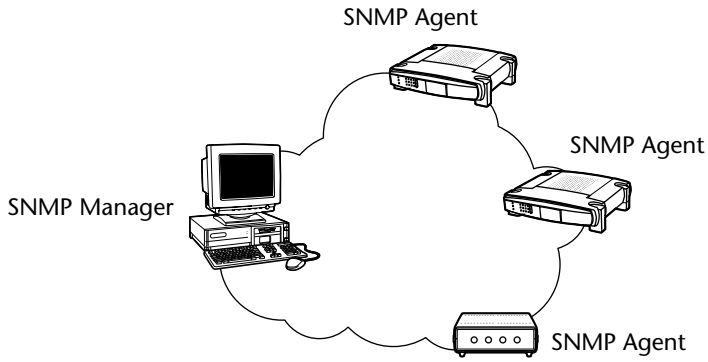


Figure 4-26: SNMP in the network

SNMP was established to improve security within a network as well as to create a more efficient pattern of retrieving information between nodes. After SNMPv2 fell short in achieving these goals, SNMPv3 was created to define the role of SNMP overall and to define security capabilities within the SNMP environment.

SNMP is organized in such a way as to ensure that it is very simple to use. SNMP uses a terse set of commands and command responses in managing the devices that they are configured to monitor. These commands are included in one of the following groups:

- SNMP Get
- SNMP Set
- SNMP Traps

SNMP is used to communicate device information over a network to an SNMP agent, where information concerning the device is collected and from which parameter changes on the device may be made.

Network management consists of two primary components:

- *Management workstation:* A workstation used to configure, monitor, and trap messages from network components that are configured as SNMP agents. The management workstation (also sometimes called an *SNMP client*) may be any PC on the network that has SNMP application software loaded on it.
- *SNMP Agent:* An entity that connects to a device in the network (such as a router, bridge, hub, or other network component) to perform SNMP Set and Get requests, as well as to send trap messages.

The managed devices on the network contain objects that may consist of hardware, configuration parameters, performance statistics, and other information that relates to the current status and operation of the device that is being managed. The objects are compiled in a virtual information database named a *Management Information Base* (*MIB*).

The use of SNMP allows the managers and agents to communicate to allow access to these objects. The management workstation requests information of the agent for inspection and/or to make a change to the device's MIB. Traps may be set so that, with certain conditions, an agent will send an alarm trap message to the management workstation.

The Nortel VPN Router supports SNMP Get and Trap operations. It does not support Set SNMP operations. So, the SNMP feature on the Nortel VPN Router is solely used to report the status of the current MIB. As illustrated in Figure 4-25, SNMP workstations may send SNMP Gets to request current status of the VPN Router that is being monitored by NOC staff members. The setting of SNMP traps allows for NOC personnel to be alerted if for any reason a VPN Router has had an abnormal condition that may require support staff interaction.

Other Management Considerations

The Nortel VPN Router supports *Network Time Protocol* (*NTP*). This feature allows for the Nortel VPN Router to communicate with an NTP server that is timed to a fixed time standard. This is an easy configuration, but a vital consideration when administering and managing the Nortel VPN Router. This is because logs are time-stamped, and if the clock on a VPN Router is not set properly, then the collected data may be meaningless if the time is skewed with the actual time of day. Also, in large installations where there are many VPN Routers interacting with each other, logs may be needed to help analyze the occurrence of an abnormality between two or more VPN Routers. In that instance, it would be immensely beneficial if all the VPN Routers were synchronized to the same clock standard.

Summary

This chapter has discussed differing scenarios involving the use of the Nortel VPN Router in the network. The illustrations were simple for discussion purposes, but the Nortel VPN Router is extremely versatile and is feature-rich with capabilities that allow it to operate in a large range of networks with differing degrees of complexity. Also discussed were the types of tunnels for clients and other VPN devices supported by the Nortel VPN Router. This chapter also included a brief discussion on the management and monitoring of the VPN Routers by using logs and SNMP.

Chapter 5 discusses connecting to the VPN Router to manage and administrate. The chapter covers basic commands and tools that are available to the VPN administrator.

CHAPTER

5

Management Options and Overview

Management is defined as the ability to collect, analyze, and adjust something in order to reach a goal. Everyone at some point during each and every day manages something in their lives. From controlling the time that you get up in the morning to choosing decaf or regular, you are able to analyze, collect, and adjust to reach a goal.

Managing your VPN Router effectively is of major importance for most network administrators. Monitoring configurations, changes, traffic patterns, and so on is a vital part of ensuring that you are meeting the present and future needs of the LAN. The Nortel VPN Router portfolio has several management options and tools available to ensure that you are able to effectively control traffic being passed through your VPN.

Managing the VPN Router also includes ensuring that users are configured correctly, users have the appropriate access capabilities, and users are assigned the correct rights and areas of access within the LAN.

The Nortel VPN Router has three main ways to access and manage the VPN Router. You can access the VPN Router through a serial interface, a Telnet session, or through the browser-based GUI interface. This chapter examines these three options and provides examples for review. Some of the sections of this chapter discuss tools and configurations, and focus on the browser-based GUI interface for examples. This was done mainly because the browser-based GUI interface is the preferred management interface used by most Nortel VPN Router administrators.

This chapter discusses the various options available to connect to your VPN Router and manage it. The discussion takes a look at the various analysis tools available as part of the standard software package for the VPN Router. Some of the concepts introduced in this chapter will be covered in more detail later in the book. This chapter is an introduction to effective and efficient management of the Nortel VPN Router.

Serial Port Management

Nortel VPN Routers have a management interface through a serial port. You can access this interface by being local to the VPN Router and attaching a direct connection via a serial cable. You can also configure and attach a modem to the serial interface to allow remote management via the serial interface menu.

Once connected successfully to the serial interface, you will be provided the following prompt to log in to the VPN Router:

```
Please enter the administrator's user name:

Please enter the administrator's password:
```

If you have provided the correct administrative credentials, the serial main menu will be displayed. The serial interface is menu-driven, which makes it a very simple way to access, configure, and maintain the VPN Router. There are 15 menu options for you to choose from. Simply choose the corresponding number or letter and press Enter. In doing this, you will then be directed to the subdirectory menu for the component that you have selected. Following are the menu options:

```
Main Menu:  System is currently in NORMAL mode.
0) Management Address
1) Interfaces
2) Administrator
3) Default Private Route Menu
4) Default Public Route Menu
5) Create A User Control Tunnel(IPsec) Profile
6) Restricted Management Mode       FALSE
7) Allow HTTP Management            TRUE
8) Firewall Options
9) Shutdown
B) System Boot Options
P) Configure Serial Port
C) Controlled Crash
L) Command Line Interface
R) Reset System to Factory Defaults
E) Exit, Save and Invoke Changes

Please select a menu choice (0 - 9,B,P,C,L,R,E):
```

Let's say you want to change the administrator login account information. The first thing you would do is locate the appropriate main menu directory pick:

```
2) Administrator
```

To access the administrator configuration through the serial interface, you will need to input the corresponding number, which is 2 in this example.

```
Please select a menu choice (0 - 9,B,P,C,L,R,E): 2
```

Once you have entered the correct number and have pressed Enter, you are directed to the submenu screen for the Administrator menu option. By looking at the following example, you can see that you have three options in this submenu. You can change the administrator's user ID and/or password, or you can opt to return to the main menu.

```
- Administrator Menu

1) Change Administrator's User ID
2) Change Administrator's Password
R) Return to the Main Menu

Please select a menu choice (1, 2, R): r
```

Command Line Interface

The Nortel VPN Router's Command Line Interface (CLI) is one way of managing the Nortel VPN Router. The CLI allows a user to type in commands that instruct the VPN Router. The CLI has a help function that assists the user in navigating through the CLI command tree.

There are two ways to access the CLI: over a Telnet session or through the serial port via the serial port menu tree.

Accessing the CLI Through a Telnet Session

The Telnet protocol is a client-server protocol that allows a client to connect to a host that supports the Telnet protocol. The Telnet protocol allows a computer to act as a terminal when you are working from a remote computer.

To be able to access the CLI with the Telnet protocol, Telnet must be configured as enabled on the VPN Router. In Microsoft Windows, you can open a MS-DOS session to initiate the Telnet session. To start the Telnet connection, you will instruct the PC to connect to the VPN Router:

```
C:\telnet 10.10.10.1
```

In this example, the user has instructed the PC to initiate a Telnet session to the management IP address of the VPN Router, 10.10.10.1. At this point, the PC will attempt to establish a Telnet session with the VPN Router. If it is successful, the login prompt will be returned, the user can log in to the VPN Router, and the CLI session will begin.

Accessing the CLI Through the Serial Port

If you are unable to access the CLI through a Telnet session, and you have access to the physical location of the VPN Router, you can optionally access the CLI through the serial interface. You can also access the serial interface via a modem, if you have configured and attached a modem to this interface.

You will need to connect to the serial port and log in to the serial menu interface. Once you have done this, you will select option "L" and press Enter. If successful, you will be given the appropriate prompt and will be in the CLI through the serial interface. Following is an example of this:

```
Main Menu:  System is currently in NORMAL mode.
0) Management Address
1) Interfaces
2) Administrator
3) Default Private Route Menu
4) Default Public Route Menu
5) Create A User Control Tunnel(IPsec) Profile
6) Restricted Management Mode       FALSE
7) Allow HTTP Management            TRUE
8) Firewall Options
9) Shutdown
B) System Boot Options
P) Configure Serial Port
C) Controlled Crash
L) Command Line Interface
R) Reset System to Factory Defaults
E) Exit, Save and Invoke Changes

Please select a menu choice (0 - 9,B,P,C,L,R,E): L

CES>
```

CLI Command Modes

The following CLI command modes are available:

- User EXEC
- Privileged EXEC
- Global Configuration

When you first access the CLI, you will be in user EXEC mode. You can tell that you are in user EXEC mode by the command-line prompt that you are given:

```
CES>
```

User EXEC Mode

The User EXEC mode is the starting mode for a CLI session, and it is a very basic command-line mode. You are not able to make configuration changes in this mode. You are not even allowed to view the configuration of the VPN Router in this mode. The User EXEC mode will support some network utilities (such as the `ping` and `traceroute` commands), but it mainly allows the user the ability to view some of the system information.

The text portion of the prompt can be renamed to assist in managing the VPN Router but will default to the text "CES." Many administrators choose to rename the text to identify the VPN Router by location or some other identifying name.

Privileged EXEC Mode

The Privileged EXEC mode is accessed through the User EXEC mode by typing **enable** at the User EXEC mode CLI prompt. You can exit out of the Privileged EXEC mode by typing **disable** or **exit** at the Privileged EXEC mode CLI prompt.

While in Privileged EXEC mode, you are able to access and use all User EXEC mode prompts, as well as utilize additional commands that are not contained within the User EXEC mode. While in this mode, you are able to view the running configuration of the VPN Router.

NOTE The Nortel VPN Router CLI supported abbreviated commands. Instead of typing the whole command, you can usually type the first few letters of each word in the command. For example, if you want to issue the command `configure terminal` you can simply type `conf term`.

To enter this mode, you simply have to type **enable** at the User EXEC mode prompt. You will then be prompted for a password, which will be the administrator password, as shown here:

```
CES>enable
Password:
```

If you have logged into Privileged EXEC mode successfully, you are given the Privileged EXEC mode prompt, which is the text name for the VPN Router along with a pound symbol (#).

```
CES#
```

Global Configuration Mode

The final command mode that is available in the VPN Router CLI interface is the Global Configuration mode. To enter the Global configuration mode, you type the command **configure terminal** at the Privileged EXEC prompt:

```
CES#configure terminal
```

If you have logged into the Global configuration mode successfully, you will be given the Global configuration mode prompt, which will be the text name prompt and the word "config" in parentheses, followed by a pound symbol (#):

```
CES(config)#
```

To exit the Global Configuration mode CLI session, you can use any one of the following commands or key sequence:

- Exit
- End
- Ctrl+Z

While in the Global Command mode CLI session, you are able to issue all of the commands that are supported in the User EXEC mode and the Privileged EXEC mode. You are also allowed to make changes to the VPN Routers running configuration.

Several configuration modes are accessed from the Global Configuration mode. These configuration modes allow you to configure the multitude of services that are supported on the VPN Router. Following is a list of the configuration modes that are available to the administrator:

- ATM or T1/E1 Controller
- Backup Interface Services (BIS)
- Branch Office Group IPsec
- Branch Office Group Connectivity
- Branch Office Group RIP
- Branch Office Group OSPF
- Branch Office Connection
- Branch Office Connection Control Tunnel
- Branch Office Static Routing
- Certificate Request
- Crypto CA
- Crypto CA Identity
- Crypto Server Certificate

- Demand Services
- Filter Rule
- Filter Tunnel
- Filter Interface
- Group IPSec
- Group L2F
- Group Connectivity
- Group L2TP
- Group PPTP
- Interface
- IPX Interface
- Packet Capture
- QoS MF Classifier
- QoS Rule
- Router Client Address Redistribution (CAR)
- Router OSPF
- Router RIP
- Router VRRP
- User
- 802.1Q, ATM, and Frame Relay Subinterface

CLI Help

The Nortel VPN Router contains a Help utility that can be used within the CLI. This is very helpful when you are navigating the directory tree and are unsure of a command. To use the Help utility while in the CLI, simply input a question mark (?) after the main command within the directory structure:

```
CES>?

Exec commands

cd              Change current directory
clear           Clears the IP routing table (user and admin mode), ARP
                cache, or event log (admin mode)
dir             To display a list of files in the current directory
enable          Enables privileged commands
exit            Enables settings and disables exec mode and enables user
                level mode
```

```
help            Displays information about using commands interactively
ls              To display a list of files in the current directory
ping            Sends a ping message to a destination
pwd             To show the current directory
reset           Resets a port
show            Displays running system information
terminal        Terminal screen configuration
trace           Enables tracing a route to a destination
verify          Verify the system
who             Displays active Telnet sessions on the CES with what
                number a particular Telnet session is since boot
```

In this example, the Help utility was initiated at the User EXEC mode prompt for assistance in determining the commands that are available within that mode. If you look at this main directory listing you can see that the decision is made to view the help directory for the command `verify`. At the CLI prompt, you would enter **verify** followed by a question mark (?). The output will be the subcommands that are available for the `verify` command.

```
CES>verify ?

  system  Verify the software system integrity
```

In this example, `system` is the only subcommand choice that is available. To issue this command, you simply enter the `system` command after the `verify` command:

```
CES>verify system
```

You can use the CLI Help utility to navigate the Privileged EXEC mode and the Global Configuration mode. Following are the CLI directory choices available to the VPN Router administrator. Remember that you have to issue the `enable` command to enter the Privileged EXEC mode, and then you have to issue the `configure terminal` command to enter the Global configuration mode.

```
CES>enable
Password:

CES#?

Exec commands

boot            Restarts the CES using specific loaded image
capture         Captures network traffic
cd              Change current directory
clear           Clears the IP routing table (user and admin mode), ARP
                cache, or event log (admin mode)
clock           Sets the system clock
```

```
configure      Enables configuration mode
connect        Establishes a desired connection
copy           Copy files or copy to file system related information
create         Creates recovery diskette or updates flash
debug          Enables debugging of some nncli commands
delete         To delete file(s)
dir            To display a list of files in the current directory
disable        Disables privileged commands
enable         Enables privileged commands
exit           Enables settings and disables exec mode and enables user
               level mode
forced-logoff  Logs off active connections
help           Displays information about using commands interactively
kill           Terminates a Telnet session
ls             To display a list of files in the current directory
microcode      Reloads firmware. Reload may take several minutes per
               card.
mkdir          To create a new directory
more           Displays the contents of a file
no             Disables or Deletes the attributes
ping           Sends a ping message to a destination
pwd            To show the current directory
reformat       Formats the floppy disk
reload         Halt and perform a cold restart
rename         To rename a file or a directory
reset          Resets a port
retrieve       Retrieves a software image for the switch
rmdir          To remove an existing directory
show           Displays running system information
ssl-vpn        SSL-VPN Accelerator commands
ssl-vpn-cli    Switch to SSL CLI
terminal       Terminal screen configuration
test-bis       Enables testing of a backup interface
trace          Enables tracing a route to a destination
verify         Verify the system
who            Displays active Telnet sessions on the CES with what
               number a particular telnet session is since boot


CES#configure ?

  terminal  Enable configuration from the terminal

CES#configure terminal

CES(config)#?

Configure commands:

aaa                      Authentication, authorization and accounting
access-hours             Adds and configures access hours
access-list              Adds an access list entry
```

```
accounting                Accounting server
adminname                 Enables administrator to enable the
                          administrator login name and password
arp                       Adds a static ARP entry
audible                   Enables audible alarm
bis                       Configures Backup Interface Services
bo-conn                   Adds or configures branch office connections
bo-group                  Enables branch office group configuration
                          commands
clear                     Disables the number of days the journal files
                          will be removed from internal RADIUS server
client-policy             Adds or modifies client policy
clip                      Configures Circuitless IP
clock                     Sets the system clock
cmp                       Enables certificate management protocol
compress-files            Enables file compression
console                   Sets or displays the restriction level of the
                          console session
controller                configure physical I/O parameters
create                    Creates Safe mode config
crl                       Enables the retrieval of certificate
                          revocation list(CRLs)
crypto                    Enables crypto certificate configuration
data-collection-interval  Displays data collection interval information
default                   Enables default switch settings configuration
dns-proxy                 Enables DNS Proxy on the CES
domain                    Edits or adds domain set or domain
end                       Exits from configure mode
erase                     Deletes a configuration file
event-log                 Specifies the size of the event log
exception                 Defines backup FTP servers for the CES
exit                      Saves settings and leaves configuration mode
filter                    Enables filter configuration
fips                      Enables federal information processing
                          standards
firewall                  Enables firewall type
frame-relay               Enables Frame Relay debug mode on a specific
                          slot and port
ftp-server                Enables file transfer protocol to the system
                          management IP Address
fwua                      Enables Firewall User Authentication
group                     Configures user groups
help                      Describes the interactive help system
hostname                  Enables the system hostname
http                      Enables HTTP protocol
https                     Enables HTTPS service
icmp                      Enables ICMP service
identification            Enables identification protocol to the system
                          management IP Address
idle-timeout              Enables an automatic logout when an
                          administrator session is not in use
```

```
interface                Selects an interface to configure OR
                         configures an interface group
ip                       Enables IP settings
ipsec                    Enables IPSEC tunnel configuration
ipx                      ipx commands
l2f                      L2F tunnel configuration
l2tp                     L2TP tunnel configuration
ldap                     Control LDAP server (Mini-CLI emulation)
ldap-server              LDAP server configuration
license                  Installs license key for paid feature
load                     Bulk load configuration commands (Mini-CLI
                         emulation)
log-file-lifetime        Sets the log file's time to live (in days)
logging                  Enables the syslog server host
logout                   Disconnect this telnet session
maximum-paths            Enables the maximum equal cost paths
multicast-boundary       Enables adding interfaces to multicast
                         boundary list
multicast-relay          Enables multicast relay
network                  Adds network and allows to assign IP address
                         and subnet mask to the network
no                       Disables features
ntp                      Enables network time protocol
ospf                     Enables the maximum equal cost paths to
                         calculate within OSPF
policy                   CSF Policy Manager
pptp                     Enables PPTP tunnel configuration
prompt                   Changes session prompt
proxy                    Enables the external LDAP authentication
                         server
qos                      Enables qos
radius                   Enables RADIUS service
radius-accounting        Enables RADIUS Accounting service
radius-client            Configures Radius Client
radius-server            Radius server configuration
restrict                 Restricts management access to CES (Mini-CLI
                         emulation)
rip                      ximum equal cost paths to calculate within RIP
route-policy             Enables the route policy feature
router                   Specifies a routing process to configure
safe-mode                Enables Safe Mode Configuration
save                     Save current boot config (Mini-CLI emulation)
scheduler                Enables scheduler settings
serial-banner            Configure the serial banner
serial-banner-fragment   Add a new line to serial banner
serial-port              Enables serial port configuration
service                  Enables services
show                     Displays configuration information
snmp-server              SNMP Server settings
split-dns                Enables DNS Server to be split between public
                         and private domains
```

```
ssh                     Enables SSH service
ssl                     Configures SSL
ssl-vpn                 SSL-VPN Acceleration configuration mode
system                  Enables system settings
system-log-to-file      Write system log to file
telnet                  Virtual terminal protocol to the system
                        management IP address
tunnel                  Enables the tunneling protocols, i.e., IPsec,
                        PPTP, L2TP, L2F
tunnel-guard            Enables to set tunnel guard properties
user                    User configuration mode
```

CLI Keystroke Shortcuts

The Nortel VPN Router supports some keystroke shortcuts that can be used while in the CLI. Getting to know and understand these shortcuts can be very useful when navigating and editing within the CLI. Table 5-1 shows a list of these shortcuts and what function each of these provides.

Table 5-1: CLI Keystroke Shortcuts

COMMAND	DESCRIPTION
Ctrl+A	Moves the cursor to the beginning of the line.
Ctrl+B	Moves the cursor back one character.
Ctrl+C	Abort.
Ctrl+D	Deletes a character.
Ctrl+E	Moves the cursor to the end of the line.
Ctrl+F	Moves the cursor ahead one character.
Ctrl+H &	Deletes the character to the left.
Ctrl+I &	Completes the command.
Ctrl+K	Deletes all of the following characters.
Ctrl+L	Re-displays the line.
Ctrl+R	Re-displays the line.
Ctrl+N	Moves to the next history command.
Ctrl+P	Moves to the previous history command.
Ctrl+Q	Escape.
Ctrl+T	Transposes characters.
Ctrl+U	Deletes the entire line.
Ctrl+W	Deletes the entire word to the left of the cursor.

Table 5-1: *(continued)*

COMMAND	DESCRIPTION
Ctrl+X	Deletes all of the characters to the left of the cursor.
Ctrl+Z	Used to exit Global Configuration mode.
Up arrow	Moves to the previous history command.
Down arrow	Moves to the next history command.
?	Accesses the help utility.
Esc+C	Converts the character at the cursor to an uppercase character.
Esc+U	Converts the character at the cursor to an uppercase character.
Esc+L	Converts the character at the cursor to a lowercase character.
Esc+B	Moves the cursor back one word.
Esc+D	Deletes the word to the right of the cursor.
Esc+F	Moves the cursor forward one word.

Web-Based Management

The VPN Router browser-based interface (BBI) is very useful, helpful, and easy-to-use. As the name implies, it is a browser-based interface, which requires a browser to connect to the interface and use it. The BBI contains a main menu, with each category breaking down into subcategories. Following are the categories that are available on the main menu screen:

- System
- Services
- Routing
- QoS
- Profiles
- Servers
- Admin
- Status
- Help

Most administrators prefer using the BBI over the other management options because of its ease of use. If you are not sure of where the subcategory you need is, you can click quickly through the menu categories to find it. If all

else fails, the BBI contains a very thorough Help utility that explains what each subcategory does.

To access the VPN Router through the BBI, the VPN Router must have an interface and management IP assigned to it. This can be set up through the serial interface. Once configured, you only have to open your BBI and enter the management IP address in the URL field of the browser, as shown in Figure 5-1.

If you are accessing a new switch for the first time, you will want to use either the Quick Start option or the Guided Config option, which helps with the configuration of the VPN Router. After you have completed the initial configuration of the VPN Router, most of the rest of the time you will be accessing the VPN Router to manage the router. The options you have now are to access it via the Manage Switch option or Manage from a Notebook option.

NOTE **If you have a slow remote connection, you can help speed up the process of accessing the BBI by selecting the Manage from a Notebook option, which is less graphics-heavy and loads quicker.**

Once you are successfully connected to the VPN Router, you will be prompted to enter the administrative user ID and password. If authenticated, then you will be granted access to the main interface screen. From this screen, you have four options from which to pick (see Figure 5-2). Each of these options includes a brief description on what that particular option is for. Following are the options:

- *Manage Switch:* The main management GUI interface used for the day-to-day management of the VPN Router.
- *Manage from a Notebook:* Similar to the manage switch option, but less graphics-intensive.
- *Quick Start:* Used to quickly configure the VPN Router.
- *Guided Config:* Provides hints to assist in the configuration of the VPN Router.

If you have successfully logged onto the GUI you will be directed to the main menu window. The main menu window consists of the menu options that are located on the left side of the window. The main screen section of the window is in the lighted shaded area. Buttons in the upper right enable you to log off and link to the Help screen. Figure 5-3 shows an example of the Manage Switch option main menu screen.



Figure 5-1: Accessing the management IP address through a browser-based interface



Figure 5-2: The browser interface introduction screen

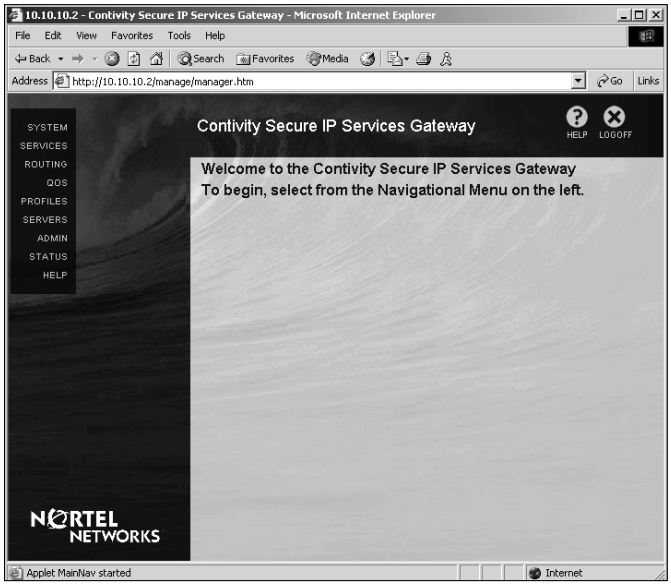


Figure 5-3: The browser-based interface's main menu screen

The menu options on the left side of the browser window contain the categories that are available to browse. Within these categories are the configuration options and viewing options for the entire VPN Router.

System

The System category menu within the BBI provides information and configuration options for items such as system identity, the LAN interfaces, the WAN interfaces, routing, certificates, and others. Following are the subcategories that can be accessed through the System category:

- Identity
- ATM
- LAN
- WAN
- Dial Interface
- Circuitless IP
- IPX
- Date and Time
- Certificates
- Settings
- Forwarding

Services

The Services category menu within the BBI provides information and configuration options for the various services that are configured on the VPN Router. System RADIUS settings, switch services, and tunnel types are all accessed through this menu pick. Following are the subcategories that are accessed through the Services category:

- Available
- Backup Interface
- IPSEC
- PPTP
- FWUA
- L2TP
- L2F
- RADIUS
- Firewall/NAT
- SYSLOG
- SSLTIS

Routing

The Routing category within the BBI provides information and configuration options for the various routing support that is configured on the VPN Router. Protocols such as OSPF, RIP, and VRRP are all accessed through this menu pick. Following are the subcategories that are accessed through the Routing category:

- Static Routes
- OSPF
- RIP
- Interfaces
- Multicast
- VRRP
- Configuration
- Route Table
- Access List
- Policy
- Client-Addr-DIS
- Interface GRP
- NAT
- Status

QoS

The QoS menu within the BBI provides information and configuration options for the Quality of Service (QoS) parameters that are configured and/or supported on the VPN Router. All QoS and Bandwidth management services are contained and are accessed through this menu pick. Following are the subcategories that are accessed through the QoS category:

- Classifiers
- Interfaces
- Bandwidth Mgmt
- Call Admission

Profiles

The Profiles menu within the BBI provides information and configuration options for the various profiles that can be configured on the VPN Router. The

user profiles and the group profiles for all remote clients are all accessed through this menu pick. Additionally, information on the tunneling protocols, authentication parameters, and encryption information is also accessed here. Following are the subcategories that are accessed through the Profiles category:

- Groups
- Users
- Filters
- Hours
- Networks
- Domains
- Branch Office
- Client Policy

Servers

The Servers menu within the BBI provides information and configuration options for the various servers that are configured on the VPN Router. RADIUS server information, LDAP server information, DHCP server information, and so on are all accessed through this menu pick. Following are the subcategories that are accessed through the Servers category:

- RADIUS Authorization
- RADIUS Accounting
- LDAP
- LDAP Proxy
- User IP Address
- DHCP Relay
- DHCP

Admin

The Admin menu within the BBI provides information pertaining to the various administrative tasks that are configured on the VPN Router. System backups, recovery disks, and system shutdown are all accessed through this menu pick. Following are the subcategories that are accessed through the Admin category:

- Administrator
- License Keys

- Auto Backup
- Tools
- Recovery
- Upgrades
- Configurations
- File System
- SNMP
- SNMP Traps
- Shutdown
- Quick Start
- Guided Configuration

Status

The Status menu within the BBI provides information and options for the various system status services that are supported on the VPN Router. Within this category, administrators are able to monitor users, traffic patterns, bandwidth requirements, system information, and system hardware information. Following are the subcategories that are accessed through the Status category:

- Sessions
- Reports
- System
- Health Check
- Statistics
- Accounting
- Security LOG
- Configuration LOG
- System LOG
- Event LOG

Help

The Help menu within the BBI provides information that can assist administrators in configuring and maintaining the VPN Router. This is a handy tool that describes everything pertaining to the VPN Router. A description of all

BBI categories is contained within the Help category. Following are the sub-categories that are accessed through the Help category:

- Help Contents
- Support
- About

VPN Router Administrator

To access and manage the Nortel VPN Router, an individual must be assigned administrator rights. There can be more than one administrator, as long as the user has been given the rights to administer the VPN Router. Administration rights can be assigned to an individual through the BBI by going to the following directory: PROFILES → USERS → EDIT.

Various admin levels can be assigned to the users that have been given administrative rights. Figure 5-4 shows an example of setting the admin levels on the VPN Router. Following are the admin levels:

- *None:* This value will be assigned to most users. Users given this value for administrative rights do not have rights to manage the VPN Router, nor do they have rights to manage the users of the VPN Router.
- *Manage:* Users given this value for administrative rights have access to view and configure all functions within the VPN Router. This is the highest privilege level that can be assigned to an administrator.
- *View:* Users given this value for administrative rights have access to view all functions within the VPN Router, but do not have the authority to make any changes.

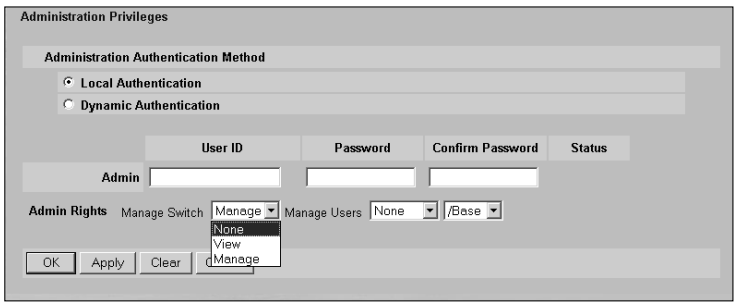


Figure 5-4: Setting the administrative rights

File Management

You can access the system file directory to find out information on specific files and directories contained on the hard drives on your VPN Router. Through the BBI you can access this information by going to the following directory: ADMIN → FILE SYSTEM.

The information contained on this page (see Figure 5-5) shows all drives that are associated with your VPN Router, as well as the files and directories that are stored on those drives. Accessing the file system through the BBI is an excellent way to maintain and manage your file system. It is an easy way to view the files on your drives and to delete any files that are no longer used or are not wanted.

If you are experiencing file-retrieval problems, accessing the file system is an easy way for you to begin troubleshooting to see what may be wrong with the file system. You can obtain information such as filename, file size, and the last date modified. All of this information can be beneficial when working with the file system.

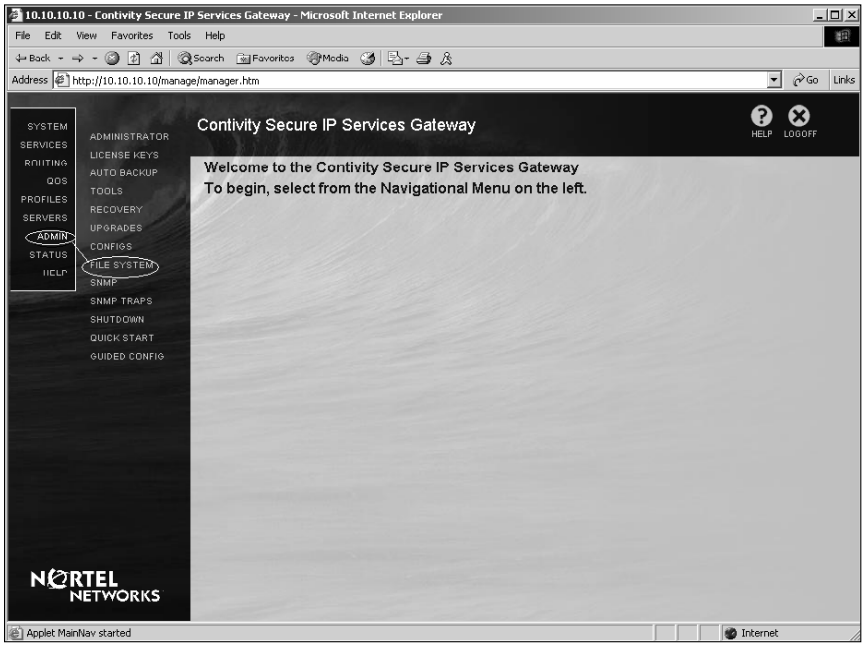


Figure 5-5: Accessing the file system from the browser-based interface

Checking the Current Status of Your VPN Router

The Nortel VPN Router contains tools to assist in monitoring, maintaining, and managing the VPN Router. The tools are located within the Status screen on the browser-based GUI interface. The information contained within the status screen from the BBI main menu will assist the VPN manager in monitoring traffic patterns, user traffic, and significant events that occur within the VPN Router. There are two main portions within the status main menu section: logs and status tools.

Logs

Most data equipment keeps a log of major events that happen during the running time of the device. Sometimes the information contained within the logs is very generic, and sometimes it is very detailed. A log can track certain events, such as a hardware failure or a network link status. A log can also be very detailed, providing status information for all activity on the device.

The Nortel VPN Router provides several logs to assist in the management of the VPN Router. The logs track information pertaining to events that occur on the VPN Router, including IP addresses and the user ID information involved in a particular logged event.

The logs that are generated by the VPN Router are stored as text files. Some of the logs are stored, while others are retained in memory and only significant events are stored. The stored files can be retrieved by using the File Transfer Program (FTP), or can simply be viewed through the browser-based GUI interface. Following are the logs saved on the VPN Router that can be accessed via the BBI:

- The Configuration log
- The Event log
- The Security log
- The System log

Configuration Log

The Configuration log can be accessed via the browser GUI management interface by going to the following directory: STATUS → CONFIG LOG.

The Configuration log maintains a record of all changes to the configuration of the VPN Routers. This includes all modifications, additions, and deletions made to the VPN Router. Following is an example:

```
*00:09:01 tRootTask 0 : cfg file setting warning
'IpxIntfOmCls.IpxPrivateLANS[256].IpxAddress=N/A'
*00:09:01 tRootTask 0 : cfg file setting warning
'IpxIntfOmCls.IPXPublicAddress=N/A'
*00:09:19 tSerialConfig 0 : DirBackup.PrimaryHost changed from '' to ''
by user '' @ ''
*00:09:19 tSerialConfig 0 : DirBackup.PrimaryPath changed from '' to ''
by user '' @ ''
*00:09:19 tSerialConfig 0 : DirBackup.PrimaryUsername changed from '' to
'' by user '' @ ''
*01:39:12 tHttpd 0 : Security.TrustedFTPEnabled changed from 'FALSE' to
'TRUE' by user 'admin' @ '10.10.10.1'
```

The first section of the Configuration log entry is the time stamp including when the entry was logged. The next portion of the Configuration log entry identifies the task that issued the event. Next, you will see either a "1" or a "0." This entry represents the CPU that reported the event. The entry "0" represents CPU0 and the entry "1" represents CPU1. If you are managing a VPN Router that contains only one disk drive, then this entry will always be a "0."

Following the CPU identifier, you will see information pertaining to what configuration change was being made. Figure 5-6 shows an example of the Configuration log that is accessed via the BBI.

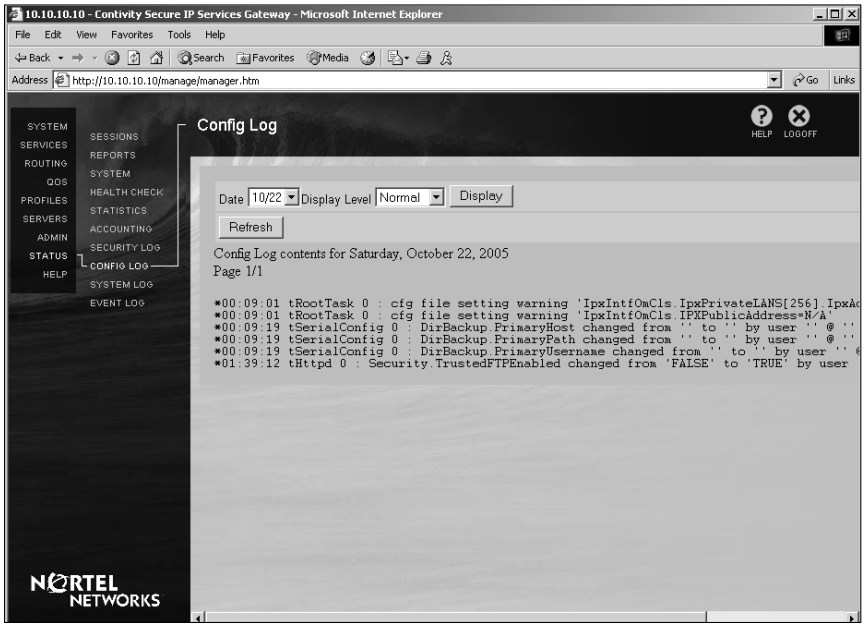


Figure 5-6: Accessing the Configuration log from the browser-based interface

Event Log

The Event log can be accessed via the browser GUI management interface by going to the following directory: STATUS → EVENT LOG.

The Event log captures data as it is occurring on the VPN Router. It holds this data in memory and writes significant events into the System log. The Event log is a running entry of all events that occur on the VPN Router. The Event log will retain all of these entries in memory and will report significant entries to the System log, to be written to the system log file and saved on disk.

The Event log retains (in memory) the last 2,000 event log entries that it has captured on the VPN Router. Once the Event log has reached the 2,000th entry, it will report the significant entries to the system log and then will begin logging again. Figure 5-7 shows an example of the Event log that is accessed via the BBI.

The information in the Event log may or may not make sense to the unlearned eye. The Event log is a very straightforward tally of the events occurring (real-time) on the VPN Router. Following is an example of some Event log entries:

```
10/22/2005 00:08:52 0 Sys [13] EventLog: The current Eventlog size is
2000 entries
10/22/2005 00:08:59 0 Boot [13] Booting in Normal mode ...
10/22/2005 00:08:59 0 Boot [13] Booting version V05_05.220, created on
Jul 28 2005, 21:54:53.
10/22/2005 00:08:59 0 CtxtReclaim [01] Created.
10/22/2005 00:08:59 0 Reclaim [01] Created.
```

The first portion of an Event log entry is the date and time that the event occurred. Following the time will be either a "1" or a "0." This entry represents the CPU that reported the event. The entry "0" represents CPU0 and the entry "1" represents CPU1. If you are managing a VPN Router that contains only one disk drive, then this entry will always be a "0."

The next portion of the Event log entry is the task that has issued the event. In the preceding example, the following tasks have issued events: `Sys`, `Boot`, `Boot`, `CtxtReclaim`, and `Reclaim`.

The next portion of the Event log entry is the priority code. This is always a two-digit number that represents information about the logging of the event and the priority assigned to it. The number is represented within brackets. The first digit of the priority code is information about where the event is being written to. The second digit of the number represents the priority code that has been assigned to the event.

If the first digit of the priority code is a 0, then the message is logged in the event log only. If the first digit of the priority code is a 1, then the message is logged in the System log. Finally, if the first digit of the priority code is a 2, then the message is logged in the System log and is also forwarded to a configured syslog server to be stored.

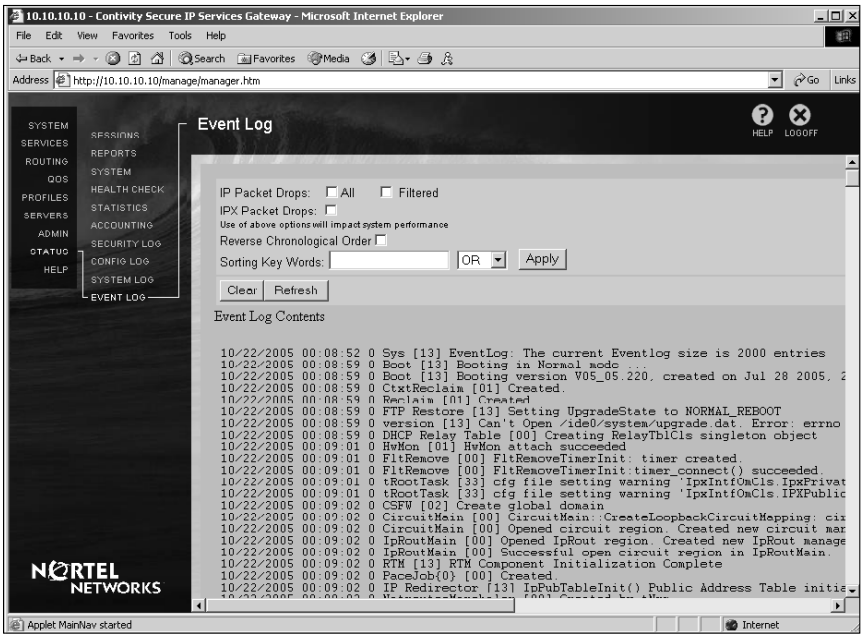


Figure 5-7: Accessing the Event log from the browser-based interface

If the second digit is a 1, the priority of the event is a low priority. If the second digit is a 2, the priority of the event is a medium priority. If the second digit is a 3, the priority of the event is a high priority.

NOTE **If the first digit of the priority code is a 2, then the second digit will identify the message type of the log entry. These codes are as follows:**

1—Alert

2—Critical

3—Error

4—Warning

5—Notice

6—Information

7—Debug

The final portion of the Event log entry is information that describes what is occurring during that event. For example, in the following Event log entry, the event that is occurring is the VPN Router is "Booting in Normal mode."

```
10/22/2005 00:08:59 0 Boot [13] Booting in Normal mode ...
```

Security Log

The Security log can be accessed via the browser GUI management interface by going to the following directory: STATUS → SECURITY LOG.

The Security log keeps a record of all activity pertaining to system security. All security events are retained within the security log. This includes information about user and VPN Router security (both failed attempts and successful attempts). Following is an example of the Security log:

```
*00:09:27 tEvtLgMgr 0 : Security [13] c_check_ca_root: user de-select
server cert
*00:09:31 tEvtLgMgr 0 : Security [13] LdapMonitorTask: Switching LDAP
locations may impact SSL certificate identification, a re-load may be
necessary.
*00:09:31 tEvtLgMgr 0 : Security [13] LdapMonitorTask: Refreshed FW and
NAT policies for new LDAP server
*01:36:00 tEvtLgMgr 0 : Security [13] Management: Request for
manager.htm denied, requires login
 01:36:06 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:1 master
admin authenticated
 01:36:06 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:1
Management: logged in from 10.10.10.1 Server Rights: Manage User Rights:
Manage
 01:36:56 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2 master
admin authenticated
 01:36:56 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2 TELNET:
logged in from 10.10.10.1
```

The first section of the Security log entry is the time stamp including when the entry was logged. The next portion of the System log entry identifies the task that issued the event.

Next, you will see either a "1" or a "0." This entry represents the CPU that reported the event. The entry "0" represents CPU0 and the entry "1" represents CPU1.

Following the CPU identifier, you will see the software module that issued the event.

The next portion of the System log is the priority code. This is always a two-digit number that represents information about the logging of the event and the priority assigned to it. The number is represented within brackets. The first digit of the priority code is information about where the event is being written to. The second digit of the number represents the priority code that has been assigned to the event.

If the first digit of the priority code is a 0, then the message is logged in the Event log only. If the first digit of the priority code is a 1, then the message is logged in the System log. Finally, if the first digit of the priority code is a 2, then the message is logged in the System log and is also forwarded to a configured Syslog server to be stored.

If the second digit is a 1, the priority of the log entry is low. If the second digit is a 2, the priority of the log entry is medium. If the second digit is a 3, the priority of the log entry is high.

NOTE **If the first digit of the priority code is a 2, then the second digit will identify the message type of the log entry. These codes are as follows:**

1—Alert

2—Critical

3—Error

4—Warning

5—Notice

6—Information

7—Debug

The final portions of the Security log detail information about the specific activity that is occurring during the log entry. This information includes why the event was generated, what was occurring, and whether or not the event succeeded. Figure 5-8 shows an example of the Security log that can be accessed via the BBI.

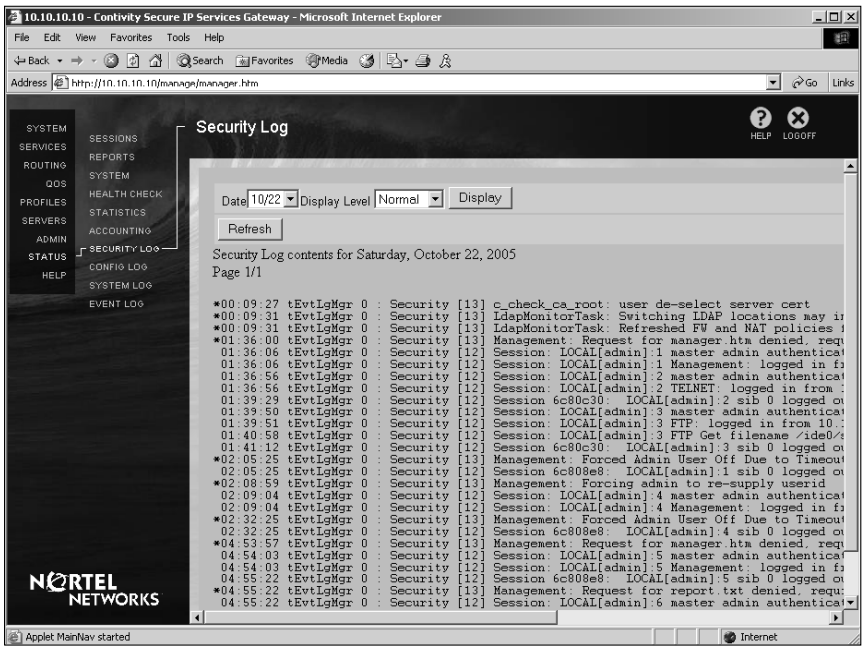


Figure 5-8: Accessing the Security log from the browser-based interface

System Log

The System log can be accessed via the browser GUI management interface by going to the following directory: STATUS → SYSTEM LOG.

The System log retains data for up to 61 days. All system log data is written to a file and is stored on the disk. The Event log will send significant events to the System log to be stored for reference purposes. This is not to say that the Event log is the only place where data is received by the System log. Take a look at the following System log entries:

```
*00:08:52 tEvtLgMgr 0 : Sys [13] EventLog: The current Eventlog size is
2000 entries
*00:08:59 tEvtLgMgr 0 : Boot [13] Booting in Normal mode ...
*00:08:59 tEvtLgMgr 0 : Boot [13] Booting version V05_05.220, created on
Jul 28 2005, 21:54:53.
*00:08:59 tEvtLgMgr 0 : FTP Restore [13] Setting UpgradeState to
NORMAL_REBOOT
*00:08:59 tEvtLgMgr 0 : version [13] Can't Open
/ide0/system/upgrade.dat. Error: errno = 0x388002
*00:09:01 tRootTask 0 : cfg file setting warning
'IpxIntfOmCls.IpxPrivateLANS[256].IpxAddress=N/A'
*00:09:01 tRootTask 0 : cfg file setting warning
'IpxIntfOmCls.IPXPublicAddress=N/A'
```

You can see that the System log entries do differ slightly from the entries of the event log. The first section of a System log entry is the time stamp, which provides the time the entry was logged. The next portion of the System log entry identifies the task that issued the event.

Next, you will see either a "1" or a "0." This entry represents the CPU that reported the event. The entry "0" represents CPU0 and the entry "1" represents CPU1. If you are managing a VPN Router that contains only one disk drive, then this entry will always be a "0."

Following the CPU identifier, you will see the software module that issued the event. For example, in the log entry `00:08:59 tEvtLgMgr 0 : Boot [13] Booting in Normal mode ...`, the software module is the `Boot` software module.

The next portion of the System log is the priority code. Like the Event log, this is always a two-digit number that represents information about the logging of the event and the priority assigned to it. The number is represented within brackets. The first digit of the priority code is information about where the event is being written to. The second digit of the number represents the priority code that has been assigned to the event.

If the first digit of the priority code is a 0, then the message is logged in the event log only. If the first digit of the priority code is a 1, then the message is logged in the system log. Finally, if the first digit of the priority code is a 2, then the message is logged in the System log, and is also forwarded to a configured syslog server to be stored.

If the second digit is a 1, the priority of the log entry is a low priority. If the second digit is a 2, the priority of the log entry is a medium priority. If the second digit is a 3, the priority of the log entry is a high priority.

NOTE If the first digit of the priority code is a 2, then the second digit will identify the message type of the log entry. These codes are as follows:

1—Alert

2—Critical

3—Error

4—Warning

5—Notice

6—Information

7—Debug

The last portions of the System log entry indicate whether the packet matches rules that are established in the corresponding section, and indicates if the matching packet has source, destination, protocol, and action configured for the rule. Figure 5-9 shows an example of the System log screen in the BBI.

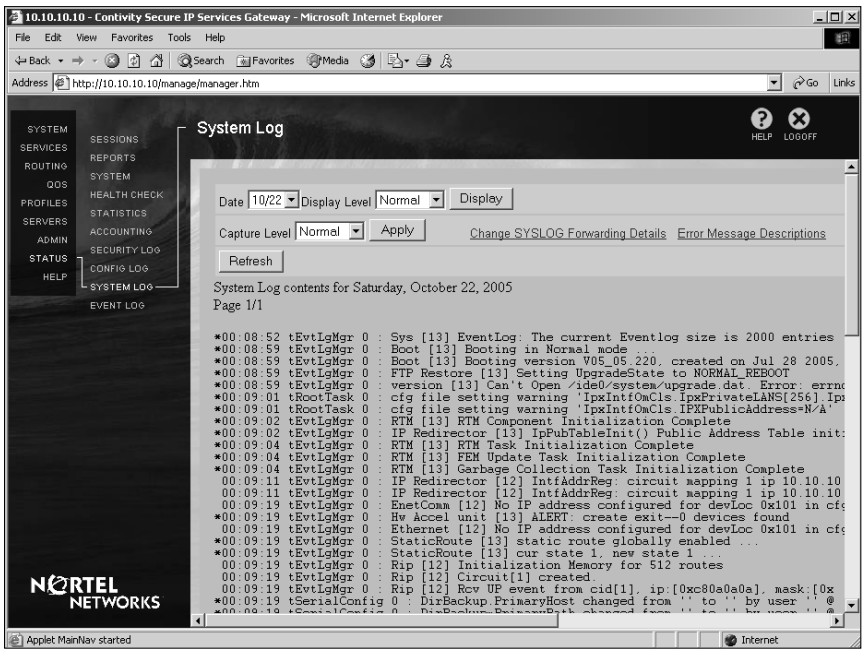


Figure 5-9: Accessing the System log from the browser-based interface

VPN Router System Status Tools

The Nortel VPN Router has several tools that assist in monitoring the current operating status of the router. The system status screen in the BBI contains information about the users who are connected to the VPN Router, and the traffic that is being generated by those users. Additionally, there is information about the hardware itself and the system files.

The status section retains logging information (discussed earlier in this chapter) that is very helpful in troubleshooting and diagnosing problems within the VPN Router. Statistical information is also available within this section. As shown in Figure 5-10, the status menu within the BBI has several subcategories to choose from:

- Sessions
- Reports
- System
- Health Check
- Statistics
- Accounting

Sessions

The Sessions menu pick provides you with information about all of the active sessions that are being processed by the VPN router. To access this screen, go to the following path within your browser-based: STATUS → SESSIONS.

The Sessions screen provides a summary of your BOT sessions, as well as your user tunnel sessions. In addition to the summary information, this screen will also provide you with individual user tunnel information and BOT.



Figure 5-10: The Status menu selection and the associated subdirectories

As the administrator, you have the ability to log off individual sessions, as well as log off everyone that is currently connected to the VPN router. This can be especially helpful when troubleshooting because you are able to determine who might be affected if you make a change.

Reports

The VPN Router has a Reports utility that allows the administrator an option to compile reports of system information. The reports can be generated on the screen, and can also be imported into a spreadsheet or a database. To access the Reports utility, you will go to the following directory within the browser-based: STATUS → REPORTS.

The Reports utility can be viewed in a text report, as well as within a graphical report format. Both current and historical reporting can be maintained and accessed. The following information is the type of information that can be gathered and viewed using the Reports screen utility:

- Administrator activity
- User activity
- System information
- Sessions information
- Failed authorizations
- Expired passwords
- RADIUS diagnostics

Figure 5-11 shows an example of the Reports screen utility within the BBI.

System

The System screen provides you with information about the status of the VPN Router. To access the System screen within the BBI, go to the following directory: STATUS → SYSTEM. The following information can be obtained from this screen:

- System uptime
- Software version
- Software build date
- Software build type
- Mac address of the router
- System serial number

- Maximum number of supported tunnels
- Hardware processor type(s)
- Memory information
- Hard drive information
- Diskette type

Health Check

The Health Check utility that is provided within the VPN Router BBI is a helpful tool used to monitor the overall condition of the VPN Router. To access the Heath Check screen within the BBI, go to the following directory: STATUS → HEALTH CHECK.

The Health Check screen contains information about the VPN Router and the current status of the entire hardware and software configuration. The Health Check screen will prioritize information from the most critical to least critical. This enables quick access to the information and also places the information that needs to be attended to at the top of the list.

There is an option to turn on or turn off an alarm on this screen. If the alarm is turned on, the VPN Router will issue a continuous beep whenever there is something within the Health Check screen that needs immediate attention. Figure 5-12 shows an example of the Health Check screen.

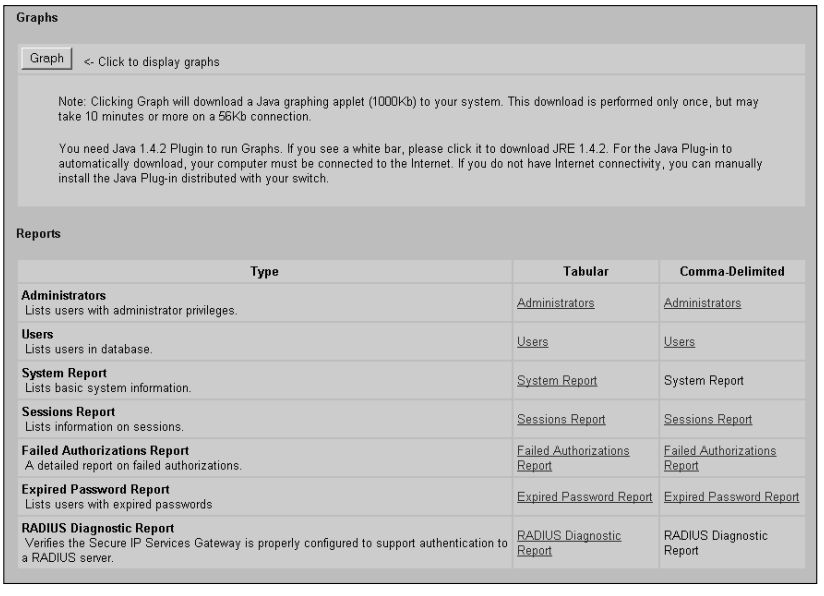


Figure 5-11: The Reports screen within the VPN Router browser-based interface

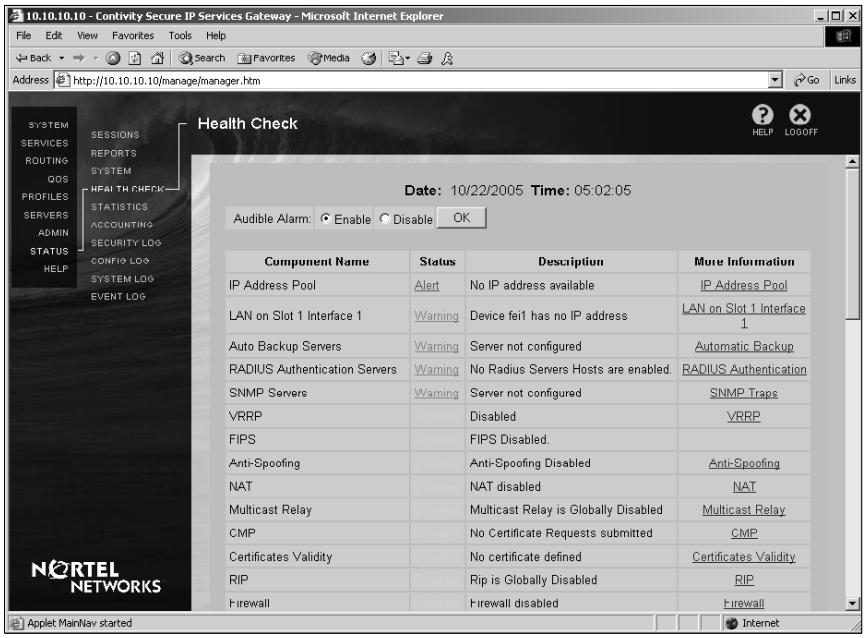


Figure 5-12: The Health Check utility

Note the Status column in the example. The VPN Router will prioritize categories from the most urgent to the least urgent. In the example, there are no IP addresses configured within the IP address pool. The VPN Router has recognized that it is not operational and has given a red alert flag. Following this item are the warning flags and then information about the services that are disabled on the VPN Router.

Understanding the Health Check screen will greatly assist the administrator in ensuring that the VPN Router is functioning at a level that ensures network access stability.

Statistics

The Statistics screen within the BBI contains a lot of valuable information that can assist in monitoring the operations of the VPN Router. This utility is valuable for troubleshooting and diagnosing any network problems that may be occurring. To access the Statistics screen, go to the following directory within the browser-based: STATUS → STATISTICS.

On the Statistics screen in the BBI are multiple categories that can be accessed. These categories contain information pertaining to general operations of the category function, as well as providing diagnostic information for the category.

Most of the information that can be accessed is information that will assist Nortel technical support in diagnosing problems that may be occurring, but there are also multiple counters and status screens that are helpful to administrators in managing the VPN Router.

Accounting

The Accounting screen in the BBI contains a log that maintains information about user sessions. The Accounting screen can be accessed by going to the following directory: STATUS → STATISTICS.

The accounting log contains the following fields of information:

- The first and last name of the user
- The assigned user ID of the user
- The start date of the session
- The date that the session ended
- The type of the tunnel that was used
- The number of bytes transferred
- The number of packets transferred

The accounting logs are very detailed and can be imported into a database or a spreadsheet for tracking and monitoring purposes. Information that is gathered is stored on the hard drive of the VPN Router.

In addition to the accounting log, the VPN Router also stores a backup copy of the RADIUS accounting record and also stores information pertaining to system data (known as the *Data Collection Task*).

Other VPN Router Tools

The VPN Router also supports standard data networking tools to assist in monitoring the VPN Router to ensure normal operating status of the router. These tools are supported both through the CLI and through the BBI. This section introduces these tools and provides examples of them performed through the BBI.

Trace Route

Trace Route is a networking tool that allows a testing device to determine the path that is taken to get from the device to another device on the network. The Trace Route utility is accessible from the BBI by going to the following directory: ADMIN → TOOLS.

Trace Route increases the Time to Live (TTL) value of each packet sent. The first packet that is sent receives a value of 1; the second packet receives a value of 2; and the third packet receives a value of 3; and so on. Each time a packet passes through a device on the network, the device will subtract the TTL value by one and will forward it to the next device, toward the destination device.

When a packet reaches a device and the TTL value is one, then the device discards the packet and sends an Internet Control Message Protocol (ICMP) time-exceeded packet to the originator. The Trace Route tool uses the return packets to generate a list of hosts that the packets have passed through on the way to its destination.

Figure 5-13 shows an example of the Trace Route utility contained within the VPN Router Browser based interface.

Ping

Ping is a networking tool that is used to send ICMP echo request messages from one networking device to another to determine reachability. The `ping` command helps determine whether a host is up and operational on the network. The `ping` command also provides the testing device with an estimate of how long it takes to get to the host and back, and whether there is any packet loss between the testing device and the host. The Ping utility is accessible from the BBI by going to the following directory: ADMIN → TOOLS.

If a host is reachable, then it will send an echo reply to the originator, letting that device know that it did receive the request.

Figure 5-14 shows an example of a `ping` issued with the Ping utility in the VPN Router BBI, and the results that are provided.

Address Resolution Protocol

The Address Resolution Protocol (ARP) is a method used to find a network device's MAC address by using its IP address. The ARP utility is accessible from the browser-based by going to the following directory: ADMIN → TOOLS.

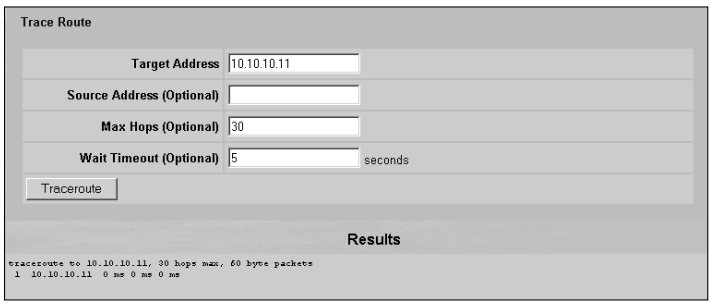


Figure 5-13: The Trace Route utility screen

The originating device will send out an ARP packet in a broadcast to the network that contains the IP address of the device that it wants to reach. Once the originator has sent its broadcast message, it waits for a reply from the destination. Included in the destination replies to the originator will be the Ethernet MAC address for the device.

Each network device maintains a cache of the addresses that it has learned to reduce the amount of time and the network traffic needed to find a destination. ARP is limited to the devices within the network that support broadcast packets.

Figure 5-15 shows an example of the ARP table that is accessible from the BBI.

Sometimes a device on the network has problems reaching other devices on the network. One of the things that can be done to try to alleviate this problem is to force the VPN Router to relearn the devices and the paths to get to them. Clearing the ARP table is an easy way to force the VPN Router to relearn these paths. Within the system tools page of the BBI, you have three ARP options. You can delete an entry from the ARP table, show the ARP table, and clear the ARP table. Figure 5-16 shows an example of this page.

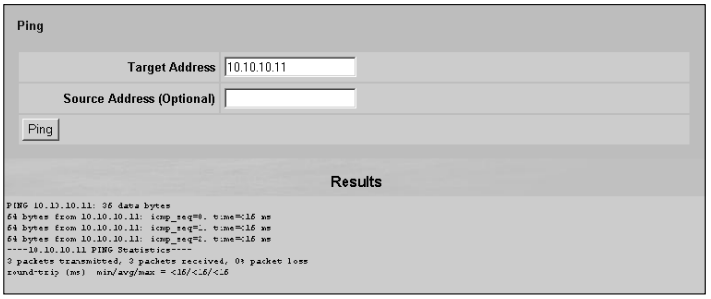


Figure 5-14: The Ping utility within the Nortel VPN Router

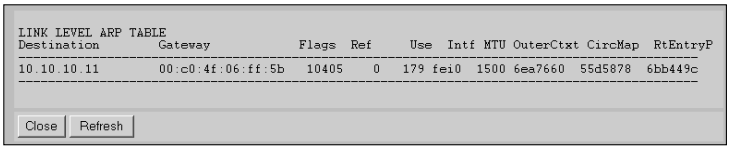


Figure 5-15: The ARP Table screen in the browser-based interface

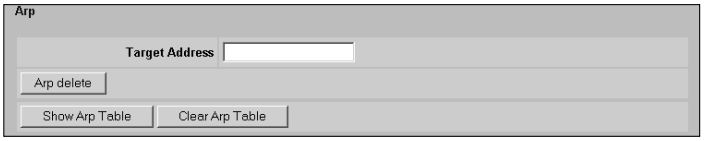


Figure 5-16: The ARP options available within the browse-based interface

VPN Router Administration

When managing the Nortel VPN Router, some proactive administrations steps can be taken to assist in ensuring the router fulfills the current needs of the network. The administrative tools that are included in the VPN Router software include the following:

- Software Upgrades
- System Shutdown
- System Recovery
- Automatic System Backups

The administrative tools are included to assist in operating the VPN Router and ensure system integrity. Utilizing the tools to assist in managing the VPN Router ensures that the tasks are completed correctly and that all necessary steps are completed. These tools are part of the Admin menu within the VPN Router BBI. Figure 5-17 shows an example of this menu selection and the subdirectories.

Software Upgrades

Chapter 3 of this book discussed VPN Router software upgrades. Nortel VPN Router software is included with the purchase of a VPN Router. The software can also be obtained on the Nortel Web site, `www.nortel.com/support`.

Nortel officially recommends that VPN Router users keep at least four versions of VPN Router software on their VPN Router system disk.

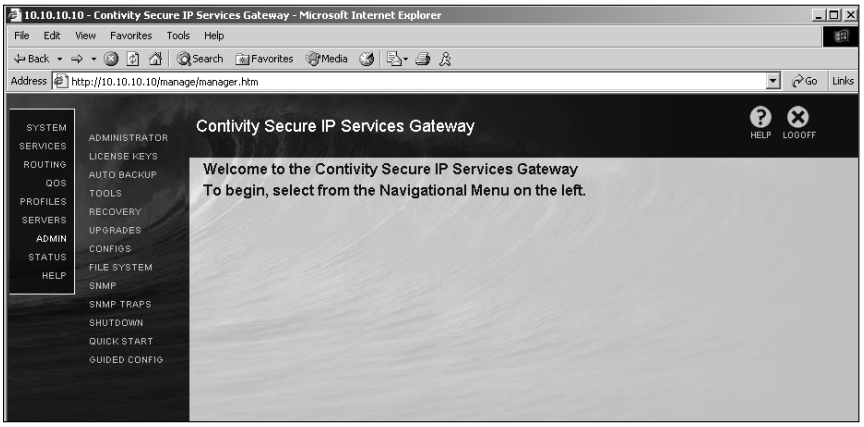


Figure 5-17: The Admin menu and the subdirectories

NOTE **The VPN Router 1010, 1050, and 1100 have only enough disk space to store 2 versions of VPN Router software, so it is necessary to remove an earlier version of code to upgrade to a newer version.**

To maintain multiple versions of VPN Router software, it is necessary for you to ensure that there is enough disk space on the system drive to support the installation file size.

Other things that you will want to do when upgrading software is to back up the system files (including the LDAP) and create a recovery disk. Finally, you want to ensure that RADIUS accounting is disabled before applying your upgrade. Disabling RADIUS accounting ensures that the VPN Router will not process pending radius updates during the upgrade process.

Lightweight Directory Access Protocol

The *Lightweight Directory Access Protocol (LDAP)* is a client/server protocol that is used for accessing information that is stored within a directory service. A directory service stores and organizes information about a network and the resources available within the network. Following are the resources that are stored in the LDAP:

- Network user information
- File information
- Shared printer information
- Server information
- Shared application information

The directory service allows network administrators to organize and manage network resources without users having to be concerned with the network topology and structure. The directory service is an interface to the directory where the information used to control access to network services is stored. The directory service can authenticate access to network resources, which manages the relationship of database components.

The LDAP directory uses a distinguished name to determine the attributes assigned to a schema, which represents individual users, groups, and so on. LDAP directory entries are contained within a hierarchical structure that reflects the geographical, political, and/or organizational boundaries.

Remote Authentication Dial-In User Service

The Remote Authentication Dial-In User Service (RADIUS) is a network security service that is used to authenticate and authorize network services for remote users. In a typical remote access enterprise network, a remote user will

attempt a connection to the corporate LAN through the VPN Router. The VPN Router will obtain authentication information from the user. The VPN Router forwards the authentication request to a RADIUS server. The RADIUS server authenticates the user and either authorizes or denies access to the network, based on the authentication information that was received.

RADIUS is often referred to as RADIUS AAA. The "AAA" refers to the functions that the RADIUS server is providing:

- *Authentication:* Authenticating the user.
- *Authorization:* Authorizing the user to network services based on the rights that have been defined for the user.
- *Accounting:* Information that is gathered about the user session for billing and network analysis purposes.

The RADIUS server will maintain its own user database and will access directories using the LDAP to obtain any additional user information that is required. RADIUS is considered a distributed security model in that the user information is stored on a RADIUS server and can be accessed by access servers. This allows large LANs to support multiple access servers with a shared RADIUS server. This negates the requirement for each VPN Router to maintain its own user authentication information. Imagine what an administrative nightmare it would be if you would have to make a change for a particular user or group, and apply that change with every VPN Router in your network.

Automatic System Backups

The Nortel VPN Router can be configured to support system file automatic backups. If enabled, then the VPN Router performs checks to ensure that any system file changes are backed up. Whenever there are changes to a system file, then the files that have changed will be backed up on the server where the files are stored.

System file automatic backups do not occur for at least five minutes after rebooting the VPN Router. This is to ensure that all resources are running and the VPN Router is operating within normal operating parameters.

When enabling auto backup, you determine if you want to perform backups during specific times or during specific interval periods. Automatic backup can be configured in the BBI in the following directory: ADMIN → AUTO BACKUP.

System Recovery

The VPN Router BBI has a utility that assists in configuring a recovery disk. The recovery disk is important because it provides a way to restore the

software image as well as the system files in case a hard disk problem occurs. To access the recovery screen, you will browse to the following path within the VPN Router BBI: ADMIN → RECOVERY.

The recovery disk is a standard floppy drive disk. Within the recovery screen, you have the option of making backup copies of the disk, which is highly recommended. You can even format disks through the recovery screen.

To access the disk drive on the VPN Router, you will need to remove the front panel of the VPN Router. Behind the panel you will locate the disk drive.

NOTE **In lieu of a disk drive, the VPN Router 600 and the 1000 series VPN Routers store recovery information within a section of memory referred to as the *Programmable Read-Only Memory (PROM)*. On these VPN Routers, there is a toggle that can be switched to initiate the recovery process.**

System Shutdown

If you are a Microsoft Windows user, you can probably recall pushing the power button or losing power to the PC during operation. With some versions of Microsoft Windows, you would be informed during the next system boot that Windows had not been shut down correctly and that the system would be scanned to ensure file system integrity. The Nortel VPN Router software operates in the same way.

The System Shutdown administrative tool that is included in the VPN Router software allows you to dictate how you would like to have the system shut down. Utilizing the System Shutdown tool ensures that proper steps are taken to ensure file system integrity during the shutdown process.

The System Shutdown administrative tool allows you to select a number of system shutdown options:

- Shut down immediately
- Shut down after current users disconnect
- Shut down at a designated time

Whenever possible, we recommend that you shut down the system using one of these parameters. Shutting down the system utilizing the administrative tools that you are provided will help ensure that there is no damage to the system files, as well as any loss of data during the shutdown process.

The System Shutdown tool also allows the administrator to select whether to shut down completely during the shutdown process, or reboot the system. Additionally, the option of selecting the named configuration file that you would like to use is available during the System Shutdown process.

Bandwidth Management

In data networking, *bandwidth* is a term that is given to the rate that data is transferred between a source and a destination on a network. The *Data Transfer Rate (DTR)* defines the amount of data that is passed between nodes on the network. The DTR can be considered the speed of the data travel—the larger the bandwidth settings, the quicker the DTR. Bandwidth management is used to ensure that there is enough bandwidth to support the network data traffic. If there is not enough bandwidth, it is necessary to manage the traffic patterns in a way to ensure that all critical data transfers are reliably delivered to their destinations.

The Nortel VPN Router supports bandwidth management, which allows administrators to monitor and adjust bandwidth resources on traffic that passes through the VPN Router. Bandwidth can be managed on all interfaces, as well as the system CPU to ensure reliable bandwidth resources for end-user support. Bandwidth management can be configured and maintained on all types of VPN Router tunnels.

Utilizing tools that are available within the Nortel VPN Router, a network manager can monitor traffic interfaces and CPU utilization to set up and maintain bandwidth support on the VPN Router.

Managing bandwidth allocation can be very complicated. Allocating too much bandwidth can cause a company to maintain bandwidth that is not utilized. Allocating less bandwidth than is required can cause bottlenecks within the network, creating traffic congestion and less-than-acceptable network performance.

Bandwidth management does not guarantee that all VPN users will be able to access the corporate LAN from remote locations, but it does provide the capability to manage bandwidth to assist in allocating and adjusting bandwidth levels, to provide additional bandwidth for users who require the additional bandwidth, and to reserve bandwidth for those who require less.

Configuring Bandwidth Management

Before bandwidth management can be configured on the Nortel VPN Router, an advanced routing license key is required. The advanced routing license key can be entered through the BBI or via the CLI.

From your browser interface, you would follow this path to enter the advanced license key required for bandwidth management support: ADMIN → LICENSE KEYS.

On the License Key screen, you will be given the option of entering the advanced routing license, additional tunnel support, and/or the Stateful Firewall license. Simply enter the license key and select OK. Once you have

entered the license key correctly, you will no longer see the option of entering the key on this screen. Instead, the key status will state that it is installed and an option to remove the key will appear.

You can also install the license key via the CLI. First you will want to connect to the CLI by either Telnetting to the VPN Routers management IP, or through the serial interface.

First, you will need to enter the CLI privileged mode:

```
CES>enable
Password:****
```

Next, you will need to access the configuration mode:

```
CES#configure terminal

CES(config)#
```

Next, you will enter the advanced routing license key:

```
CES(config)#license install ar [license key number]
```

Once the advanced routing license key is installed, you are able to configure the Bandwidth Management policies. From the BBI, you will need to determine the bandwidth rates that are defined on the VPN Router. To access this, follow this directory: QoS → BANDWIDTH RATES.

On the Bandwidth Rates page, you will see a list of several pre-defined bandwidth rate settings, as well as the option to define your own bandwidth rate settings. Bandwidth rates are configured in *bits per second (bps)*, which is the number of bits that can be transferred within a single second.

After you have verified that the bandwidth rates that you want to support have been saved within the QoS parameters, your next step will be to configure the bandwidth rates for your configured users and groups. To do this, you will want to go to the following directory within your BBI: GROUP → PROFILES.

On this Profiles page, you will go to the section of the page that is titled, "User Bandwidth Policy." Here, you have the option of configuring the user-configured bandwidth rate and the excess rate. There is also a drop-down menu where you select the action to take if a user exceeds the defined excess bandwidth rate.

Finally, you will want to enable Bandwidth Management. This is done by going to the following directory within your BBI: QoS → BANDWIDTH MGMT.

This page has a drop-down menu that you can use to either enable or disable the bandwidth management option on the VPN Router. Selecting Enable directs the VPN Router to set the bandwidth limits that you have defined for their group.

Summary

Implementing a design plan for a network is a daunting task. Many hours of time and effort go into designing and rolling out the design into a fully functioning network. Networks are evolving at a steady pace. Many of the technologies that were in place 15 to 20 years ago are now outdated. Effectively meeting the needs of a network and ensuring those that depend on reliable service is a top priority with most companies today. Because of this, it is imperative that administrators keep on top of their network and the devices that make up the infrastructure of the network.

Management of the VPN Router is no exception. As more and more users develop the need to get into the network quickly and reliably, the importance of ensuring that connectivity is higher today than ever. That is why it is important to understand the VPN Router and how to manage it effectively.

This chapter reviewed the Nortel VPN Router and the tools that are available to monitor and manage it effectively. An overview of these tools was provided, as well as an introduction to the interface options that are available. You should now have a firm understanding of the VPN Router interface and the management functions of the router.

Chapter 6 provides an overview of authentication and how it relates to the Nortel VPN Router.

CHAPTER

6

Authentication

Authentication deals with authorization that allows users and Branch Office Tunnels (BOTs) to be permitted access to the protected private network. The use of authentication processes can determine levels of access by setting the rights given to users, groups, or tunnels. The Nortel VPN Router has an internal Lightweight Directory Access Protocol (LDAP) for authentication, and also will service external authentication servers such as External LDAP servers, RADIUS servers, and Certificate servers. This chapter presents an overview of what authentication entails, along with examples and scenarios of the Nortel VPN Router with external authentication servers.

Figure 6-1 illustrates the use of the Nortel VPN Router with internal LDAP server and external authentication servers such as an External LDAP server, Remote Authentication Dial-in User Services (RADIUS) server, Entrust Certificate Authority (CA), and Token server.

The users accessing the private network through the VPN Router may have access rights that can be either group- or user-specific. The use of groups allows for common attributes to be assigned to a number of users. They may include the encryption being used, filters to be applied, quality of service attributes, as well as other settings. However, you have the flexibility to modify a user's access profile so that specific individuals can be given required attributes that are particular to that user. This is all accomplished with the use of a user identity to identify the user who is trying to access the private network via the VPN Router. Using a user identity facilitates mobile users, as well as users who may be accessing the private network and who belong to a different organization.

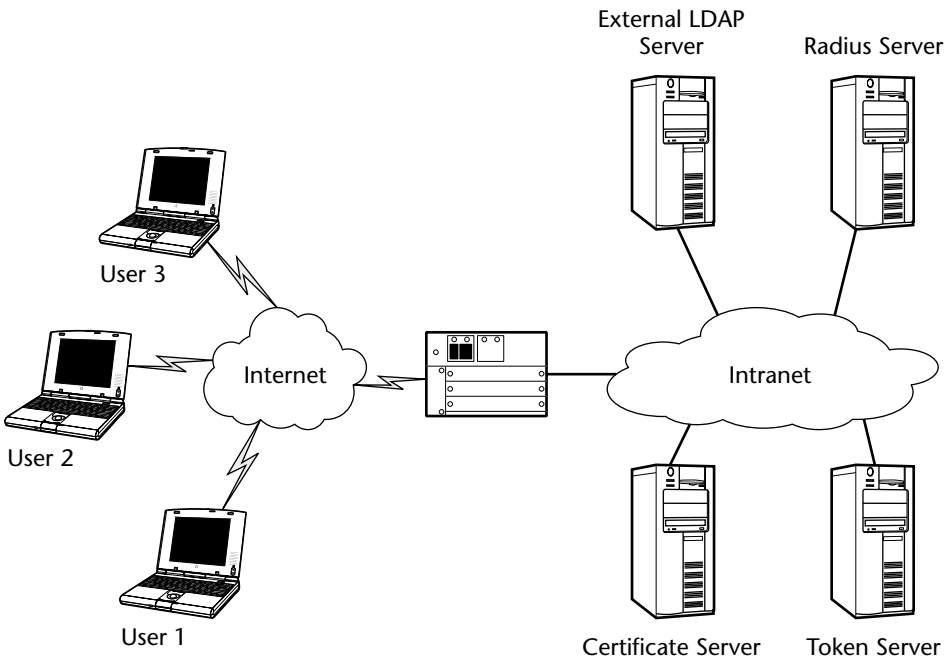


Figure 6-1: Nortel VPN Router with authentication servers

Understanding LDAP

The Nortel VPN Router uses an internal LDAP database for authentication of users. The use of LDAP has emerged from X.500 directory service and has gained in popularity. It is being used as a model for directory services for the Internet. X.500 is an International Standards Organization (ISO) and International Telecommunications Union (ITU) standard that defines how global directories should be structured. It uses hierarchical directories and differing levels of categories of information (such as country, state, city, and so on). LDAP has gained widespread acceptance and is supported in products distributed by major software manufacturers in their directory service strategies.

LDAP uses an Internet identity schema that defines common attributes. It may include extended attributes as directory entries. A *directory service* is a repository of user information. The Nortel VPN Router internal LDAP server supports the following elements:

- Groups
- Users
- Filters
- Services

The use of LDAP provides a standard protocol that runs over TCP/IP, is optimized for lookups, can access virtually any type of data, and, with authenticated binds, can provide a level of security. Further information on the LDAP is found in RFC 1777, "Lightweight Directory Access Protocol."

LDAP Principles

The LDAP directory service model is based upon entries. An *entry* is a collection of attributes called a Distinguished Name (DN). The DN is used to refer to an entry unambiguously. Each of the attributes in an entry has a type and will have one or more values associated with it. Types are typically mnemonic strings such as "cn" for common name and "mail" for an e-mail address. Values are dependent on the type of the attribute in which it is contained. An example of a value would be a mail attribute, which contains the following value:

```
john.smith@myorganization.org
```

As mentioned, LDAP is a hierarchical tree-like structure where directory entries are arranged to reflect boundaries determined by geographic, political, or organizational descriptions. As an example of how entries are arranged, consider that an entry representing a country would be at the top of the tree, and below that entry would be entries representing geographic locales (such as a state or province), or they may be national organizations associated within that country. Below these entries in the tree structure there may be entries representing pretty much anything at all. As an example, these entries may contain people, organizational units, printers, documents, and so on. LDAP utilizes a special attribute called an `objectclass` to control which attributes are required and which are allowed within an entry. The `objectclass` attribute values determine the schema rules that an entry must follow.

LDAP defines the operations for the interrogating of and the maintenance and updating of the directory. The primary function of LDAP is to service inquiries by searching for information contained within the directory. Each directory search is accomplished with the use of criteria specified in a search filter to find matching entries. With each entry found to match the search criteria, information may be requested.

Depending on the directory service used there may not be any security, which would allow anyone to view the information contained within the directory. LDAP has a method that requires the client to authenticate or provide proof of its identity to a directory server before it allows access to the information. This is shown in Figure 6-2.

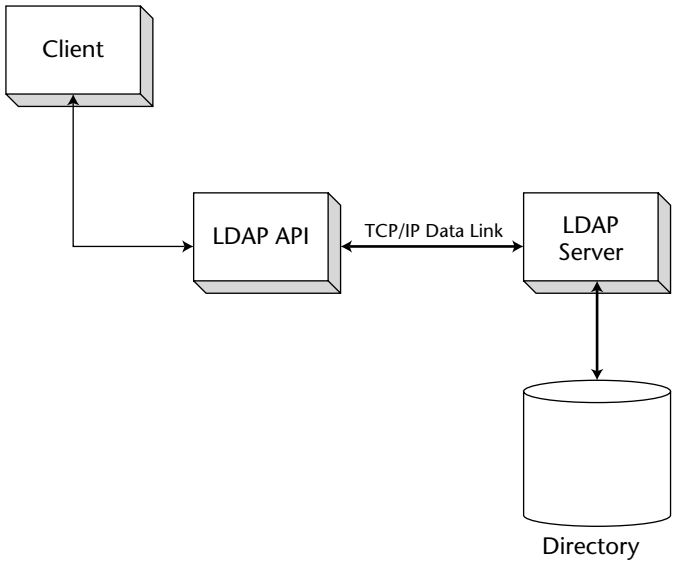


Figure 6-2: LDAP model

In Figure 6-2, a client loads an LDAP Application Program Interface (API) that allows it to open a secure TCP/IP socket connection to the LDAP server. Upon authentication with the LDAP server, the client is allowed access to the directory. The types of authentication supported by LDAP v2 are anonymous, simple (which is a clear-text password), and Kerberos V4. Kerberos is an authentication protocol used primarily in client/server applications that allows for users to verify their identities to one another.

LDAP Request Flowchart

Figure 6-3 shows a flowchart of the process involved with an LDAP request.

A client initiates an LDAP request by opening a TCP/IP connection to the host at the port servicing LDAP requests. After the client passes the authentication phase, it is bound to the server and submits a query using LDAP. The results of the query are returned to the client. After the client has completed its querying, it unbinds from the server and closes its TCP/IP connection. This completes the LDAP query transaction.

Configuring Internal LDAP

The Nortel VPN Router Internal LDAP does not respond to external LDAP queries, so two or more Nortel VPN Routers may not share the same Internal LDAP database. If there is a need to share a common LDAP database among more than one Nortel VPN Router, then an external LDAP-based directory service is recommended. When the Nortel VPN Router is used with an external

directory service, there is latency when updates may be synchronized between it and the external directory service. So, edits made on user data may not be updated immediately.

To configure the Nortel VPN Router Internal LDAP server, select SERVERS from the main menu and then select LDAP. Figure 6-4 shows a portion of the internal LDAP Server configuration screen.

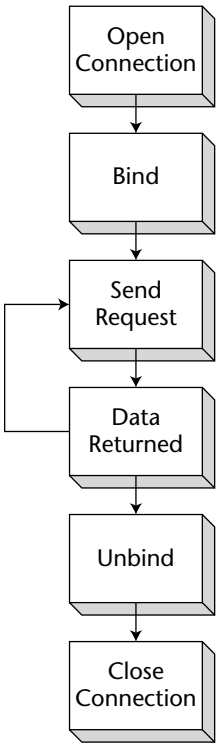


Figure 6-3: LDAP request flowchart

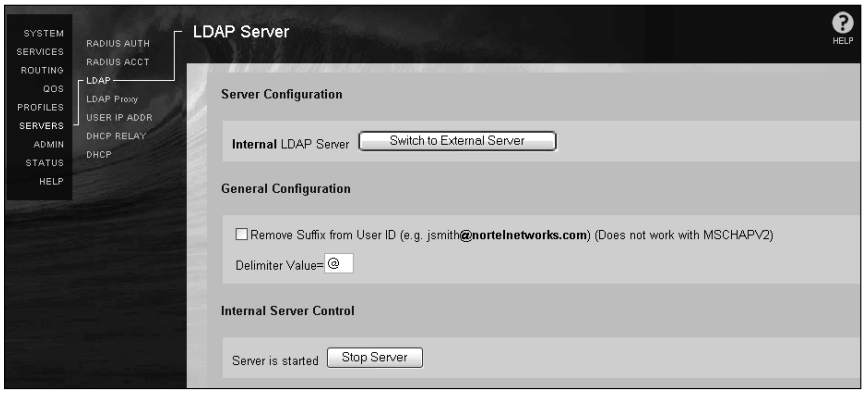


Figure 6-4: Nortel VPN Router internal LDAP Server configuration screen

In the Server configuration portion of the screen is a button labeled "Switch to External Server." This switches the LDAP to be located on an external LDAP server. If the button label says "Switch to Internal Server," the Nortel VPN Router had been configured to use an External LDAP server. If you want to use an Internal LDAP server, ensure that the legend in this area indicates that the Internal LDAP server is in use, as shown in Figure 6-4.

In the General Configuration section, there is a Remove Suffix from User ID check box. Check this box to remove the suffix or the Fully Qualified Domain Name (FQDN) portion of the User ID (UID). For example, in the case of `johndoe@mydomain.org`, the `@mydomain.org` suffix will be removed and only the `johndoe` portion of the UID will be used to authenticate the user. By default, the Delimiter Value is set to `@`, but this may be changed to the character that is being used for a delimiter in the UID.

In the Internal Server Control section of Figure 6-4, the Stop Server button is used to stop the Internal LDAP server. If the LDAP has been stopped, this button's label would say "Start Server." The need to stop the Internal LDAP server is for maintenance purposes. The LDAP server must be stopped when either backing up or restoring the LDAP. The Internal Server Control must be set to "Server is started" for users to be authenticated. The remainder of the SERVERS → LDAP configuration screen is shown in Figure 6-5.

In the Backup/Restore Internal LDAP Database section of the LDAP Server configuration screen are Backup Now and Restore Now buttons to perform the backup and restore functions of the Internal LDAP database. To perform either of these functions, the Internal LDAP server must be stopped.

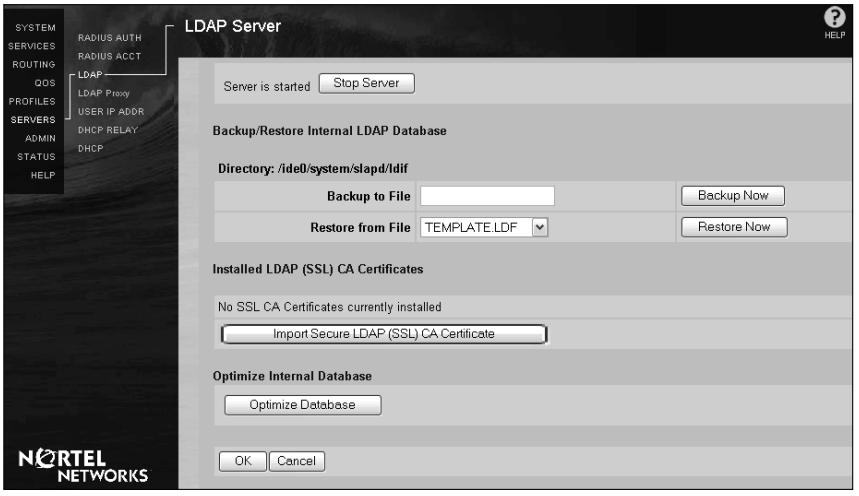


Figure 6-5: Internal LDAP Server configuration screen

To back up the Internal LDAP file, enter a filename of eight characters maximum in the Backup to File box, and then click the Backup Now button. The backup procedure backs up changes to the internal *LDAP Interchange Format* (*LDIF*) file only. The LDIF file is an intermediate database file that can be used to move data between LDAP servers.

To restore from a file, use the Restore from File drop-down menu to select the name of the file you would like to restore from, and then click the Restore Now button. Both the restore and backup processes may take an extended period of time to accomplish, depending on the size of the LDAP database.

The Installed LDAP (SSL) CA Certificates section of the LDAP Configuration screen shows what certificates are installed (if any). To install a certificate, click the Import Secure LDAP (SSL) CA Certificate button to import a CA certificate. When this button is clicked, an edit box is opened, allowing for the pasting in of a PKC#7 Base-64 certificate.

Public Key Cryptography (PKC) standards and specifications were developed by RSA Security in cooperation with system developers for the purpose of deploying the use of public key cryptography. *PKC#7* is a cryptographic message syntax standard that defines a generic syntax for a message that has cryptography applied to it. *PKC#7 Base-64* certificates adhere to these standards using the common block cipher size of 64 bits.

NOTE **Certificates are discussed in detail later in this chapter.**

When all the entries on the LDAP Configuration screen have been completed, click OK to accept these setting. If for any reason they are not completed, just click the Cancel button to not accept any additions or changes to this screen.

The Optimize Internal Database section of the LDAP Server configuration screen is for maintenance purposes. Clicking the Optimize Database button brings up a CONFIRMATION screen with OK and Cancel buttons. Because optimization of the LDAP database may take an extended period of time, depending on its size, we recommend that this be accomplished in a scheduled maintenance window because the database will not be available for authentication purposes during this time. On completion of the optimization process, a status is indicated at the top of the LDAP configuration screen.

External LDAP

The main advantage of using an External LDAP is the ability to have multiple VPN Routers using a common LDAP. A single LDAP database allows for ease of administration, whereas separate LDAP databases for each device will

require entries to be added and edited separately on each unit if there is a client that has access privileges on multiple VPN Routers. Using a common LDAP database is not only easier to administer, but also provides uniformity and adds a degree of reliability (because when a client entry is either added or removed, all devices using that LDAP will grant the same access to that client).

Figure 6-6 illustrates a scenario where a single External LDAP server is being used by a number of Nortel VPN Routers for user authentication. In this illustration, the External LDAP server must be populated directly from the Nortel VPN Router because the LDAP is used for more than just simple username and password. If the Nortel VPN Router is to be used with an External LDAP server that had already existed on a corporate LAN, and had been populated by another type of device, then a method that may be used to overcome this issue is to add a RADIUS server between the Nortel VPN Router and the External LDAP server. This is shown in Figure 6-7.

In Figure 6-7, the Nortel VPN Router sends LDAP requests to the RADIUS Sever. The RADIUS server must support LDAP proxy so that it proxies the Nortel VPN Router LDAP requests to the Pre-populated External LDAP server.

NOTE **The RADIUS server is discussed in more detail later in this chapter.**

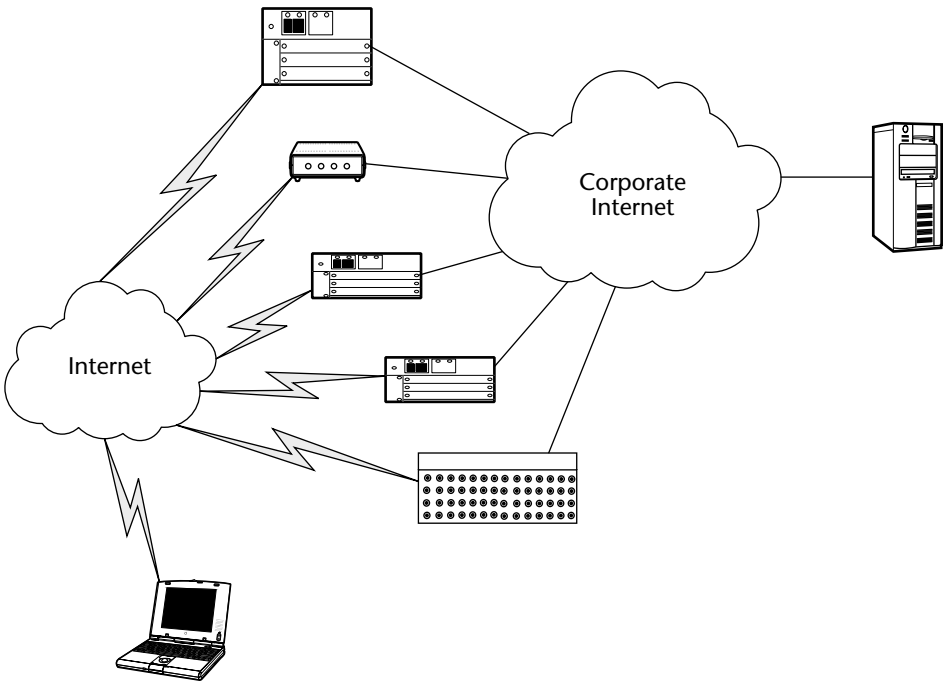


Figure 6-6: External LDAP server used with multiple Nortel VPN Routers

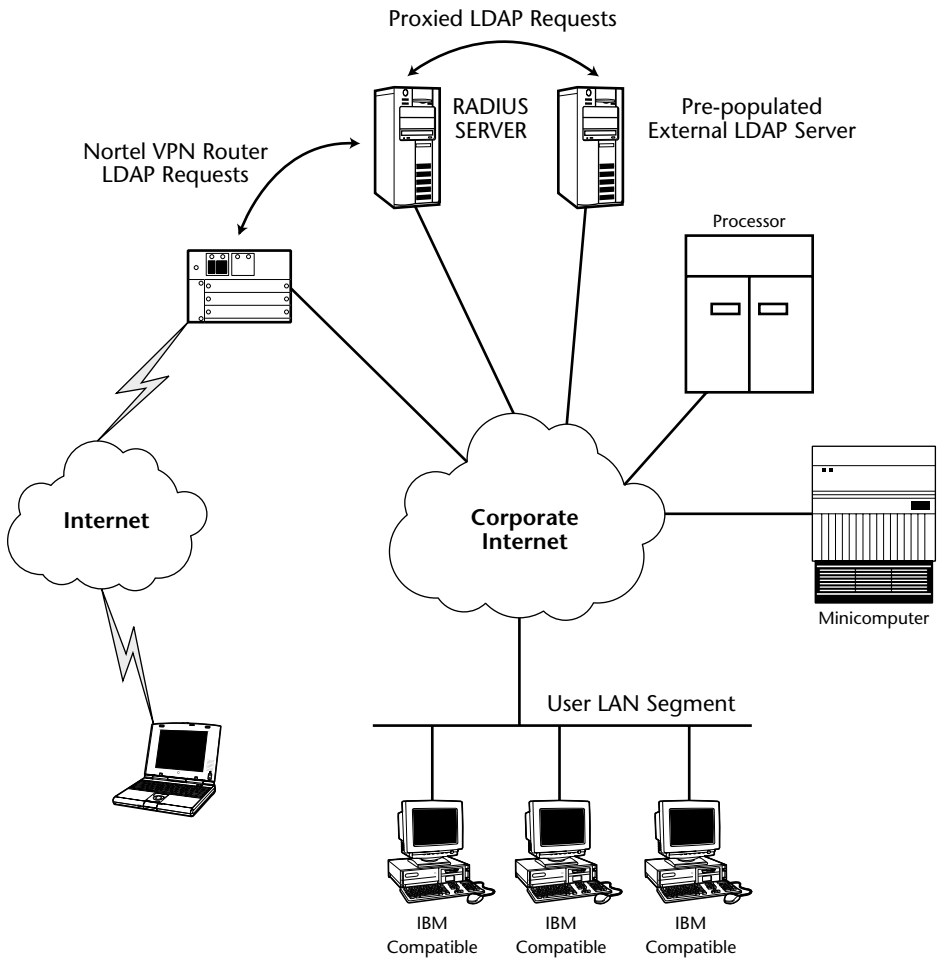


Figure 6-7: Pre-populated External LDAP server with Nortel VPN Router

Enabling LDAP Proxy

The Nortel VPN Router supports authentication with an existing LDAP server that had been previously populated by another device. This is accomplished utilizing the LDAP Proxy feature. The authentication server being used to proxy LDAP requests may reside on the private or public network that is connected to the Nortel VPN Router. The type of authentication method being used by the existing LDAP server may also be selected. Following are the five available authentication methods:

- *Password Authentication Protocol (PAP):* This is an authentication protocol where the user name and password are passed in plain text.

- *PAP with Bind Authentication:* This is authentication where the user name and password permit the user to bind to a set of services defined in policies.
- *Challenge Handshake Authentication Protocol (CHAP):* This is authentication where the user and authenticator share a secret that the user must respond with each time it receives a challenge from the authenticator.
- *MS-CHAP:* This is Microsoft's implementation of the CHAP protocol, which is an extension of that standard with additional capabilities.
- *MS-CHAP V2:* This is a more secure than MS-CHAP and it provides mutual authentication, stronger encryption keys, and the use of different encryption keys for transmitted and received data.

The Nortel VPN Router supports LDAP V2 and LDAP V3 servers.

To enable and configure LDAP Proxy, select SERVERS from the main menu and then LDAP Proxy. To enable the LDPA Proxy feature, check the box "Enable Access to LDAP Proxy servers", as shown in Figure 6-8.

Check the box labeled "Remove Suffix from User ID" to remove the FQDN suffix before sending it on to the LDAP server. The character used for the Delimiter Value is, by default, the @ sign, but this may be changed to whichever character is being used to delimit these fields.

LDAP Proxy users obtain their default settings from the group they are assigned to. In the drop-down menu labeled "LDAP Proxy Server Users Obtain Default Settings from the Group," select the group for those users.

The Response Timeout Interval is the amount of time (in seconds) that the Nortel VPN Router will wait for a response from the LDAP server. The default is 4 seconds, but this may be adjusted via the drop-down from 1 to 15 seconds. This value should be increased only if there is additional latency on the network the LDAP server resides on to eliminate false timeouts caused by the increased latency.

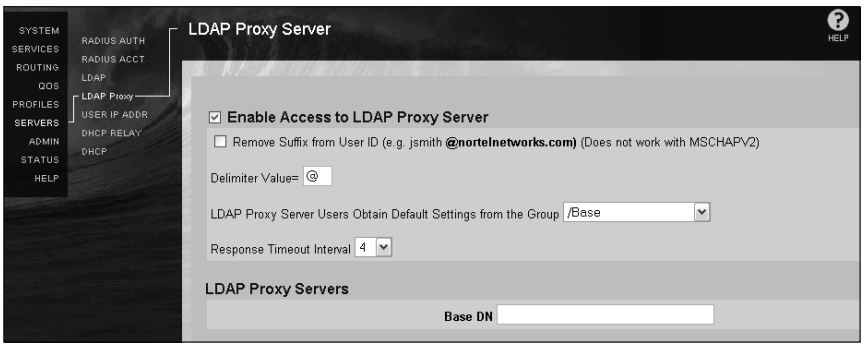


Figure 6-8: Enabling LDAP Proxy

In the LDAP Proxy Servers section of the configuration screen is a box to fill in the Base DN being used to communicate with the LDAP server. The base DN (Distinguished Name) is usually in the form `ou=organizational unit, o=organization, c=country`.

Figure 6-9 illustrates the selection data entries required for the LDAP server.

In the Host Name or IP Address data entry boxes, enter either the IP address or the FQDN of the Master LDAP Server and, if available, for Slave 1 and Slave 2 LDAP Servers. Should the Master LDAP Server not be available, the Nortel VPN Router will use a search order sequence to initiate a connection to Slave 1 and, if no response, then Slave 2. The Port selection has the default settings of port 389 and for SSL port 636. However, these values may be changed if the LDAP server is using different port values for these services. In the Bind DN field, enter the Bind Distinguished Name (DN), which is the LDAP equivalent of a user ID and is required to access the base DN and its subentries. If the LDAP server allows for anonymous access, these fields may be left blank. Enter the Bind Password and Confirm Password entries. The password may be up to 32 characters long, and it is used to prove its identity (the Bind DN) to the LDAP server.

In the Username/Password Access section of the LDAP Proxy Server configuration screen, you can use the Username Attributes field, User Password Attribute field, and LDAP Filter field to specify attributes used to store the Nortel VPN Router group, static IP address/netmask, and customized user filter, respectively. These fields can hold case-insensitive character strings that are allowable in LDAP search filters. By default, these fields are left blank. Without a specified attribute name, the LDAP Proxy server will not attempt to extract this information.

Figure 6-10 shows the User Certificate Access section of the LDAP Proxy Server configuration screen

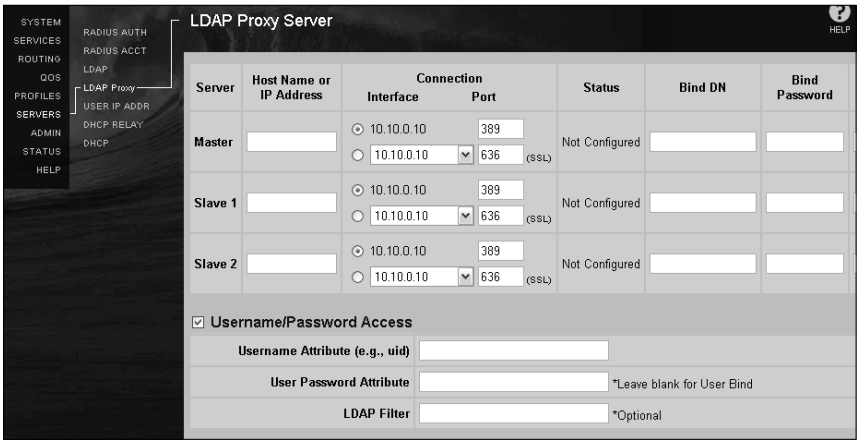


Figure 6-9: Selecting the LDAP server

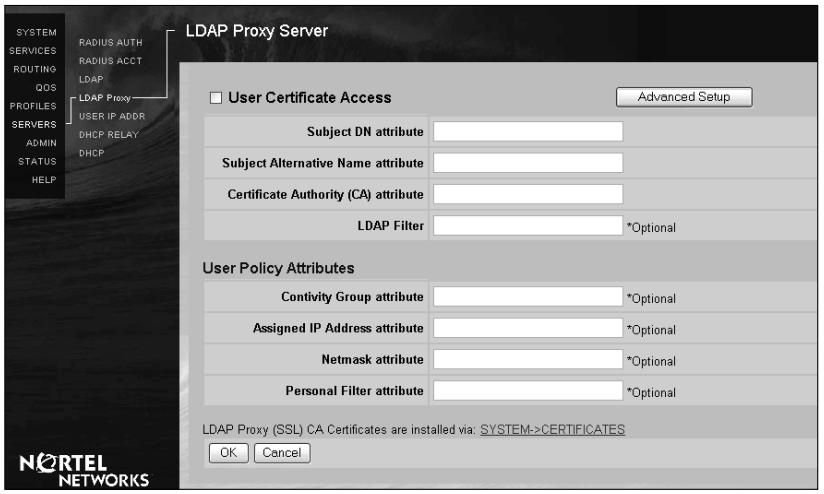


Figure 6-10: LDAP Proxy User Certificate Access section

NOTE **User Certificates are discussed in detail later in this chapter.**

User Certificate Access allows for the use of digital certificates support for authentication. In the Subject DN Attribute field, enter the attributes (such as common name, organizational unit, and country). In the following data boxes, enter the Subject Alternative Name Attribute, Certificate Authority (CA) attribute, and LDAP Filter name.

The User Policy Attributes section is used to specify attributes used to store the Nortel VPN Router group, static IP address/netmask, and customized user filter. These fields can be filled in with case-insensitive character strings that are allowable in LDAP search filters. The default value for these fields is blank. Without a specified attribute name, the LDAP Proxy server will not attempt to extract this information.

Monitoring LDAP Servers

Ping (Packet Internet Groper) is a basic network command used to test the connectivity between IP hosts. Ping utilizes a series of Internet Control Message Protocol (ICMP) echo messages to determine that a remote host is present and active.

The Nortel VPN Router uses `ping` to determine the status of each of the configured LDAP servers. If the VPN Routers receive an ICMP Reply, the LDAP server is considered available and authentication attempts will be made to the LDAP Proxy server. This type of monitoring is also used for The Nortel VPN Router to determine the availability of RADIUS servers. If the VPN Router does not receive any replies from any of its configured LDAP servers,

it considers that they are unavailable. If the Nortel VPN Router determines that the LDAP Proxy servers are not available, it continues to operate passing traffic, but it will not authenticate users whose information is stored on a third-party LDAP directory.

With External LDAP servers, the behavior is different in that the server must reply to the ICMP request from the Nortel VPN Router and accept a directory bind before the VPN Router considers the External LDAP server to be available. On initialization of the External LDAP server, the Nortel VPN Router monitors the health of each External LDAP server to determine the availability of a server. If it cannot connect its directory, the Nortel VPN Router will continue to operate, but will not terminate tunnels or pass network traffic.

The Nortel VPN Router monitors the status of all External LDAP servers that have been configured. If the VPN Router has marked a server as being up, it will monitor the status of the server by binding and conducting a search against the directory every 15 minutes. If an External LDAP server has been marked as down by the VPN Router, it monitors the status of that server by sending an ICMP Echo Request to it every 15 minutes. If the VPN Router receives an ICMP Echo Reply, it then attempts to bind and search the server's directory. If the bind and search are successful, the Nortel VPN Router will change the status of the server to being up and will return that server back into the server list as operational. If either the bind or search directory is unsuccessful, the server is left in a down state.

Once the primary External LDAP server has been initialized the Nortel VPN Router issues an ICMP Echo Request to all of the secondary server IP addresses and follows the same procedure as previously described for each secondary server.

The Nortel VPN Router assumes only read/write access to the primary External LDAP server. Because of this, it does not configure any secondary server directories as directory storage. Instead, the Nortel VPN Router relies on the LDAP replication agreements between the primary LDAP server and secondary LDAP servers to populate the secondary servers with the appropriate directory information.

With normal operation, the Nortel VPN Router uses the primary External LDAP server. In the case of a primary External LDAP server failure, the Nortel VPN Router will failover to the next secondary LDAP server configured in a sequential manner. The Nortel VPN router will only attempt to connect to the LDAP servers that are marked as being up. Once the Nortel VPN Router determines that the primary External LDAP server has returned to normal operation, it will use it exclusively for authentication.

With multiple systems using an External LDAP server, any change of parameters added or removed to its database by a system will not be visible by the other systems until the database caches are flushed. Cache flushes occur on a timed interval.

Using Remote Authentication Dial-in User Service

The Nortel VPN Router supports a Remote Authentication Dial-in User Service (RADIUS), which is a distributed security system commonly used to authenticate remote connections. RADIUS is widely used to perform remote user authentication by many vendors. The RADIUS application consists of two components, the RADIUS server and the RADIUS client.

The RADIUS server application is run on a server computer that is usually located at the central office. The access and authentication information that is contained within the RADIUS server must be in a format that is compatible with the RADIUS client. The RADIUS server on the central office network can do both authentication and accounting, or these services may be separated and a server for each service would be required.

The RADIUS client usually resides on a network device that is at the edge of the central office network. These network devices are used by remote users to gain access into the central office network. When a user attempts to gain access by connecting to the device, the device communicates with the RADIUS server, which usually is resident in close proximity on the central office network. With RADIUS Authentication, the remote users are identified and, if they meet with all the authentication criteria, they are then permitted to gain access to the central office network. With RADIUS, accounting data is collected on the user after a user is permitted access to the central office network. The collected data on the RADIUS Accounting server then can be used for billing purposes.

The Nortel VPN Router supports multiple RADIUS Authentication servers, which may be accessed either on its private LAN, or routed out its public interface to servers accessible over the Internet. It also supports RADIUS Proxy on these same interfaces. However, it supports only a single RADIUS Accounting server, which must be located on its private LAN.

Enabling RADIUS Authentication

Enabling RADIUS Authentication on the Nortel VPN Router is accomplished by using the Web-enabled Graphical User Interface (GUI) to configure it. The selections of SERVERS → RADIUS AUTH brings up the RADIUS Authentication screen. To enable RADIUS Authentication, you simply check the Enable Access to RADIUS Authentication box, as shown in Figure 6-11.

This portion of the RADIUS Authentication screen also shows the group that users being authenticated will receive their default settings from. The default is set to /Base. However, any configured user group may be selected from the drop-down menu by clicking the down arrow to the right of the selection box. However, if the RADIUS server returns a valid group identifier, then the Nortel VPN Router uses the settings of that group profile for the user. If a valid group is not returned by the RADIUS Authentication server, then the group profile of the selected default group will be assigned to the user.

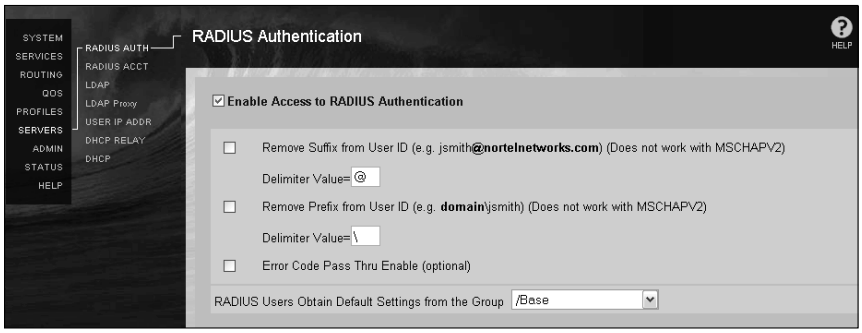


Figure 6-11: Enabling the RADIUS Authentication screen

The other selections in this portion of the RADIUS Authentication screen deal with information sent to and received from the RADIUS Authentication server by the Nortel VPN Router. The Remove Suffix from User ID option is used to remove the suffix portion of a User Identifier (UID). An example of this would be `jsmith@mydomain.org`, where the user identifier (UID) is `jsmith` and the domain information is `mydomain.org`. The default delimiter value shown is the `@` sign. However, this may be changed if a different character is used to delimit the UID from the suffix domain information.

The Remove Prefix from User ID option is used where the user identifier (UID) is of the format `mydomain.org\jsmith`. The default delimiter character is the `\`. However, this may be changed if a different character is used for the delimiter.

The use of the Remove Suffix from User ID or Remove Prefix from User ID option requires that the Nortel VPN Router be properly configured for Domain Name Services (DNS), thus eliminating the need to send a fully qualified user ID to the RADIUS Authentication server.

The Error Code Pass Thru Enable option allows error messages to be sent to the Nortel VPN Router by the RADIUS server. These can be passed through it to the client originating the request. The default selection for this feature is disabled.

RADIUS Server Selection

Figure 6-12 illustrates the RADIUS Servers portion of the RADIUS Authentication configuration screen. RADIUS server information must be entered in order for the Nortel VPN Router to use RADIUS Authentication to identify and qualify remote users.

As shown in Figure 6-12, a primary and two alternate RADIUS servers may be identified either by FQDN or IP address.

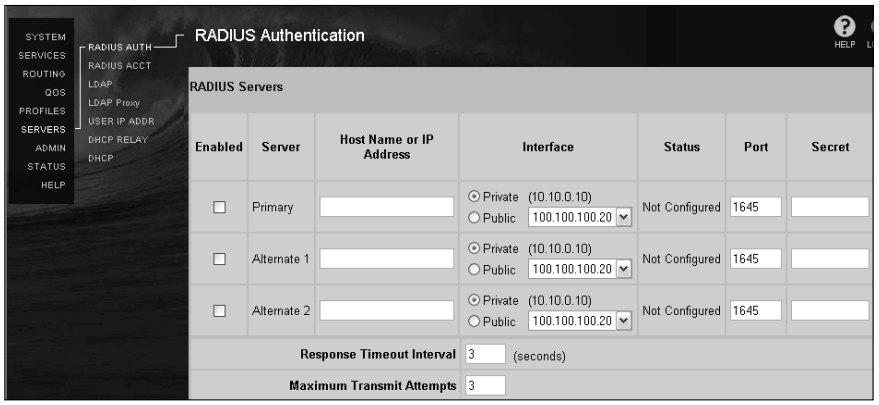


Figure 6-12: RADIUS Servers selection

The Interface section is dependent upon where the RADIUS server to be used for authentication is located in relation to the Nortel VPN Router. The default selection for the interface is Private and the IP address that is displayed is the management IP address of the Nortel VPN Router. The default selection is appropriate when the RADIUS server being used is located somewhere on the secured intranet of the organization. However, if the RADIUS server that is to be used is not accessible on the private intranet, then the Public selection is used to select a RADIUS server available over the Internet. The Public IP address selection box is automatically populated by the Nortel VPN Router and is dependent on the number of interfaces configured as public interfaces on the unit. In many cases, only one public interface is specified so the drop-down IP address selection box displays only the one address.

The default port setting of 1645 is displayed, but this may be changed to the appropriate port on which the selected RADIUS server is responding to authentication requests.

The RADIUS server requires a secret that is shared with the Nortel VPN Router. The shared secret is a string of characters that may consist of alpha, numeric, and approved special characters. It allows for the verification of the authenticity of each request sent to the RADIUS server and the responses back to the Nortel VPN Router. The shared secret must be entered in both the Secret box and Confirm Secret box to verify that the shared secret has been entered correctly. It is recommended for increased security purposes that the shared secret for each configured RADIUS server be different.

Once all the appropriate selections and required data are entered for each RADIUS server that is to be used, ensure that the Enabled box is selected for those servers to enable the Nortel VPN Router to use those servers for authentication.

The Response Timeout Interval by default is set for 3 seconds. The minimum value that it may be set to is 1 second. This value is the time that the Nortel VPN Router expects a response back from the RADIUS server. It is

dependent on the propagation time to and back from the server, as well as the response time of the RADIUS server in its ability to handle authentication requests. In most cases, the default value is adequate. However there may be instances (dependent on topology, processing speed of the server, and overall speed of the network that the request is being made over) that require this value to be increased slightly to allow the request/response transaction to complete.

The Maximum Transmit Attempts also has a default value of 3. This value is for the number of attempts that the Nortel VPN Router should use to try to authenticate a user. In most instances, the default value of 3 is adequate. Again, particular installations may require adjustment of this value, dependent on the network over which it is running.

RADIUS Authentication Options

Figure 6-13 shows the authentication options that are supported on the Nortel VPN Router. Select the options that are supported by the RADIUS Authentication server that you expect to use.

The Nortel VPN Router may be configured for each of the following authentication options:

- *CHALLENGE:* Challenge/response token cards require the user to supply user ID along with a password, plus the password supplied by the token card. An example of this would be the `AXENT OmniGuard/Defender`.
- *RESPONSE:* Response-only token hardware allows the user to create a one-time password based on a specialized algorithm using unique seed values that are time-sensitive. An example of this would be `Security Dynamics SecurID`.
- *MS-CHAP-V2:* MS-CHAP v2 encrypted authentication allows clients to be authenticated and supports the external Microsoft RADIUS server's ability to enforce the changing of password at the next logon.
- *MS-CHAP:* This option is for MS-CHAP–encrypted authentication.
- *RFC-2548:* This check box is to enable the Nortel VPN Router interoperability with Microsoft RADIUS Server version 2.2 or later, and version 2.1 with the Microsoft Hotfix applied. This box should remain unchecked if using Microsoft RADIUS Server V2.1 without Hotfix or earlier versions.
- *CHAP:* This enables CHAP authentication.
- *PAP:* This enables PAP authentication.

A brief description of these protocols may be found in the earlier section, "Enabling LDAP Proxy."

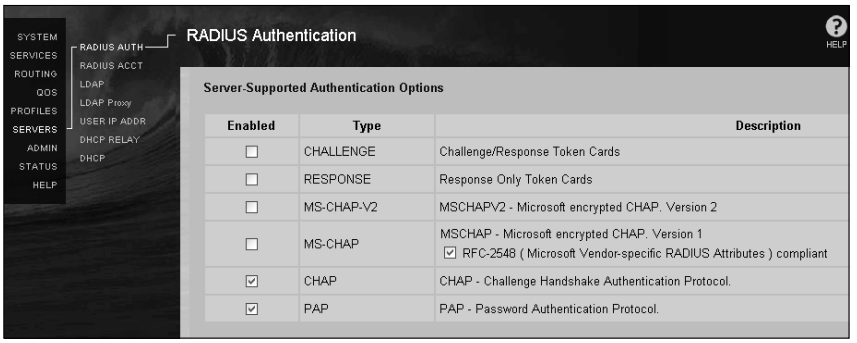


Figure 6-13: RADIUS authentication options

RADIUS Diagnostics

At the bottom of the RADIUS Authentication screen are selections for testing RADIUS Server configuration and operation. The RADIUS Diagnostic Report link causes a report to be generated verifying that the settings entered on the RADIUS Authentication screen correspond to the settings that have been specified on other Nortel VPN Router configuration screens. The title of each section of this diagnostic report lists the name of the related configuration screen. An example would be that the IPSec RADIUS Configuration section of the report would contain information associated with the IPSEC screen accessed through the SERVICES main menu selection.

The Reset Server Ordering button is used to cause the Nortel VPN Router to resume using the Primary server that is configured for authentication after a failover event has occurred. When a RADIUS server is unavailable, the Nortel VPN Router will failover to use the next available operational RADIUS server. Once failed over to another server, the Nortel VPN Router will continue to authenticate against the first server to which it was able to successfully connect. These may be either Alternate 1 or Alternate 2 if they have been configured and enabled. Clicking the Reset Server Ordering button restores the order of RADIUS servers so that the primary configured RADIUS server will be used first for authentication.

RADIUS Proxy

The Nortel VPN Router may be enabled to act like a RADIUS server for requests from clients on either the Private or Public interface. This is accomplished by selecting SERVICES from the main menu and then AVAILABLE. Within the Services configuration screen is a section labeled Authentication Protocol, and for the RADIUS selections there are check boxes for Public and Private, as shown in Figure 6-14.

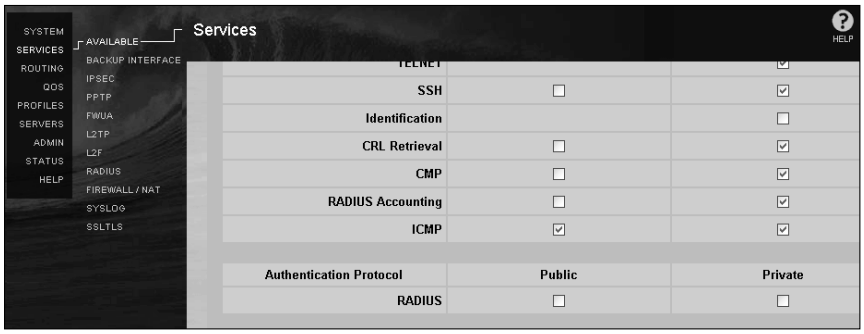


Figure 6-14: Nortel VPN Router as RADIUS server

Checking either or both the Private and Public interface check boxes causes the Nortel VPN Router to accept RADIUS Requests on those interfaces. If RADIUS Service is enabled on this screen, then RADIUS must also be enabled on the main menu selection SERVICES → RADIUS configuration screen, which is shown in Figure 6-15.

Checking the Enable RADIUS Service check box allows the Nortel VPN Router to function as a simple RADIUS server. If a user has multiple user accounts, the RADIUS Service will attempt to authenticate the user against each account type. If the entered username/password combination matches any of the user's accounts, then the user is authenticated. The order in which authentication is accomplished is PPTP, IPSec, L2F, and L2TP.

NOTE **See Chapter 1 for more information on PPTP, IPSec, L2F, and L2TP.**

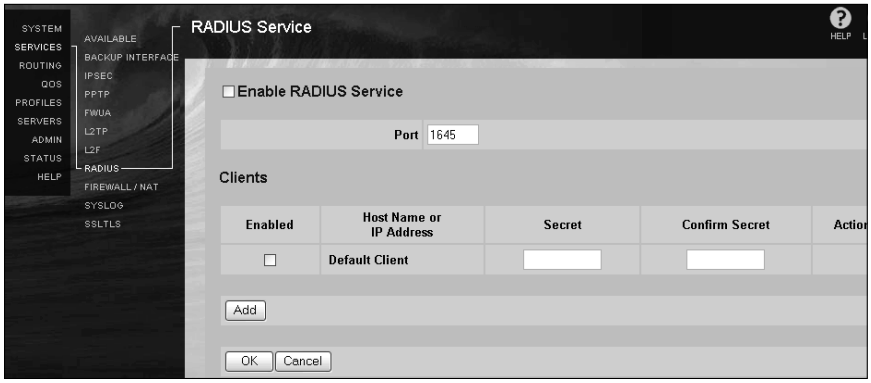


Figure 6-15: Enabling RADIUS service

With the Enable RADIUS Service box checked, the Nortel VPN Router listens on port 1645 (set by default), which is commonly used, or may be changed to another port value. Per the RADIUS RFC, the port it specifies is Port 1812. The value of the port is determined by the port number being used by the RADIUS clients being serviced by the Nortel VPN Router.

The Clients section of the RADIUS Service configuration screen enables you to either add clients that the Nortel VPN Router will service, or, if an administrator so chooses, to allow the use of the Default client for all RADIUS clients requesting service that present the correct shared secret entered in both the Secret and Confirm Secret boxes. Although the use of the Default client is extremely convenient for administrators, it does have some security implications to be considered before utilizing it. The Default client may be used alone or in combination with additional RADIUS clients added by clicking the Add button.

Adding RADIUS clients requires either the IP address of the RADIUS client or an FQDN and the secret it will be using to send requests to the Nortel VPN Router. Once the appropriate data has been entered, the Enabled check box may be used to enable the client and allow RADIUS requests to be serviced. Added RADIUS clients may be edited or deleted as needed. However, the Default client may not be deleted. The default condition of the Default client is disabled.

At the bottom of the RADIUS Service configuration screen is a section labeled Authentication Order. This allows the administrator to set the order of precedence for authentication. By default, the Internal LDAP is set first in the order. However, if you want to have the RADIUS server perform the authentication process first, then you can use the Swap button at the bottom of that section to accomplish swapping the order.

Enabling RADIUS Accounting

The Nortel VPN Router runs a RADIUS Accounting server, which stores the accounting data locally. However, this may optionally be accomplished with the use of an external RADIUS Accounting server. Configuration of RADIUS Accounting is accomplished by selecting SERVERS on the main menu and then RADIUS ACCT. A portion of the RADIUS Accounting configuration screen is shown in Figure 6-16.

To enable or disable RADIUS Accounting, the Enable check box may be either checked or unchecked. The Nortel VPN Router's internal RADIUS Accounting server is enabled by default.

The Session Update Interval value is the time interval when a snapshot of the current active tunnel sessions is to be recorded in a journal file. Following is the format used for the interval value:

```
hh:mm:ss
```

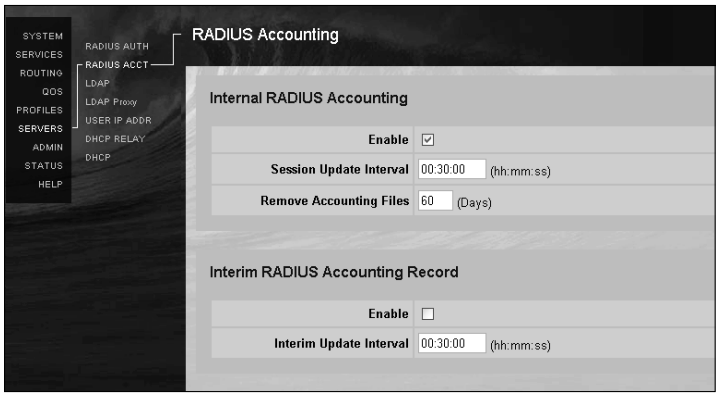


Figure 6-16: Configuring RADIUS Accounting

The default interval is set at 10 minutes. The journal file stores the session information until the user logs out of the tunnel session. With the user tunnel logs off, a session stop record is saved on the local disk. In the event of a system crash, upon re-initialization, the Nortel VPN Router translates the journal file into a series of stop records on a per-session basis to minimize accounting data loss. Although the Session Update Interval can be adjusted lower than its default, a time interval that's too low will result in increased system overhead because of the additional processing that would be required.

The Remove Accounting Files value is the number of days the RADIUS Accounting files are store locally until they are automatically removed. The default it set to 60 days.

The Interim RADIUS Accounting Record section in Figure 6-16 is for enabling and setting the Interim Update Interval, which is used to set when RADIUS Accounting records are to be sent to a configured external RADIUS Accounting server. The time format and precaution of a lower interval value are the same as those mentioned previously dealing with the Internal RADIUS Accounting.

Figure 6-17 shows additional parameters that must be configured to move and store RADIUS Accounting records to an External RADIUS Accounting server.

To enable or disable the Response Timeout for Radius Accounting server, simply check or uncheck the Enable check box. The Response Timeout for Radius Accounting server is, by default, set to 3 seconds. It may be adjusted if a longer timeout is required because of latency over the network.

Unlike the RADIUS Authentication Server configuration screen (where multiple servers can be added), only one External RADIUS Accounting server is supported on the Nortel VPN Router.

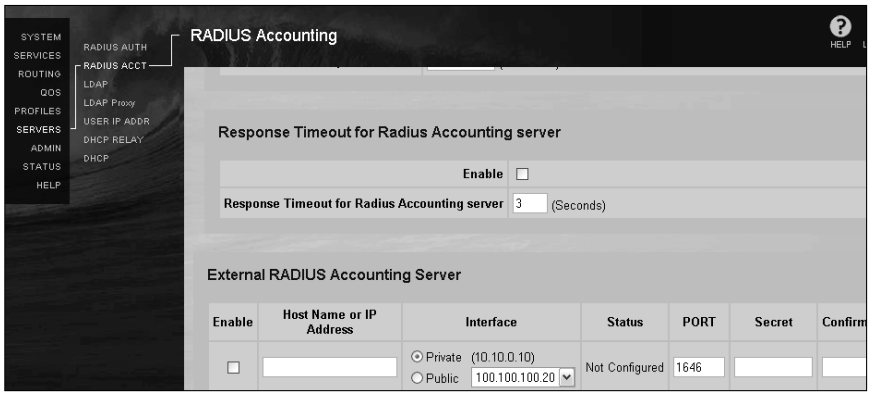


Figure 6-17: Configuring External RADIUS Accounting

The host IP address may be used or an FQDN may be used to identify the External RADIUS Accounting server. The use of the FQDN to identify an External RADIUS Accounting server that is accessed through the Public Interface may be advantageous in cases where the remote server is to be moved or replaced by another RADIUS Accounting server.

The interface field is automatically populated. However, administrators are able to select whether a Private or Public RADIUS server is to be used for the storage of the RADIUS Accounting records. The port used is set to 1646 by default but may be adjusted if the External Radius Accounting server uses a different port to respond to for RADIUS Accounting requests.

The Secret and Confirm Secret data boxes are where the secret used to establish a session with the External RADIUS Accounting server is entered.

Once the Enable check box is checked, the Nortel VPN Router is configured and ready to send accounting records to the External Radius Accounting server.

Once all the required configuration parameters for the External RADIUS Accounting server have been entered, then the Test Server button at the bottom of the configuration screen can be used to test and verify the connectivity between the Nortel VPN Router and the External RADIUS Accounting server. A message displaying the results of the test is displayed at the top of the Radius Accounting Configuration screen.

Understanding Certificates

The use of Digital Certificates provides a means to bind an entity's identity to a public encryption or signing key, which is identified, verified, and validated by a trusted third party called the *Certification Authority* (*CA*). The authentication of LDAP and VPN connections may be accomplished with the use of Digital Certificates.

SSL Encryption with LDAP Server

The Nortel VPN Router is able to communicate with an External LDAP server securely and privately with the use of Secure Socket Layer (SSL), which is a protocol that provides security and privacy over the Internet. It negotiates encryption keys to be used and authenticates the server before any information is exchanged. Using SSL, the transmission channel's security and integrity is maintained through encryption, authentication, and message-authentication codes. The following encryption methods are supported with the implementation of SSL:

- RC4 128-bit Message Digest 5 (MD5) encryption provides the most security for clients. The longer the encryption key, the more secure is the overall encryption. United States export laws regulate 128-bit encryption.
- Data Encryption Standard (DES) 56-bit Secure Hash Algorithm (SHA) encryption provides mid-level security for clients. It is less secure than RC3 128-bit encryption but more secure than RC4 40-bit encryption.
- RC4 40-bit encryption is the least secure encryption offered to clients.

NOTE SSL parameters on the Nortel VPN Router may be configured when authentication is switched from Internal LDAP to External LDAP.

LDAP Certificate Installation

Authentication of the Directory Server and the Nortel VPN Router occurs asymmetrically over the LDAP connection between the two. It is initialized by the Directory Server sending its certificate to the Nortel VPN Router over a one-way SSL-authenticated connection. Once SSL authentication is established, it is used by the Nortel VPN Router to authenticate itself to the Directory Server by sending its LDAP bind DN and password.

The Nortel VPN Router must trust the issuer of the certificate presented by the Directory Server during the initial SSL authentication for the SSL connection to be successful. The steps required to import an SSL certificate are as follows:

1. On the configuration screen, select SYSTEM from the main menu and then CERTIFICATES.
2. Select Import and then SSL Certificate.
3. Paste the PKCS #7 formatted CA certificate into the input box.
4. Click OK.

LDAP Special Characters

Previously, special characters such as a comma were not allowed within a certificate subject DN. With the addition of the LDAP Special Character feature, previously unsupported characters that are compliant with RFC 2253 are now supported. This feature need not be enabled if the certificate subject DN does not contain any previously unsupported characters. Figure 6-18 shows the portion of the Certificate Configuration screen where Special Character Support may be enabled.

As shown in Figure 6-18, the Enable Special Characters Support for Subject DN option is disabled by default. To enable it, check the box to the left of this field and click OK.

External LDAP Proxy

The External LDAP Proxy feature has been enhanced to allow for more flexibility in the location of a user record. It allows for the input to the subject DN attributes, which will be mapped to define the following LDAP attributes:

- *Common Name Attribute:* User's common name (for example, John Doe)
- *E-mail Attribute:* User's email address (for example, `jdoe@mydomain.com`)
- *Rfc822 Mailbox Attribute:* User's alternate mail alias (for example, johndoe)
- *UID Attribute:* User's ID (for example, jdoe)
- *Surname (SN) Attribute:* User's surname (for example, Doe)



Figure 6-18: Certificate Configuration screen

This new feature is accessed from the configuration screen by choosing SERVERS on the main menu and then LDAP Proxy. In the User Certificate Access section, enable this feature by checking the box to the left of this field and clicking the Advanced Setup button. Use the drop-down menu to select the desired attribute that is to be entered to form the LDAP Filter. This portion of the LDAP Proxy Server Configuration screen is shown in Figure 6-19.

Tunnel Certificates

The Nortel VPN Router uses X.509 certificates for the authentication of IPSec tunnel and L2TP/IPSec tunnel connections. X.509 is an ITU recommendation and currently not an approved standard. However, it is widely used as a *de facto* standard for defining digital certificates. The Nortel VPN Router supports RSA digital signature authentication in the IPSec Internet Key Exchange (IKE) key management protocol.

Users are able to authenticate themselves with the Nortel VPN Router with the use of their own public key pair and a certificate as credentials. In return, the Nortel VPN Router uses its own key pair and certificate to authenticate itself to the user. The Nortel VPN Router must be able to import and trust the CA certificate that had issued the certificate to the tunnel's initiator. The Nortel VPN Router currently supports certificates from Entrust and VeriSign.

The Nortel VPN Router supports the retrieval of X.509v3 certificates from Microsoft certificate storage with use of the Microsoft CryptoAPI (MS CAPI). Microsoft certificate storage is a mechanism that may be used to import digital certificates that have been granted by third-party CAs. This is accomplished by the use of standard messages (PKCS#12) that describe the transfer syntax for personal identity information (including private keys, certificates, miscellaneous secrets, and extensions). This allows the Nortel VPN Router and the Nortel VPN client to use CAs that are not tightly integrated with the client and the VPN Router.

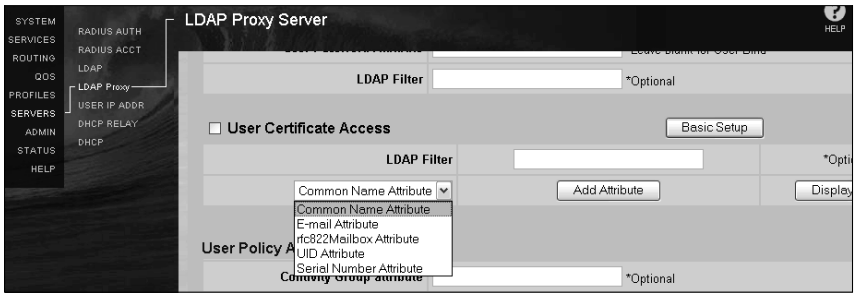


Figure 6-19: User Certificate Access

PKCS#12 Personal Information Exchange Syntax is a standard that was developed by RSA Data Security. It describes the syntax for the transfer of personal identity information, including private keys, miscellaneous secrets, and extensions. The standard supports the direct transfer of personal information with the use of integrity and privacy modes that utilize either password-based or public/private key pairs to ensure that the data is secured.

Using Public Key Infrastructure

Public Key Infrastructure (PKI) is a set of algorithms (Public Key/Private Key combinations) that can be used for key generation and distribution, data encryption, and digital signing. Its infrastructure is a framework of protocols and services that consist of the following:

- *Certificates:* A document that ties a specific Public Key to an individual or an entity.
- *Certification Authority:* Registers a certificate, providing assurance that the certificate and its relationship between the certificate and an individual are accurate.
- *Administrative tools:* These are needed for the storage, distribution, revocation, verification of status, backup, and recovery of certificates.

PKI Setup

The setup of a PKI to issue and manage certificates for both network and end users is very dependent on the type of CA services that are required. One method would be to purchase a commercially available CA solution from a vendor such as Entrust. This type of solution resides on your local network and is administered by the organization that purchased it. An alternative would be to subscribe to a CA provider such as VeriSign OnSite service, where the CA is operated and maintained by VeriSign from a remote location.

CA and X.509 Certificates

The CA is responsible for the issuance and revocation of certificates within a PKI. The CA certifies the validity of each certificate by signing each digital certificate with its own digital signature. The certificates are then stored in a certificate repository that is publicly accessible. The repository is used by certificate users to verify the validity of other user certificates.

Loading Certificates

The Nortel VPN Router must load two types of certificates: server certificates and trusted CA certificates. *Server certificates* are those that the Nortel VPN Router requests for itself and uses to validate its identity to connecting tunnels. The *CA certificates* are those that are end-user or BOT certificates imported by the Nortel VPN Router to establish a common trust. Server certificates can either be requested manually by cutting and pasting PKCS #7 or #10, or automatically with the use of Certificate Management Protocol (CMP).

Requesting a Server Certificate

The CA user documentation should be consulted for directions on how to generate reference numbers and authorization codes, along with overall instructions for CA administration. Using an Entrust CA–generated certificate with the Nortel VPN Router will work properly if it is done with an HTTP-based cut-and-paste operation utilizing either an Entrust Web certificate or an Entrust Enterprise certificate. If CMP automated life cycle management is to be used for requesting and renewing, the user must be aware that Entrust does not support CMP renewal for Web certificates.

Server Certificates Using CMP

With the use of the CMP, a compliant CMP certificate request can be accomplished. CMP provides management functions for the entire certificate/key life for enrollment, renewal, recovery, and revocation. It provides definition for message formats, which include its own message protection. A CA may be located on the private network if it has a publicly accessible IP address to allow it to communicate with the CA Root Authority (RA). This is shown in Figure 6-20.

In Figure 6-20, the CA Server located on the private network has the ability to communicate to the CA Root Authority (RA) over the public network. The local Nortel VPN Router communicates with the local CA over the private network allowing it to validate both user and branch office tunnels with the use of certificates.

To set up the Nortel VPN Router for initial certificate enrollment using CMP, you must first obtain the following information:

- *Issuer name:* This is the CA DN.
- *Subject name:* This is the Entrust Enrollment distinguished name (common name, organization, organizational unit).
- *Reference number:* This is used to identify the secret value.
- *Transaction ID/authorization code:* This is the initial secret value.

- *Enrollment URL/destination:* This may be either a host name or an IP address with optional port number.
- *Imported root CA certificate:* The certificate issued by the primary certificate authority.

You can create a CMP-compliant certificate request by using the Certificate Request configuration screen. CMP is derived from the Entrust PKI management protocol, and it includes management functions for the entire certificate and the key life cycle. CMP uses Certificate Request Message Format (CRMF) for the definition of the certificate request message. CRMF defines the syntax that is used to send a certificate request to a CA for the purpose of producing an X.509 certificate. The request typically includes a public key, along with other associated information for registration as outlined in RFC 2511, "Internet X.509 Certificate Request Message Format."

To perform the CMP configuration on the Nortel VPN Router, select SYSTEM from the main configuration screen and then CERTIFICATES. Figure 6-21 shows the screen on which the Private Key Password must be entered to continue with the remainder of CMP configuration.

Once the Private Key Password has been entered and confirmed, click OK. This will bring up the Certification Request—CMP screen where the status of outstanding requests may be seen, and where the data to create a new request may be entered.

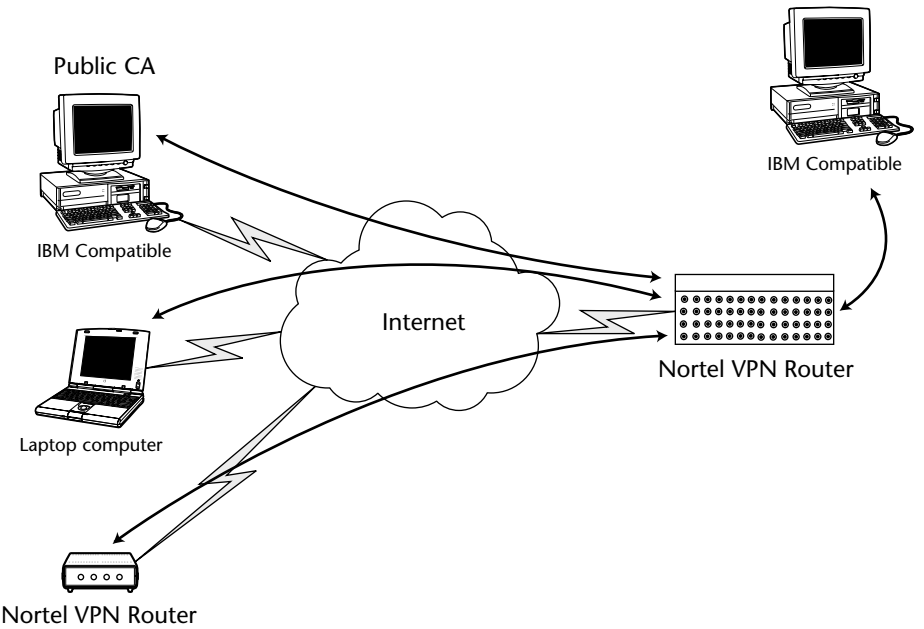


Figure 6-20: CMP environment

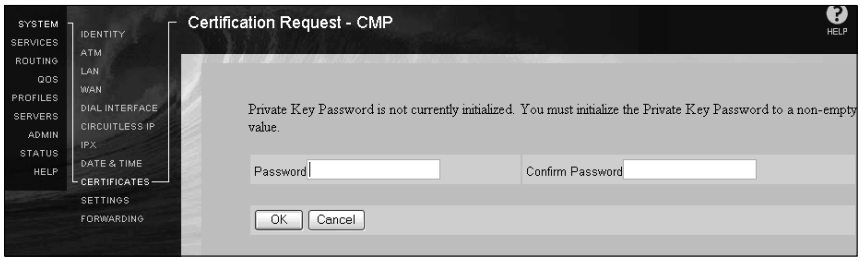


Figure 6-21: Private Key Password entry

The first portion of the CMP New Request screen is shown in Figure 6-22.

Figure 6-22 shows the status of the Current Request(s) at the top of the screen. Updates to the current status can be seen by clicking the Refresh button.

To create a new request, enter the requested information in the Certification Request—CMP screen. In the New Request portion of the screen enter the Reference Number supplied by the CA, which is used to identify the secret value. In the space provided for the Authentication Code, enter the authentication key that has been supplied by the CA. In the Key Size drop-down menu, select the exportable public key size in the number of bits. Generally, the larger the key, the more secure it is. The choices presented are 512, 768, 1024, and 2048. The 2048 Key Size is for US use only. In the space provided, enter the port number that is to be used. In the Registration Address/URL box, enter either that IP address or the FQDN of the CA server, and check the Import Issuer CA Certificate to automatically import the CA Root Certificate with this request.

To continue with the remainder of the Certification Request—CMP, fill in the optional Subject Distinguished Name and Issuer Distinguished Name portions of the screen, as shown in Figure 6-23.

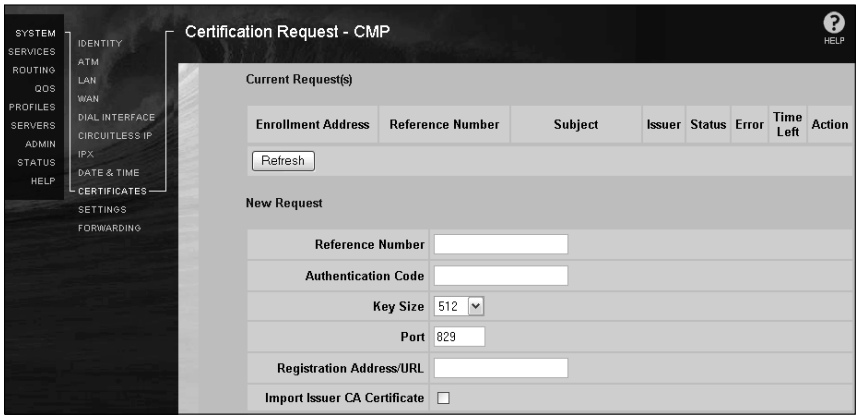


Figure 6-22: CMP Request configuration

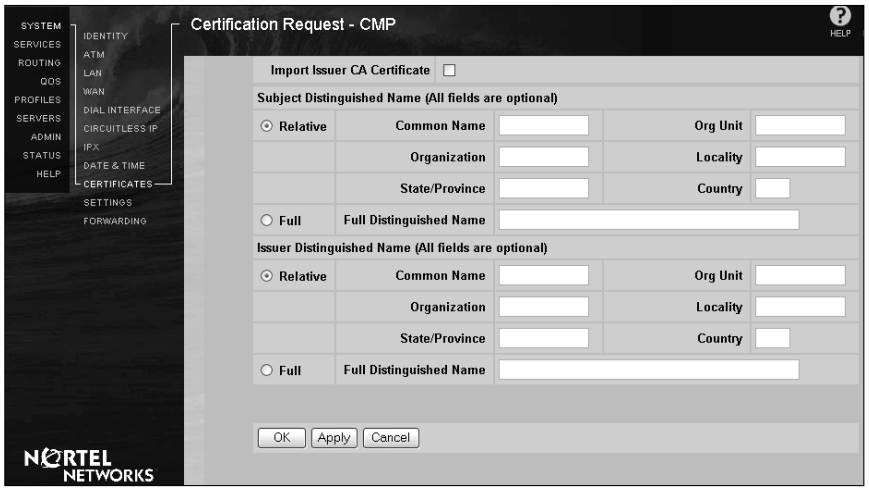


Figure 6-23: Subject/Issuer Distinguished Name

The Subject Distinguished Name area is where optional information may be entered for the request. The main choices are either Relative or Full. If the Full radio button is selected, then the Full Distinguished Name must be entered in the provided box. If the Relative radio button is selected, then enter the following Relative Distinguished Name (RDN) details:

- *Common Name:* Enter the common name that is associated with the Nortel VPN Router.
- *Org Unit:* Enter the name of the organizational unit with which the Nortel VPN Router is associated.
- *Organization:* Enter the name of the organization associated with the Nortel VPN Router.
- *Locality:* Enter the location where the Nortel VPN Router resides.
- *State/Province:* Enter the name of the state or the province where the Nortel VPN Router resides.
- *Country:* Enter the name of the country where the Nortel VPN Router resides.

The Issuer Distinguished Name area is where optional information may be entered for the request. The main choices are either Relative or Full. If the Full radio button is selected, then the Full Distinguished Name must be entered in the provided box. If the Relative radio button is selected then enter the following RDN details:

- *Common Name:* Enter the common name that is associated with the Nortel VPN Router.
- *Org Unit:* Enter the name of the organizational unit with which the Nortel VPN Router is associated.

- *Organization:* Enter the name of the organization associated with the Nortel VPN Router.
- *Locality:* Enter the location where the Nortel VPN Router resides.
- *State/Province:* Enter the name of the state or the province where the Nortel VPN Router resides.
- *Country:* Enter the name of the country where the Nortel VPN Router resides.

After all the optional information for the Subject Distinguished Name and the Issuer Distinguished Name has been entered, click the Apply button. Figure 6-24 shows the request and status that were generated when the Apply button was clicked. The Refresh button, when clicked, provides the current condition of the request. The Edit button allows for the Current Request to be edited and resubmitted. The Delete button removes the request altogether.

Once the requested certificate has been installed, its details can be displayed by selecting SYSTEM from the main menu, and then selecting CERTIFICATES. Clicking the Details button brings up a screen that provides the certificate details, including the owner of the certificate and the issuer of the certificate. This screen also displays the validity date, certificate fingerprint and, if it is a CA certificate, the Certificate Revocation List (CRL) details. The displayed fields are as follows:

- *This Certificate Belongs To:* Displays the certificate owner's X.500 Distinguished Name.
- *This Certificate Was Issued By:* Displays the CA that issued it, along with the main attributes and the certificate's serial number.
- *Validity Dates:* Displays the starting and ending dates for which the certificate is valid.
- *Certificate Fingerprint:* Displays the unique identifier derived from the MD5 hashing of the certificates. This identifier should be compared with the fingerprint that was supplied directly by the certificate's issuer or CA. If these fingerprints do not match exactly, then the certificate has been either forged or modified in some manner.
- *Version:* Displays the certificate's version.
- *Signature Algorithm:* Displays information about the signature algorithm.
- *Public Key:* Displays the public key information.
- *Extensions:* Displays information about the extensions being used.
- *Certificate Enrollment Configuration:* This is the information that was used during the certificate enrollment process. It provides the address required for the key update, key recovery, and revocation purposes.
- *Port:* This is the port number used to communicate with the CA.

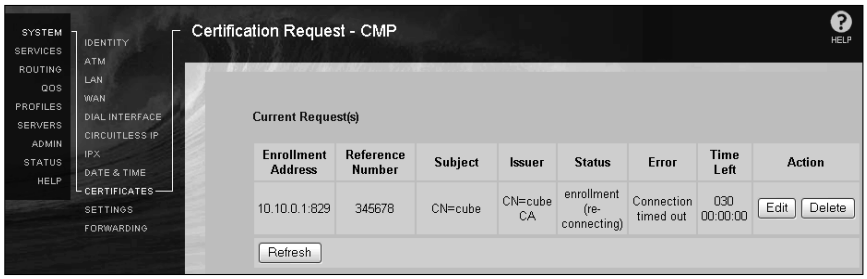


Figure 6-24: Certification Request—CMP screen

- *Enrollment Address:* This is the IP address of the CA.
- *Renew Certificate Now:* Check this box to renew the certificate now.
- *Renew Days before expiration:* This option is selected to automatically renew the certificate a specified number of days before the expiration date.
- *Recover Certificate:* This option is selected to recover a specific certificate. To accomplish this function, enter the certificate's Reference Number and Authentication Code in the corresponding field.
- *Revoke Certificate Now:* This option is selected to revoke the certificate. The certificate will be removed from the Nortel VPN Router upon a successful revocation of the certificate.

NOTE **The CRL is discussed in detail later in this chapter.**

Trusted CA Certificate Installation

For remote users or BOTs to authenticate, they must use a certificate issued by the Trusted CA Certificate. It must be loaded on the Nortel VPN Router and be marked as trusted. This is accomplished by selecting SYSTEM from the main menu, and then CERTIFICATES, and finally by clicking the Import Tunnel or Transport Certificate button to bring up the Import Tunnel or Transport Certificate configuration screen, as shown in Figure 6-25.

The Trusted CA Certificate radio button must be selected. You must copy and paste into the box provided the certificate that HTTP requested from the trusted CA. Click OK. The installed tunnel certificate is displayed in the certificate table. Click Enable Allow All and click OK. The CA certificate that remote users can authenticate against has now been obtained. This process may be repeated if there are multiple CA servers that will be issuing user certificates.

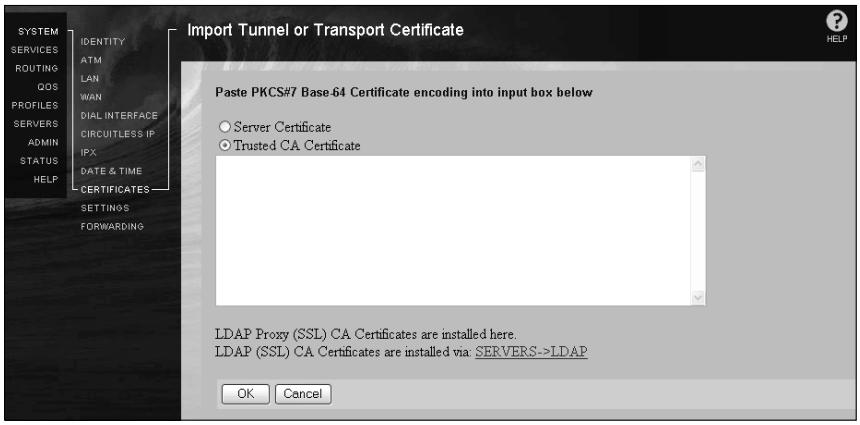


Figure 6-25: Import Tunnel or Transport Certificate screen

As an option, a CRL distribution point may be configured to enable revocation checking of user certificates. This is accomplished by selecting SYSTEM from the main menu and then CERTIFICATES. From the list of installed Tunnel Certificates, click the CA Details button (which will allow the appropriate CRL information to be entered), and then click OK.

Checking the Enabled check box enables CRL checking of certificates for that particular CA server. For access into the CRL LDAP directory store, the values for Search Base, Host, and Connection all must be entered. With this feature enabled, the Nortel VPN Router will attempt to retrieve a CRL from the configured directory. If CRL retrieval is successful, the Nortel VPN Router will verify the revocation status of all presented certificates. If this feature is not enabled, the Nortel VPN Router will not attempt to retrieve a CRL, and certificates will not verify the revocation status of the certificates with which it is presented. Not enabling this feature is essentially shutting off CRL checking on the Nortel VPN Router.

NOTE **The CRL is discussed in detail later in this chapter.**

Trusted CA Certificate Settings

Each CA certificate must be associated with a group for usage of authentication of incoming tunnel requests. This is accomplished either by finding the user as provisioned within the Nortel VPN Router directory (whether it is internal or external), or by allowing all users that have been issued by a particular CA to gain access. If you are allowing all access from a particular CA, then group association is determined by the tunnel initiator being assigned into a group directly, because of a group being assigned to that CA, or the use of access control based upon the subject DN.

User Identification Group Assignment

When the subject DN of a certificate presented by a remote initiator of a tunnel is by a user located on the Nortel VPN Router, the group that the user is bound to is indicated within that user's configuration.

Allow All Policy

With the use of the Allow All Policy, the Nortel VPN Router relies on the trusted CA to establish the true identity of the user. When presented, if the user's certificate is within the certificate validity dates period, its signature can be verified against the CA certificate, and the user's certificate does not appear on the CA's CRL, then the tunnel connection is permitted. The Allow All Policy permits users that are certified by the CA to create a tunnel connection, as long as their certificate is in good standing.

Users may be allowed to authenticate with certificates issued by this particular CA with the Nortel VPN Router, regardless of whether or not they have a user entry in the Nortel VPN Routers LDAP database. By default, the CA certificate does not allow all users to be authenticated.

Users with a subject DN (entered by selecting PROFILES from the main menu and then selecting USERS, thus bringing up the User Management configuration screen) are only allowed to be authenticated using certificates issued by that CA. If Allow All users to authenticate is enabled, then a group must be selected for these users from the default Group drop-down menu. If you want to have only specific users to authenticate with the CA authority, then each user must be configured. Select PROFILES from the main menu and USERS to bring up the User Management configuration screen. Then select Edit to disable Allow All authentication for this CA.

Without the Allow All Policy, only the users with the correct DN can perform IPSec RSA Digital Signature Authentication using certificates issued by that particular CA.

If multiple CA certificates are used, then the Allow All feature must be enabled for each CA certificate where authentication of a user is permitted without an explicit user entry. This allows a user with a valid certificate from a particular CA to establish a tunnel connection. However, a default group must be associated with that certificate. A client creating a connection using this method acquires and uses the attributes associated with that group. A specific group can be assigned to the authenticated user using the certificate from that particular CA by matching the relative DN. Use of the DN eliminates the limitation that only the attributes of the assigned default group may be used.

The Allow All Policy is used only for tunnels created by user tunnel requests. BOT requests must, therefore, be explicitly configured.

Access Control by Subject DN

The use of mapping the subject DN to groups allows the subject DN of incoming certificates to be parsed to a configured depth, and to be associated with a

corresponding group. This is accomplished during the client authentication process when the Nortel VPN Router attempts to match the client's certificate subject DN with all the associations of the CA. The match may be a partial or an exact one. In the circumstance of a partial match the longest match from the root DN is used to assign the client to that corresponding group. If a match is not made, then the client is assigned to the default group that is associated with that CA.

A DN consists of multiple components (known as the RDN). Following are the most commonly used of these:

- Common name (CN)
- Organizational Unit (OU)
- Organization (O)
- Locality name (L)
- State/province name (S)
- Country (C)

The RDN order of the various components does not matter unless there are multiple instances of OU present. However, the ordering of the DN in the following sequence does avoid ambiguity: C, S, L, O, OU, and CN.

Configuration of Group and Certificate Association

You can use this feature to gain a finer control of user association to a group for IPSec tunnel connections where each CA can set up a lookup table between the certificate subject DN and a Nortel VPN Router group. When a new tunnel is being established using the certificate, and it gets authenticated, the Nortel VPN Router utilizes the certificate's DN to look up the group in the table. With an exact or partial match, the new tunnel will bind to the group specified in the table.

If using the certificate's DN does not produce a match with the lookup table, the new tunnel will be bound to the specified default group only if the Allow All feature has been enabled. If it has not, then the tunnel will be denied.

All the attributes that are used to bind a user to a group are CA-specific. To configure the Group and Certificate Lookup Table, select SYSTEM from the main menu and then CERTIFICATES. Select the CA to be configured and click the Details button. Under the Group Access Control selection, click the Add button. Most times, a partial Subject DN should be used by omitting one or more of the leftmost fields to simplify the configuration. Either Relative of Full may be selected to specify the partial subject DN. Using the Relative selection automatically generates the DN string. If it exists in a certificate's subject DN, no field within the middle portion of the DN should be omitted (such as `o=Nortel` or `s=MA`). Once all the necessary information has been entered, just click OK to accept these values.

CA Key Update

Key update is performed for security or a number of other reasons. The CA key update feature provides for a BOT authenticated by the use of a certificate to remain uninterrupted before, during, and after an Entrust Key Update function is being performed by a CA in a given PKI environment.

The process used is as follows. Prior to a key update, the original CA certificate (which is a self-signed root certificate) is sent to the directory by the CA, along with the CRL it produced. The CRL is a list of revoked certificates that are digitally signed by the CA certificate. Both the Nortel VPN Router and the user's PC have a certificate signed by the CA, as well as a self-signed CA certificate that it signed. The user authenticates the Nortel VPN Router certificate because it has the original CA certificate that was used to create the Nortel VPN Router certificate (which is stored locally). The Nortel VPN Router can also authenticate the user because it has the CA certificate that was used to issue the user certificate. The Nortel VPN Router can also verify that the user's certificate has not been revoked because it had been configured to periodically retrieve the latest CRL from the directory. It is able to authenticate the CRL because it has the CA certificate that was used to sign it.

After a key update has been completed, the directory will contain four certificates: the original self-signed one, the new self-signed one, and the two cross-signed certificates. After the key update, all CRLs issued by the CA will be signed by the updated CA.

No Nortel VPN Router or user tunnel authentication issues exist at this point because the certificates presented by the Nortel VPN Router and the user are signed by the original CA certificate (which had been stored locally for authentication).

However, there is a problem with the Nortel VPN Router being able to authenticate the CRL at this point because it is signed by the update CA certificate. The Nortel VPN Router does not have that certificate stored locally to authenticate that CRL signature. The solution is to import the updated CA certificate into the Nortel VPN Router.

Importing the updated CA certificate is a requirement that must be accomplished immediately after the CA key update. If it is not done immediately after the key update, all of the post-update CRL processing, along with tunnel authentication, will fail until this process has been completed.

Certificate Revocation List Configuration

A CA will revoke user and server certificates whenever the associated keys are no longer valid, the key pair had been compromised, the user has left the organization, a server has been retired, or for a number of other reasons. When a certificate has been revoked, the CA updates the associated revocation list with the serial number of the revoked certificate. The modified list is referred to as

the Certificate Revocation List (CRL). A CA may have one or more associated CRLs. If attempting to remove a certificate, and the certificate has been referenced, the certificate will not be removed and an error message will be posted. The certificate cannot be removed until all references to that certificate have been removed prior to deleting it.

The CA publishes its CRL in an associated LDAP-accessible directory service. The frequency of publication is set by the CA administrator. Within an Entrust environment, a new CRL can be automatically published at a set time, at any time manually set by the administrator, or whenever a certificate has been revoked. In the VeriSign OnSite environment, a new CRL is published at a fixed interval (typically set for every 24 hours).

When a CRL directory is located on the public side of the Nortel VPN Router it retrieves the CRLs through its public interface. The CRL reply packets may be dropped if the size of the CRL is large enough that the LDAP response will include approximately 40 IP packets or more. This may be corrected by enabling the stateful firewall on the Nortel VPN Router.

The Nortel VPN Router can optionally use CRLs to verify the revocation status of user certificates. When it is enabled on the Nortel VPN Router, CRLs are periodically retrieved from the CA's LDAP directory store and cached into the Nortel VPN Router's associated LDAP database. This permits rapid verification of user certificates during the time an IPSec tunnel is being established. The frequency at which the Nortel VPN Router checks for a new CRL is configurable.

A CRL is protected against tampering because it is signed by the CA's private key. The Nortel VPN Router verifies the CRL signature each time it is used in the CRL retrieval process. A CRL server must be configured for each trusted CA certificate that is imported into the Nortel VPN Router. The LDAP server that contains the CA certificates on the Nortel VPN Router must be reachable from either its public or private networks.

CRL Server Configuration

The following list explains the CRL settings:

- *CRL Checking Enabled:* This displays the CRL usage enabled on the Nortel VPN Router on a per-CA basis. To enable the use of CRLs, from the main menu, select SYSTEM and then CERTIFICATES. When the Certificate Configuration screen is displayed, click the Details button. The section labeled "Certificate Revocation List Information" is used to configure the necessary information. CRL checking of certificates is turned on by checking the Enabled check box for the particular CA. The Search Base, Host, Connection, and Update frequency values must be set for the proper access of the CRL LDAP directory store.

- *CRL Retrieval Enabled:* This determines whether the Nortel VPN Router will attempt to retrieve a CRL from the configured directory. If the CRL retrieval is successful, the Nortel VPN Router will verify the revocation status of the presented certificates. If this option is not selected, the Nortel VPN Router will not attempt to retrieve a CRL and will not verify the revocation status of the presented certificates. The deselecting of this option is, in effect, turning off CRL checking.
- *CRL Checking Mandatory:* This determines if a CRL must be present when an IPSec tunnel is established to a particular CA. When this is selected, the Nortel VPN Router must have a CRL present for the tunnel connections to be successful. Deselecting this option on the Nortel VPN Router will allow certificate authenticated tunnels when no CRL is present.
- *CRL Update Frequency:* This allows you to enter a value (in minutes) that will represent the frequency with which the Nortel VPN Router should query the LDAP server for a newly published CRL. The default value is set to zero, indicating that the Nortel VPN Router does not update any CRLs. This option is useful when more than one Nortel VPN Router shares the same LDAP database, and you must ensure that only one of the Nortel VPN Routers actually performs the update process. To minimize the load on an external LDAP server, it is important to make certain that only one or two Nortel VPN Routers are updating a shared CRL entry in a multiple VPN Router shared external LDAP environment.
- *CRL System Status:* This is read-only and is automatically updated by the Nortel VPN Router to reflect the CRL updating activity.

Follow these steps to configure CRL servers:

1. From the main menu select SYSTEM and then CERTIFICATES from the submenu. Click the CA certificate Details button. From the Details screen, click the Manage CRL Servers button to access the Manage CRL Servers screen. A list of currently configured CRL servers for the CA that can be edited or deleted will be displayed at the top of the screen. The New CRL Server portion of the screen allows for the configuration and addition of a new CRL server.
2. In the Search Base field, enter the portion of the X.500 directory where the CA stores the CRLs. The following is a sample search base entry:

   ```
   ou=Support,    o=Nortel,     c=US
   ```

3. In the Host field, enter the FQDN of the host or the IP address of the LDAP-accessible directory server that is storing the published CRLs. If an FQDN is used in place of an IP address, then one or more DNS servers must be configured on the Nortel VPN Routers System Identity

screen. This is accomplished by selecting SYSTEM from the main menu, and then IDENTITY from the submenu. In the DNS Server Configuration portion of the System Identity configuration screen, enter a Primary DNS server IP address and one or more secondary DNS servers.

4. In the connection field, enter the port number that is being used with the LDAP server. If desired, you can enable the use of the Secure Socket Layer (SSL) option to secure the connection with the LDAP server. SSL is not really required in handling the CRL because it is signed and, therefore, protected against modification or spoofing.
5. The CRL server may be enabled or disabled by selecting Enabled or Disabled from the list box.

CRL Distribution Points

CRL vendor-specific information is obtained through the use of CRL Distribution Points (CDPs). This feature is supported for use with Entrust CAs. With this implementation, the users authenticate only against the CRL that is specified in the certificate CDP. The use of this method provides for faster tunnel establishment.

Authentication is performed only against the CRL that is specified within the certificate CDP results in a tunnel being established in a shorter timeframe. When a certificate is presented for verification, the CDP from the certificate is obtained. Utilizing the CDP information, a filter for the LDAP query is built that only allows records that match with the CDP to be obtained. This method ensures that the certificate is authenticated against one CRL, instead of all of the available CRLs.

Even when the list of CRLs is long, performance of the Nortel VPN Router will not be affected because only one CRL is being used. If CRL checking has been set to mandatory, and CRLs are not present on the Nortel VPN Router, a request would be made to the CA LDAP to obtain only the CRL that is specified in the user certificate CDP. With CRL optimization enabled, only that CRL will be loaded into the Nortel VPN Router.

With CRL optimization enabled, CRL checking is performed using Global CRL collection. Global CRL collection is stored within the Nortel VPN Router's memory. With CDP support implemented, a user certificate obtained from an Entrust CA is verified against one CRL from Global CRL collection. CDP information is obtained from the certificate and is used to determine which CRL from Global Collection to use. The search will not be at a great expense as far as time required because the Global CRL collection is already located in memory. However, if Global CRL collection has not been loaded in

memory, all the CRLs are loaded from the Nortel VPN Router LDAP into Global CRL collection. When Global CRL collection is enabled, users will not reference LDAP, but rather the Global CRL collection and, for this reason, all the CRLs in a Global CRL collection need to be kept.

CRL Retrieval

Periodically, all the CRL records are retrieved. The time that CRLs are required to be updated depends on a configured interval. When an Entrust user is authenticated, only one CRL is obtained from the Nortel VPN Router LDAP. Each CRL record has the next update time set to determine if the CRL record is fresh or stale. If the CRL record is stale, it is refreshed from the CA LDAP. Because the collection of CRLs has only one specific CDP-based CRL, the next update time is always specific for one CRL record.

At times, a CA must go through a key update procedure. When that occurs, the Nortel VPN Router could possibly have two CA certificates with the same DN name. The same CDP support logic is used for both CAs' CRL collections.

Enabling Certificate Use for Tunnels

With the use of IPSec, RSA digital signature support must be enabled for any default groups associated with CAs and the groups containing any specific instances of users that utilize certificate-based authentication. Figure 6-26 shows the configuration screen for configuring RSA digital signature support.

To configure RSA digital signature support on the Nortel VPN Router, perform the following steps:

1. From the main menu, select PROFILES and then the GROUPS submenu to bring up the Groups selection screen.
2. Click the Edit button for the group to which you want to add RSA digital signature support.
3. On the Groups Edit screen, navigate down to the IPSec section and click the Configure button.
4. On the Groups Edit IPSec screen in the Database Authentication (LDAP) portion of the Authentication area, check the RSA Digital Signature selection check box to enable RSA digital signature support.
5. From the Default Server Certificate drop-down selection menu, select the appropriate default server certificate. This is the certificate that will be sent to the clients to authenticate the Nortel VPN Router's identity. This server certificate should be issued from the same CA PKI that issued the remote-access client certificates.
6. Navigate to the bottom of the screen to click OK to accept these RSA digital signature support settings.

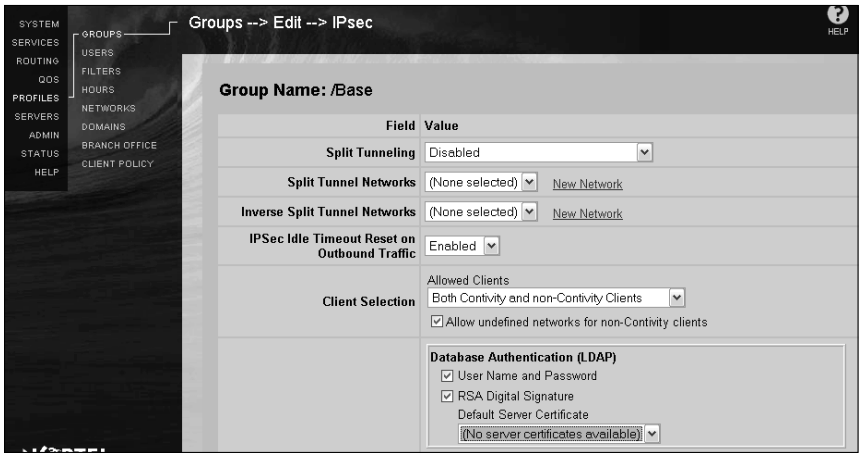


Figure 6-26: Configuring RSA digital signature support

Identifying Individual Users with Certificates

An alternative to allowing all users from a particular CA to gain access to the Nortel VPN Router is to identify users explicitly with the use of certificate attributes. To accomplish this, an existing user may be modified by selecting the user and clicking the Edit button. You can also click the Add User button to add a new user. With the addition of a new user, all other pertinent information for that user must be entered to configure the user properly.

Users are edited and created by selecting the PROFILES from the main menu and selecting USERS from the submenu. From the User Management configuration screen, existing users may be edited or created. If you scroll down to the area of IPSec Certificate Credentials, as shown in Figure 6-27, the user may be configured to be identified with the use of the certificate being used to authenticate.

In the Remote Identity portion of the screen, using the Valid Issuer Certificate Authority drop-down selection menu, select the appropriate CA for this user. This CA would be one of the ones created and configured from the System Certificates Request screen accessed from the main menu SYSTEM selection along with the submenu selection of CERTIFICATES.

In the Subject Distinguished Name area, enter either the Full Distinguished Name with the selection of the Full radio button or by selecting the Relative radio button to enter an RDN. As mentioned, an RDN is a collection of the following components that will uniquely identify the remote user identity in an IPSec certificate environment:

- *Common Name:* Enter a name that is associated with the user.
- *Org Unit:* Enter the organizational unit with which the user is associated.

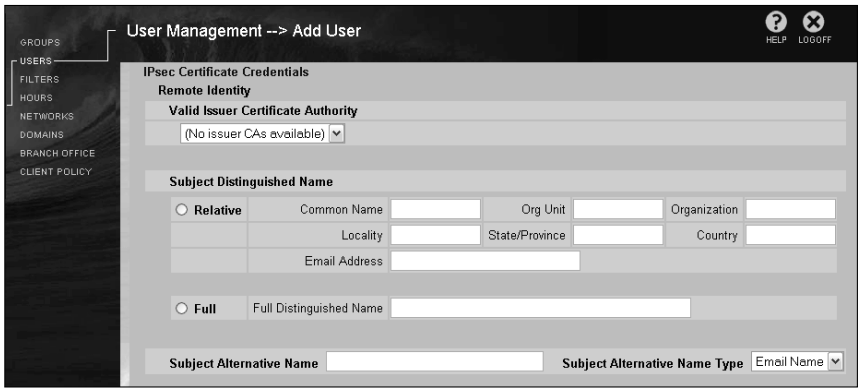


Figure 6-27: User Identity using Certificate Credentials

- *Organization:* Enter the organization that is associated with the user.
- *Locality:* Enter the location where the user resides.
- *State/Province:* Enter the state or province where the user resides.
- *Country:* Enter the country in which the user resides.
- *Email Address:* Enter the user's email address.

If using the Full Distinguished Name (FDN) field in place of the individual components used in the RDN fields, select the Full radio button and enter the Full Distinguished Name in the box provided for the entry. A sample FDN entry may appear as follows:

```
cn=NameOfUser,  o=CompanyName,  c=US
```

As an alternative, a Subject Alternative Name may be used. The following selections may be used from the Subject Alternative Name Type drop-down selection menu:

- *Email Name:* Enter the full email address, such as the following:

  `jdoe@thecomany.com`
- *DNS Name:* Enter an FQDN for the user, such as the following:

  `smith.myorganization.org`
- *IP Address:* Enter an IP address for the user (for example, 172.16.90.12).

Identifying Branch Offices with Certificates

Branch Office connections may be edited or created by selecting PROFILES from the main menu selection and BRANCH OFFICE to bring up the Connection configuration screen. The Tunnel Type that is to be used between the Nortel VPN Router and another VPN device is selected from the Tunnel Type drop-down menu, as shown in Figure 6-28.

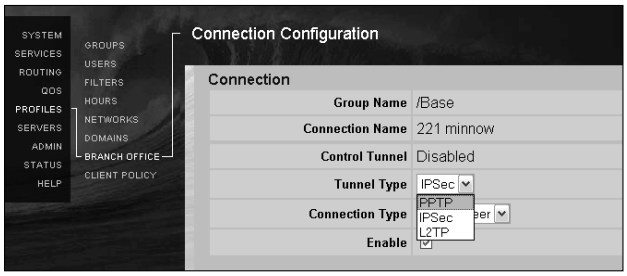


Figure 6-28: Branch Office connection configuration

The selections for Tunnel type are PPTP, IPSec, and L2TP. Select the authentication type to be used. When you are editing an existing authentication type, the screen changes immediately to reflect the requirement for the new authentication method. Any changes made on the previous screen in the Authentication area will be lost.

IPSec Authentication

With the Tunnel Type set to IPSec, scroll to the Authentication portion of the Connection Configuration screen, as shown in Figure 6-29.

In the Authentication drop-down menu, select Certificates. The screen will change to allow for the configuration of the certificates that are associated with each endpoint Nortel VPN Router to allow mutual authentication between the two connections. In this certificate authentication portion of the screen is information about the remote Branch Office system, the authority that issued the certificate, and the certificate identification, along with information regarding the local Nortel VPN Router that is being configured.

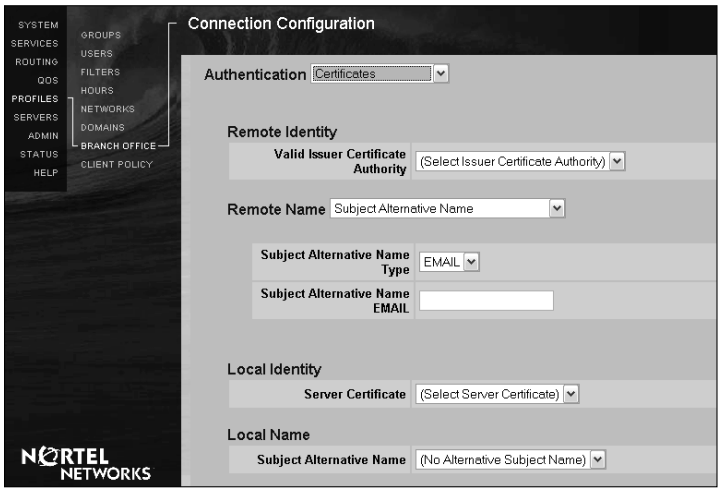


Figure 6-29: IPSec Tunnel authentication

In the Remote Identity section, the Valid Issuer Certificate Authority field allows you to select a valid issuer CA from the Certificate Authority list. The CA is the issuer of the remote peer's certificate, or a higher-level CA in the remote peer's hierarchy. The trusted flag must be set on the CA that was configured on the certificates screen. When using a CA hierarchy, all the intermediate CAs below the trusted CA must be imported into the Nortel VPN Router. These CAs are the ones that were configured from the Generate Certificate Request screen accessed by selecting SYSTEM from the main menu and CERTIFICATES from the submenu.

The Remote Name drop-down menu allows for the selection of how the Remote Identity is to be described. The selections are Subject Alternative Name, Subject Distinguished Name—Relative, Subject Distinguished Name—Full, and Unique Identifier.

If Subject Alternative Name is selected, then the Subject Alternative Name Type can be selected from the drop-down menu with the selections being IP, DNS, or EMAIL. Enter the appropriate information in the Subject Alternative Name entry box that corresponds with the Subject Alternative Name Type that was selected.

If Subject Distinguished Name—Relative was selected for the Remote Name, then the following information must be entered:

- Common Name
- Organizational Unit
- Organization
- Locality
- State/Province
- Country
- Email Address

If Subject Distinguished Name—Full is selected for the Remote Name, enter the DN that exactly matches the DN in the remote peer's certificate in the Subject Distinguished Name entry Box.

If Unique Identifier is selected for the Remote Name, the Unique Identifier Type is an FQDN in the FQDN entry box. An example of an FQDN would appear as:

```
RemoteVPN.Company.com
```

The Local Identity is the name that the Nortel VPN Router uses to identify itself when initiating or responding to a connection request. Either a Subject

Distinguished Name or a Subject Alternative Name can be used to uniquely identify the Nortel VPN Router. If Subject Alternative Name is selected from the Nortel VPN Router's certificate, then that identity is used in place of the Router's subject DN when it communicates with peers.

The Nortel VPN Router server certificate has only a Subject Alternative Name if the CA issues the certificate with alternative names. For example, while using Entrust PKI, the VPN connector can issue certificates with Email, DNS names, or IP addresses as alternative names.

The Local Identity Server Certificate drop-down menu displays all the certificates that have been issued to the Nortel VPN Router and were configured from the Generate Certificate Request screen, which is selected from the SYSTEM main menu and the CERTIFICATES submenu. Select the appropriate certificate that the Nortel VPN Router is to be identified and authenticated with.

L2TP/IPSec Authentication

You can either edit or create a new BOT to use L2TP by selecting PROFILES on the main menu and then BRANCH OFFICE to bring up the Branch Office configuration screen. Either select a tunnel to edit and click the Configure button, or click the Add button to add a new BOT connection. In the Connection Configuration Screen portion of the screen, select L2TP from the Tunnel Type drop-down menu. After the screen has been refreshed, scroll down to the Authentication portion of the screen, as shown in Figure 6-30.

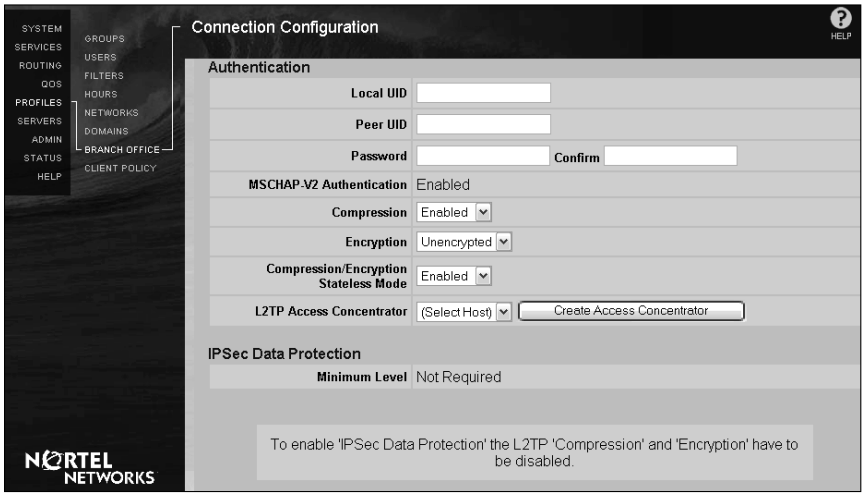


Figure 6-30: L2TP authentication configuration

Perform the following steps to configure L2TP authentication on the Nortel VPN Router:

1. Enter the ID of the local Nortel VPN Router that you are currently configuring in the Local UID field.
2. In the Peer UID field, enter the user ID of the remote peer Nortel VPN Router connection for which this tunnel is being configured.
3. Enter the password that is being used for the Local UID of the local Nortel VPN Router in both the Password field, and once again in the Confirm field to verify the accuracy of the password being entered. If a variation of MSCHAP-V2 Authentication has been selected, then no password is required for the Local UID.
4. Select either Enabled or Disabled for Compression from the drop-down menu.
5. Select either Enabled or Disabled for the Compression/Encryption Stateless Mode from the drop-down menu. This option is not used if both the Compression and Encryption fields are in a disabled state (Compression being set to Disabled and Encryption being set to Unencrypted).

The L2TP Access Concentrator is used only for L2TP authentication. This field appears when the Tunnel Type of L2TP has been selected for the BOT. This entry is used to select the L2TP Access Concentrator that is to be used to perform authentication between the Nortel VPN Router and the Network Access Server (NAS). If there are no available selections for the L2TP Access Concentrator, then the Create Access Concentrator button must be clicked to bring up the L2TP Settings configuration screen. Here you click the Add button in the L2TP Access Concentrators portion of the screen to allow for creation of the L2TP Access Concentrator, which is to be used for this connection. Steps for configuring the new L2TP Access Concentrator appear in the following section, "Adding L2TP Access Concentrators."

With Compression Disabled and Encryption set to Unencrypted, the IPSec Data Protection Minimum Level selection will be enabled to allow for the selection of the minimum level of IPSec (which is 56-bit DES). Higher encryption levels may be selected if they are displayed in the selection window.

Adding L2TP Access Concentrators

The addition of an L2TP Access Concentrator can be accomplished by selecting SERVICES from the main menu and L2TP from the submenu to bring up the L2TP Settings configuration screen. Scroll down toward the bottom of the screen to the L2TP Access Concentrators portion of the L2TP Settings configuration screen and click the Add button. The Add L2TP Access Concentrators configuration screen appears, as shown in Figure 6-31.

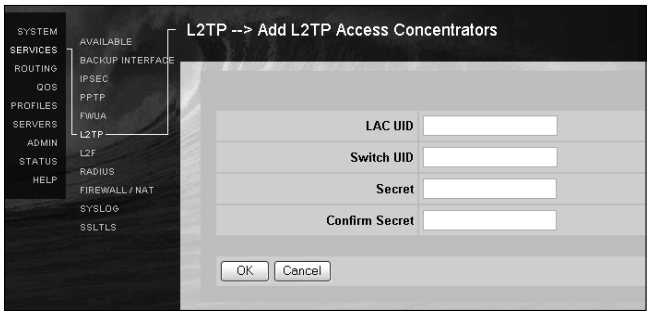


Figure 6-31: L2TP Access Concentrators screen

The L2TP Add Access Concentrators screen allows for the configuration of authentication between the Nortel VPN Router and the NAS. To edit an existing L2TP Access Concentrator, just click the Edit button for that concentrator in the L2TP Access Concentrators portion of the L2TP Settings configuration screen. Adding a new L2TP Access Concentrator requires the agreed-upon User IDs and the Secret that is to be used. In the LAC UID field, enter the ID that is used for the L2TP Access Concentrator that the Nortel VPN Router is forming a connection with. In the Switch UID field, enter the ID of the Nortel VPN Router that you are currently configuring to form a connection to the NAS. In the Secret and Confirm Secret fields, enter the agreed-upon secret between the Nortel VPN Router and the administrator of the L2TP Access Concentrator that the tunnel is to be established with.

Click OK to accept the entered information and to complete the creation of the L2TP Access Concentrator.

Summary

This chapter discussed various authentication environments and types. The discussion included the use and configuration of Internal and External LDAP, LDAP Proxy, RADIUS, and certificate servers.

This chapter also included an overview of LDAP principles and how they affect user access and control and provided information on monitoring the availability and health of external authentication servers used by the Nortel VPN Router. Use and configuration of multiple RADIUS servers, RADIUS accounting, and RADIUS proxy were also demonstrated.

The discussion on the use of certificates also included their use within the authentication process for servers, tunnels, and users. Also covered was the ability of the NVR to use Certificate Management Protocol (CMP) to facilitate the use and management of certificates for tunnels and users.

Finally, this chapter discussed the use of Certificate Revocations Lists (CRL), CRL Distribution Points, authentication for L2TP users and tunnels, and the configuration and implementation of each authentication type.

CHAPTER

7

Security

There is no absolute definition of what network security is. Network security can be far-ranging—from a total lockdown of the network where no data is allowed to enter or leave the protected network, to wide-open access that exposes the network to any security breach imaginable. However, from a practical business standpoint, it is desirable to provide controlled access to and from the protected network, while maximizing security that will ensure that the network is totally protected from intrusion and/or any malicious intent.

The Nortel VPN Router provides access flexibility for non-tunneled traffic with the use of filters and a stateful firewall. With the stateful firewall, the Nortel VPN Router can perform a number of secured routing functions with increased performance because of its ability for optimized packet inspection. The Nortel VPN Router stateful firewall is capable of providing full firewall functionality to ensure the highest level of network security. The use of interface filters on the Nortel VPN Router provides an effective, cost-efficient level of network security. However, interface filters may be disabled only if the Nortel VPN Router's stateful firewall has been enabled.

Stateful Firewall Basics

The Nortel VPN Router is primarily used as a secured access gateway between a public network (for example, the Internet) and a private internal network. With its stateful firewall functionality, it provides protection against unauthorized

access to the protected internal private network. With the use of rules and policies, the stateful firewall will allow traffic that is acceptable to be permitted to either enter or exit the internal private network. Based upon the access rules and policies established by administrators of the Nortel VPN Router, packets and sessions are monitored to determine the action that is to be taken with that traffic. Packets and sessions that do not meet any of the preset criteria are dropped. The stateful firewall is also capable of logging significant events that may include network connections, changes in firewall status, or possible system failure. The logged information may be used to help with enhancement of network security, or the reporting and tracking of unauthorized use.

Using Stateful Inspection

The use of traditional filtering methods makes it difficult at times to allow traffic to securely pass through the firewall. An example of this would be the use of *Passive FTP,* where the control port is a well-known port, but the port used for passing the data content is a random port value. Because it is undesirable to open a large number of ports through the firewall, it can be accomplished only with the use of *stateful inspection*. This is done by inspecting the packets at the application layer to determine the port being used by the data connection. When the port for the data connection has been determined, then all traffic on that port is allowed to pass through the firewall for the duration of that particular FTP session.

Application stateful inspection is unique for each application because of the use of random ports that are not predictable. For each application, the port being used is validated and traffic using that port is allowed through the firewall. The following is a list of applications that are inspected:

- FTP
- TFTP
- RCMD
- SQLNET
- VDOLive
- RealAudio

Stateful inspection at the transport layer enables you to secure TCP traffic, making it difficult for interception and modification. This is accomplished by verifying the consistency of the TCP header and the use of randomized TCP sequence numbers.

Interfaces

The Nortel VPN Router has many interfaces. They consist of physical interfaces and virtual interfaces. The *physical interfaces* are the actual hardware

interfaces on the unit (such as Ethernet and a number of differing WAN interface options). *Virtual interfaces* are created with the establishment of either Branch Office Tunnels (BOTs) or user tunnels. On the Nortel VPN Router, packets are classified by the interface on which they arrive (called the *source interface*) or the interface on which they depart (called the *destination interface*).

Policy rules may be constructed using these interface classifications. However, if a rule is constructed using "Any" as the interface designation, then the classification is ignored. If an interface or group of interfaces is designated, then these classifications will apply.

The following is a list of interface designations that may be used when constructing a policy:

- *Any:* Any physical interface or tunnel.
- *Trusted:* Any private physical interface or tunnel.
- *Untrusted:* Any public physical interface.
- *Tunnel:Any:* Any tunnel.
- *Tunnels:* May be specified by group name for user tunnels, or specific named BOT.
- *Tunnel:/base:* Specifies a specific BOT. For example, `/base/sales /concord` specifies the BOT named `concord`, which is a member of the group `/base/sales`.
- *Tunnel:user:* Specifies a group name for the user tunnels within that group. For example, `/base/support` specifies all user tunnels within that particular group.
- *Interface name:* Specifies the value assigned to either the LAN or WAN interface Description field. If this field is left blank, then the name will be the default description in the Interface field.

Physical interfaces may be configured to be either private or public. However, the default setting is that LAN interface (Slot 0) is designated as private, and all other physical interfaces as public.

Filter Rules

Filter rules are used in the determination of which packets are to be allowed through the firewall. The usual rule options are either to accept or drop the packet. The following is a list of actions these rules may use:

- *Accept:* Accept the packet.
- *Drop:* Drop the packet.

- *Reject*: A rejection notification is sent to the source address specified within the packet.
- *Log*: Provides logging locally and may be used with the actions previously mentioned.

Anti-Spoofing

To prevent packets from having their source IP addresses forged or spoofed, each packet source IP address is examined and validated. (*Spoofing* is when a packet illegally claims to be from an address from which it was not actually sent.) The following is a list of checks that are done with the use of anti-spoofing:

- Source address does not equal the destination address.
- Source address is not set to zero.
- Source address of a packet received from an external network is not set to an address of a connected network.

Attack Detection

A variety of attacks may be launched against a protected network. The firewall being used to protect that network should be capable of detecting these attacks. Packets used in the attack should be dropped, thus preventing denial-of-service as well as unauthorized intruders. The Nortel VPN Router is capable of defending against denial-of-service attacks, as well as the following:

- *Jolt2:* A fragmentation attack that affects Windows PCs by repeatedly sending the same fragment.
- *Linux Blind Spoof:* Attempts to establish a spoofed connection in place of sending a final `ACK` with the correct sequence number with no flags set. Linux does not verify that the `ACK` is not set. Any packet that does not have the `ACK` set is dropped by the firewall.
- *SYN flood:* Has the ability to disable network services by flooding those services with connection requests. The `SYN` queue (which maintains a list of un-established incoming connections) is filled, forcing it to not accept any additional connection requests.
- *UDP Bomb:* Sends malformed User Datagram Protocol (UDP) packets to a remote system in an attempt to crash it.
- *Teardrop/Teardrop-2:* A fragmentation attack that sends invalid fragmented IP packets to trigger a bug within some operating systems' IP fragment reassembly code.

- *Land Attack:* Sends a TCP packet to a running service on a host with the source address set to the address of the host itself. The TCP packet is a `SYN` packet requesting a new connection from the same TCP source port as the destination port. When the targeted host accepts the packet, it causes a loop within the operating system, causing the system to lock.
- *Ping of Death:* Sends a fragmented packet that is larger than 65536 bytes, which causes the remote system to incorrectly process the packet. This can cause a remote system attempting to process such a packet to either panic or reboot.
- *Smurf:* Sends a large number of Internet Control Message Protocol (ICMP) ping echo messages to an IP broadcast address with a source address that has been forged to the IP address of the intended target host to be attacked. A routing device that is forwarding traffic to those broadcast IP addresses performs a layer 2 broadcast, causing most network hosts to accept the ICMP Echo Request and issue a reply for each. This will cause traffic to be multiplied by the number of hosts responding, thus degrading the responsiveness of the network under attack.
- *Fraggle:* Sends a large quantity of UDP echo messages. If this occurs on a multi-access broadcast network, there is the possibility of hundreds of machines replying to each packet, degrading the response of the network under attack.
- *ICMP unreachable:* Sends ICMP unreachable packets to a host from a spoofed address, which will cause the host to stop all legitimate TCP connections to the host whose address is being spoofed in the ICMP packet.
- *Data Flood:* Sends a large quantity of data to a host as a means of accomplishing a denial-of-service–type attack by attempting to exhaust all of the available resources of the target host, thus preventing responses of the host to legitimate requests.
- *FTP Command Overflow:* Causes FTP servers that have buffer overflows for commands that use arguments to crash. Such a command is the `user` command, which does not require a valid user account on the system to crash it.

Access Control Filters

Access control is an important security function to control which users may have access to network resources. Filtering can be used to fine-tune who is allowed access to network hosts and services. All users based upon their

group profile have a custom filter profile defining the resources they are permitted to access on the network. These filters may be defined by the following:

- Protocol ID
- Direction
- Source and Destination IP addresses
- Source and Destination Port addresses
- TCP established connections

A *filter profile* consists of a list of rules that were created to perform a precise action. This list performs a sequential filtering process, so the order of the rules is extremely important (since the rules are tested in order until a match is found). If a packet passes through all the rules on the list without a match, the packet is dropped. Thus, only packets that meet a specific filter criteria are permitted to pass.

Network Address Translation

Network Address Translation (*NAT*) is a function of the Nortel VPN Router that can be used when connecting multiple private networks. It allows the combination of these networks to form an extranet without the need to reconfigure the existing address spaces. These networks can be combined using secure tunnels to form the extranet without concern of conflicting private address spaces, thus eliminating the need that all private addresses be unique across the entire extranet.

Following are two major factors for using NAT functionality:

- *IP Address shortage:* Internet service providers (ISPs) usually allocate one dynamically assigned address to each subscriber. This means that only one host computer may be connected to the Internet at a time. However, with the use of NAT, it is possible to share the single IP address with multiple computers, allowing them simultaneous access to the Internet. The resources on the Internet are aware of only the one assigned address, thus leaving them to believe they are communicating with a single computer.
- *Security:* Because NAT only permits the establishment of connections that originate on the private network, it provides a built-in security because connections from the public network are not allowed by default. However, services on the private network may be available to the public network with static mapping of internal addresses to addresses that are accessible from the public network. Thus, a Web server resident on the private network may be browsed from the Internet under control of the firewall.

Configuring Stateful Firewall

Use of the stateful firewall on the Nortel VPN Router requires the installation of a license key to enable the stateful firewall service. Without the stateful firewall enabled on the Nortel VPN Router, the only traffic forwarding allowed is:

- Private physical interface to private physical interface
- Private physical interface to user or BOTs
- Tunnel to tunnel including user and BOTs

With the stateful firewall enabled, the Nortel VPN Router will also permit routing of traffic from public to private interfaces.

Tunnel traffic rules must be created so that traffic on existing tunnels is allowed. The principle the Nortel VPN Router operates under is that traffic not specifically allowed is disallowed by default. The rules of the active policy are applied to all traffic, including tunneled and non-tunneled traffic. When the Nortel VPN Router's stateful firewall is first enabled, all traffic is disallowed until rules to allow certain traffic are configured. A good practice would be to enable the stateful firewall for the first time when there is low traffic volume on the Nortel VPN Router to minimize the inconvenience to users.

Configuration Prerequisites

The following information is required prior to configuring the stateful firewall on the Nortel VPN Router:

- *Management IP address of the Nortel VPN Router:* The address may be found on the SYSTEM → IDENTITY configuration screen.
- *Firewall license key:* Enter the key obtained from Nortel in the box provided for the stateful firewall license key on the ADMIN → LICENSE KEYS configuration screen, and click the Install button. The license key need only be entered once on the Nortel VPN Router. You can remove the key by clicking the Remove button on the line for the stateful firewall.
- *Host name assigned to the Nortel VPN Router:* This is the name contained in the DNS Host Name field of Domain Identity located on the SYSTEM → IDENTITY configuration screen.
- *Name and IP address of each of the Nortel VPN Router's interfaces:* These may be obtained by selecting the STATUS → STATISTICS menu and clicking the Interfaces button.

Stateful Firewall Manager System Requirements

Following are requirements for the Stateful Firewall Manager system:

- *Operating systems:* Supported operating systems are Microsoft Windows* and Solaris* on x86 or SPARC platforms.
- *Required software:* The Sun Microsystems Java 2 Plug-in, which allows applets written in the Java 2 Run-time Environment (J2RE) to run within Netscape and Internet Explorer. The J2RE is available for automatic download for Windows platforms on all Nortel VPN Routers except for NVR models 1010, 1050, and 1100. Installation files for J2RE for both Windows and Solaris are available on the CD provided with the NVR in the `tools/java` directory.
- *Browsers:* Supported browsers are Internet Explorer* and Netscape Navigator*.

NOTE The * indicates that in case of a question of supported versions, you should check the Nortel VPN Router documentation or call Nortel VPN Router Support.

Enabling Firewall Options

The following firewall options are available on the Nortel VPN Router:

- *Firewall:* Enables the stateful firewall feature. With the firewall enabled the following options are available and may be used in any combination:
  - Stateful Firewall
  - Interface Filter
  - Interface NAT
  - Anti-spoofing
- *No Firewall:* All firewall features on the Nortel VPN Router are disabled. In this mode, the Nortel VPN Router performs only VPN routing.

On the SERVICES → FIREWALL/NAT configuration screen, select the desired firewall options and then click the OK button at the bottom of the configuration screen. If the Firewall option has been enabled, the Nortel VPN Router must be rebooted before the firewall is active. Once the firewall is active, the firewall must be configured with rules to allow traffic to flow. A firewall license key is required to enable firewall features, except for the Interface Filter component, which does not require the license key for it to be enabled.

Enabling the Stateful Firewall Feature

The following is a brief description of the process required to enable and configure the Nortel VPN Router's stateful firewall:

1. From the SYSTEM → LAN configuration screen, click the Configure button and enter a Description name for each interface. This descriptor name will be used to identify the interfaces in the creation of the security policy rules.
2. From the SERVICES → FIREWALL/NAT screen select the stateful firewall feature and click the OK button at the bottom of the screen. A dialog box will appear at the top of the screen stating that the firewall will not take effect until a reboot. Click the Schedule System Reboot link in the dialog box. On the System Shutdown screen, ensure that System Shutdown Now is selected and click the OK button at the bottom of the screen for the reboot to occur.
3. After the Nortel VPN Router has rebooted, return to the SERVICES → FIREWALL/NAT configuration screen and click the Manage Policies button to load the stateful firewall applet. If this is the first time that this applet is loaded on the workstation, a prompt appears to load the Java applet. A dialog box appears with the message "Retrieving policy names."
4. Select the System Default policy and click the View button. The System Default policy is read-only and includes a predefined set of Implied Rules.
5. Toggling between the Stateful Firewall Manager applet screen and the Nortel VPN Router browser configuration screen is permitted. However, changes made in configuration will not be reflected on the Stateful Firewall Manager screen. To refresh the list of policies and other configuration settings, click the Stateful Firewall Manager screen and then click the Firewall icon in the upper-left portion of the screen. Changes made with the Stateful Firewall Manager applet do not appear in the Nortel VPN Router SERVICES → FIREWALL/NAT screen until the policy has been saved.
6. To exit the Stateful Firewall Manager screen, select the Manager drop-down menu and select Exit.
7. Return to the Nortel VPN Router browser screen at the SERVICES → FIREWALL/NAT configuration screen and click the Refresh button on the bottom of the screen. Only one policy may be in effect at a time. The policy that was just created is not automatically in effect. It must be selected from the drop-down Policy menu on the Stateful Firewall row. After the policy has been selected, click OK at the bottom of the screen. This named policy is now in effect.

Policies on the Nortel VPN Router are not able to be either exported or imported. However, there is no limitation on the number of policies that may be created. However, only one policy may be in effect at a given time.

Connection Limitation and Logging

Select SERVICES → FIREWALL/NAT and select the Edit button on the Stateful Firewall row to edit connection limits and logging options. Figure 7-1 illustrates this configuration screen.

To limit the number of connections, check the Enforce TCP Conversation Rules box and enter the number of connections allowed in the box labeled Maximum Connection Number. The value used is dependent upon the model of Nortel VPN Router that is being configured and the amount of memory it has installed. Because the firewall tracks conversations, it reserves memory in advance. With the determination of the optimum memory allocation, the Nortel VPN Router can be tuned to facilitate the anticipated firewall traffic.

Firewall activity can be logged into the Nortel VPN Router's event log and is controlled by the selection of the options available on the configuration screen illustrated in Figure 7-1. The options that may be selected are:

- *All:* Includes Traffic, Policy Manager, Firewall, and NAT.
- *Traffic:* Logs creation and removal of conversations and flows.
- *Policy Manager:* Logs the creation of rules and policies and firewall processes.
- *Firewall:* Logs the actions the firewall takes with packets within a flow.
- *NAT:* Logs events that are NAT related.
- *Debug:* This is for the logging of special messages intended for use by Nortel Customer Support personnel.
- *Implied Rule Log Level:* This option is used for logging information of the implied rules. The level of logging can be None, Brief, Detail, or Trap. The implied rules are used to control traffic that either is terminated or originated from the Nortel VPN Router.

Application-Specific Logging

Application-specific logging can be accomplished with the use of firewall rules. Figure 7-2 shows firewall rules for HTTP and FTP with logging enabled. Logging level may be brief or detailed.

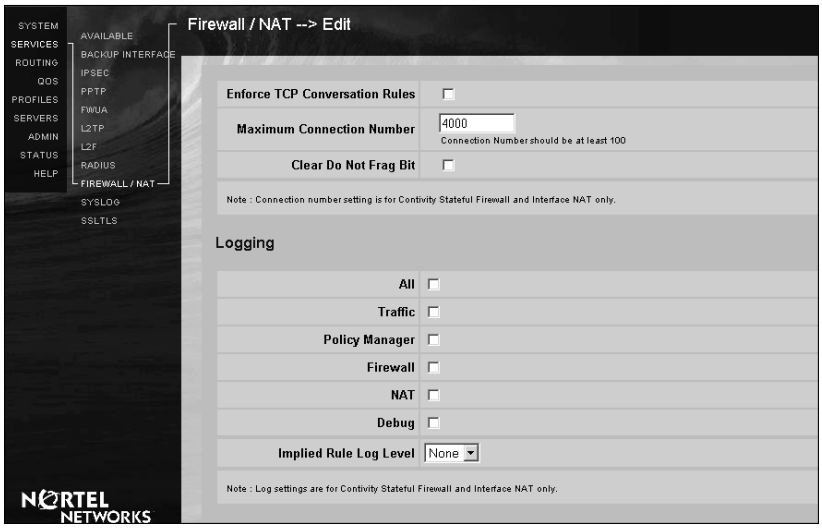


Figure 7-1: Connection Maximum/Logging configuration screen

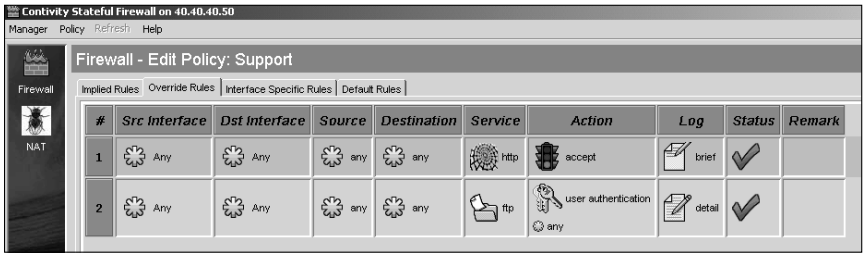


Figure 7-2: Application-specific logging

Application-specific logs for HTTP and FTP contain a unique connection identifier that allows events to be traced from start to end of that TCP session.

Firewall-specific logging includes logs of application-specific, denial-of-service attack, and the ability to send this logged information to a remote Syslog server.

Remote Logging of Firewall Events

Firewall-specific events can be sent to a remote server utilizing the syslog functionality of the Nortel VPN Router. Configuration of the logging to the Syslog server can include all events, or only firewall-specific events. The remote Syslog server can be configured by selecting SERVICES → SYSLOG to bring up the syslog configuration screen, as illustrated in Figure 7-3.

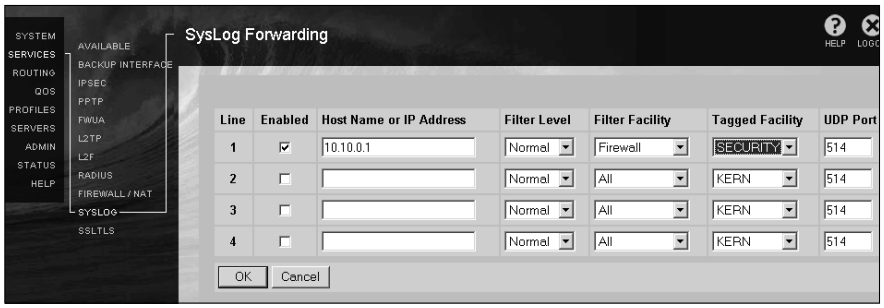


Figure 7-3: Remote Syslog server configuration

Enter a host name or the IP address for the remote Syslog server. Select Firewall for the Filter Facility and SECURITY for the Tagged Facility. The UPD Port is by default 514. However, if this differs from the remote Syslog server being used, then enter the appropriate port number used for the syslog function on that server. To verify the logging of firewall events, with the remote Syslog server running, initiate traffic through the Nortel VPN Router that will generate firewall events. Examine the remote Syslog server's logs to verify that the firewall events were captured and logged.

Anti-Spoofing Configuration

Anti-Spoofing can be configured from the SERVICES → FIREWALL/NAT configuration by checking the checkbox on the line for Anti-Spoofing and clicking the Edit button. Figure 7-4 illustrates the Anti-Spoofing configuration screen.

To enable Anti-Spoofing on a public interface, select the check box next to it and click OK. Anti-Spoofing may be enabled on each configured public interface.

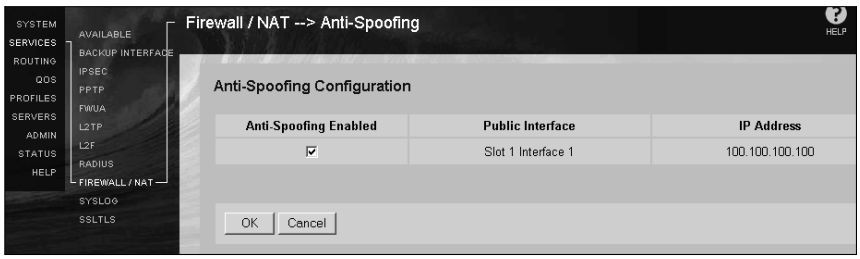


Figure 7-4: Anti-Spoofing configuration

Malicious Scan Detection Configuration

Malicious Scan Detection is configured by selecting SERVICES → FIREWALL/NAT and, on the Firewall/NAT configuration screen, by selecting the check box adjacent to the line for Malicious Scan Detection. Click the Edit button to bring up the Malicious Scan Detection configuration screen, as illustrated in Figure 7-5.

Following are the values that can be entered in the Scan Detector Configuration area:

- *Detection Interval:* This setting may be set from 1 to 60 minutes. This value is the interval setting over which the number of port or hosts scans is to be monitored. If the number exceeds the configured threshold setting, then the scan is logged to the security log.
- *Port Scan Threshold:* This value may be set from 1 to 10,000 and represents the number of allowable connections on the private interface that a hostile computer can send scan packets within the specified Detection Interval to trigger the event being logged to the security log.
- *Network Scan threshold:* This value may be set from 1 to 10,000 and represents the number of one-to-many connections/ports on the private interface that a hostile computer may send scan packet to within the Detection Interval to trigger the event being logged to the security log.

The values shown in Figure 7-5 are default values and may be modified to the environment in which the Nortel VPN Router is installed. After configuring the values for these fields, click OK to accept these values to be used for Malicious Scan Detection.

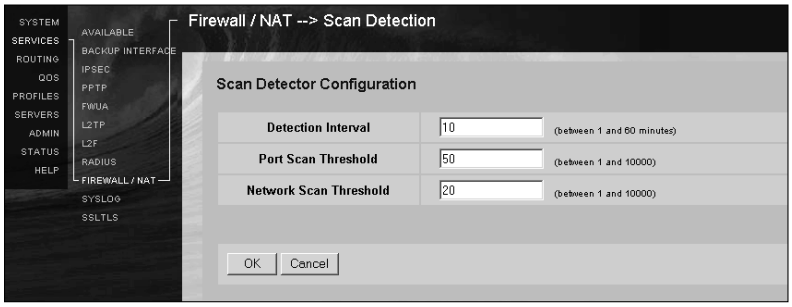


Figure 7-5: Malicious Scan Detection configuration

Firewall Policies

The two primary components to the Firewall Service are service properties and the security policy. *Service properties* are the services being offered, and include a service name, the protocol being used (for example, ICMP, UDP, or TCP), and a port number (or range of port numbers) that the service may be offered on. A *security policy* is a set of rules used to determine if a service is to be allowed or denied.

Service objects are used to define all the rule fields for a service policy. Each rule is a combination of network objects, services, actions, and logging mechanisms. Custom policies may be used when more complex security is required and the standard policies are insufficient. With customization the policies can be used to further refine control over traffic flow on the internal private network.

Firewall policies utilize standard actions that are represented in the commonly used policies. A specific security policy is defined by a set of rules. Each rule defines whether traffic should be accepted or rejected, and, if desired, logged based upon its source, destination, and service.

Rules for tunnel traffic must be created before traffic is allowed on previously configured tunnels. The Nortel VPN Router operates on the principle that whatever traffic is not specifically allowed is not allowed. The active policy rule set is applied to all traffic (which includes both tunneled and non-tunneled traffic). So, when the Nortel VPN Router stateful firewall is enabled for the first time, all traffic is not allowed until rules have been configured to allow desired traffic to flow.

Firewall Policy Creation and Editing

The Nortel VPN Router Graphical User Interface (GUI) or the Command Line Interface (CLI) may be used to implement access-control parameters. With use of either interface, the following may be configured:

- Network objects
- Service objects
- Rules

This chapter will be describing only the use of the browser-based GUI for policy/rule creation and editing. For use of CLI commands, refer to Nortel's *CLI Command Line Reference for the Nortel VPN Router* for a list of commands.

Policy Creation

From the SERVICES → FIREWALL/NAT configuration screen, click the Manage Policies on the stateful firewall line to bring up the Nortel VPN Router's Firewall Manager screen, as illustrated in Figure 7-6.

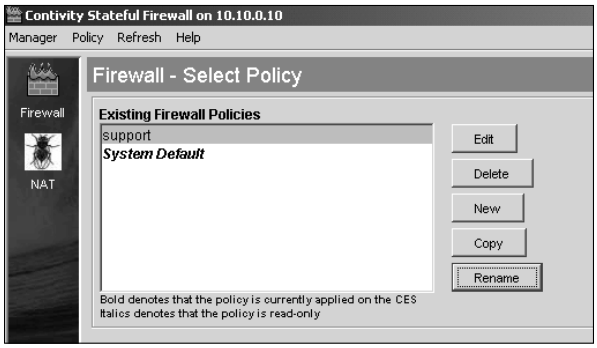


Figure 7-6: Firewall Select Policy screen

The Firewall Select Policy screen provides selections to create, edit, delete, rename, or copy a firewall policy. The currently applied Firewall policy on the Nortel VPN Router is denoted in bold, and the use of italics denotes policies that are read-only. You can see in Figure 7-6 that System Default is both bold and italicized, so it is a read-only policy (because it is the system default) and it is the currently applied policy. The System Default policy may not be deleted or edited, and is the policy that is in effect when no other policy has been created and applied.

Adding a Policy

A new policy may be added by clicking the New button, which brings up a dialog box where the name of the new policy may be entered. The policy name must begin with an alpha character and must not contain any characters that are not alpha or numeric (for example, -=+},;" characters). After the policy name has been entered, click OK to bring up the Policy Edit screen, which will display a blank firewall policy. If a new policy is not to be created at this time, click on the Cancel button to return to the firewall policy selection screen.

Deleting a Policy

Only policies that are not read-only or not currently applied may be deleted from the firewall policy selection screen. If one of these policies is selected, then the Delete button in not enabled. To delete a policy (which is neither read-only, nor currently in use), select the policy and click on the Delete button. A delete policy confirmation dialog box will appear and clicking OK button removes the selected policy.

Copying a Policy

To copy a firewall policy, select the policy to be copied and click the Copy button. A copy dialog box appears where the name of the policy being created using the copied policy is to be entered. After the name for the new policy has

been entered, click OK. The new policy name appears on the list of policies on the firewall policy selection screen, and will contain the same rules of the policy from which it had been copied.

Renaming a Policy

Renaming a policy can only be accomplished on policies that are not read-only nor currently applied on the Nortel VPN Router. If either of these are selected, the Rename button will not be enabled. To rename a policy, select it from the list of policies on the firewall policy selection screen, and click the Rename button. A Rename dialog box appears where the new name of the policy may be entered. Click OK and the renamed policy appears on the list of policies on the firewall policy selection screen.

Rules

With the Firewall Edit Policy screen, rules within a policy may be added, deleted, or modified. From this screen the following rule groups are available:

- Implied Rules
- Override Rules
- Interface Specific Rules
- Default Rules

NOTE **Creating a firewall rule under Interface Specific rules lists Slot 7 Interface 1, which is the serial port. For versions prior to 4.80, the serial port listing was not available on the Nortel VPN Router.**

Implied Rules

The firewall processes Implied Rules first. These rules allow for tunnel termination and access to the management interface. The rules are generated from SERVICES → AVAILABLE and other configuration screens, such as those for Router Information Protocol (RIP), Open Shortest Path First (OSPF), and Virtual Router Redundancy Protocol (VRRP). Some of the rules are statically generated and are illustrated in Figure 7-7. These are read-only because they are defined by configuration settings on the Nortel VPN Router.

Implied Rules cannot be modified, but are for display purposes only. The Nortel VPN Router Implied Rules are used to regulate traffic that has either originated from or is terminated by it. Routed traffic that is not directed to the Nortel VPN Router is controlled with the use of Override Rules, Interface Specific, or Default Rules.

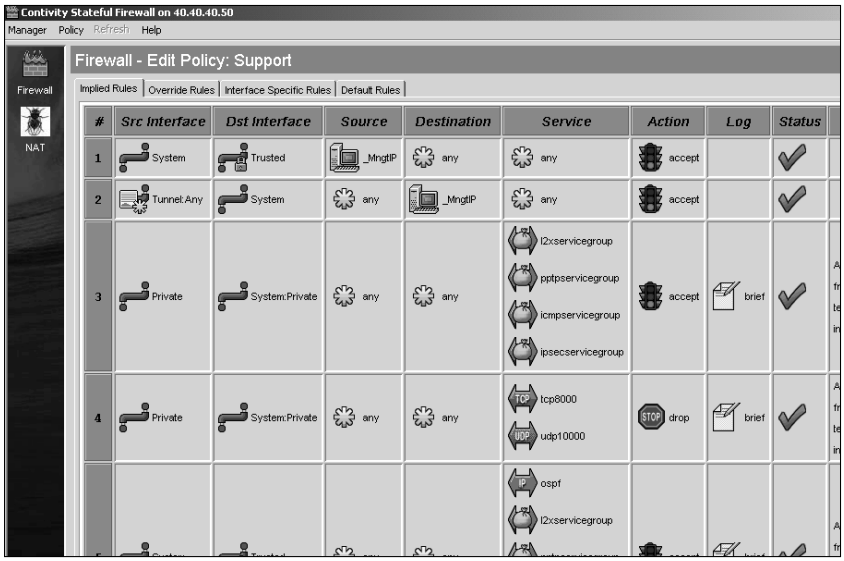


Figure 7-7: Implied Rules

Static Pre-Implied Rules

In the Implied Rules section, the first rule is the only one that is statically assigned. It is always in the Implied Rules section, no matter what configuration is placed on the Nortel VPN Router. This rule permits the listed services to be passed from the Nortel VPN Router to any of its private interfaces, as long as the service has originated from it. Table 7-1 lists the server types and the corresponding configuration screen for that service.

Table 7-1: Server Types and Corresponding Configuration Screens

SERVERS	CONFIGURATION SCREEN	DESCRIPTION
DHCP Relay	SERVERS → DHCP RELAY	Enable/Disable and configure DHCP Relay
DNS	SYSTEM → IDENTITY	Enable/Disable and configure DNS server
Remote-RPC	[not configurable]	UDP port 12185
Nbdatagram	[not configurable]	Remote Netbios
PPTP	SERVICES → AVAILABLE	Enable/Disable PPTP on public and/or private interfaces
IPSEC	SERVICES → AVAILABLE	Enable/Disable IPSec on public and/or private interfaces

(continued)

Table 7-1: *(continued)*

SERVERS	CONFIGURATION SCREEN	DESCRIPTION
L2TP & L2F	SERVICES → AVAILABLE	Enable/Disable L2TP and L2F on public and/or private interfaces
FWUA	SERVICES → AVAILABLE	Enable/Disable Firewall User Authentication on public and/or private interfaces
RADIUS	SERVICES → AVAILABLE	Enable/Disable RADIUS on public and/or private interfaces
HTTP, HTTPS	SERVICES → AVAILABLE	Enable/Disable HTTP/HTTPS on public and/or private interfaces
SNMP	SERVICES → AVAILABLE	Enable/Disable SNMP on public and/or private interfaces
FTP	SERVICES → AVAILABLE	Enable/Disable FTP on private interface
TELNET	SERVICES → AVAILABLE	Enable/Disable TELNET on private interface
CRL	SERVICES → AVAILABLE	Enable/Disable CRL on public and/or private interfaces
CMP	SERVICES → AVAILABLE	Enable/Disable CMP on public and/or private interfaces
LDAP	SERVERS → LDAP	Enable/Disable and configure LDAP server
UDP Wrapper	SERVICES → IPSEC (IPSec Settings)	Enable/Disable NAT Traversal UDP configured port
NTP	SYSTEM → DATE & TIME Network Time Protocol	Enable/Disable and configure NTP service
VRRP	ROUTING → VRRP	Enable/Disable & configure VRRP routing protocol
RIP	ROUTING → RIP	Enable/Disable & configure RIP routing protocol
OSPF	ROUTING → OSPF	Enable/Disable & configure OSPF routing protocol

Dynamic Implied Rules

All the configured services from the SERVICES → AVAILABLE configuration screen generate the Dynamic Implied Rules. For those services that do not use well-known ports, the Implied Rules name consists of the protocol and the

port number. An example would be a `tcp10` rule, which is generated from ports associated with external LDAP, RADIUS servers, and configurable Firewall User Authentication (FWUA) ports.

Override Rules

The first set of modifiable rules in a policy is the Override Rules. An illustration of an Override Rule is shown in Figure 7-8.

The purpose of the Override Rules is to quickly override all the rules described in the policy. This may be useful to apply an override rule for a short period of time so that an issue may be debugged. With Override Rules, there is no source or destination interface specified. Only interface groupings may be selected, such as Any, Trusted, Untrusted, or Tunnel:Any.

Interface Specific Rules

Packets that enter or leave through one specific interface of the Nortel VPN Router (whether it is a physical interface or a tunnel) are controlled with the use of Interface Specific Rules. There are two types of Interface Specific Rules: source rules and destination rules. Figure 7-9 illustrates an Interface Specific Source Rule and Figure 7-10 illustrates an Interface Specific Destination Rule.

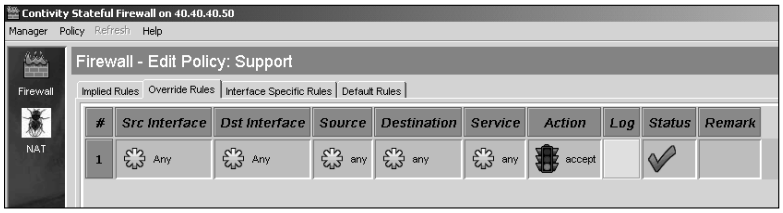


Figure 7-8: Override Rules tab

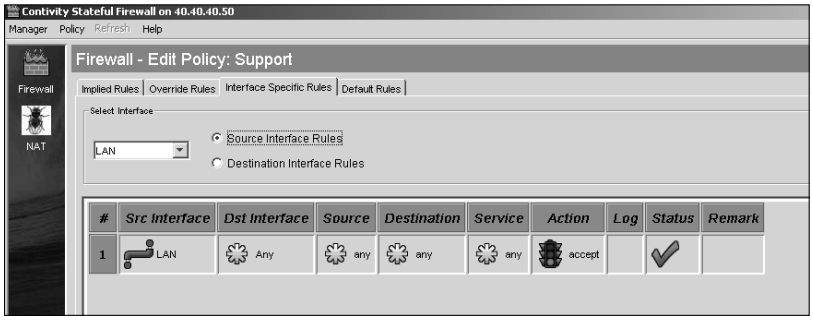


Figure 7-9: Interface Specific source rule

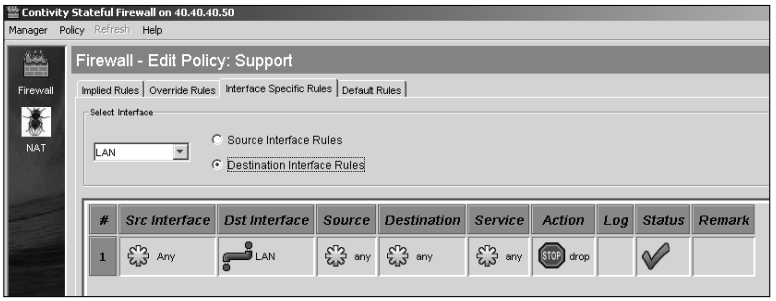


Figure 7-10: Interface Specific destination rule

Source rules define the selected interface as the source, while *destination rules* define the selected interface as the destination. The names of physical interfaces correspond to the names they were given when the interfaces were configured using either SYSTEM → LAN or SYSTEM → WAN configuration screens. Tunnels also are considered interfaces of the Nortel VPN Router and consist of both user tunnels and BOTs. Tunnel interface names are the group name in the case of user tunnels and the name assigned to a BOT at the time it was configured. The Interface Specific Rules section of a policy displays only a single interface at a time. However, all Interface Specific Rules may be viewed by selecting All Interfaces from the Select Interface drop-down menu.

Default Rules

Default Rules are policy rules that are applied to all traffic and not restricted to any specific interface. These rules use interface groupings such as Any, Trusted, Untrusted and Tunnel:Any in the specification of the source and destination fields. Figure 7-11 shows an illustration of the Default Rules.

Rule Creation

Actions required for rule creation are controlled by menus that are accessed by right-clicking on any particular option. Each menu controls a different aspect of the rule.

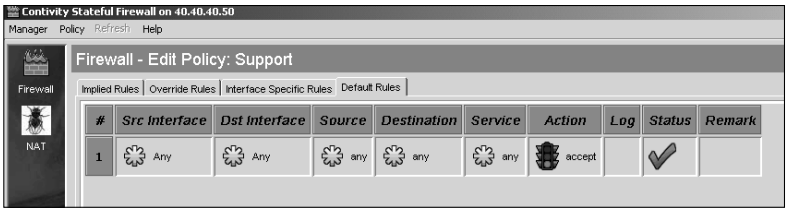


Figure 7-11: Default Rules

Header Row Menu

Right-clicking on any particular header cell will cause the Header Row menu to appear. There is only one item to be selected on this menu and that is Add New Rule. Selecting this menu item causes a new rule to be added to the top of the list. Because this rule appears in the rule one position, all existing rules have their positions incremented by one.

Row Menu

Right-clicking on any particular row number next to an existing rule causes the Row menu to be displayed. This menu allows for the insertion of a new rule either before or after the rule that the row number was right-clicked on. It also allows the selected rule to be deleted, copied, or cut. The cut operation allows for the removed rule to be pasted back in a different position by right clicking on a rule row number to bring up the Row menu. The cut rule can then be pasted in either before or after the selected rule row. Figure 7-12 shows an illustration of a Row menu.

Cell Menus

Cell menus are cell-specific menus and are displayed by right-clicking on any one particular cell. There are two types of Cell menus: an option menu and a procedure menu. *Option menus* display a list of various options that will vary, depending on the type of cell being selected. The options for the cell are displayed in a drop-down menu and may be selected by clicking on the option. The selected option will be inserted into the cell position, as illustrated in Figure 7-13.

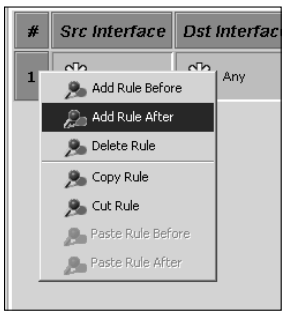


Figure 7-12: Row menu

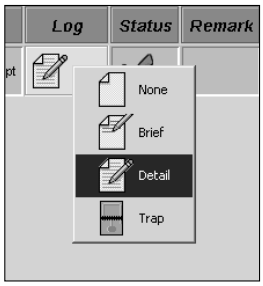


Figure 7-13: Cell Option menu

A Cell Procedure menu provides a list of operations that may be performed on a cell. These include Add, Edit, Remove, Copy, and Cut. When one of the operations is selected, it is either performed immediately (as is the case with the Copy operation), or an additional dialog box appears requesting additional information (as is the case with the Add operation). Figure 7-14 shows an illustration of a Cell Procedure menu.

Rule Columns

Rule column headers specify the attributes contained within each section of a firewall policy. All rules with a policy have the same attributes. These attributes are as follows:

- #
- Src Interface
- Dst Interface
- Source
- Destination
- Service
- Action
- Log
- Status
- Remark

#

This column indicates the position value of the rule. It is used to maintain the order of rules. It applies only to the rules within the section that is being currently displayed, and has no bearing on rule order in any other rule section of the policy. If logging is enabled for a rule, the rule number represented in the # column for that rule will be contained in the log information.

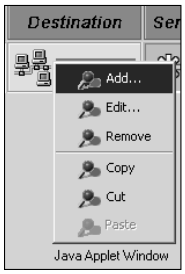


Figure 7-14: Cell Procedure menu

Src Interface / Dst Interface

These columns are used to specify the source and destination interfaces to be used for the rule. Right-clicking on one of these cells displays a list of interface options. The options that are available on the drop-down menu are dependent on which section of the firewall policy is being displayed. Only interface groupings are displayed for the Override Rules and Default Rules sections. Following is a listing of interfaces:

- *Any:* Any tunnel or physical interface
- *System:* Management interface
- *Trusted:* Any tunnel or private physical interface
- *Untrusted:* Any public interface
- *Tunnel:Any:* Any tunnel (all physical interfaces are excluded)

Figure 7-15 illustrates an example of a rule column.

Rule columns for Interface Specific Rules may contain interfaces that are either interface groupings, or individual interfaces that may be either tunnel or physical interfaces. Figure 7-16 illustrates an example of a rule column for an Interface Specific Rule.



Figure 7-15: Rule column

When a User Tunnel is selected from the list of options of an Interface Specific column rule, a tunnel selection dialog box is displayed. This allows a particular user group to be selected. This tunnel interface will consist of all the users within that group that are authorized to tunnel to the Nortel VPN Router. Figure 7-17 illustrates an example of the user tunnel selection dialog box.

When a Branch Tunnel is selected from the list of options of an Interface Specific column rule, a tunnel selection dialog box is displayed. This allows for the selection of a particular BOT for the Branch Tunnel interface. Figure 7-18 illustrates an example of the BOT selection dialog box.

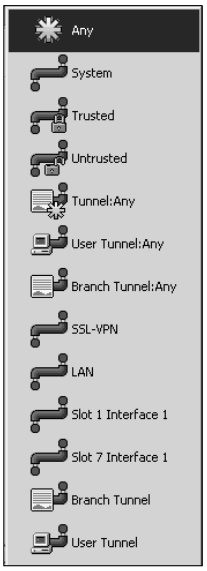


Figure 7-16: Interface Specific rule column

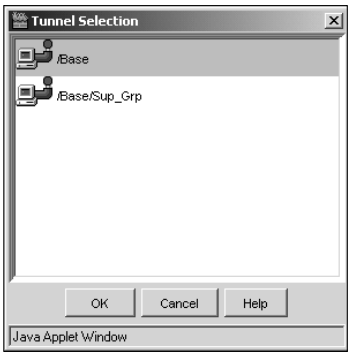


Figure 7-17: User tunnel selection

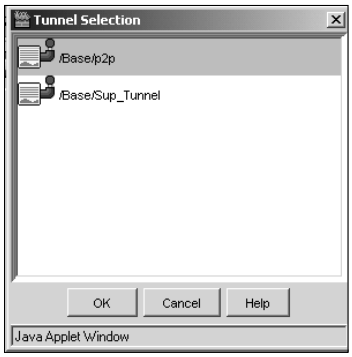


Figure 7-18: BOT selection

Source/Destination

These columns are used to designate the source and destination network objects to be used for the rule. These objects may be modified by right-clicking on a cell within one of these columns, which will cause a procedure menu to be displayed. More than one source or destination address may be added to a rule.

Selecting the Add option displays a Network Object Selection dialog box (see Figure 7-19). With the use of this box, a new network object may be defined and applied. The following network objects may be created: host, network, IP range, and group (which may include a collection of any of these objects). The `NOT` operand may be used to specify those networks that are not to be included within the group.

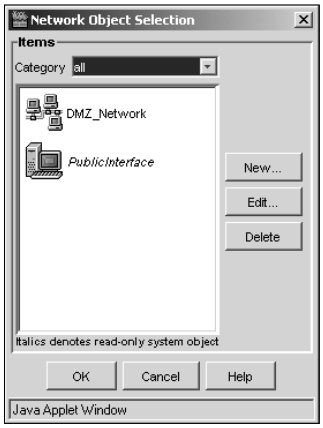


Figure 7-19: Network Object Selection dialog box

Objects that are italicized in the Network Object Selection dialog box are read-only and cannot be modified. Modifiable network objects may be edited with use of the Edit button, or removed by selecting the Delete button. If the object to be removed is the last object, then it reverts back to an object with default values. New network objects may be created by selecting the New button.

Selecting a network object that is modifiable and clicking on the Edit button displays a Network Object Edit dialog box (see Figure 7-20). The object's attributes may be modified and accepted on completion by clicking OK.

Network objects are also allowed to be copied, cut, and pasted using the object that is currently selected.

Service

The Service column specifies the service objects that the rule is being used to control. When the cell is right-clicked, the standard procedure menu with Add and Edit is displayed.

Selecting Add displays the Service Object Selection dialog box (see Figure 7-21), which is used to define and apply a new service object to the rule. The following service objects may be created: TCP, UDP, ICMP, IP protocols, and a group object (which is a collection of these objects). A rule may contain more than one service.

Objects in the Service Object Selection dialog box that are italicized are read-only and are not modifiable. Selection of the New button allows for the creation of service objects, while the Delete button is used to remove the currently selected service object from the dialog box. If the service object to be removed is the last object in the cell, then it will revert to its default value. To modify an existing service object, select it and click the Edit button. The attributes of the selected service object may be altered in the edit box that is displayed. Figure 7-22 shows an example of a service dialog edit dialog box.

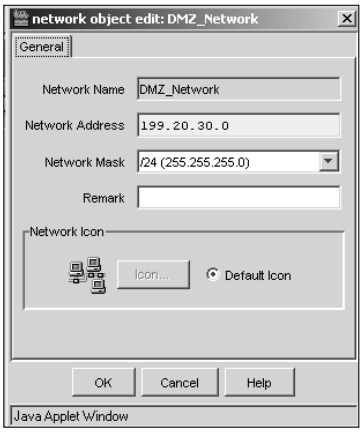


Figure 7-20: Network Object Edit dialog box

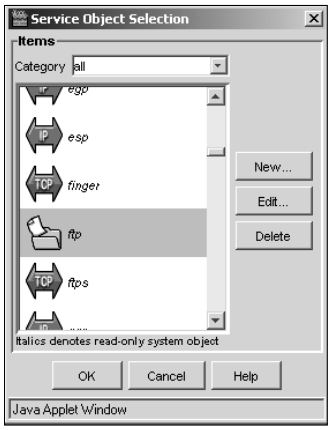


Figure 7-21: Service Object Selection dialog box

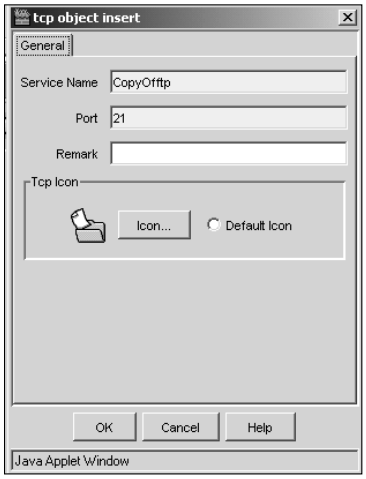


Figure 7-22: Service object edit dialog box

Service objects can also be copied, cut, or pasted using the operations of Copy, Cut, or Paste on the currently selected object.

Action

The Action column specifies the action the rule is to take when the rule has been activated. Right-clicking on a cell in this column displays an option list with the selections for Accept, Drop, Reject, and User Authentication. User Authentication requires a user to enter a user ID and a password. The desired action may be selected by highlighting and clicking it. Figure 7-23 shows an example of an Action menu.



Figure 7-23: Action selection

Log

The logging level of a rule may be set using the Log column for its selection. Right-clicking on a cell in this column causes an option list to be displayed. The selections on the Log menu for logging levels are None, Brief, Detail, and Trap. Figure 7-24 shows an example of Log options.

Status

Right-clicking a cell in this column allows for the status of the selected rule to be set. A rule status may be either Enabled or Disabled. Figure 7-25 shows an example of a Status menu.

Remark

Right-clicking a cell in this column allows for the attachment of a remark to a particular rule. An option menu appears with the selection to Edit a remark. When selected, a Policy Rule Remark dialog box is presented and allows for the entry of a new remark, or for an existing remark to be cleared or edited.

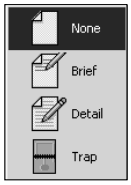


Figure 7-24: Log option selection



Figure 7-25: Status selection

Creating a New Policy

The following process provides the basic steps required in the creation of a new policy:

1. Log on to the Nortel VPN Router with an administrator user ID and password. Select SERVICES → FIREWALL/NAT to display the firewall Configuration screen.
2. On the Configuration screen select the radio button adjacent to the Firewall.
3. On the row for the stateful firewall, click the Manage Policies button. A login dialog screen will appear to enter the Administrator user ID and password. The Firewall Select Policy window will appear.
4. To create a new policy, click the New button. A New Policy dialog box will appear where a policy name is to be entered. The policy name must begin with an alpha character and not include the characters +=],;". After the name has been entered click OK to accept the name.
5. The "Firewall: Edit Policy: <entered Policy Name>" message is displayed with no rules defined. This screen is used to add, delete, and modify rules for this policy.
6. Any of the following rule groups may be selected:
   a. Implied Rules (Read Only)
   b. Override Rules
   c. Interface Specific Rules
   d. Default Rules
7. Select the Interface Specific Rules tab.
8. Select an interface and a sub-interface from the appropriate Select Interface drop-down menu.
9. Select either the Source Interface Rules or Destination Rules radio button for the rules to be added.
10. Right-click the cells to modify the selected options and actions desired for the rule.
11. These steps may be repeated as many times as necessary to enter all of the desired rules for this policy.

12. After all rule entry has been completed, click the Policy drop-down menu and select Save Policy to save rules changes and additions.
13. After the save policy has completed, the Firewall Manager screen is closed by selecting the Manager drop-down menu and selecting Exit SF/NAT.

The successful completion of the preceding steps indicates that the Nortel VPN Router's firewall is operational and that the configured routing options are available.

Firewall Configuration Verification

When the configuration tasks for the firewall have been completed, the Nortel VPN Router's routing patterns should be verified. To ensure that the firewall is functioning properly, the following suggested procedure is recommended:

1. Verify that the firewall is using a security policy that allows the type of traffic that is being used for the test. If needed, an Accept All policy may be used for purposes of conducting the test.
2. Verify public-to-private traffic. This can be done using a service such as FTP from a host on the public side of the Nortel VPN Router to a host on its private side.
3. Verify private-to-public traffic. This can be done using a service such as FTP from a host on the private side of the Nortel VPN Router to a host on its public side.
4. Verify tunnel-to-internal network traffic. This can be accomplished by configuring a tunnel on another Nortel VPN Router to connect to the Nortel VPN Router that is under test. When the tunnel has been successfully established, use a PC located on the private network of the remote VPN Router to access a Web page from a Web server that is connected to the local VPN Router's private network.
5. Verify tunnel-to-Internet traffic. Use a PC with the Nortel VPN Client loaded on it to establish a user to the Nortel VPN Router that is under test. From the client PC, access a Web server on the Internet.

Sample Security Policy Configuration

For this sample configuration, the following assigned interfaces and IP addresses will be used:

- Public IP address 172.16.10.11 (Internet)
- Private IP address 192.168.15.208 (LAN)
- FTP server IP address 172.16.10.12

The security policy only allows users to access the FTP server to download files without any other access to the Internet being permitted.

The following is a description of a procedure required to implement a security policy on the stateful firewall:

1. Select SERVICES → FIREWALL/NAT to display the firewall Configuration screen. On the stateful firewall row, click the Manage Policies button.
2. Enter the Administrator user ID and password. Click Yes to bring up the Firewall Select Policy window.
3. Click the New button to display the New Policy dialog box. Enter the name **FTP_Access** and click OK.
4. On the Firewall Edit Policy screen, select the Interface Specific Rules tab.
5. Select the Source Interface Rules radio button to make changes to the interface or sub-interface. Select Interface drop-down menus.
6. Right-click the # column box and select Add New Rule.
7. The Dst Interface cell for the new rule has the default value of Any. Right-click the cell and select SSL-VPN.
8. The Destination cell for the new rule has the default value of Any. Right-click the call and select Add.
9. The Network Object Selection dialog box will appear. Click the New button.
10. The Network Object Type Selection dialog box appears. Select "host" as the type of object to create and click OK.
11. The host object insert dialog box will appear. In the Host Name field enter the name for the host. In this example, enter **Big_FTP_Server**. In the IP Address field, enter the IP address for the host. For this example, enter the address **172.16.10.12** and click OK.
12. The Network Object Selection dialog box will again appear. Click OK to add the Big_FTP_Server network object into the Destination cell.
13. The Service cell for the new rule has the default value of Any. Right-click on the cell, and then select Add to display the Service Object Selection dialog box. Scroll down to find and select the selection for "ftp." The services are listed alphabetically. When "ftp" is selected, click OK.
14. The Action cell for the new rule has the default value of "drop." Right-click the cell and click the Accept action to enter it in the cell.
15. The Log cell of the new rule has no value (blank) assigned to it by default. Right-click the cell to display the Log selection menu. For this example, select Brief and click to enter it in the cell.

16. The Status cell of the new rule has the default value of being enabled (checkmark symbol). The status field may be changed by right-clicking the cell. The options are a checkmark for Enabled and X for Disabled. For this example, the rule is to be enabled.
17. Click the Manager drop-down menu and select Exit SF/NAT. A dialog box appears to confirm exiting the firewall manager. Click the Yes button. A dialog box appears asking to save changes. Click the Yes button.
18. Select SERVICES → FIREWALL/NAT to display the firewall Configuration screen. Click the down arrow on the Policy drop-down menu to display the list of available policies. Select the rule FTP_Access. Only a single policy may be applied to the Nortel VPN Router.

NOTE If the policy that was created does not appear in the Policy drop-down menu, refresh the browser window.

19. Ensure that the Firewall radio button is selected for Enabled and that the Stateful Firewall checkbox is selected. Click OK at the bottom of the firewall configuration screen. A prompt to reboot to activate the new policy on the Nortel VPN Router will appear. After the reboot, the new policy will be in effect.

The new policy is shown in Figure 7-26 as it is displayed in the Firewall Edit Policy window.

Firewall Examples

Security policies are customizable and may be applied to either individual subscribers, or as a template to be applied to many subscribers.

The following should be considered in the creation and application of firewall rules:

- List the IP addresses for all servers that are to be accessible through the firewall. These servers/hosts may include FTP, DNS, Web, mail, and other application servers.
- If NAT is to be used, list the IP addresses that should be available and that normally would not be accessible.
- List other applications that are not part of normal network traffic that will be passing traffic through the firewall.

Residential Example

The normal operating environment for a residential firewall is that, in general, it is designed to allow user-initiated traffic on the private network to access resources on the Internet while blocking all incoming traffic and port scans.

This type of configuration can be accomplished with either an Override Rule or an Interface Specific Rule. In either case, the Dst Interface, Source, Destination, and Service are all set to Any. The Src Interface for the Override Rule is set Trusted, while on the Interface Specific Rule the radio button for Source Interface Rules is selected and the Select Interface drop-down menu is set to LAN. The cell for Src Interface will also be displaying LAN as the selected interface.

Either rule will permit users on the private protected network access to the Internet while preventing traffic from the public network access to the private network. Remember, allowed traffic must be enabled explicitly because the Nortel VPN Router's firewall by default implicitly denies all traffic.

Business Example

In a business environment, a firewall requires a more complex set of rules. A user in this environment will need access to internal sources such as mail and Web servers. Depending on the required services, choices will have to be made for which protocols are to be accepted or rejected by the firewall. The usual protocols will include HTTP, SMTP, FTP, and any necessary network protocols (such as ICMP). Figure 7-27 illustrates a typical business firewall environment.

Override Rules must be set when configuring a firewall in a business environment. The following criteria should be considered:

- Prior to accessing resources on the internal private network, branch office users must be authenticated.
- User tunnel traffic should be permitted to go anywhere.
- Non-tunneled traffic for FTP and HTTP should be allowed to gain access to these servers located in the DMZ.

Along with these Override Rules, an Interface Specific Rule must be created that will allow all traffic that enters the Nortel VPN Router from the private LAN to go anywhere. Figure 7-28 illustrates the firewall rules that meet the required criteria.



Figure 7-26: The Firewall Edit Policy window

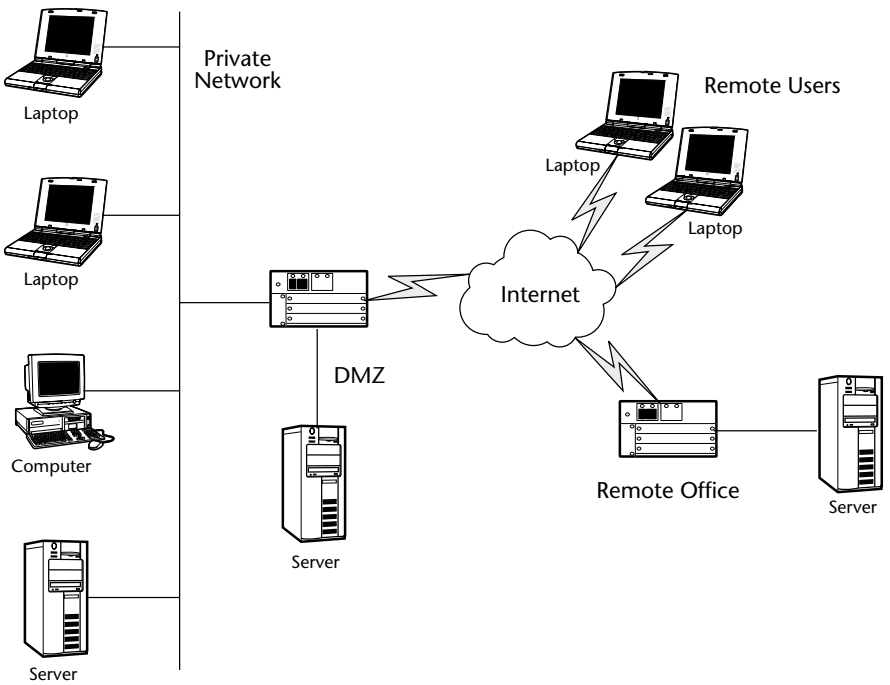


Figure 7-27: Business firewall environment

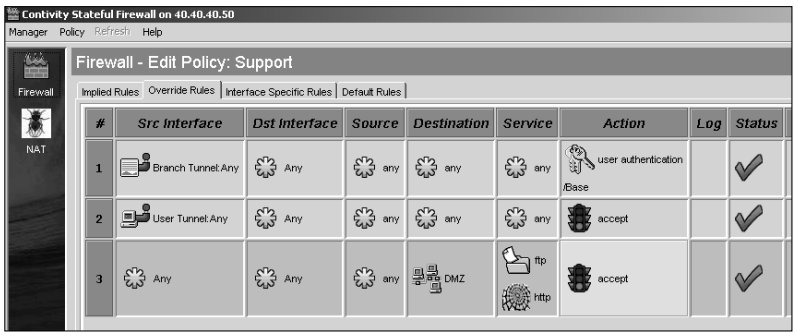


Figure 7-28: Business Override Rules

Filters

The Nortel VPN Router utilizes *tunnel filters* to manage users within a group and *interface filters* to control traffic that enters or leaves a LAN or WAN interface. Tunnel filters do not take effect while a tunnel is established. For the changes applied to a tunnel filter to have an effect on the tunnel traffic, the tunnel will need to be re-established.

Select PROFILES → FILTERS to display the Filters configuration screen. This screen displays the Current Tunnel Filters and the Current Interface Filters. A filter is usually made up of one or more inbound rules to control traffic coming in to the network, and one or more outbound rules to control traffic that is leaving the network. Naming filters is a means of aiding in the management of a set of filter rules.

Adding / Editing Filters

To add or edit an existing filter, select PROFILES → FILTERS to display the Filters configuration screen. If editing an existing Tunnel Filter, select the filter name by clicking it and then clicking the Edit button. A new filter is created by entering the name for the Tunnel Filter and then clicking the Create button. Clicking either the Edit or Create button will display the Tunnel Filters Edit screen, as illustrated in Figure 7-29.

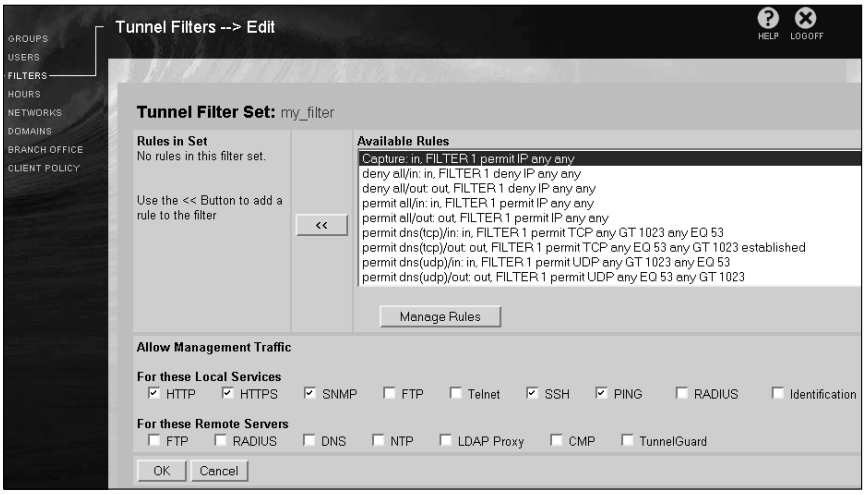


Figure 7-29: Tunnel Filter Edit screen

Rules are added to the filter set by selecting the rule from the list of Available Rules on the right, and clicking the << button to add the rule to the named Filter set being created or edited. Rules are entered into the filter set in the order they are selected. Rules may be moved to different positions in the Filter set by selecting the rule in the filter set, and then clicking the up arrow to move the rule up in the order, or by clicking the down arrow to move the rule down in order.

The list of Available Rules is all the rules that are available on the Nortel VPN Router to add to a filter set. They are displayed using the format "Name: rule string." Clicking the Manage Rules button displays the list of Current Rules that may be edited, deleted, or copied. New rules many be created on this screen and added to the Current Rules list by clicking the Create button. To exit the Manage Rules screen and return to the Edit screen, scroll to the bottom of the page and click the Close button.

The Allow Management Traffic portion of the Edit screen is only applicable to tunnel filters and does not appear on the Edit screen for interface filters. Management access to the Nortel VPN Router through tunnels may be controlled and restricted using the Allow Management options. By specifying the management services allowed through a tunnel, you have control of which groups of users are permitted to perform various management tasks while tunneled to the Nortel VPN Router.

The Nortel VPN Router's default filter is Permit All, which allows HTTP, SNMP, and PING. However, if a new filter is created, all management traffic settings are disabled by default.

The Allow Management Traffic options are divided into two groups: Local Services and Remote Servers. Local Services options are for those services that reside on the Nortel VPN Router. Remote Servers options are for services that reside on other systems that the Nortel VPN Router uses. When enabled, network traffic for these services is permitted through tunnels. These management services apply to both user and BOT connections. The selection of these options has no effect on HTTP, SNMP, FTP, Telnet, and PING protocol traffic, which is being passed through the Nortel VPN Router outside of a tunnel.

Following are Local Services that may be selected:

- *HTTP:* Permit/disallow access to the Nortel VPN Router's internal Web server.
- *HTTPS:* Permit/disallow remote HTTPS access to the Nortel VPN Router.
- *SNMP:* Permit/disallow SNMP gets from the Nortel VPN Router.

- *FTP:* Permit/disallow FTP puts or gets to or from the Nortel VPN Router.
- *Telnet:* Permit/disallow Telnet access to the Nortel VPN Router.
- *SSH*: Permit/disallow remote SSH access to the Nortel VPN Router.
- *PING:* Permit/disallow PING access to the Nortel VPN Router.
- *RADIUS:* Permit/disallow access to the Nortel VPN Router's RADIUS authentication service.
- *Identification:* Permit/disallow access via identification services.

Selection of the Remote Server options permits access to services provided by these servers through a tunnel. The Nortel VPN Router can be configured to restrict which tunnels will carry the protocol traffic for the services that are provided by these servers. The following is a list of servers that access may be permitted to through a tunnel:

- *FTP:* Allow/disallow FTP access from the Nortel VPN Router to FTP servers located at the remote end of a tunnel. FTP is used for backup and software upgrades and is an example of the use of external services.
- *RADIUS:* Allow/disallow the Nortel VPN Router's ability to access a remote RADIUS server.
- *DNS:* Allow/disallow remote users from using the Domain Name Server (DNS) service for the Nortel VPN Router.
- *NTP:* Allow/disallow access to the remote Network Time Protocol (NTP) server.
- *LDAP Proxy:* Allow/disallow access to external LDAP Proxy server.
- *CMP:* Allow/disallow access to a remote Certificate Management Protocol (CMP) server.
- *TunnelGuard:* Allow/disallow TunnelGuard traffic.

Use the Copy Filter buttons (up arrow from Interface Filters to Tunnel Filters, and the down arrow for from Tunnel Filters to Interface Filters) to copy a filter set from one to the other.

An example of how this may be used is if a Tunnel Filter has been created and you wanted to use it as an Interface Filter on the Nortel VPN Router. This is accomplished by highlighting that particular rule and clicking the down arrow button. A Copy Filter confirmation screen will appear asking if the named filter is to be copied from Tunnel Filters to Interface Filters. To confirm the selection, simply click OK to accept it, or, if a selection was made in error, click the Cancel button to reject it.

Next Hop Traffic Filter

Next Hop traffic filters are used to control the next hop selection and route traffic within their domain. When a packet matches the filter criteria, a forwarding lookup is performed using the configured next hop, and is forwarded based on that routing table instance. If the lookup fails, traditional destination-based routing occurs using the routing table.

IP interfaces may have inbound and/or outbound filters. These filters initiate a particular action to be taken on packets that match the filter's criteria. When a packet matches the criteria of a filter that is configured with Next Hop, the filter accepts the packet and uses the next hop for forwarding. Table 7-2 shows an example of a Next Hop filter rule.

In the Next Hop Filter rule shown in Table 7-2, the packets matching the criteria are forwarded to the next hop address of 204.198.68.211. Packets arriving at the interface from the 192.168.0.0 network and destined for the 199.200.169.0 network are forwarded to the next hop address. There is an assumption that the next hop address is a reachable route. If the route in non-reachable, then the destination in the IP header for the packet is used and normal routing is used to forward the packet.

For tunnel traffic, the next hop address should be an address that is beyond the remote endpoint address of the tunnel. However, the address used for the next hop must be an address that is on the path that leads to the destination.

To configure Next Hop traffic filters, select PROFILES → FILTERS to display the Filters configuration screen. Select the filter rule that is to be edited and click the Edit button. When the Edit Rules screen is displayed, click the Nexthop radio button on the Filter Action line. The screen will update with the fields to be used to configure the Next Hop Filter rule, as illustrated in Figure 7-30.

To enable private network to tunnel traffic forwarding, select SYSTEM → FORWARDING. When the Forwarding configuration screen is displayed, scroll down to the Next Hop Forwarding portion of the screen and check the box labeled "Apply Packet Filter on Private to Tunnel Traffic" to enable it, and then click OK to apply this feature.

Table 7-2: Next Hop Filter Rule

SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	ACTION	NEXT HOP ADDRESS
192.168.0.0 (255.255.0.0)	199.200.169.0 (255.255.255.0)	IP	Next hop	204.198.68.211

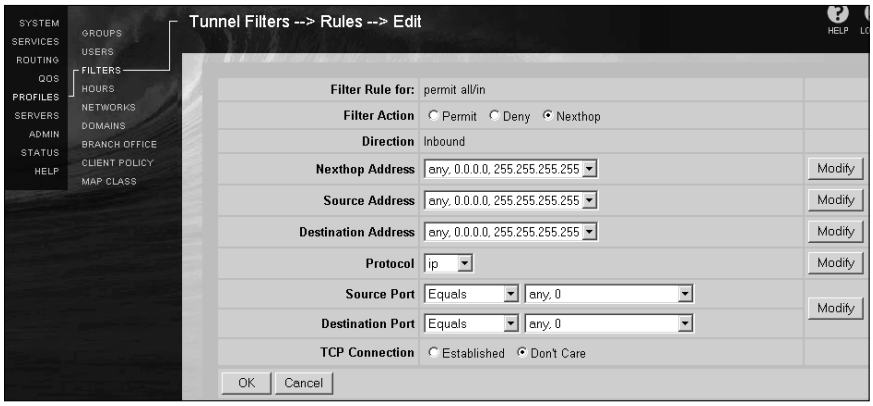


Figure 7-30: Next Hop Filter rule edit

NAT

Network Address Translation (NAT) allows ports on the private network to access the Internet using one or more globally unique IP addresses. With the use of NAT, multiple intranets with conflicting IP address space are able to communicate. With the configuration of BOTs, IP traffic is securely routed between these private networks without requiring that they need to have unique IP address space across the entire extranet.

NAT uses a pool of available global addresses that are continually reused. This allows a network to use one set of network addresses for internal networks and another set of different network addresses when dealing with external networks. The internal network addresses that are used are allocated with consideration of the internal network. The global addresses that are used must remain unique to allow for different hosts to be distinguished from one another.

When a packet is routed from the private address space to the public address space, NAT replaces the internal private address with a global address. Once an application session using the NAT has ended, the global address is returned to the pool for use by subsequent connection requests. NAT may also be used to modify the source and destination ports on a packet.

Types of Address Translation

Address translation may be configured as permanent (static), or dynamically allocated to allow many devices on the internal private network to share a few IP addresses. With static translation, one external host address is allocated for each internal address that is converted to a different global IP address. With dynamic address translation allocation of addresses occurs when a session is first started. There is no preset one-to-one mapping with dynamic address translation.

An example of dynamic translation is port mapping. *Port mapping* utilizes the TCP/UDP source port and source address to allow multiple sessions from many private hosts to connect out to the Internet using a single public NAT address. The Nortel VPN Router supports the following address translations:

- Dynamic Many-to-One
- Dynamic Many-to-Many
- Static One-to-One
- Port Forwarding
- IPSec Aware NAT
- Double NAT

Dynamic Many-to-One NAT

Network Address Port Translation (*NAPT*) allows many devices with an internal private IP address to be hidden behind a single external public address by using ports that are dynamically assigned to differentiate between the addresses. This type of translation is especially useful in situations where several IP address are required, but only one IP address has been allocated by the ISP. Dynamic Many-to-One translation can only be used where the traffic is initiated from an internal private host.

When a request from an internal host on private network is presented to NAT, it attempts to assign a port from a corresponding port list. If the port on which the request was made is available, then that port is assigned to the packet. If the requested port is not available, NAT attempts to assign a port from the largest port number that is smaller than the original requesting port. If all ports that are smaller are unavailable, NAT assigns a port that is greater than the requested port. If there are no ports available, then the packet is dropped.

Figure 7-31 illustrates a Dynamic Many-to-One configuration. The internal private network behind the Nortel VPN Router is set at 192.168.32.0 with a 28-bit subnet mask, which is 255.255.255.240. This allows addresses 192.168.32.1 through 192.168.32.14 to be used for the NAT rule.

Table 7-3 shows an example of two PCs on the internal private network making page requests of a Web server over the Internet. PCs at 192.168.32.1 and 192.32.32.5 send a Web page request to the server 204.32.232.19 using port 80 as the destination address and port. Table 7-3 shows how the packet is modified by NAT with a dynamic port allocated to track the connection. When the packet arrives at the Web server, it uses the NAT source address and port to respond to the request. When the response packet is received by the Nortel VPN Router, it uses the dynamically assigned ports to return the packet to the original requesting PC on the same address and port that the original request was made on.

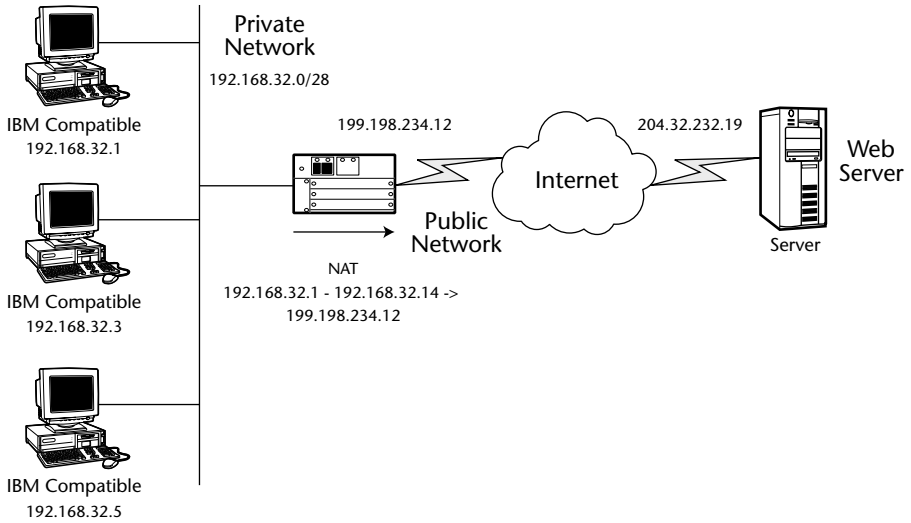


Figure 7-31: Dynamic Many-to-One NAT

Dynamic Many-to-Many NAT

With Dynamic Many-to-Many NAT, only addresses are translated and there is no translation of port numbers. In this type of NAT, a pool of addresses is used to perform the translation. In many instances, the pooled public IP addresses that are available are fewer in number than the private IP addresses being hidden behind them. Each request made by a PC on the private network that is received by the Nortel VPN Router is translated to a public IP address that is currently unused within the pool of IP addresses allocated for the translation. Dynamic Many-to-Many address translation can only be used for traffic that is initiated from a PC residing on the internal private network. Figure 7-32 illustrates a Dynamic Many-to-Many NAT configuration.

Table 7-3: Dynamic One-to-One Example

ORIGINAL SOURCE	NAT SOURCE
192.168.32.1 Port 80	199.198.234.12 Port 2302
192.168.32.5 Port 80	199.198.234.12 Port 2303

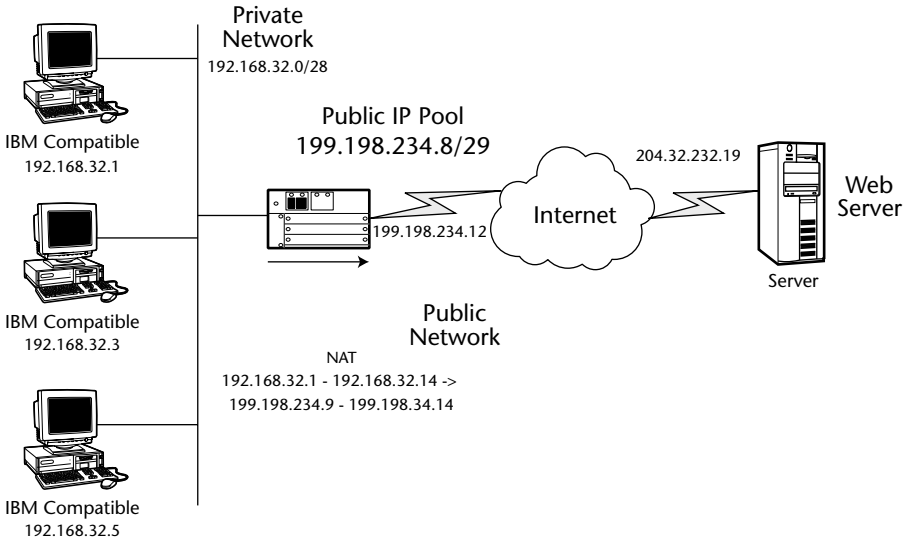


Figure 7-32: Dynamic Many-to-Many NAT

Table 7-4 shows an example of two PCs on the internal private network making page requests of a Web server over the Internet. PCs at 192.168.32.1 and 192.32.32.5 send a Web page request to the server 204.32.232.19 using port 80 as the destination address and port. Table 7-4 shows how the NAT packet is modified by replacing the original IP address of the requesting PC with one that is available from the public IP address pool. The Web server returns the packet to the source address and port that was in the requesting packet. When the response packet is received by the Nortel VPN Router, it uses the address translation table to return the packet to the PC that made the original request.

Static One-to-One NAT

Static One-to-One address translation requires an external IP address for each address that is to be translated on the internal private network. The allocation of addresses remains fixed between internal private hosts and their assigned public IP address.

Table 7-4: Dynamic Many-to-Many Example

ORIGINAL SOURCE	NAT SOURCE
192.168.32.1 Port 80	199.198.234.9 Port 80
192.168.32.5 Port 80	199.198.234.10 Port 80

An example of Static One-to-One address translation would be a private network with a network address of 192.168.48.0/24 residing on the internal private network behind a Nortel VPN Router. A public IP network subnet 207.250.34.88/29 is to be used to perform a Static One-to-One address translation for several hosts residing on the internal private network. In this particular example, the private network space can accommodate 254 host addresses while the public subnet has provision for unique addressing for 6 hosts. So, in the example address mapping illustrated in Table 7-5, six private addressed hosts are selected to be statically mapped to a public IP address.

Although the address translation is fixed, a rule may be modified if needed to replace one internal private IP address for another. This is much different than dynamic address translation because that is done automatically without administrator interaction. Static One-to-One translation is usually reserved for resources that are fixed such as dedicated servers.

Port Forwarding NAT

Port Forwarding translation allows for a single publicly addressable IP address to forward requests for differing services to different servers residing on the internal private IP network based on the protocol being used. This is illustrated in Figure 7-33 where an FTP server, a Web server, and an SMTP mail server all reside on the internal private network residing behind the Nortel VPN Router. The private network is 192.168.34.0/24 and the public IP address being used for Port Forwarding translation is 208.199.32.89. There is a Port Forwarding rule for each protocol being used. In this example, port 21 is being forwarded for FTP, port 80 is being forwarded for HTTP, and port 25 is being forwarded for SMTP.

Table 7-5: Static One-to-One Example

PRIVATE IP HOST ADDRESS	MAPPED PUBLIC IP ADDRESS
192.168.48.32	207.250.34.89
192.168.48.67	207.250.34.90
192.168.48.79	207.250.34.91
192.168.48.108	207.250.34.92
192.168.48.199	207.250.34.93
192.168.48.204	207.250.34.94

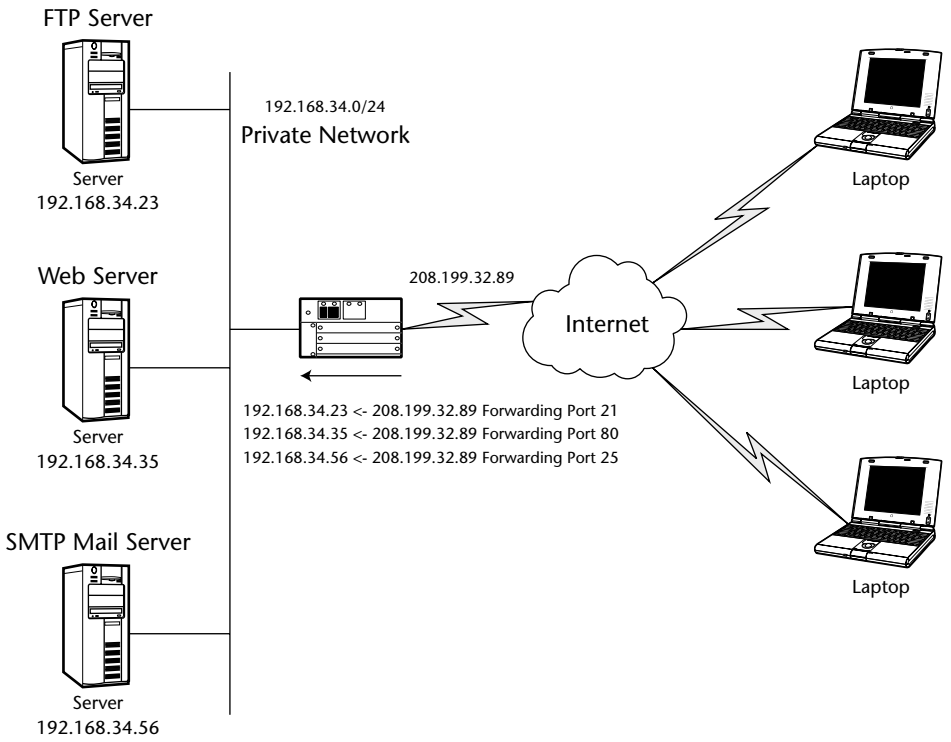


Figure 7-33: Port Forwarding NAT

Double NAT

Double NAT allows both external public IP addresses and internal private addresses to undergo translation at the same time. As a result, each packet entering or leaving the Nortel VPN Router may have both the source and destination addresses modified. This is accomplished on the Nortel VPN Router using one rule to perform translation on the source address and another rule to translate the destination address. The rule used for the destination address translation must be static. Figure 7-34 shows an example of Double NAT.

In Figure 7-34, a host on the Internet at 209.174.13.90 sends a request to the public IP address of the Nortel VPN Router using a destination address of 197.34.43.89. The packet undergoes a translation changing the destination address to that of the internal private network host at 192.168.54.10. Another rule modifies the source address and translates it to 172.16.32.32. So, when the packet is placed on the private network, the destination address is set to 192.168.54.10 and the source address is set to 172.16.32.32. The usefulness of Double NAT is to allow two hosts residing on different networks to be able to communicate and allow their actual IP addresses to remain unknown.

IPSec Aware NAT

IPSec Aware NAT prevents the alteration of TCP/IP headers that is usually performed by NAT. IPSec Aware NAT translation is used when an IPSec tunnel passes through a Nortel VPN Router performing NAT translation, but the tunnel does not terminate on the unit itself. This functionality allows for interoperability with IPSec configurations that do not support the UDP wrapper solution to perform NAT on IPSec traffic. IPSec Aware NAT is always on and is not configurable. Figure 7-35 illustrates an example where IPSec Aware NAT may be used.

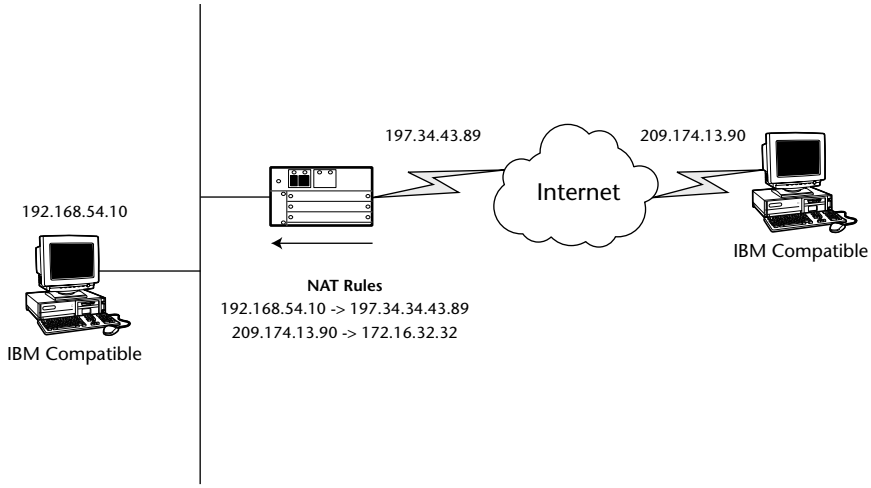


Figure 7-34: Double NAT

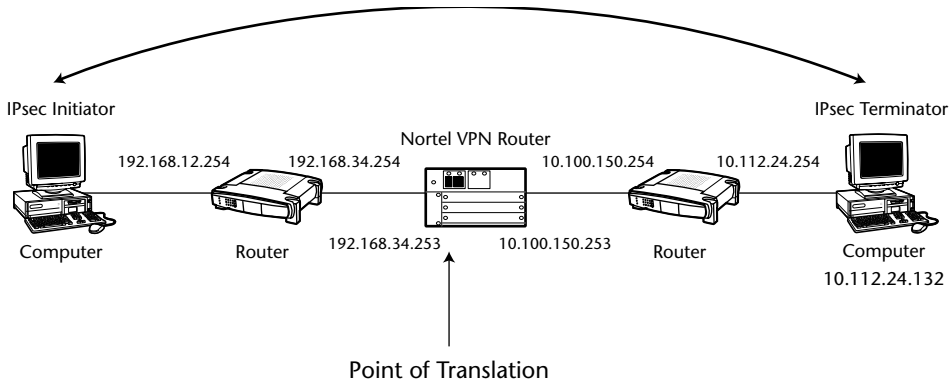


Figure 7-35: IPSec Aware NAT

In Figure 7-35, an IPSec initiator is establishing an IPSec session over a network that has a Nortel VPN Router performing translation between networks. Because it is IPSec Aware, it does not modify the TCP/IP header that would invalidate an IPSec tunnel. Thus, the IPSec traffic can pass between initiator and responder without being affected by translation that is not IPSec Aware.

NAT Modes

NAT types can be classified by their handling of UDP packets. Following are the four NAT modes:

- Full Cone NAT
- Restricted Cone NAT
- Port Restricted Cone NAT
- Symmetric NAT

The Nortel VPN Router supports Restricted Cone NAT and Symmetric NAT. Any references to Cone NAT on the Nortel VPN Router are referring to Restricted Cone NAT.

Full Cone NAT

Full Cone NAT is the mapping of all requests from the same internal private IP address and port to the same external public IP address and port. Any host residing on the external public network can send packets to the host that resides on the internal private network by sending the packets to the mapped external address. Figure 7-36 illustrates an example of Full Cone NAT.

In Figure 7-36, a client on the private network behind a NAT with an IP address of 192.168.37.11 sending and receiving on port 9101 is mapped through NAT to the public IP address of 198.201.34.89 using port 13505. This allows any host on the public network to send packets to the public IP and port on the external public side of the NAT, which then translates those packets to the internal private IP address and port of the internal private client.

Restricted Cone NAT

Restricted Cone NAT maps the requests from an internal client's IP address and port to the same external public IP address and port. However, unlike Full Cone NAT, an external host residing on the public network can send packets only to the internal host on the private network if that client has previously sent packets to that particular host.

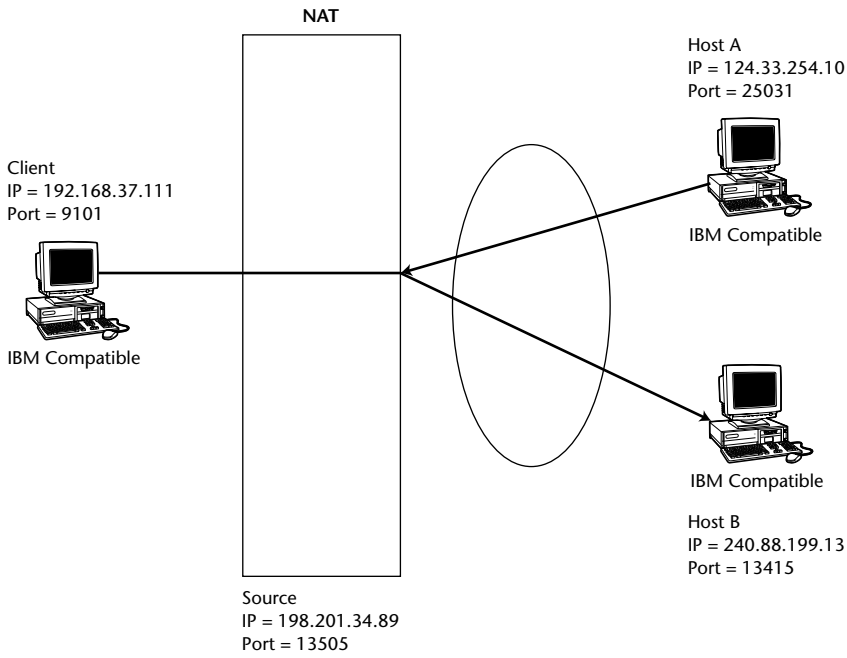


Figure 7-36: Full Cone NAT

Figure 7-36 illustrates the manner in which Restricted Cone NAT functions. Although similar to Full Cone NAT, it is different in that the session always needs to first be established from the internal host. The client residing on the private network at 192.168.37.111 using port 9101 is mapped to 198.201.34.89 port 13505. It sends a packet to Host A to open a session, which allows Host A to send packets to the public IP and port to be translated back to the client on the private internal network. Meanwhile, Host B is unable to communicate with the client on the internal private network until the client sends packets to it allowing it then to communicate with the client.

Port Restricted Cone NAT

Port Restricted Cone NAT is similar to Restricted Cone NAT. However, there is a restriction that also includes port numbers. With Port Restricted Cone NAT, an external host can send packets only to the client residing on the internal private network if the client first sends packets to that public host IP address and port.

Figure 7-36 can be used to illustrate the functionality of Port Restricted NAT. The client residing on the internal private network sends a packet to Host A residing on the public network at IP address 124.33.254.10 using port 25031.

Host A returns packets to the public NAT IP and port address of 198.201.34.89 port 13505. NAT translates the packet to the client residing on the internal private network because the source IP address and port that Host A used is the same as the destination address and port contained in the packet sent by the client. The internal client may send requests to multiple external public hosts that all respond back to the same NAT public IP address and port. NAT will translate all those requests in a similar fashion, while still maintaining translation information in regard to the external hosts and client-established sessions.

Symmetric NAT

Symmetric NAT maps requests from the same internal IP address and port to a particular specific destination IP address and port that are mapped to the same external IP address and port. However, if the same internal client sends packets with the same source address and port to a different host IP address, then different mapping is used. Only the external hosts that receive packets from the client residing on the internal private network can send packets to that client. An example of Symmetric NAT is illustrated in Figure 7-37.

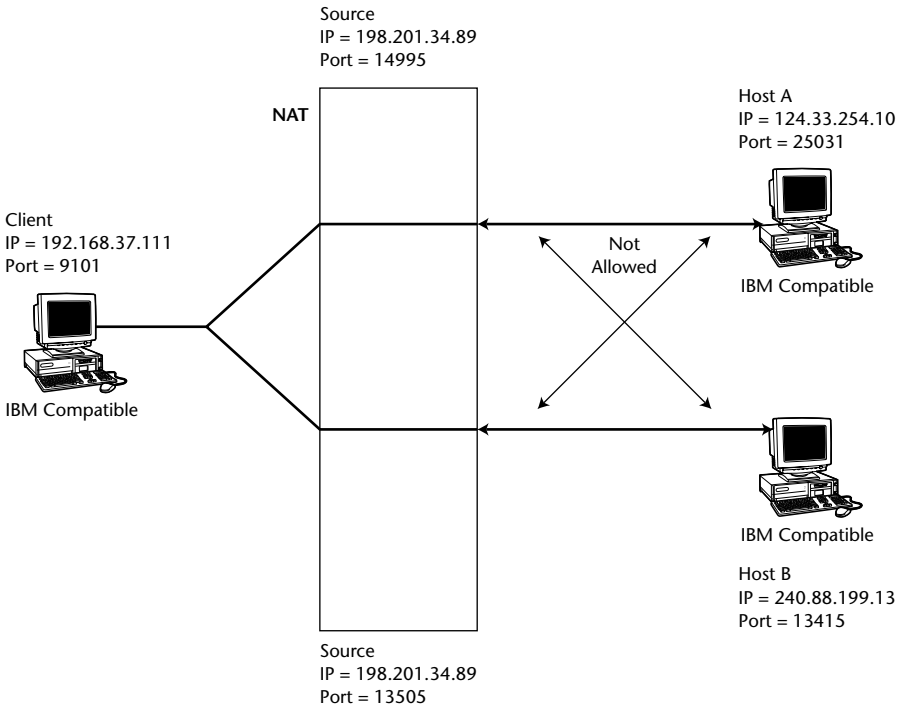


Figure 7-37: Symmetric NAT

In Figure 7-37, the client on the internal private network sends a packet to Host A on the external public network. The packet is mapped to a source address of 198.201.34.89 port 14995 and routed to Host A IP address of 124.33.254.10 Port 25031. For Host A to communicate with the internal client, it must respond to the same IP address and port that was the source address and port of the packet it received from the client. The client can similarly communicate with Host B on the public network with a mapping that uses IP address 198.201.34.89 port 13505. Host B can only communicate with the client using that source address and port that it received in the packet from the client.

The Nortel VPN Router default NAT Mode is set to Symmetric NAT. To select Restricted Cone NAT, from the main menu select SERVICES → FIREWALL/NAT to display the Firewall/NAT Configuration screen. Click the Edit button on the same line as Firewall to display the Firewall/NAT Edit screen. Scroll down to the NAT Mode area and select the Cone NAT radio button to select Restricted Cone NAT.

NAT Traversal

NAT Traversal allows the Nortel VPN Router client or server client mode tunnels to traverse networks that may contain routers or gateways that may possibly NAT the packet. This is especially true for mobile users using Internet services at airports, hotels, or other public Internet access points that use private, non-routable IP space to accommodate a number of users. NAT Traversal may be enabled on the Nortel VPN Router by selecting SERVICES → IPSEC to display the IPSec Settings configuration screen. By default, NAT Traversal is disabled on the Nortel VPN Router.

When NAT Traversal is enabled, a UDP port must be specified that all client connections to the Nortel VPN Router would use. The port must be a unique and unused UDP port within the private network. The supported range of addresses for this purpose is 1025 to 49151. By default there is no port number assigned to the UDP port, so one must be selected and entered when enabling NAT Traversal.

When using IPSec clients, NAT Traversal must be enabled at the user group level. By default, NAT Traversal is not allowed. So, if it is not enabled and NAT is detected between the client and the Nortel VPN Router, then encapsulation of ESP data will not happen. With the selection of Auto Detect NAT, the client and the Nortel VPN Router will UDP-encapsulate ESP data when NAT is detected. This allows the client and the Nortel VPN Router to UDP-encapsulate ESP data, but only if the detected NAT is not IPSec-aware. Non-IPSec–aware devices do not allow for IPSec pass-through.

There is a large variety of NAT devices in use with varying IPSec pass-through implementations. As a result, not all environments with NAT functionality are guaranteed to perform properly in Auto Detect IPSec NAT mode. In environments where the NAT devices are well-known, the use of the Auto Detect NAT mode setting is recommended.

NAT Traversal for clients may be set by selecting PROFILES → GROUPS, and then selecting the group to edit by clicking the Edit button adjacent to it. The Groups Edit IPSec screen will be displayed. The NAT Traversal settings can be configured by scrolling down to the IPSec area of this screen and clicking the Configure button. The NAT Traversal option is near the bottom of the display screen. Click the Configure button on this line to make the NAT Traversal options available for selection for this group.

The UDP port for NAT Traversal is blank by default on the Nortel VPN Router. Nortel recommends that port 10001 be used for this option. If you do not use this port value, then ports to avoid using are 1701, which is used for L2TP/L2F, or port 3386, which is used for General Packet Radio Service (GPRS). Also, if you do not use the recommended port value, to avoid possible conflict with ports that are used on the network, select one that is positively determined not in use on that network.

NAT and VoIP

Normally, NAT translates IP addresses and port numbers in private address space into public addresses when traffic traverses between the private and public networks connected to the Nortel VPN Router. However, the IP endpoints in a VoIP network (such as IP phones and soft phone clients) are typically assigned private addresses to conceal their identity from the public network. Normally, voice calls from and to the public network must be able to reach endpoints on the private network. Then network address translation is required for the proper routing of media traffic to endpoints with private addresses.

A number of complexities are introduced by VoIP protocols because they carry IP address and port information within the body of the message that is not accessible to NAT. NAT does not have the capability to conduct translation on private IP addresses embedded within the payload of application layer messages. Because of this, the voice media that is directed to the private IP address identified within the signaling message cannot be routed to that private address, which results in a one-way speech path.

The challenges for VoIP traversal in NAT result from the following:

- NAT inspects only layer 3 addressing.
- VoIP signaling embeds IP addresses at layer 5.
- Both Routing Table Protocol (RTP) and Real Time Transfer Control Protocol (RTCP) work at layer 5.

The two most common solutions offered to repair the NAT Traversal issue are:

- Application Level Gateway (ALG)
- Address/Port Discovery

NOTE **ALG is discussed in more detail later in this chapter in the section "Application Level Gateways."**

Address/Port Discovery

With Address/Port Discovery the media endpoints dynamically discover the public IP address and port used for a specific media stream by sending probe packets to the server that will echo back to the endpoint its source IP address after NAT translation.

Simple Traversal of UDP through NAT (STUN) is a lightweight protocol that provides applications a means to discover the presence of and the type of NATs and firewalls that are between an application and the Internet. With its use, the applications are also capable of determining the public IP addresses allocated via NAT.

STUN is able to identify the public side IP NAT information by inspecting exploratory STUN messages that arrive at the STUN server. The STUN-enabled client sends an exploratory message to the external STUN server in order to determine the transmit and receive ports that should be used. Incoming messages are examined by the STUN server and it informs the client which public IP address and ports were used by NAT. Then these are used in the call establishment messages sent to a Session Initiation Protocol (SIP) server. The STUN server does not sit in the signaling or media data flows.

For the IP addresses and ports that were discovered to be valid, it is imperative that the same IP address and port binding be used by NAT, regardless of where the packet is being routed to. For this reason, Symmetric NAT will not work for peer-to-peer media with Address/Port Discovery. Any Cone NAT implementation would work with STUN. However, using Restricted Cone NAT increases the security of the Nortel VPN Router.

NAT Usage

When NAT is applied to BOTs, it is referred to as *Branch Office NAT.* When NAT is applied to physical interfaces, it is referred to as *Interface NAT*. NAT is applied to routed traffic passing through interfaces and branch office interfaces using separate NAT policies. Each BOT has one NAT policy, and there is one global NAT policy that is applied to all non-tunneled traffic.

When changes are made to Branch Office parameters, the Branch Office must be disabled and then re-enabled for the changes to take effect. The flow cache clear capability can be used to have NAT changes take effect on existing sessions.

Branch Office Tunnel NAT

In a scenario where two branch offices are using the same private address space addressing scheme, NAT must be used so that the two offices will be able to communicate with each other.

A typical scenario may entail two branch offices that have the same subnet address being used on the internal private. For this example, both networks are 10.10.0.0/24 networks. So, a client on LAN A with an address of 10.10.0.25 would not be able to communicate with a server on LAN B (the remote network residing at an internal private address of 10.10.0.55 using natural routing). This is because the Nortel VPN Router that is connected to LAN A when it receives a packet with a destination address of 10.10.0.55 will determine that the server is resident on its own internal private network and will not attempt to establish a tunnel with the remote office network. Because there is no Interior Gateway Protocol (IGP) to dynamically learn routes at the remote end of the tunnel (which would allow the client to access the desired server on LAN B), NAT will be required on both ends of the Branch Office connection. This is a common issue when connecting numbers of remote offices when there will be remote networks that have address spaces that may overlap with one another.

In performing NAT on each end of the tunnel, the client on LAN A will be able to communicate with the server on LAN B. To accomplish this, the Nortel VPN Router connected to LAN A defines a remote-accessible network of 12.0.0.0 and the Nortel VPN Router which is connected to LAN B defines an remote accessible network at 11.0.0.0. The Nortel VPN Router connected to LAN A uses a translation of the client address 10.10.0.25 to 11.0.0.1. The Nortel VPN Router connected to LAN B uses a translation of the server address of 10.10.0.55 to 12.0.0.1.

With NAT implemented on both sides of the Branch Office connection, the client on LAN A is able to access the server on LAN B. The client generates a packet with a source address of 10.10.0.25 and a destination address of 12.0.0.1. The LAN A Nortel VPN Router recognizes that 12.0.0.0 is a remote-accessible network that is accessed through the Branch Office connection. The packet then is modified to have a source address of 11.0.0.1 based on the NAT table. When the Nortel VPN Router connected to LAN B receives the packet, it translates the destination address to the server address at 10.10.0.55 based on its NAT, while leaving the source address of 11.0.0.1 unmodified.

Interface NAT

Interface NAT is applied to IP packets either leaving or entering the Nortel VPN Router through physical interfaces that cause either the source or destination IP address to be translated to another IP address that is dependent upon the NAT policy. The difference between Interface NAT and Branch Office NAT is when and where the policy is applied.

Interface NAT is configured by selecting SERVICES → FIREWALL/NAT to display the Firewall/NAT Configuration screen. The following types of rules may be selected for Interface NAT:

- *Static:* With static mapping, an internal private address range is mapped on a one-to-one basis to an external address range.
- *Port forwarding:* With port forwarding mapping, packets arriving at the external public interface are routed on a specified port to an internal host that is specified in the mapping.
- *Port:* With port mapping, an internal private range of addresses is hidden behind a single external address. The external addresses are distinguished by using dynamically assigned port numbers.
- *Pooled:* With pooled mapping, an internal private address range is dynamically mapped to the next available address from a range of external public addresses.

Interface NAT applies only to non-tunneled traffic that is routed through the Nortel VPN Router. Branch Office NAT applies only to specific BOT traffic. If interface NAT is disabled, Branch Office NAT is not affected.

Dynamic Routing Protocols

NAT routes are advertised on all interfaces. Route distribution can be restricted only to specific interfaces with the use of the routing policy list.

Previously, routing protocols such as RIP and OSPF could send packets only to translated addresses if they were statically configured. However, now whenever a NAT policy is applied to an interface or BOT, the routes translated to IP addresses are added to the routing table. If NAT is deleted, then the routes to those translated IP addresses are deleted from the routing table. Destination NAT adds the original destination address to the packet, and source NAT adds the translated source address to the packet.

NAT routes are distributed by RIP and OSPF protocols by default. However, there is an option to disable route distribution for a particular protocol by selecting ROUTING → POLICY to display the Policy screen where the Redistribution Table may be modified.

NAT on a branch office may be enabled with dynamic routing running. If NAT is configured on a branch office, you will not want to announce the route to the original IP addresses. A routing policy may be used to block the route advertisement to the original IP address. However, it cannot announce part of a subnet. As a result, if NAT is applied to part of a subnet, then there will not be a route advertisement to that entire subnet.

A translated address range may be added to the routing table as a single subnet. However, if a non-subnet IP address range is selected, those addresses may be added as individual host routes, or as a group of smaller subnets, which is called *summarization*. Summarization reduces the number of required NAT route entries in the Route Table Manager (RTM), thus reducing the number of entries that need to be redistributed. Summarization is enabled by default. However, there are options to disable and enable it.

A BOT should not be enabled if there is no routing policy associated with the corresponding branch office interface in cases when both NAT and dynamic routing are configured. A routing policy for it must be created on the ROUTING → POLICY configuration screen.

NAT utilizes a port mapping table to track the ports for each client's outgoing packets. The port routing table holds the relationship of the client's actual IP address and source port to its translated source port number to a destination IP address and port. NAT uses the table to reverse the process for returning packets to route them back to the original client that initiated the request. This port mapping table is applicable only to TCP and UDP traffic.

Configuring a NAT Policy

NAT policies consist of service properties and a security policy. *Service properties* define the service being offered, which includes the service name, the protocol, and the port number or range on which the service is utilizing.

Security policies are a set of rules that specify the service to be allowed or denied. Rule fields are specified for service policies using service objects. Each rule consists of a combination of network objects, services, actions, and logging mechanisms. Custom policies may be defined when more complex security policies are required and the standard policies are insufficient.

NAT Policy Sets

The Nortel VPN Router maintains one set of a source and destination pair of global NAT policies for all non-tunneled traffic, and a configurable NAT policy set for each BOT definition. NAT policies for interface and branch offices may be viewed by selecting STATUS → STATISTICS and then scrolling down the Statistics screen to the Security section. There are buttons to select Active Interface NAT Policy and Active Branch Office NAT Policy to display the policies currently in effect. This area has buttons to view NAT Stats and NAT Translations.

NAT obtains a cached policy if it exists while the Nortel VPN Router is in the initialization process at system startup. If a cached policy does not exist, then a default policy of no NAT translation is used. However, the default policy for Nortel VPN Router models 1010, 1050, and 1100 map their private address space to their public IP address.

As the Nortel VPN Router completes its initialization, the NAT policy is retrieved from the LDAP database and becomes the active policy. When the policy is changed, it is stored on the local storage media as a cached policy and in the LDAP database. This new policy is used by NAT for all new sessions, while existing sessions continue using the original policy.

Creating Rules

The configuration process for NAT rules is similar to that of configuring the stateful firewall. The examples illustrated for the menus of Header Row, Row, and Cell are almost identical, except that it is performed on the NAT Edit Policy screen. For further information refer to the Nortel VPN Router released document on configuring firewalls, filters, and NAT.

NAT ALG for SIP

Layer 5 addresses are not translated by traditional NAT. Thus, VoIP signaling and RTP/RTCP are unreachable after NAT translation because of the embedded IP address and port specified within its IP payload.

Following are two solutions that correct the NAT traversal issue:

- Application Level Gateway (ALG)
- Address/Port Discovery

Address/Port Discovery was discussed earlier in this chapter. This section will focus on NAT ALG for SIP to support VoIP phones that use SIP as their signaling protocol.

Application Level Gateways

NAT Application Level Gateways (ALG) are used to translate any embedded IP addresses and ports contained within an application's protocol messages. It provides support for FTP, ICMP, Berkeley R commands, NetBIOS, IPSec (ESP only), and SNMP. An ALG is required for application traffic flows that embed an IP address in the data portion, as is done with FTP or NetBIOS.

SNMP ALG support allows the use of SNMP traps with NAT. Data within SNMP traps are translated, preventing inconsistencies within the packet. SNMP ALG is applied to SNMP traps originating from the Nortel VPN Router only if there are NAT rules that translate that traffic originating from the router.

The SNMP management system must be enabled to send SNMP `Gets` from the SNMP screen, which is displayed by selecting ADMIN → SNMP.

NAT ALG provides support for SIP traffic to and from Nortel i2004 phones model NTEX00 and the MCS 5100 SIP server.

Configuring NAT ALG for SIP

NAT ALG for SIP may be enabled or disabled with either the use of the GUI configuration screen or CLI commands. For the use of CLI commands, refer to Nortel's *VPN Router Command Line Interface (CLI)* manual.

To configure NAT ALG for SIP using the GUI interface, select SERVICES → FIREWALL/NAT to display the Firewall/NAT display screen. Click the Edit button (which is on the same row as Firewall) to display the Firewall/NAT Edit screen. Scroll down to the NAT Application Level Gateway section and click the check box adjacent to SIP. Scroll down and click OK. The Firewall/NAT screen will be displayed once again with the new configuration applied.

Firewall SIP ALG

By default, firewalls do not have the intelligence to identify port numbers within the payload of signaling protocols and cannot dynamically open ports for media traversal, resulting in the blocking of voice traffic. Firewalls are designed to operate with layer 3 and/or layer 4 information and are unable to access information contained in higher-layer protocols.

This issue was resolved for VoIP signaling protocols with the development of ALGs. The SIP ALG performs the necessary translation of IP addresses embedded within the SIP messages and updates the SDP information. The firewall ALG examines the SDP information, identifies the RTP port number for the call, and opens a port in the firewall during the call setup. Firewall ALG raises a flag to indicate that NAT should perform an application-level translation. The ALG then performs the address/port mapping and state setup to ensure that data channels get mapped according to the information in the SDP. The ALG closes the port upon call termination. This mechanism provides the capability to dynamically open and close ports in the firewall and increases network security with the restriction of voice traffic to only active sessions.

Hairpinning

When two IP phones behind the same NAT need to communicate, it requires a functionality called *hairpinning*. Nortel VPN Router NAT blocks packets coming from the private side of the NAT that are destined for the private side for

which a NAT binding to a specific port already exists. This prevents peer-to-peer communication between two endpoints behind the same NAT if they attempt to use their public address. Hairpinning corrects this issue by examining the destination address of a packet. It evaluates the destination address, NAT binding, and makes a determination for hairpinning.

NAT hairpinning does payload translation on SIP and UNIStim messages. (UNIStim is a proprietary Nortel protocol.)

Hairpinning with SIP

There are special considerations required to handle the problem when voice phones are on one side of a NAT boundary and the call server is on the other side. SIP NAT ALG translates the IP addresses of the phones from private address space to public. When the call server is queried for the IP address of the phone that is being called, it responds back with the public IP address. It also supplies the called phone with the public IP address of the caller.

Although both clients reside in the same private address space, each thinks the other resides in the public address space. Media traffic between clients must go to and from the public addresses looping through the NAT device.

Hairpinning with a UNIStim Call Server

When a UNIStim call server sends an Open Audio Stream (OAS) message to an IP phone, it always uses the public address as the far-end address for the other IP phone. When both IP phones are behind the same NAT, this creates issues because media packets are being sent to the NAT device, which is unaware of what these packets are for. If the NAT device supports hairpinning, it is able to redirect packets to the right destination, thus helping to generate the voice path.

Hairpinning support is only part of the solution and can coexist with other portions of the solution. For example, non-encrypted UNIStim message hairpinning logic automatically turns off and a direct media path can be achieved.

Hairpinning with a STUN Server

When NAT traversal for phones behind a NAT is based on STUN, the port discovery protocol between the phones and the STUN server allows the phones to discover their public addresses and use the discovered public addresses for peer-to-peer communications.

Hairpinning Requirements

There are two requirements for NAT hairpinning:

- IP phones may not accept packets from arbitrary IP addresses. Thus, the source IP address must be the public IP address of the NAT.
- If a device is performing NAT on a VPN tunnel, then packets sent from private devices to the assigned VPN IP are hairpinned back without entering the VPN tunnel. When the packets reach the private endpoint, the source IP address must be the assigned VPN IP address.

Hairpinning Configuration

Hairpinning of packets can be either turned on or off from the GUI or CLI. For the CLI commands used to configure hairpinning, refer to Nortel's *Command Line Interface (CLI)* manual.

To accomplish hairpinning with the GUI interface, select SERVICES → FIREWALL/NAT to display the Firewall/NAT configuration page. Click the Edit button on the row with the Firewall selection option to display the Firewall/NAT Edit screen. Scroll down to the NAT Hairpinning area and click the check box to Enable Hairpinning. Click OK to accept this selection. To disable hairpinning, simply uncheck the hairpinning Enable check box.

Time-Outs

When a session terminates, NAT deletes the associated translations. However, if a server should go down unexpectedly, the associated translation must age out to prevent available translation addresses from being exhausted. NAT time-outs are grouped by protocol as follows:

- ICMP*:* 3 minutes
- UDP*:* 3 minutes
- TCP*:* 120 minutes

NAT Statistics

The following statistics counters are provided for source and destination NAT services:

- *Source Translated:* The number of packets that have their source address translated.
- *Destination Translated:* The number of packets that have their destination address translated.

- *Flows Translated:* The number of flows that are translated by NAT service.
- *No Action:* The number of flows for which no translation has been performed.
- *Dropped:* The number of packets dropped because of NAT being unable to translate the source or destination address.
- *Pooled Address Translation Failed:* The number of packets dropped because of NAT not being able to map a new address from the available address pool.
- *Port Translations Failed:* The number of packets dropped because of NAT not being able to map a new port for translation.

To view NAT statistics, select STATUS → STATISTICS to display the Statistics screen. Scroll down to the Security area and click the NAT Stats button to display the NAT statistics.

Proxy ARP

Proxy ARP is required if the translated address assigned by NAT to a private host has it appearing as if the private host is residing on the other host's network. The host on that network will use the Address Resolution Protocol (ARP) for the requesting host and not receive a response unless Proxy ARP is enabled for physical interfaces on the Nortel VPN Router.

To enable Proxy ARP for physical interfaces, select SYSTEM → FORWARDING to display the Forwarding configuration screen. In the Proxy ARP area of the screen, select the Physical Interfaces check box to enable Proxy ARP. Click OK to accept the selection.

Summary

This chapter discussed the Nortel VPN Router's stateful firewall, filters, and NAT. With the use of these features, the router is versatile in fulfilling many of today's networking requirements securely. Also included in this chapter is a discussion of special considerations required for the support of VoIP.

There are several books on the market today that deal with security. As the Internet grows, and more people use the Internet, the need for security continues to rise. This chapter has provided an overview of security as it relates to the Nortel VPN Router, including configuration and functionality considerations.

Chapter 8 discusses an overview of routing and routed protocols and how they relate to the Nortel VPN Router. It is important to always keep in mind that the VPN Router is a router as much as it is a VPN device. Understanding the technologies and protocols that are supported by the Nortel VPN Router is a must for anyone who is tasked with administering the router within their network.

CHAPTER

8

Overview of Ethernet LANs and Network Routing

The Nortel VPN Router provides secure remote access to a LAN. Remote users can now do much of what they can do in the office without having to be located onsite. Whether the remote users are just checking email or processing invoices, they can do so safely and securely in real time.

Chapter 1 contained an overview of some basic networking protocols and standards. In Chapters 8 and 9, a more in-depth overview of some of the supported protocols and standards is provided. In any network, it is important to have an understanding of these standards.

Understanding how RIP, OSPF, BGP, Ethernet, and so on operate will improve the effectiveness of anyone who will be tasked with maintaining the Nortel VPN Router. Whether implementing a new configuration, or troubleshooting issues with an existing implementation, understanding how data is transferred is a must.

This chapter discusses the many LAN and routing standards that are supported by the Nortel VPN Router. This is not a configuration guide. Many of these standards contain multiple variables that may or may not apply to any given LAN. Chapter 11 provides lab exercises that cover the configuration of a lot of these concepts.

Ethernet Networking

Ethernet was developed in the early 1970s as a way to provide data communications within a local area network (LAN). As companies started implementing networking data solutions in the 1980s, the need for standardization became apparent.

Eventually, the IEEE 802.3 standard became the Ethernet LAN networking standard that is in use today. Figure 8-1 shows an example of an Ethernet LAN topology.

By the 1990s, Ethernet became the most widely used LAN data communications technology and had replaced most of the other LAN technologies. Although others are still in use, Ethernet is used by the majority of LANs.

Ethernet basically allows nodes on a network to communicate with one another. Each node on the network is identified by a Media Access Control (MAC) address, which is unique to that node and identifies the node.

Ethernet communications were originally supported by connecting all nodes to a main signal cable. As LANs began to develop, the need to change the physical topology of the LAN grew. Other networking nodes (such as repeaters, hubs, concentrators, and so on) were introduced to Ethernet segments, and the physical topology changed.

Because traffic collisions within an Ethernet segment are a reality, Ethernet utilizes a technology known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD). The CSMA/CD protocol assists in ensuring that loss of data is recognized within an Ethernet segment, and that the data can be retransmitted. This helps ensure reliable data delivery.

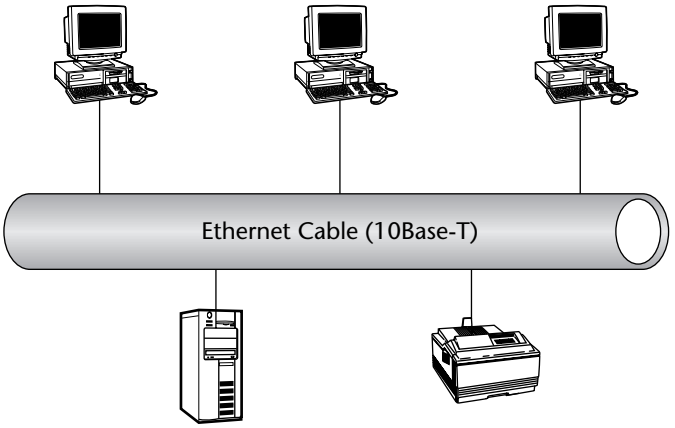


Figure 8-1: Ethernet LAN

Basic Physical Topology Types

A *physical topology* in networking is defined by the way that the nodes in the network are connected to one another. This should not be confused with the *logical topology* of the network, which is concerned with the protocols and standards that are implemented to get data passed from one node to another.

Ethernet is usually implemented in either a bus topology configuration or a star topology configuration. Although there are other topology types, these are the basic Ethernet implementation types.

Bus Topology

The *bus topology* is simply a cable run that all nodes connect to. The cable has terminators at each end, and all nodes tap into the cable directly. Figure 8-2 shows an example of the bus topology.

One of the advantages of using a bus topology is that it requires less cabling to implement than the star topology does. The bus topology is also easy to implement because nodes are tapped into the cable directly.

Disadvantages exist with the bus topology as well. One of the main disadvantages is that the entire network segment must remain intact, and all nodes on the cable segment will lose connectivity if there is a break in the cabling. Another disadvantage is that this type of topology is difficult to troubleshoot when a segment or the entire network goes down.

Star Topology

The *star topology* usually utilizes a hub or a switch to connect to data nodes within the network. Instead of tapping into a main cable run, each node has a cable that connects to the hub or switch. All data within a subnet will pass through the hub, and then onto the devices that are connected to the hub. Figure 8-3 shows an example of the star topology.

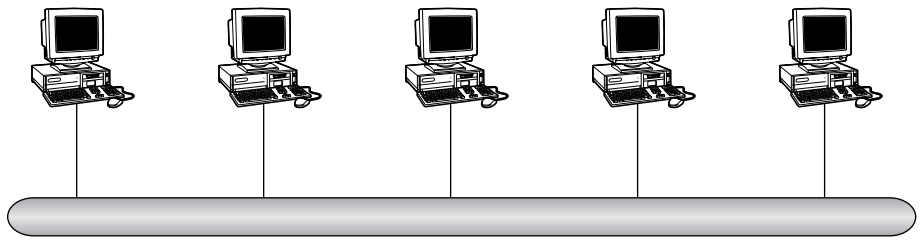


Figure 8-2: Bus topology

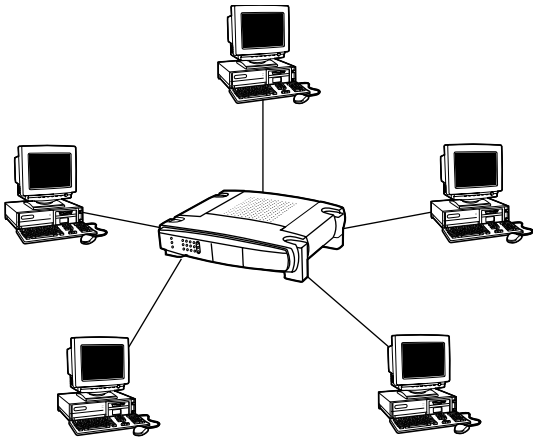


Figure 8-3: Star topology

As with any other physical implementation in data networking, the star topology has a few advantages as well as disadvantages. Some advantages are that it is easy to implement and there is no disruption to traffic to other nodes if a cable to a particular node goes down. Also, it is easier to troubleshoot than the bus topology because you can eliminate nodes that have not lost connectivity and can get a lot more granular in diagnosing problem nodes.

Some examples of disadvantages would be that the star topology is more expensive to implement than the bus topology because it requires additional equipment as well as additional cabling. Also, there is a potential of segment failure if the hub or switch fails.

Carrier Sense Multiple Access with Collision Detection

Ethernet provided a method for getting data transmitted from node to node within a LAN. But how does each node control when to send data, and how does a node recognize whether or not data is received? If these types of questions are not addressed, then the potential of losing data always exists.

A collision occurs when two nodes transmit data on a LAN segment at the same time. Because of this, a standard must be implemented to recover from the collision condition. The overall effect of this would be that a lot of data that is sent would never make it to its destination. Figure 8-4 shows an example of a collision occurring on an Ethernet LAN segment.

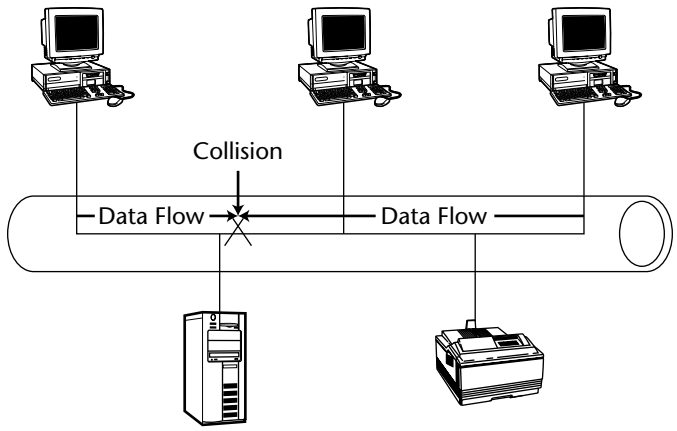


Figure 8-4: Collision on an Ethernet segment

A data delivery protocol known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is utilized by Ethernet to improve the integrity of data delivery. There are three main components in CSMA/CD:

- *Carrier Sense:* This means that devices on a network "listen" to the line to wait until there is no activity before sending.
- *Multiple Access:* This means that there are multiple nodes accessing the line.
- *Collision Detection:* This means that the sending nodes have the capability to recognize when a collision occurs.

When a node wants to transmit data upon an Ethernet segment, it listens to the line to wait until there is an available moment to send that data. The node receives notification if there is a collision, and it waits for a moment and then it resends. It continues to do this until it no longer is notified of a collision.

Collisions in a LAN happen. CSMA/CD provides for recovery from these collision, and helps to ensure that data is transmitted and received within a LAN.

Ethernet Variants

As mentioned previously, Ethernet became an IEEE standard in the 1980s. As technology improves, the need to support new standards and implementations is required. Therefore, Ethernet improvements are introduced to keep up with the demands of implementing new standards.

Supporting technology is an ever-changing process. Because it is the most commonly used LAN technology, Ethernet has experienced a lot of changes in the last 30 years. In this section, the following Ethernet variations are discussed:

- Traditional Ethernet
- Fast Ethernet
- Gigabit Ethernet

Traditional Ethernet

Traditional Ethernet standards are defined by the cable types (and associated hardware) needed to support data transmission within a traditional Ethernet LAN. Traditional Ethernet segments can support data transmission rates up to 10 Mbps. The following Ethernet cabling variants are considered Traditional Ethernet types:

- *10Base-2:* Often referred to as "Thinnet," this is a coaxial cable that supports Ethernet segments up to 185 meters in length.
- *10Base-5:* Often referred to as "Thicknet," this is a coaxial cable that supports Ethernet segments up to 500 meters in length.
- *10Base-T:* This is a twisted-pair cable that supports Ethernet segments up to 100 meters in length.
- *10Base-FL:* This is a fiber-optic cable that supports Ethernet segments up to 4 kilometers in length.

NOTE **Cabling types are discussed in more detail later in this chapter in the section, "Network Cables."**

Fast Ethernet

Fast Ethernet standards are defined by the cable types (and associated hardware) needed to support data transmission within a fast Ethernet LAN. Fast Ethernet segments can support data transmission rates up to 100 Mbps. The following Ethernet cabling variants are considered fast Ethernet types:

- *100Base-TX:* This variant comprises either two pairs of unshielded twisted-pair cable (Category 5 UTP) or shielded twisted-pair cable (Category 1). It supports a distance of up to 100 meters.
- *100BASE-FX:* This is a fiber-optic cable that supports a distance of up to 2 kilometers.

Gigabit Ethernet

Gigabit Ethernet (also known as *Gig Ethernet* or *Gig-E*) standards are defined by the cable types, and associated hardware, needed to support data transmission within a gigabit Ethernet LAN. Gigabit Ethernet segments can support data transmission rates up to 1,000 Mbps. The following Ethernet cabling variants are considered gigabit Ethernet types:

- *1000Base-CX:* A high data rate, twisted-pair cable that supports short distances of up to 25 meters. This is mainly used to connect devices that are local to each other within a segment closet.
- *1000Base-LX:* A fiber-optic cable that supports lengths of up to 3,000 meters.
- *1000Base-SX:* A fiber-optic cable that supports lengths of up to 220 meters.
- *1000Base-T:* A four-pair Category 5 cable that supports distances of up to 205 meters, end to end.

Network Cables

Network cables are the physical medium that is used within a network to pass data from one node to another. Usually, a cable is simply two or more wires that are banded together and normally covered by a protective sheath or insulation. A fiber-optic cable consists of fibers that are wrapped in insulation, and it is used to transmit data through light waves.

An Ethernet network can consist of one particular type of cabling or can incorporate multiple cable types. The needs of the network will determine the types of cabling that is used. This section provides information on the following common forms of cabling used in Ethernet LANs:

- Coaxial cable
- Twisted-pair cable
- Fiber-optic cable

Coaxial Cable

The *coaxial cable* is the traditional Ethernet cable type. Usually, coaxial cable is more expensive than twisted-pair cabling and can be harder to install and implement. Figure 8-5 shows an example of the coaxial cable.

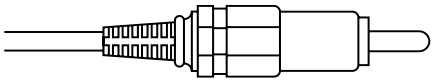


Figure 8-5: Example of coaxial cabling

When using coaxial cabling, each node within a segment is able to tap into the cable by using what is known as a "*T*" connector. The "T" connector is simply a connector that allows for a node to connect to the cable, while maintaining the integrity of the cable. At each end of the cable is a connector that is known as a *terminator*. The terminator connector simply terminates the cable run.

Coaxial cabling is made up of a copper connector that is in the middle of the cable. The copper connector is surrounded by insulation and a wire mesh, and finally it is wrapped in a plastic covering.

Twisted-Pair

Twisted-pair cabling is used by fast Ethernet and some gigabit Ethernet segments for data communications. The twisted-pair is simply a pair of wires twisted together. They are twisted together to help in the elimination of electrical noise and interference, thus reducing signal interference and ensuring data integrity. Figure 8-6 shows an example of twisted-pair cabling.

Twisted-pair cabling can be either shielded or unshielded. *Shielded twisted-pair cabling* is more reliable over long distances because the shielding helps protect from outside interference. *Unshielded twisted-pair* is far less expensive and is still very reliable. There are currently five categories of unshielded twisted-pair cables, including the following:

- *Category 1 (Cat1):* Used for low-speed data applications.
- *Category 2 (Cat2):* Used for medium-speed data applications.
- *Category 3 (Cat3):* Used for high-speed data applications.
- *Category 4 (Cat4):* Used to transfer high-speed data over long distances.
- *Category 5 (Cat5):* Used to transfer high-speed data over long distances. This is the most commonly used unshielded twisted-pair cabling type.

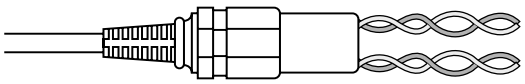


Figure 8-6: Example of twisted-pair cabling

Twisted-pair cabling is made up of at least two pairs of insulated copper wires that are twisted around one another. If it is shielded twisted-pair, then the wires are surrounded by an insulation shield, and finally it is wrapped in a plastic covering. If the cabling is unshielded, then it will not contain the insulation shield.

Fiber-Optic

Fiber-optic cabling is used by gigabit Ethernet segments for data communications. Fiber-optic cabling is more expensive than the traditional copper wire–based cabling, but it is less susceptible to line noise because it uses light instead of voltage to transfer data. Figure 8-7 shows an example of fiber-optic cabling.

Fiber-optic cabling contains a glass tube inner core, which is surrounded by a reflective cladding. The core and the cladding are then surrounded by a protective plastic outer jacket, which protects the core from moisture and light.

Data communications takes the form of light waves that are transmitted from one end of the cable to the other. The light travels through the inner core and, because the light reflects off of the reflective cladding, almost all of the light is able to reach the opposite end.

Fiber-optic cabling is available in either multimode fiber or single-mode fiber. *Multimode fiber-optic cabling* is made with a larger inner core and uses less expensive LEDs to generate a signal. On the other hand, *single-mode cabling* uses a smaller-diameter inner core and laser signaling.

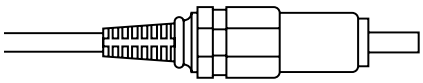


Figure 8-7: Example of fiber-optic cabling

Data Transmission Modes

In data communication, the transmission of data can take one of two forms:

- *Simplex transmission:* Used by a node that sends data, but does not receive return data
- *Duplex transmission:* Used by a node that requires both sending and receiving data

Simplex

Simplex transmission means that data is transferred in only one direction at all times. Although not very common in today's data networks, simplex systems are still in use in areas where a broadcasting node does not require a reply from receiving nodes. Figure 8-8 shows an example of simplex communication.

Simplex communication is analogous to driving on a one-way street in your town: All traffic is allowed to go in one direction, and one direction only.

Half-Duplex

Half-duplex transmission means that data is transferred in only one direction at any time. This is not to say that data is restricted in always traveling in the same direction, as with simplex transmission, but it does mean that you can go only one direction (either direction) at the same time. Figure 8-9 shows an example of half-duplex transmission.

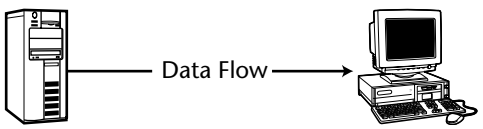


Figure 8-8 Simplex communication

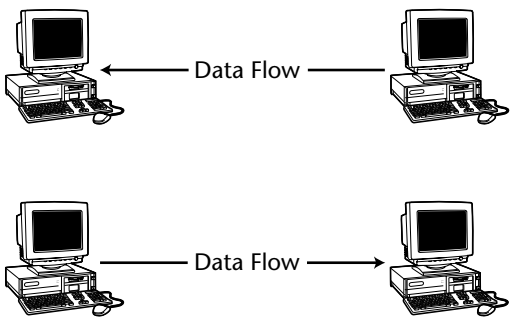


Figure 8-9: Half-duplex data transmission

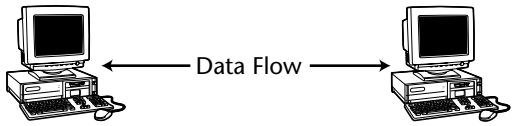


Figure 8-10: Full-duplex transmission

Half-duplex data transmission would be analogous to driving on a one-lane, bi-directional street in your town. Because this street is only one lane wide, traffic can only go one way or the other at any time.

Full-Duplex

Full-duplex transmission means that data is transferred in both directions at the same time. Figure 8-10 shows an example of full-duplex transmission.

Full-duplex data transmission would be analogous to driving on a multiple lane, two-way street in your town. Because this street has more than one lane and it is bi-directional, traffic can travel in both ways at any time.

Collision Domains

Previously in this chapter, we covered the concept of collisions. CSMA/CD employs a strategy to help Ethernet networks deal with collisions. This is accomplished by a node on the network by monitoring voltage changes on the Ethernet segment. When a node that needs to transmit data recognizes that a line is not busy, it transmits the data. Sometimes, another node transmits data onto the line at the same time. When this occurs, a collision occurs and both nodes wait a period of time and try to resend the data when they recognize the segment as not being busy.

A *domain* can be defined as a logical area within a data communications network. A *collision domain* can thus be considered a grouping of data communications nodes within a logical area that share an Ethernet segment. This can be a grouping of a few computers, or several hundred nodes within a LAN. Figure 8-11 shows an example of a collision domain. Notice that all the computers in the example are connected to the same Ethernet segment.

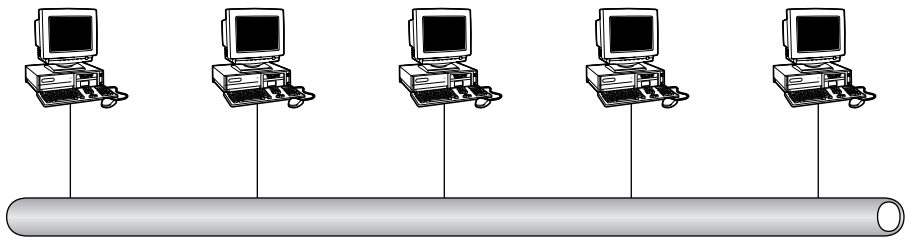


Figure 8-11: Collision domain

Consider that you have an Ethernet segment with 200 nodes connected to it. This would be your collision domain. Because all of these nodes can send and receive messages from all of the other nodes within the segment, it is considered a broadcast domain as well. If you have 200 nodes trying to access and utilize the Ethernet, you can see that the potential for collisions can be very high.

Broadcast Domains

A *broadcast* is a packet that is sent from a node within a LAN that can be received, in theory, by all other nodes within the LAN. Broadcasting is supported by Ethernet LANs. Broadcasts are limited to the nodes that are members of a broadcast domain. A *broadcast domain* is all of the nodes that can communicate directly to one another without having to pass through a router. A broadcast domain can be a group of a few computers or can be several hundred computers.

A *broadcast address* is used to broadcast messages with a broadcast domain. The broadcast address will be identified by the subnet identity of the broadcast domain and a special address consisting of all 1's in the user portion of the IP address scheme.

Two collision domains can be joined together to form one broadcast domain. This is done by placing a bridge between the collision domains. The bridge will separate issues within a collision domain so that the issues are not propagated to the remaining nodes within the broadcast domain. Additionally, by separating the collision domains, the nodes within a collision domain do not have to compete with as many nodes for use of the data line.

Remember the collision domain that was mentioned in the previous section? There were 200 nodes within the collision domain that had to work with one another to utilize the line to pass data. By placing a switch between the nodes and splitting them into two separate collision domains, you reduce the number of nodes that have to share the Ethernet segment. In Figure 8-12, you can see that there are two collision domains that make up one broadcast domain. All nodes within the two collision domains listen to broadcast messages that are sent within the broadcast domain, but when passing traffic, there are fewer nodes trying to use the line.

In a LAN segment that is separated by a router, the router will serve as the boundary for the broadcast domain. Broadcast messages do not propagate through the router.

NOTE **Most routers can be configured to support bridging and can, therefore, be used as a bridge to join collision domains into a broadcast domain.**

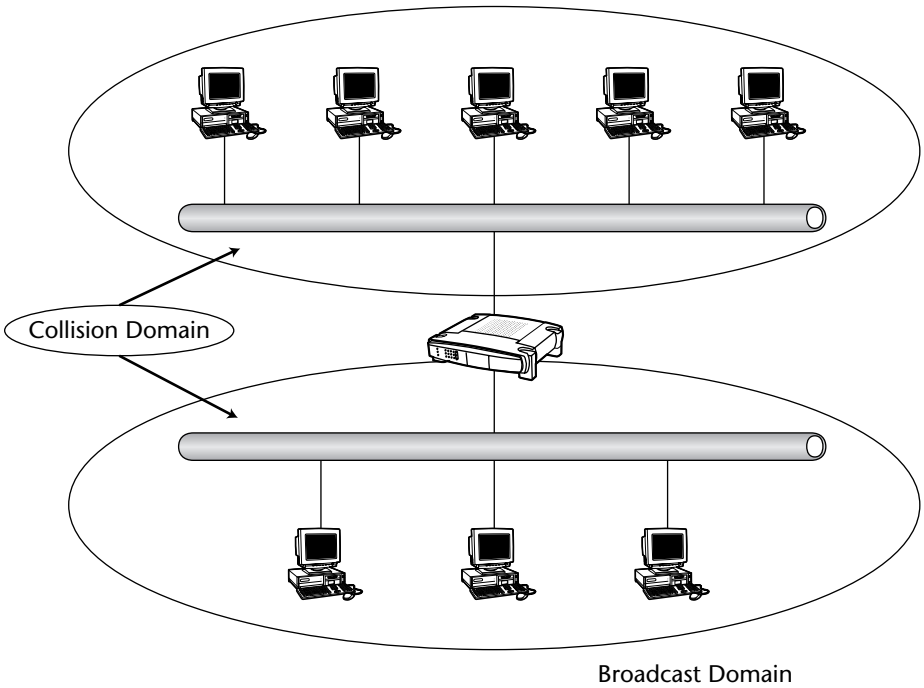


Figure 8-12: Broadcast domain

Network Addressing

A *network address* is used to identify a node within a network. In data communications, two types of network addresses are used. In a LAN segment where there are no routers propagating data traffic, the nodes within the segment are able to identify one another by the MAC address that is assigned to them. When a router is involved to deliver data between LAN segments, the address that is used for the delivery of the data is the IP address that is assigned to the destination node.

Data network addressing can be understood by comparing it to mail delivery. Any place that mail can be delivered to has a physical street address. The physical street address is equivalent to the MAC address of nodes within a data network. To move mail to other parts of the country, a ZIP code is used. When delivering mail to a ZIP code area, the Post Office is acting like a router delivering a packet to a subnetwork that contains the same IP addressing scheme as the packet's destination.

Media Access Control (MAC Addressing)

A *MAC address* is a hardware physical address that identifies the node to the other nodes on the network. MAC addressing is used by layer 2 nodes to identify the device and formulate data traffic paths to that device. Every node in a network has a MAC address. Figure 8-13 shows an example of MAC addressing of nodes within a LAN segment.

Not all networking protocols will use the MAC address, but on broadcast networks, the MAC address allows all of the nodes in the network to be identified and allows delivery of frames intended for a specific destination. MAC addresses are permanently attached to a device and are assigned by product manufacturers.

MAC addressing is administered by the IEEE. The IEEE ensures that there is no duplication of MAC addresses, so all Network Interface Cards (NICs) have a unique MAC address that is assigned to it by the manufacturer. Because of this, the end user can install a NIC anywhere within a network and not be concerned about duplication of MAC addresses.

MAC addresses are 48 bits long. The first 24 bits are known as the *Organization Unique Identifier* (*OUI*) and they identify the manufacturer of the device. The remaining 24 bits make up a unique number that is assigned by the manufacturer to identify the individual component.

NOTE **You can determine the manufacturer's OUI code by searching on the IEEE Web site.**

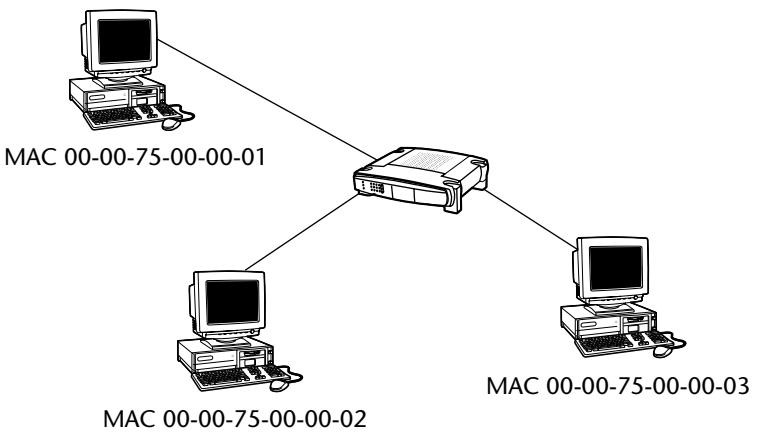


Figure 8-13: MAC addressing

Internet Protocol (IP Addressing)

An IP address is a unique number that is used by layer 3 nodes to communicate with one another in a network. An IP address is assigned to each host interface within a network. To route data between subnets, the IP address of the sending and the receiving nodes must be known. Figure 8-14 shows an example of three subnets, connected with a router and, therefore, capable of communicating with IP addressing.

An IP address may be permanently assigned to a node. This type of IP address is known as a *static IP address*. An IP address may be assigned to a node on a temporary basis and can be reused by other nodes when the node is removed from the network (for example, a PC shut down at the end of the day). This type of an IP address is known as a *dynamic IP address*. To use dynamic addressing, a server must be available to assign the IP addresses to these nodes.

Address Resolution Protocol

As mentioned, MAC addresses are assigned to nodes within a LAN. IP addresses are assigning to nodes and can be static or dynamically learned. The *Address resolution Protocol* (*ARP*) is used within a LAN to connect a device by assigning IP addresses with its MAC address.

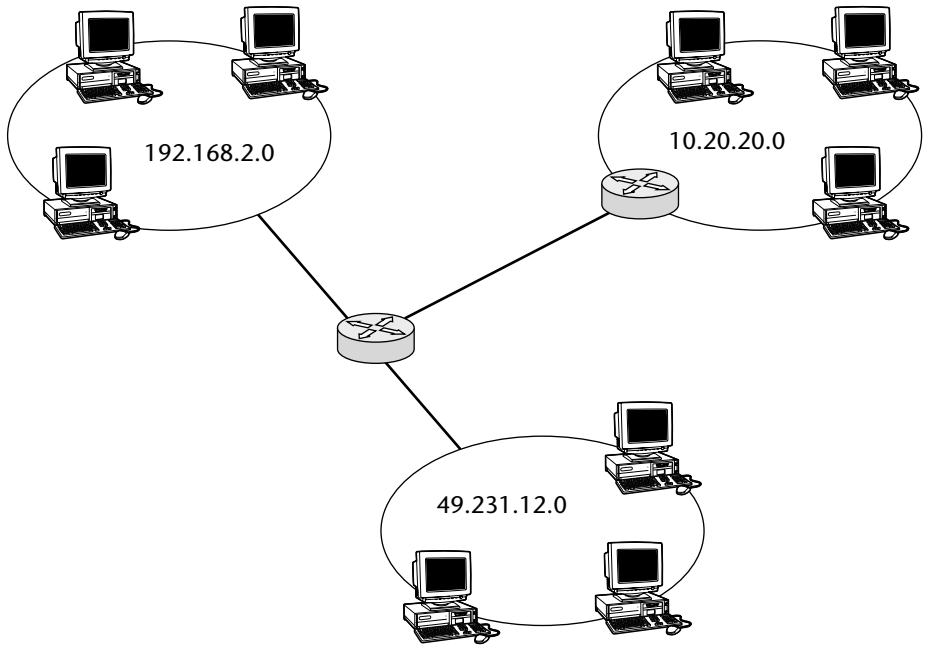


Figure 8-14: Example of IP addressing

Because MAC addresses are used by nodes to forward data to other nodes within the same subnet, MAC addresses cannot be used to send data to nodes within other subnets. The only way that data can get to the other subnets is by the IP address of the device within the other subnet. ARP is also used by nodes within the same subnet to discover the MAC address of the other nodes within the subnet. Figure 8-15 shows an example of how ARP works.

In Figure 8-15, two subnets (Subnet A and Subnet B) are connected to each other by a router. PC-AA and PC-AB are in Subnet A, while PC-BC and PC-BD are in Subnet B.

PC-AA knows the IP address of PC-AB, but does not have the MAC address and will need to get the MAC address to send its data to PC-AB. PC-AA will send out an ARP broadcast to all of the nodes within the subnet. PC-AB will recognize the IP address as its own and will be the only node within the subnet that responds to the ARP request. The ARP response will contain the MAC address of PC-AB. Now that PC-AA knows the MAC address, it will forward the data to the MAC address of PC-AB.

Now, consider that PC-AB wants to send data to PC-BD. PC-AB will send out an ARP request to all of the nodes within the subnet. The router will recognize the IP subnet address for the subnet that PC-BD resides on and will respond to the ARP request. PC-AB will then send all of the data that is destined for PC-BD to the MAC address of the router. It is assumed that the router has already learned the MAC address for PC-BD and it will forward the data to its destination.

ARP data that is collected by a node is stored in what is known as an *ARP cache*, or an *ARP table*. The data resides there unless it is not used for a period of time and then it is cleared out. By maintaining an ARP cache, nodes within a network save time because they do not have to "re-ARP" for nodes that they have already learned.

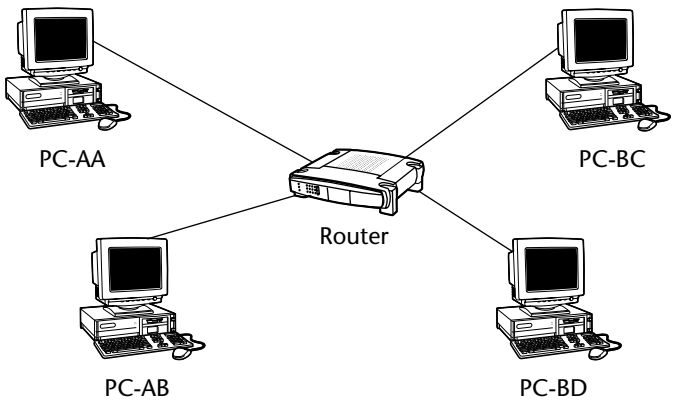


Figure 8-15: An example of ARP

Reverse Address Resolution Protocol

The *Reverse Address Resolution Protocol* (*RARP*) performs the opposite function of ARP. It is used to find the IP address of a node by translating the MAC address to the IP address. RARP is mainly used by nodes that do not have a storage medium and cannot store an IP address.

To obtain an IP address, the node sends a MAC broadcast, which will be answered by a server that supports RARP. The server will match the MAC address of the node that sent the broadcast and will respond with the IP address of the node.

Virtual Local Area Network

An Ethernet LAN is simply a *flat network* that lumps all nodes within the LAN into a single broadcast domain. This is simple to implement, and it allows all nodes to directly speak with each other. These broadcast domains can be split up by introducing routers into the topology. Collision domains are separated by a bridging device, but if there is no router in place, the broadcast domain applies to all nodes within the flat network.

Although a flat network is easy to implement, it can create problems within the LAN. Because of the size of many broadcast domains, security is a big concern with a flat network. Also, data traffic issues can be a big concern because of the amount of broadcasts that are inevitable in a flat network.

A *Virtual Local Area Network* (*VLAN*) can be configured to help split up the broadcast domain. VLAN implementation guidelines are outlined in the IEEE 802.1Q standard. Simply put, a VLAN allows an administrator the ability to logically subdivide the flat network.

VLANs allow any node within a physical network to be part of any configured VLAN. Therefore, a node on the fourth floor of a building can participate in a VLAN no matter where the other nodes physically reside. This allows all of the nodes within a VLAN to send and receive broadcast messages within the VLAN, and to share network resources such as printers. To communicate between VLANs, a router will need to be available to forward the data. Routers enable VLANs to keep broadcasts within the VLAN, and to forward data to other VLANs, when required (see Figure 8-16).

Because routing packets is slower than switching them, VLANs will route the first packet and then will switch any additional packets between VLANs. For example, VLAN 1 has to send a packet to a node in VLAN 2. The first packet will pass to the router and then will be handed up to VLAN 2. After that, all subsequent packets (see Figure 8-17) will be passed through a switch between the VLANs. The reason that the first packet has to be routed is so that the VLAN can learn the route to the other VLAN.

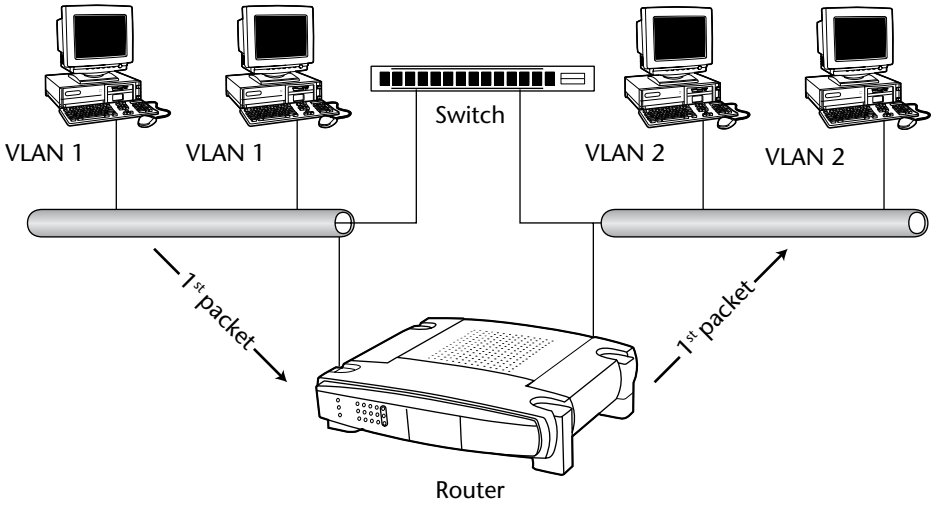


Figure 8-16: Routing the first packet between VLANs

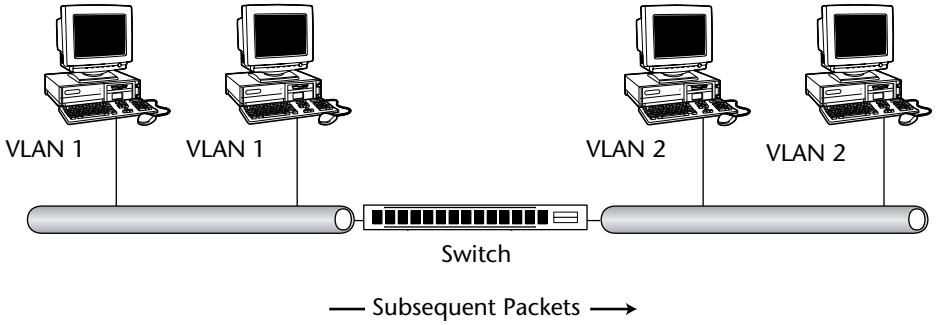


Figure 8-17: Switching packets between VLANs

VLANs are normally broken down into groups. They are especially helpful when users of a group are physically located in various locations within the network. VLANs allow such users to utilize the resources assigned to their group (such as storage devices and application servers), and to be part of the same broadcast domain—all while being physically located in various locations.

When configuring VLANs, the network administrator must decide what type of VLAN to implement. The types of VLANs that are supported by the Nortel VPN Router are as follows:

- *MAC address-based VLAN:* Allows the MAC address of a device to determine VLAN membership. The switch will retain information about MAC addresses and what VLANs the MAC address belongs to.
- *Port-based VLAN:* Groups a series of ports together to form a VLAN. The ports that are within the VLAN can all be part of the same switch, or can be from various switches.

- *Protocol-based VLAN:* Determines VLAN membership based on the layer 3 protocol assigned to the frame received by the switch.
- *Subnet-based VLAN:* Assigns nodes to a VLAN based on the subnet value of the IP address.

Network Routing

A LAN is an *autonomous system* that is controlled by a single administrator for the purposes of providing network users the ability to share and access resources available within the autonomous system. Autonomous systems are often referred to as *routing domains*. Autonomous systems share information within the users of the domain with an *Interior Gateway Protocol* (*IGP*). IGP is a protocol that allows for the exchange of routing information among gateways or hosts within the autonomous system.

The Internet is made up of multiple autonomous systems, each controlled by a separate administrator, that connect to one another with routers. Figure 8-18 shows an example of routing information over a WAN among three autonomous systems.

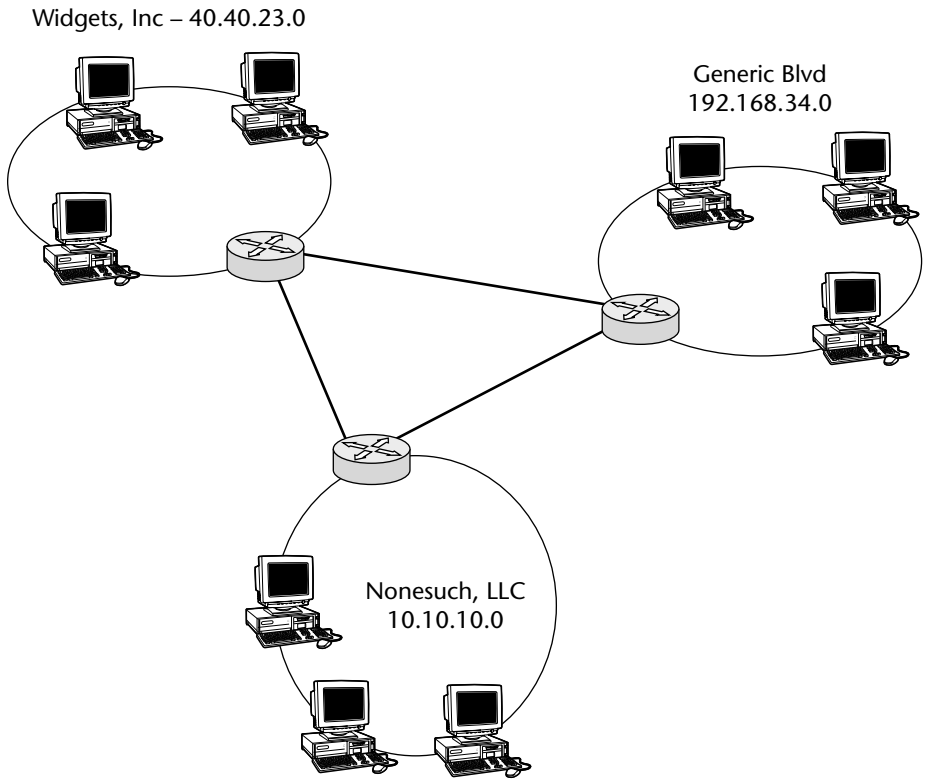


Figure 8-18: Routing data between autonomous systems

These collections of autonomous systems exchange routing information among each other so that all data can be shared within their own autonomous systems. The information is shared between autonomous systems by an *Exterior Gateway Protocol* (*EGP*). EGP is a protocol that allows for the exchange of routing information between gateways to autonomous systems on the Internet. This section discusses the basics of network routing, how routing decisions are made, and how information ultimately reaches its destination.

Routing Basics

Routing is a process of exchanging packets between separate networks that are connected to one another by a router. When a node needs to send a packet to another node within the same subnet, a router is not required because the instruction to get the data to the destination node is learned by ARP and is then retained in the ARP cache of the sending node. When a node needs to send data to another node that is in a different subnet than its own, the sending node will forward the data to a router, which will deliver the data to the path destined for the subnet that the destination node belongs to.

As shown in Figure 8-19, there are three autonomous systems:

- 10.10.10.0
- 192.168.14.0
- 66.74.12.0

Each autonomous system has two workstations. If workstation 10.10.10.1 wants to send data to workstations 10.10.10.2, a router is not required, because by ARP for the destination's IP, 10.10.10.1 recognizes that 10.10.10.2 is within its autonomous system and it will deliver the data to this workstation directly.

Now, imagine that workstation 10.10.10.1 wants to send data to workstation 192.168.14.2. It recognizes that 192.168.14.2 does not reside within its routing domain and will send the data to Router A. Router A refers to its routing table and recognizes a route to the 192.168.14.0 autonomous system. Router A sends the data to that subnet, which will deliver the data to its destination.

If workstation 10.10.10.1 wants to send data to workstation 66.74.12.2, it will send the data to Router A. Router A will recognize that the correct course of action would be to forward the data to Router B. Router B will find the appropriate route and will deliver the data to the autonomous system 66.74.12.0, and ultimately the data will be delivered to workstation 66.74.12.2.

Routers make routing decisions by maintaining a *routing table*. The routing table will provide information on how to get a packet to the next router for delivery to its destination.

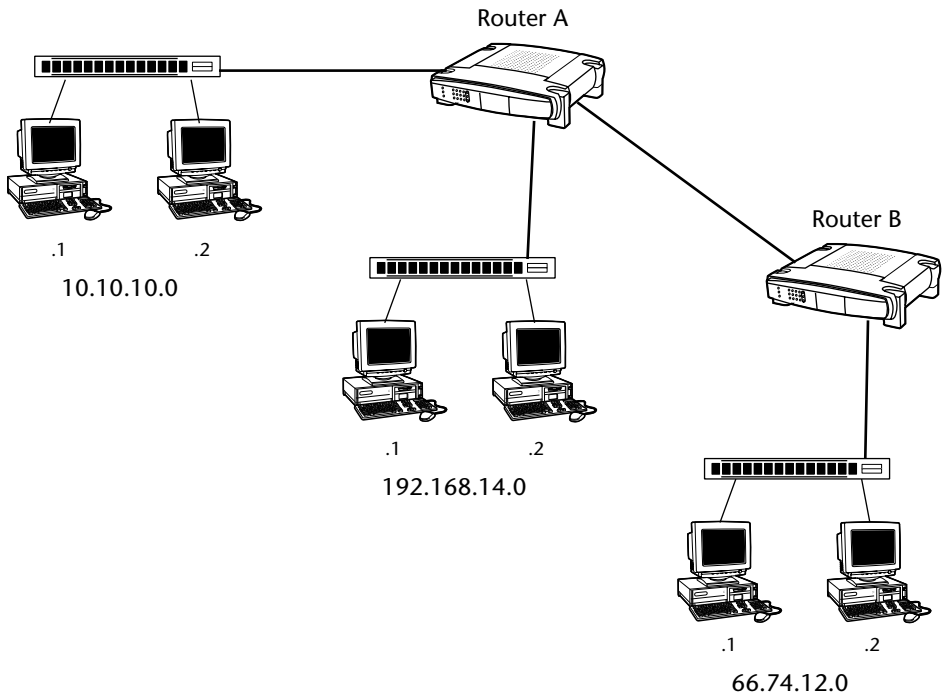


Figure 8-19: Routing data between autonomous systems

Figure 8-20 shows several routers with multiple paths between PC-A and PC-B. If PC-A wants to deliver data to PC-B, it will forward the packet to its border router, which will then use its routing table to determine which of its neighboring routers it needs to forward the packet to in order to deliver it to PC-B.

NOTE **Each router does not determine the entire path to a destination. Each router is only aware of (and concerned with) the path to the next router.**

When building a routing table, a router determines the best path based on several variables. Some of the variables are the shortest path to a destination, if a link is down, if there is congestion on the network, and so on. Additionally, a primary path can be configured by a system administrator by assigning metrics to define the best path to take.

Layer 2 switched networks are limited to growth because of size and node numbering limitations. Routing provides for growth in LANs because it can be used to join subnets within an autonomous system. For Internet data communications, routing is a requirement for allowing multiple autonomous systems to be able to communicate with one another while maintaining the integrity of each individual autonomous system.

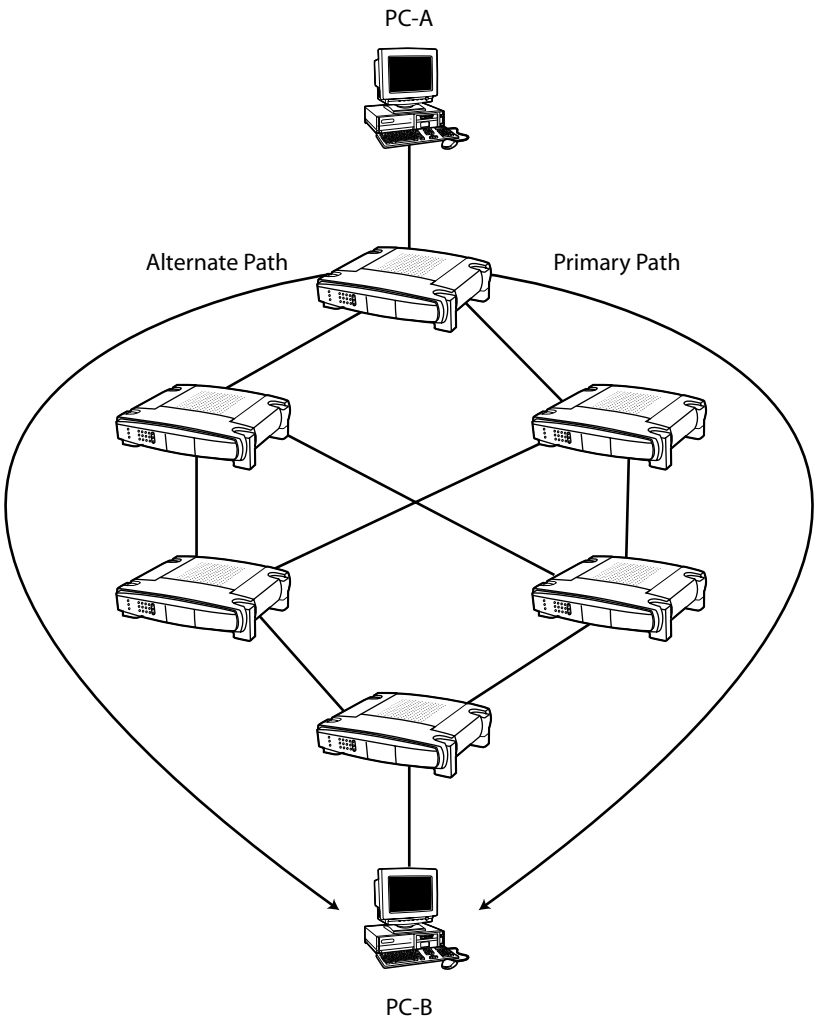


Figure 8-20: Choosing paths to a destination

Routing Tables

Routers retain routing information in a routing table. Routing tables are very important because the basic function of a router is to receive a packet, determine the destination IP address for the packet, look up the routing information in the routing table, and then forward the packet along the correct path toward the destination. Here is an example of a routing table:

```
Active Routes:
Ntwk Dest       Netmask          Gateway         Interface       Metric
 0.0.0.0        0.0.0.0          192.168.1.1   192.168.1.100       1
```

```
127.0.0.0      255.0.0.0       127.0.0.1     127.0.0.1          1
192.168.1.100  255.255.255.255 127.0.0.1     127.0.0.1          1
Default Gateway:       192.168.1.1
===========================================================================
Persistent Routes:
  None
```

The routing table will contain the basic information needed to get packets transferred from point to point until the packet reaches its destination. The routing table will contain the following information:

- The destination IP (usually a subnet address)
- The subnet mask of the destination
- The next hop gateway address between the router and the destination
- The IP address of the interface to be used to get to the next hop gateway
- Routing metric

Each router will maintain its own version of the routing table. This is because the routing information will vary from router to router. Keep in mind that each router has a different position in the mesh, and that the path to a given destination will vary from router to router.

At one time, all paths in a routers routing table were manually inserted by a system administrator. As networks grew, the need for routing information to be inserted dynamically grew as well. This is not only because of the growth that most networks experience, but also to accommodate failed links and node changes. Routing information is still entered statically in some instances, but for the most part, routing table information is built dynamically.

In order for routing tables to be built dynamically, a routing protocol must be used. Routers exchange routing information between one another and update routing tables based on the information that is received. If a link that is connected to a router goes down, the router will recognize this change and will use a routing algorithm to calculate the best new path to get to the destination. The router will then send a routing table update to notify the other routers of the change. A router will also receive routing table updates from other routers, and will perform the same calculations to determine if there are any route path updates that need to be changed and forwarded.

Routing Algorithms

Routing algorithms are used by routers to calculate the best route path to take to get to a destination. The number of steps that a packet takes to arrive at a destination is determined by what is referred to as a *hop*. A *hop count* increments each time a router is reached along a data path between two nodes.

When calculating the best route, information such as the number of hops, traffic congestion, link integrity, and cost is taken into account. Following are the two main algorithms that are used by routers in making these routing decisions:

- *Distance-vector algorithms:* Used when the router maintains information about the other routers it is connected to and is not aware of any other router status within the network.
- *Link-state algorithms:* Used when a router maintains information about the status of the other routers throughout the network along with the traffic status of the network.

This section discusses the differences between these two algorithms and which routing protocols use each algorithm type for routing data in a network.

Distance-Vector Routing

Distance-vector routing is a routing algorithm type that is used by routing protocols to discover routes and to determine the best path to a destination. The most common routing protocol that uses distance vector routing is the *Routing Information Protocol* (*RIP*), which is discussed later in this chapter. The distance-vector routing algorithm in its basic form is used to determine the distance and direction to any known link within the network.

When using distance-vector routing, routing information is shared between routers by advertising the distance and the direction that must be taken in order to arrive at a destination. The distance is calculated in hops (more on hops in the section on RIP later in this chapter). The direction is determined by the interface that leads to the destination.

Distance-vector routing algorithms will provide routing table updates by sending a copy of its routing table to neighboring routers (see Figure 8-21). Each router will receive the routing table that was handed off to it by a directly connected router. In the example, Router A receives a routing table update from Router B. Router B received updates from both Router A and Router C. Router C receives an update from Router B and Router D. Finally, Router D receives an update from Router C.

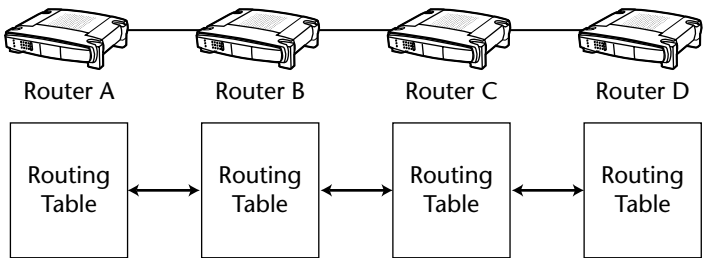


Figure 8-21: Distance-vector routing updates

For example, imagine that the only change that is occurring between updates is that Router A notices a link has gone down. It will calculate a new distance vector and will update this in its routing table. Router A will then forward the new routing information to Router B. Router B will increase the distance vector and will then forward the update to Router C. This process will continue until the routing update is provided to all of the routers in the network.

The distance-vector routing algorithm becomes a bit more complex when there are multiple paths to a destination. When there are multiple paths, the router will determine which path is the best path based on the distance vector. The router will use the best path until such time as another path takes preference, and it will then switch routing to the alternate path (which has become the best path). Most often, the best path is the one with the shortest distance vector.

Distance vector is easy to maintain and is most commonly used in small to mid-sized LANs. Once of the main disadvantages of a distance-vector solution is that it requires periodic routing updates, even when no changes have been made or recognized by any routers within the LAN. This not only consumes bandwidth, it also requires some resources to process the routing table update. Another disadvantage is that routing table updates occur at a periodic timeline and may not reflect any new changes that occur between updates.

Link-State Routing

Link-state routing is a routing algorithm type that is used by routing protocols to discover routes and determine the best path to a destination. The most common routing protocol that uses link-state routing is the *Open Shortest Path First* (*OSPF*) routing protocol, which is discussed later in this chapter. The link-state routing algorithm keeps track of the entire topology of the network.

Unlike routers in a distance-vector routing topology, link-state routers keep track of information about all routers and how they connect to one another. Routers using the link-state routing algorithm employ the following functions:

- Link-State Advertisements (LSAs)
- Topological information
- Link State DataBase (LSDB)
- Shortest Path First (SPF) algorithm
- Routing tables

Each router in a link-state network will provide routing updates to one another in the form of LSAs. An LSA is a packet of information shared between routers. The LSA contains link-state information known by the originating routers and shared with others. The information that is obtained in an LSA is used to develop a topological database, which is nothing more than a repository of information that has been gathered from the LSAs that have been received.

Once a router has routing information in the database, it will use the Shortest Path First Algorithm to calculate the best, shortest path from the router to the destination. The result of the calculation is what is known as the *SPF Tree*. The SPF tree is structured data with the owning router as the root and branches going to other known routers, representing the network router topology. Finally, a list of all known data transport paths and the interfaces that they connect to is stored in the routing table of the router.

In a link-state environment, the router that first recognizes a change in link state will forward the information about the link-state change so the other routers are aware of and can send updates. Each router will keep track of its routing tables and will also keep track of the neighbor routers. The router will then develop an LSA packet that will contain the following information:

- Router name
- Status of the interface
- Neighbor link costing information
- New neighbor information
- Changes in link cost
- Invalid link information

The LSA is then flooded so other routers can update their routing information. Every time that an LSA is received, it changes information in the link-state database and routing table updates.

Link-state routing requires more data processing than distance-vector routing does. The routers utilize resources to retain information received, build database information, build the SPF tree, and update routing tables. When link-state initial convergence occurs, it consumes a lot of bandwidth to accomplish all of these functions. However, after the initial updates are done and convergence is achieved, then updates are all triggered by a link-state change and, therefore, will require a minimum amount of bandwidth to accomplish the updates.

Routing Protocols

Without question, one of the most important networking functions is routing. Routing occurs at layer 3 of the OSI reference model (the network layer). Although responsible for a few other functions, routing is the function that most people associate with the network layer. It is the job of the router to accept packets, determine where the packets are destined for, and to forward data on toward its destination. The router uses a routing protocol to develop and maintain routing information, as well as passing data.

Routing Protocol Types

There are two basic types of routing protocols. The first type is known as Interior Gateway Protocol (IGP), which defines the routing process for routers on the interior of an autonomous system. The second type is known as an Exterior Gateway Protocol (EGP), which defines the routing process between autonomous systems.

The most common IGP routing protocols that are in use by most LANs are Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF). The most commonly used EGP standard is the Border Gateway Protocol (BGP). These routing protocols can be considered the core protocols of their respective routing protocol types.

Routing Protocol Concepts

As mentioned, an autonomous system is a collection of routers that is passing information within a network. Within the autonomous system are two basic types of routers:

- *Internal router:* Routers that are passing data to users within the autonomous system
- *Border router:* Routers that are passing data not only within the autonomous system, but also to other border routers in other autonomous systems

Because internal routers route information within an autonomous system, they utilize only an IGP routing protocol type to do so. Border routers are a little different. They not only are passing information within an autonomous system, they also pass data to other border routers over the Internet. Because of the need to pass internal as well as external routing data, the border routers utilize both an IGP and an EGP routing protocol type. Figure 8-22 shows an example of interior and border routers.

In Figure 8-22, there are three interior routers and two border routers. Because Border Router A and Border Router B need to communicate with one another, they must employ an EGP routing protocol to be able to pass information to one another. Otherwise, they would not have a mechanism to use to be able to learn about each other and, therefore, would not be able to send data to and from each other.

Because Border Router A and Border Router B also must route data within the autonomous systems, they have to be running some type of an IGP routing protocol. This allows them to learn of destinations that are needed in order to pass data within the autonomous system.

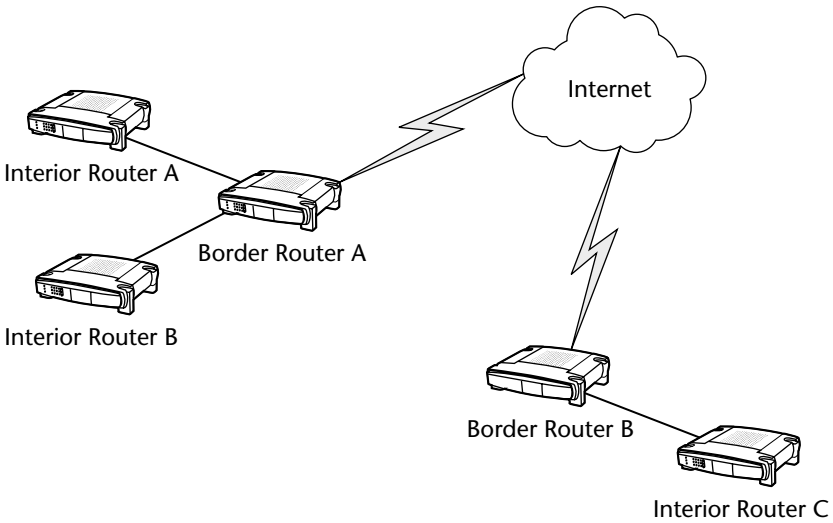


Figure 8-22: Example of interior and border routers

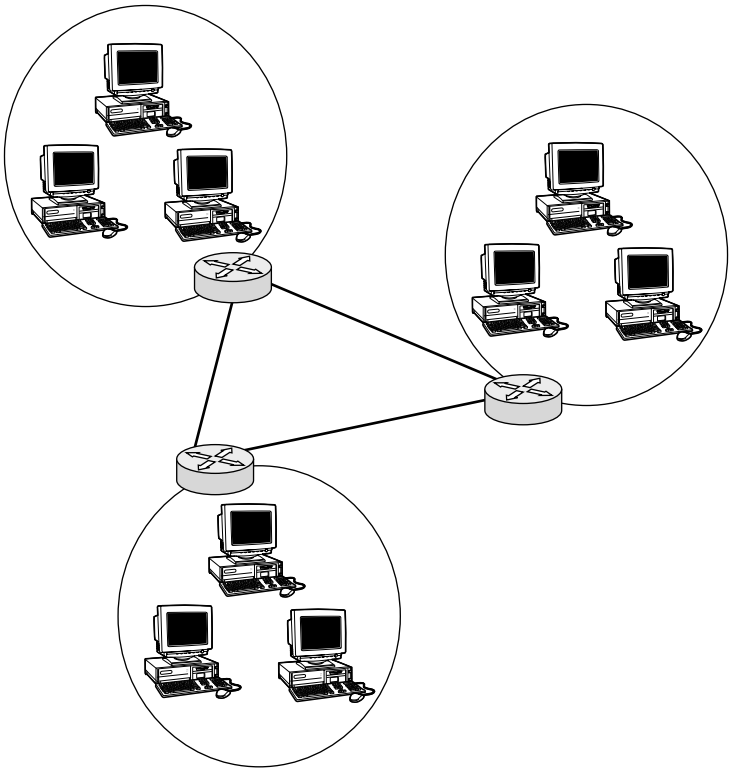
Routing Information Protocol

The *Routing Information Protocol (RIP)* is the most common Interior Gateway Protocol (IGP) used in most LANs today. RIP is used to route data by managing the information that is provided to a router in a network.

Any subnet edge node that supports RIP will send out RIP information to other edge devices. The routing information that is sent out is known as a routing table, which contains information about all of the IP devices that the edge device knows about. Each of the neighboring devices then sends out routing information to its neighbors with the information that it has learned, along with the information of the devices that are local to it. Figure 8-23 shows an example of a RIP routed network.

As mentioned previously in this chapter, the data path that is taken from one node to another within a network is determined by what is referred to as a hop. A hop count increments each time a router is reached along a data path between two nodes. RIP will use the information in the routing table to determine how many hops it will take to get from the source to the destination. RIP will then use the path that contains the least number of hops to get from point A to point B.

For example, in Figure 8-24, it takes one hop to get from Router A to Router B; from Router A to Router C would be two hops, and so on. Router A will receive a routing update from Router B (its only connected node). Router A will know how many hops it takes to get to Router F, which is simple considering there is only one path to take. Router A knows that in order to get to Router F, it will take five hops.



Routing Information Protocol Domain

Figure 8-23: Example of an RIP routed network

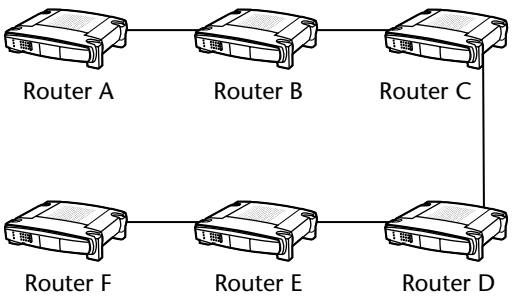


Figure 8-24: Example of hop count along a single data path

Now, take a look at Figure 8-25. Notice that there are now two directions that data traffic can pass to get from one router to another. In making routing table decisions, Router A will receive routing table updates from both Routers B and F. Realizing that it is now only one hop between Router A and Router F, Router A will update its routing table to ensure that all data traffic destined for the Router F subnet is routed over the link with the least hop count.

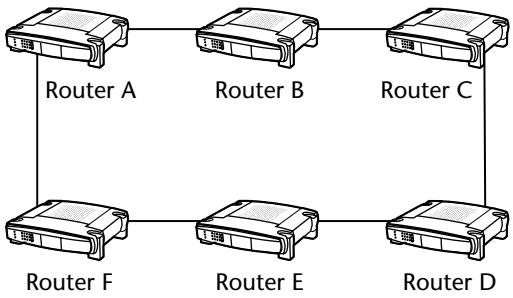


Figure 8-25: Example of hop count based on alternate data paths

RIP makes routing decisions based on the distance between two communicating devices. RIP table updates are sent out every 30 seconds. All RIP nodes will compare the information received to what is contained in its current routing table and will make the appropriate updates or changes. The node will then send the updated routing table to its neighboring RIP nodes, and the process continues throughout the RIP nodes in the network.

RIP History Overview

In the early years of the Internet, most technical companies had their own routing protocol that was used to allow their equipment to communicate with one another within a LAN. The concept of networking continued to grow, and, as it did, so did the routing protocols that were being developed. You could say that these developing protocols were early versions of RIP because the ideals used were eventually incorporated into RIP.

RIP began to become a standard in 1982 at the University of California at Berkeley. This early version of RIP was actually named *Routed* (*Route-d* or *Route-daemon*) and it was developed for use with the Berkeley Standard Distribution (BSD) implemented within the UNIX operating system. At this time, a lot of platforms were running this standard. Because of the wide distribution of this standard, RIP quickly became the standard for routing within internal LANs. RIP did not become an official standard until 1988, when the first RIP RFC was published. This original version of RIP is often referred to as *RIP version 1* or *RIP-1*.

Because RIP was developed in the early years of the TCP/IP protocol, eventually it had to be updated to support the many changes that had occurred to TCP/IP over the years. In the early 1990s, *RIP version 2* (*RIP-2*) was released. There were several new features in RIP-2, most notably:

- Classless Inter-Domain Routing (CIDR)/Variable Length Subnet Masking (VLSM)
- Authentication
- Support for multicasting

For the last several years, progress has been made on the development of a new implementation of the IP protocol standard. The most common version of IP that is implemented throughout is *IPv4* (*IP version 4*). The new implementation is IPv6. Because of this new IP standard, a new version of RIP is also being developed, which is needed to support many of the changes in IP. The new version of RIP is called *RIPng* (*RIP next generation*).

RIP Route Determination

RIP uses a distance-vector routing algorithm for making routing decisions. The main function of RIP is to provide information about routes to its neighboring routers. All of the routers in a RIP domain maintain a routing table that contains information about the network and the hosts that it has learned. The routing table will contain such information as:

- The destination IP (usually a subnet address)
- The subnet mask of the destination
- The next hop gateway address between the router and the destination
- The IP address of the interface to be used to get to the next hop gateway
- Routing metric

RIP determines the number of hops it takes to get to a destination. The maximum number of hops that RIP will allow is 15. A network or a host is determined to be unreachable if the hop count reaches 16 before the destination is obtained.

RIP routers will send out routing updates periodically throughout the network. Each router will send an update to its neighboring routers, containing information about the routes that it is aware of. The receiving routers will compare the information in the routing table that it has received to its own routing table. If a route to a network is a shorter hop count in the receive routing table, then the router will update its routing table, will add a hop count of one, and will forward its updated routing table to the next router. This process continues until all routers have received updates.

NOTE A RIP router will update a route in its routing table only if it receives information about a shorter route to a network. Otherwise, it does not change the entry in its routing table.

In addition to periodic updates, RIP routers will also generate and send routing table updates whenever there is a topology change within an attached network.

RIP Updates

RIP routers communicate with one another through RIP messages. Routers send out what are known as *RIP requests* when it wants another router to send the routing table, or a portion of the routing table. Routers send out *RIP responses* when responding to a RIP request or when sending out a routing table update.

RIP Request

A router will send out a RIP request when it needs an update to a routing table. Normally this occurs when the router is first booted up. Another example of when a RIP request is sent out is when you are troubleshooting connectivity issues with a route.

RIP Response

There are three scenarios when a router would send out a RIP response:

- When it has received a RIP request
- When it sends out a periodic update
- When it sends out an update because of a topology change

In Figure 8-26, there are four routers. Each of the routers connects two subnets within an autonomous system. Router A connects to Subnet A and Subnet B. Router B and Router C connect to Subnet B and Subnet C. Router D connects to Subnet C and Subnet D.

Assume that Router A is having problems reaching nodes in Subnet D. While troubleshooting the issue, a decision is made to "flush" the routing table on Router A. This is done to clear the routing table and to force the router to relearn routes.

Router A will send out a RIP request to Router B and Router C. In the RIP request, Router A will send its routing table, which will contain information about the routes that it is aware of. In this case, Router A will have only a route to Subnet A and to Subnet B in its routing table. Because the distance to each of these subnets is one hop, the metric of 1 will be in the routing table.

Router B and Router C will receive the RIP request and will increase the hop count metric by 1. Each of these routers will compare the received routing table with information that they have in their own routing tables. In this example, each of these routers already has a route to Subnet B. In the received routing table, the hop count to Subnet B is now 2. In the routing table on these routers, the hop count is set at 1, so they will not update this route. Each router will now add the route to Subnet A to their routing table (this is assuming that there was not a route to the subnet already—it had been flushed from the routing table). After these routers are complete with their routing table updates, they will send their routing tables to the directly connected routers.

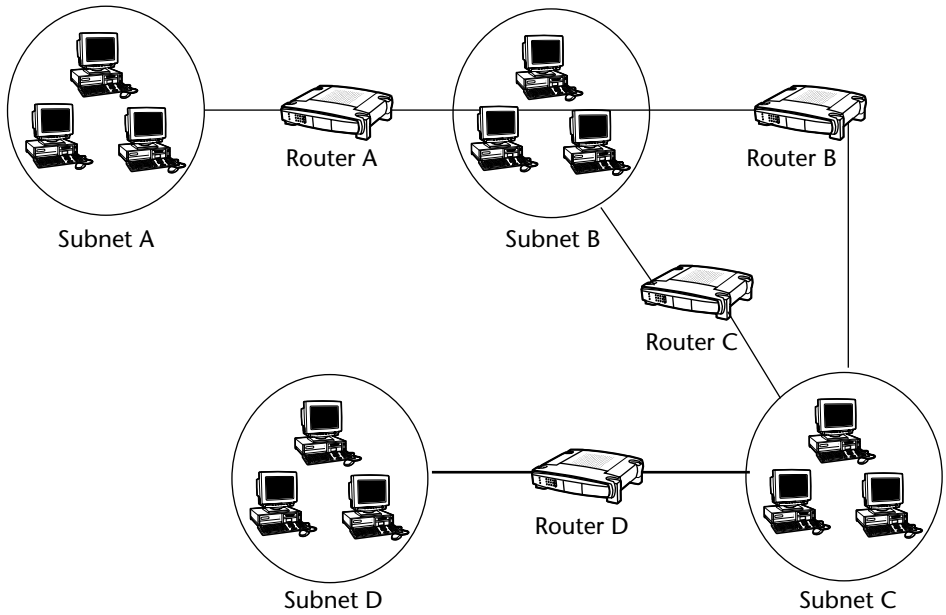


Figure 8-26: Rip updates

Router A and Router D will receive the RIP response routing table updates and will compare the information received with the information that is in their respective routing tables. This will continue until all routing updates have been sent and all routing tables have been updated.

Timelines

RIP periodic updates occur every 30 seconds. Because of this, RIP normally will only respond to entire routing table requests or will just wait for the periodic update to respond to a partial routing table request. The 30-second updates are determined by a timer. When the timer expires, a routing table update is sent and then the timer is reset. This method ensures that all routing information in all routers is kept as up to date as possible.

Each individual route in a routing table also has a timer. Every time a route is received, the timer is reset. If the router does not see any updates for a particular route before the timer for that route expires, then hop count is set to 16 for that route and it becomes unreachable. The router timer default value is normally 180 seconds. RIP routers will remove routes that have expired after 120 seconds from the time they have expired. This gives the route time to recover before it is completely removed from the router's routing table.

Open Shortest Path First

The *Open Shortest Path First* (*OSPF*) protocol is another IGP used in networks. Because of the routing updates required by RIP, many larger LANs rely on OSPF to provide the routing updates and ensure that data reaches its destination.

Unlike RIP, which sends routing updates every 30 seconds, in an OSPF domain, each node will maintain its own routing table and the only time that a routing update is provided is when there is a change to that node's routing table.

OSPF can operate securely in a network. It authenticates peers before forming an adjacency with the peers. An OSPF network consists normally of several small networks, known as *areas*. A central area, known as the *backbone area,* serves as the core of the OSPF network. All areas in an OSPF network must connect to the backbone. Figure 8-27 shows an example of an OSPF network.

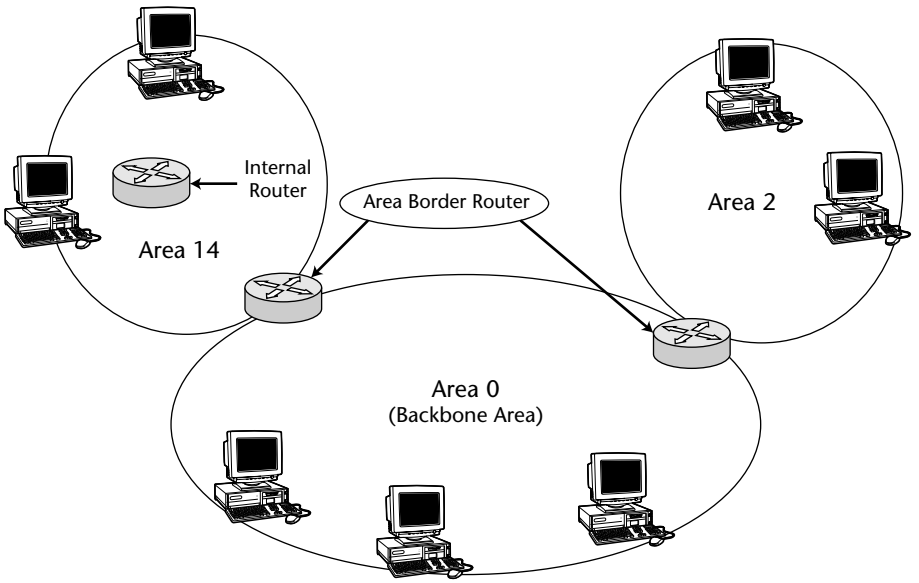


Figure 8-27: Overview example of an OSPF domain

OSPF History

For the early years of networking, RIP was the IGP routing protocol that was the standard used by most LANs. It was fairly simple to maintain and, because it was a standard, most TCP/IP nodes supported RIP. RIP did have its share of problems, however. The main problem was that as networking grew, RIP was unable to meet the demands brought upon by this growth. Following were the main concerns with RIP:

- The bandwidth necessary to provide routing table updates increased.
- The 16-hop limitation did not meet the needs in LANs that had hops that were legitimately more than 16 hops away.
- The distance-vector algorithm had difficulty keeping up with changes that occurred regularly in larger LANs. Therefore, the best route was not always chosen.

Realizing that networking for some had outgrown the limitations of RIP, the Internet Engineering Task Force (IETF) set up a committee to come up with an alternate routing protocol that could assist in resolving some of the issues that larger LANs faced with RIP. The committee was formed in 1988 and it was decided that the new protocol should utilize a link-state algorithm instead of the distance-vector algorithm, which is what RIP uses. In October of 1989, the OSPF routing protocol was introduced as a TCP/IP standard. The name for the protocol appropriately described its function:

- *Open:* Because it was an open TCP/IP standard, free to be utilized and openly available
- *Shortest Path First:* Because the link-state routing algorithm is also known as the Shortest Path First algorithm

OSPF went through several changes in its formidable years and *OSPF version 2* (*OSPF-2* or *OSPFv2*) was introduced in July of 1991. Since then, there have been a few updates, but no revision number changes. OSPF version 2 is the standard version of OSPF used in networking.

OSPF Considerations

When implementing OSPF, a few considerations must be understood and taken into account. This section discusses some of these considerations. It is important to understand these few concepts about OSPF.

Router Unique Name

OSPF requires that each routing within the OSPF autonomous system has a *unique router ID*. These router IDs can be assigned manually by the network administrator, or they can be assigned automatically by the protocol itself. If the routing name is automatically assigned, then the unique name that will be given will match the highest IP address value out of all of the router's active interfaces.

Adjacencies

OSPF routers must also form what is known as an *adjacency* with each of its neighboring routers before a connection can be formed and routing can take place between the two routers. Once a router has discovered a neighbor router, communication takes place between the two routers until the adjacency is formed. An adjacency is basically an agreement between the two routers to share routing information and to maintain an active link between one another.

OSPF allows for routers to be connected to one another over Ethernet, Point-to-Point Protocol (PPP), Non-Broadcast Multiple Access (NBMA) links, Ethernet LANs, frame relay, and ATM. The type of adjacency that can be formed between neighbors depends on the type of connection they share.

OSPF Processes

OSPF utilizes some sub-protocol processes that allow it to discover neighboring routers, form a communication channel with a neighbor, and share routing information. Following are some of these features:

- *Exchange:* The exchange process allows routers to exchange routing information with one another. Any information that is received from a neighbor is placed into a database known as the Link State DataBase (LSDB). All routers are required to ensure that their LSDBs are in sync with one another.
- *Flooding:* Routers send out link-state updates through a process known as flooding. Whenever a router notices a change in link state, it will flood Link-State Advertisements (LSAs) out all of its interfaces. Each router that receives an LSA will compare the information with the information contained in its own LSDB. If the information is already in its LSDB, the router takes no further action. If the information is not in its LSBD, the router will then flood an LSA out of all of its interfaces except the interface that it originally received the LSA from.
- *Routing table:* Routers will build and maintain a routing table that will contain route path information that was developed by the SPF algorithm. Every router in an OSPF domain will have its own topological location within the domain and, therefore, will maintain a routing table that is unique to that router.

OSPF Areas

OSPF utilizes the concept of areas, which allows for the dividing up of the network to assist in reducing the amount of routing information exchange that is occurring within the autonomous system. OSPF areas will provide detailed routing information about the area within the area and will only provide basic routing information to other areas. Overall, this reduces the amount of routing updates that occur within the autonomous system.

OSPF is an IGP and, therefore, routes information within an autonomous system. OSPF is also able to route information to other autonomous systems. When routing over the Internet, OSPF utilizes the servers of BGP to route information to other autonomous systems.

OSPF utilizes areas within an autonomous system. Remember, an area is a collection of routers that share routing information with one another. OSPF areas will share information with other areas, but the information shared is only a single route for the range of addresses within the area. When the SPF algorithm is run for the routers within an area, only routers in that area are considered.

Recall that routers contained within an area are known as internal routers. Routers that have interfaces that connect outside of the area are known as *Area Border Routers* (*ABRs*). ABRs will summarize route information for the area that they are members of and will provide this information to other ABRs. ABRs maintain an LSDB for each area that they are a member of. Figure 8-28 shows an example of ABRs and internal routers.

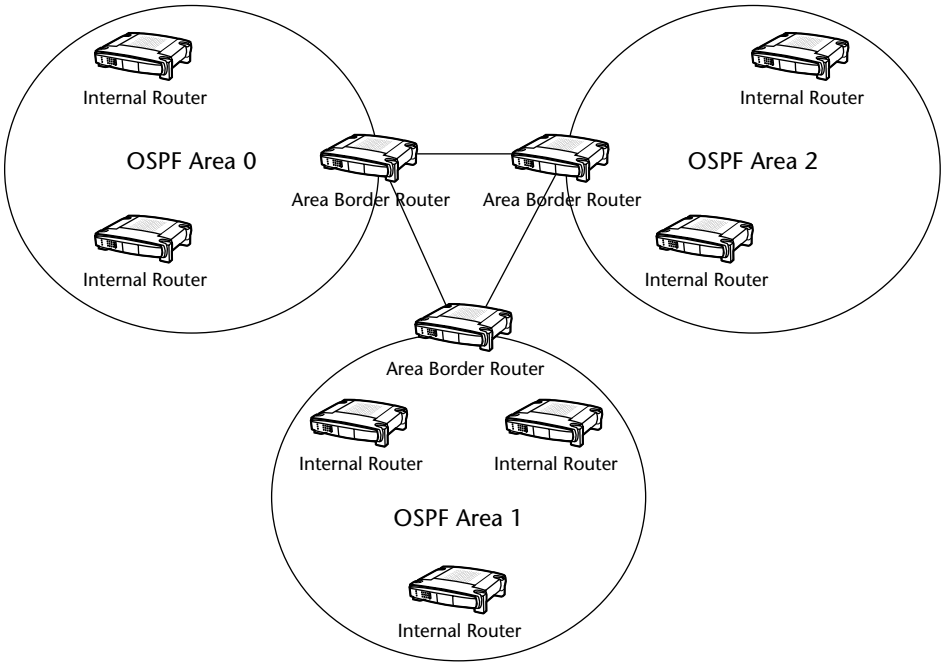


Figure 8-28: OSPF areas

Autonomous systems connect to one another with what is known as an *Autonomous System Boundary Router* (*ASBR*). ASBRs exchange summary information with other ASBRs. OSPF is the routing protocol that is used to exchange this information. If the information is exchanged over the Internet with another autonomous system, then BGP is the routing protocol that is used. Figure 8-29 shows an example of an ASBR connecting to an ISP.

OSPF Overview

When a router in an OSPF routing autonomous system originally joins the domain, it begins learning routing information about the links that it is connected to, as well as the links that are known by its neighbors. The router will then take the routing information that it has learned and place it in its LSBD. Once it has learned all of the known routes, it calculates the SPF information and enters this information into a route-forwarding table.

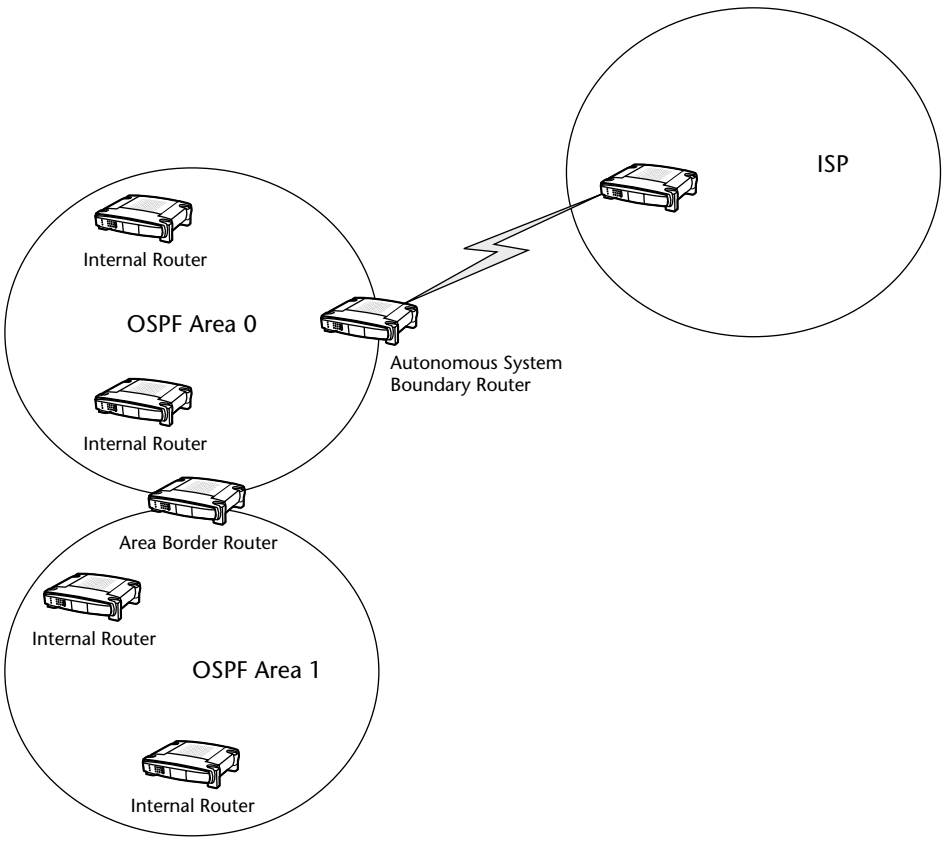


Figure 8-29: Example of an ASBR connecting to an ISP

Hello Messages

Routers learn information about neighboring routers by exchanging hello messages between one another. Once the hello messages are exchanged, the neighboring routers form adjacencies with one another. The hello messages will contain the routers unique ID and network information.

The hello process allows a router to discover its neighbors. Once neighbors have been discovered, a relationship is built between the two routers. Depending on the connection type, these hello packets are either multicast packets, or are packets that are directly sent to neighboring routers.

Hello messages are sent out periodically to check the status of neighbors and links. If a hello message is sent and a reply is not received, then the router will assume that a link is down, or that a neighboring router is down. In this case, the router will rebuild its topology information.

Routers in an OSPF autonomous system will respond to hello messages by returning a hello message. In the return hello message, the router reports its unique ID, and a list of the routers that it is aware of. When this return message is received, the originating router assumes that two-way communications is up.

LSDB

Each router in an OSPF autonomous system builds an LSDB based on the topology information it receives from its neighboring routers, as well as the topology information that it learns from its own direct links. The LSDBs for all of the routers within an area must have matching entries. This is ensured by the routers through the process of synchronization. When LSDB synchronization is completed, each router builds a routing table based on the SPF algorithm.

When routers first learn about one another, they send out data description packets. The information in the data description packets provide the information needed for the initial setup of the LSDB. Once established, all future updates are handled by LSAs. LSAs are processed by the router immediately upon receipt. This ensures that routing information is updated quickly and contributes to the stability of routing information. LSAs are received with sequence numbers attached to them. This helps identify duplicate routing information that may be coming from other routers.

Shortest Path First

Once a router has completed updating its LSDB and the LSDBs are synchronized with the other routers within the area, the router will use the SPF algorithm to update the routing table. This is done by building a tree in which the router is the root and it builds topology information for all known links. During this process, the router will use this tree to trace paths from itself to a destination. The costing for each successive link within the tree is added up and the router determines, by the total, which path is the shortest path to a destination.

After the router has verified that the LSDB is in sync with the other routers' LSDB, then the router will implement the Shortest Path First (SPF) algorithm (also known as *Dijkstras Algorithm*). The SPF algorithm will extract information from the LSDB and will use this information to determine the shortest path from itself to its destination. Sometimes a cost may be assigned to a path that will override the default shortest path, thus utilizing a path that is preference-picked and is not necessarily the shortest path.

Border Gateway Protocol

The Border Gateway Protocol (BGP) is an EGP that provide routing information between boundary routers of separate autonomous systems. Because this is a routing protocol that updates routing information over the Internet, an autonomous system often will be the ISP that is known by the LAN boundary router on the other end of the link.

Just as an IGP routing protocol is used to update routing information within an autonomous system, an EGP provides this function over the Internet between autonomous systems.

BGP is the most commonly used EGP routing protocol today. Most ISPs use BGP to exchange routing information between the autonomous systems that they connect to. Many ISP core routers maintain hundreds of thousands of routes in their routing tables.

BGP History

The predecessor to BGP was the Exterior Gateway Protocol (EGP). EGP performed well and was able to handle most exterior routing services for many years. As time passed and autonomous systems grew, the need for a more updated EGP routing protocol became apparent. In June of 1989, the BGP standard was introduced.

Work has continued with the BGP standard, with many revisions being introduced for features and/or fixes to issues that developed along the way. The most current version of BGP was introduced in July of 1994 and it was called *BGP version 4* (*BGPv4* or *BGP4*). BGP4 has an updated revision that came out in March of 1995. Still referred to as BGP4, the latest revision included support for Classless Inter-Domain Routing (CIDR). This is the version that is in use today.

BGP Overview

The main function of BGP is to exchange routing information between autonomous systems. To be able to route information between autonomous systems, at least one router within the autonomous system must be running BGP.

Each router that is running BGP will maintain routing information about networks that it has learned, and the routes that are used to get to those networks. The routing information is shared between BGP routers, thus allowing autonomous systems to communicate with one another. Here are a few key points to note:

- BGP routers connect to one another in any manner.
- There can be more than one BGP router in an autonomous system.
- BGP routers within an autonomous system can communicate with one another.

BGP keeps information about destination paths instead of simply storing next hop information. The path information is the order of autonomous systems between the router and its destination.

The routes that are chosen by BGP are determined by collecting information about paths to destinations and then choosing a reliable route to a destination. The algorithm used by BGP is aware of routing loops and other communication problems, and it chooses paths that avoid these problem conditions. BGP routes can also be forced by configuring path attributes to ensure that BGP uses the administrator's preferred path. The path chosen by BGP is not necessarily the best path because BGP has no way of controlling data flow within autonomous systems that may affect traffic data flow on the exterior of the autonomous system.

BGP communicates with neighboring routers to provide and receive routing information. Following are the message types that are exchanged between neighboring BGP routers:

- *Open messages:* Used to make initial contact with neighbor routers and to establish the initial BGP session.
- *Update messages:* Used to provide routing update information about known routes that are accessible. BGP updates are only sent when a change notification is required.
- *Keepalive messages:* Used to keep sessions up.
- *Notification messages:* Used to announce recognized errors.

BGP Topologies

Because BGP can be implemented between external links within autonomous systems as well as between autonomous systems, it is very resilient and can support multiple topology configuration types. Whether the environment is fully meshed (see Figure 8-30) or sequential in nature (see Figure 8-31), BGP can support the topology.

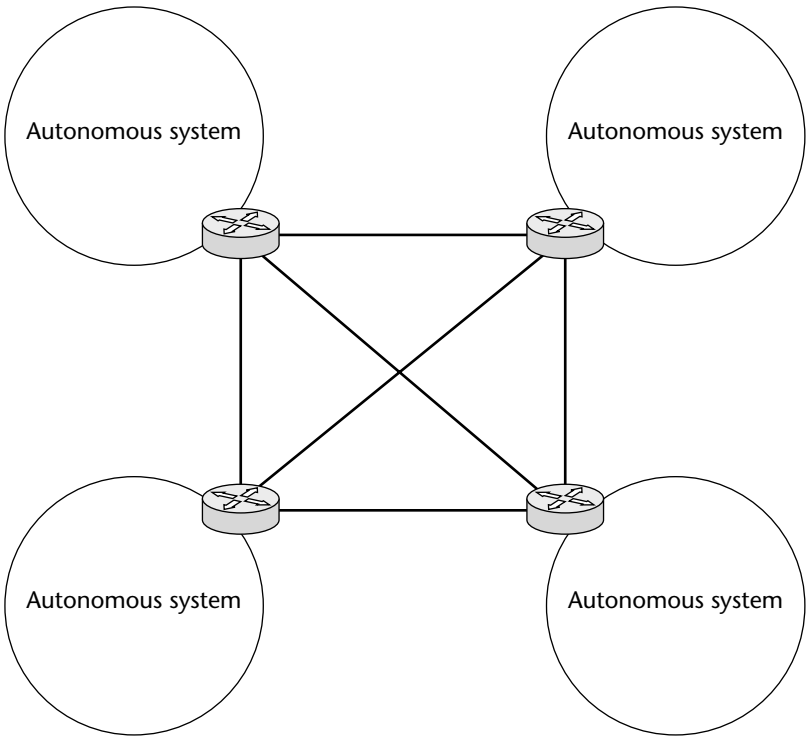


Figure 8-30: Fully meshed topology

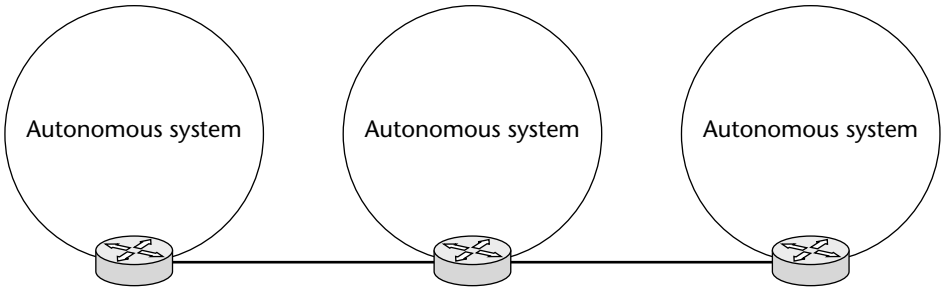


Figure 8-31: Sequential topology

Routing Concepts

BGP is an EGP routing protocol. This means that BGP is not aware of what routing is taking place within autonomous systems. BGP only concerns itself with the routing taking place on the exterior of the autonomous system.

In BGP, routers that are contained within an autonomous system are referred to as internal routers. The routers that are running BGP that connect

the autonomous system with another autonomous system are referred to as Border Routers. Any BGP router that resides on an autonomous system that communications with peers is known as a *speaker*. It is called this because the router communicates with other peers to send, receive, and process routing updates.

Most BGP border routers connect to more than one BGP border router. This helps ensure that there are multiple paths to a destination, ultimately ensuring that the routers are more efficient because of multiple direct routing path choices and redundancy. BGP routers establish and maintain neighbors with routers that they connect to. A BGP router can form a neighbor relationship with another BGP router within its same autonomous system. These neighbor relationships are referred to as *internal peers*. A BGP router can also form a neighbor relationship with another BGP router that is not a member of its autonomous system. These neighbor relationships are referred to as *external peers*.

Routing Information

The purpose of BGP is to provide routing information, to receive routing information, and to process the routing information. The BGP router will utilize the information that it receives and learns about to determine the most effective route to a destination. Every BGP speaker is required to follow BGP guidelines to manage routing information.

Routing Information Base

BGP routers maintain routing information in the *Routing Information Base* (*RIB*), which consists of three sections of information:

- *Adj-RIBs-In:* Contains route information that has been received by the router's peers. These are the routes that are ready to be processed.
- *Adj-RIBs-Out:* Contains route information that the router is prepared to send to its peers.
- *Loc-RIB:* Contains routing information that the router has received and has determined to be valid routing information.

The three sections of RIB information can be stored separately or combined into one part. That determination is made by the system administrator who will set the appropriate configuration parameters that will determine the choice.

Managing Route Information

Managing routing information on the Internet is a very important process. There are multitudes of nodes processing data and there are even more autonomous system activities that are relying on getting data to other autonomous systems.

To ensure that route management is handled correctly, BGP routers perform four central tasks that are used for the purpose of acquiring, processing, and sharing routing information:

- *Advertisement:* This process is used by the speaker to notify peers of topology information.
- *Update:* This is a message type that is used to deliver the routing information that is received and sent to and from the BGP speaker.
- *Selection:* This is the process used to determine the most efficient route to a destination.
- *Storage:* This is the process of keeping routing information stored in the RIB.

Path Vector Routing Algorithm

Previously in this chapter, you learned that RIP uses the distance-vector routing algorithm and OSPF uses the link state routing algorithm. The routing algorithm that is used by BGP to process routing information is the *path-vector routing algorithm*.

Because BGP is an EGP and keeps routing information on multiple autonomous systems, the path-vector protocol is used. Path-vector allows the BGP routers to understand not only the direction to take to get to a destination, but also the state of the path. This ensures that the router is sending data over the more efficient path. Path-vector updates between pairs contain destination addresses, as well as information about the complete path to a destination.

BGP speakers will advertise routing information while including what is known as a *path attribute*. Following are the four types of path attributes that can be used:

- Well-Known Mandatory
- Well-Known Discretionary
- Optional Transitive
- Optional Non-Transitive

Some of the path attribute types are very straightforward, while the others can be confusing. BGP relies on the path attribute types when determining the most efficient path to a destination.

Virtual Router Redundancy Protocol

Routers are used to connect subnetworks to one another. This can be within an autonomous system or between autonomous systems. In some network configurations, there is a single link to get from one subnet node to a node in another subnet. If that single link fails and there are no other paths to the destination, then the link is considered the single point of failure. Figure 8-32 shows an example of this. The link between Router A and Router B has failed. Because there is not an alternate path between the two subnetworks, data flow is stopped until communication on the link between Router A and Router B is restored.

Virtual Router Redundancy Protocol (*VRRP*) is used to eliminate the single point of failure by allowing the system administrator the ability to configure a virtual address on two separate routers. By doing this, redundancy to the link is introduced, which increases the efficiency of the network. VRRP allows the routers to act in a master/backup relationship, with the backup taking over the task of routing when the link to the master fails.

Now, take a look at the example in Figure 8-33. Router 1 needs to get data to VRRP Router A. There is a link failure between Router 1 and VRRP Router A. Because VRRP is configured on VRRP Router A, the data will be passed to VRRP Router B, which will forward the data on to its destination. VRRP allows data traffic to flow uninterrupted even when link failure occurs.

VRRP allows communications between autonomous systems to continue virtually uninterrupted. When two routers are configured with VRRP, they are considered VRRP pairs. When the VRRP is first initialized, they perform an election process that allows them to make a determination of which will be the master VRRP router and which will back up the master.

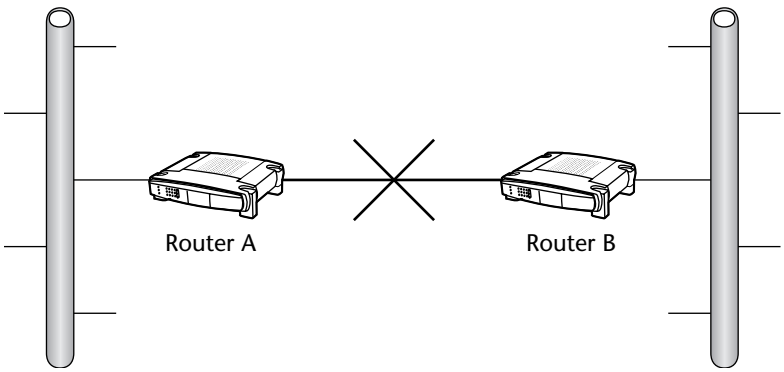


Figure 8-32: Single point of failure link between two subnets

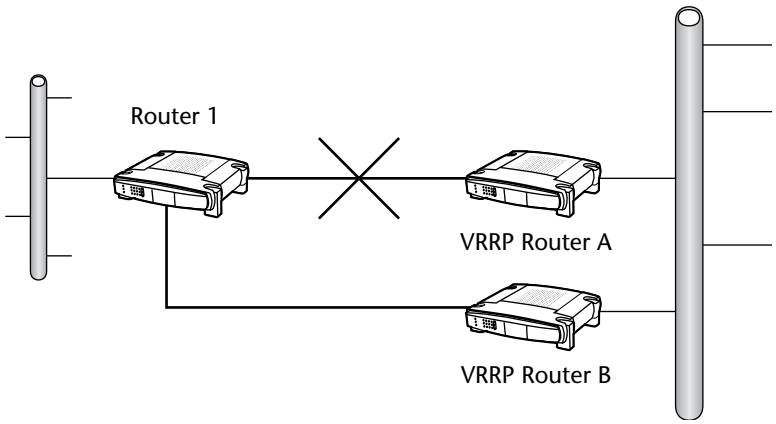


Figure 8-33: VRRP link failover

VRRP Failover

VRRP routers will elect a master during the initialization process. Once a master is chosen, the master VRRP router will be the primary router for passing data to a destination. The master router will send advertisement messages to the backup router on a periodic basis. The messages that are sent inform the backup router of the master status.

The backup VRRP router listens for the advertisement messages from the master. When it does not receive the advertisement as expected, it will determine that the primary has failed, and it will initiate the process of becoming the master.

Link failover in VRRP provides for quick recovery. Routing protocols will route to the VRRP virtual IP address, so routing convergence does not need to occur when the primary link goes down. In other words, Router 1 in Figure 8-33 never knows that the link to VRRP Router A has failed. Its routing table contains the VRRP IP address and the data is automatically redirected to VRRP Router B.

Summary

This chapter provided an overview of Ethernet LANs, as well as an overview of routing protocols. The chapter also covered some feature protocols that are used to increase network integrity and efficiency. The information in this chapter is simply an overview used to provide you with an understanding of the concepts of each of these technologies. Virtually every individual section in this chapter has books dedicated to the process the protocol follows.

It's important to understand the information contained within this chapter because these are some of the fundamental protocols that are used by the Nortel VPN Router. If you are involved with the implementation or management of the Nortel VPN Router, then you will need to have an understanding of these features and standards because you are bound to come across these at some point.

Chapter 9 discusses other important features and standards that are supported by the Nortel VPN Router. Most notably are tunneling protocols and Voice over IP (VoIP).

CHAPTER

9

Tunneling, VoIP, and Other Features

A VPN tunnel provides a secure method for exchanging information between a corporate LAN and a remote user or group of users. The VPN tunnel can do this through the use of a tunneling protocol. Understanding how Layer 2 Forwarding (L2F), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IP Security (IPSec) tunneling protocol work is an important part of any VPN administrator's job. To be able to understand and implement these processes is a necessity in any VPN environment. This chapter discusses all of the tunneling protocols that are supported by the Nortel VPN Router.

This chapter also provides an overview of Quality of Service (QoS), Voice over IP (VoIP), Client Address Redistribution (CAR), and some other features that are supported by the VPN Router. Having an understanding of these features is important for gaining an overall understanding of the capabilities of the VPN Router.

This chapter provides only a basic overview of these protocols and features. A lot of other materials are available that provide an in-depth understanding of many of these topics, but this chapter will help VPN administrators in the performance of their jobs.

This chapter enriches what was discussed in Chapter 8, and provides further information on the features and the functions available within the VPN Router family. As with Chapter 9, this is not a configuration guide. Many of these standards contain multiple variables that may or may not apply to any given LAN.

Layer 2 Forwarding

The Layer 2 Forwarding (L2F) protocol is used for providing a secure tunnel over a public infrastructure such as the Internet. This tunnel is created between the Internet service provider (ISP) and the device at the central site that the tunnel is to be terminated on. This is accomplished by the ISP providing a Network Access Server (NAS) to establish the tunnel with a central site location. Figure 9-1 shows a network providing L2F tunneling capability.

This type of tunneling does not require that the user's PC use client-based tunneling software. However, the user must be able to establish a Point-to-Point Protocol (PPP) link to an ISP using either dial-up or another communication means. Because there is no requirement for special software on the user's PC in most instances, the user is able to establish a session with a home office server (such as a mail server) by using only the utilities that are already included with the Windows operating system.

When a user establishes a connection to an ISP, a determination is made by the provider based upon the user ID that the user is associated with for a particular domain. Once that determination is made, an L2F tunnel is created for that user between the ISP's NAS and the domain's central site. Once the tunnel is established, the user is able to access servers and services that are available on the private network at the central site.

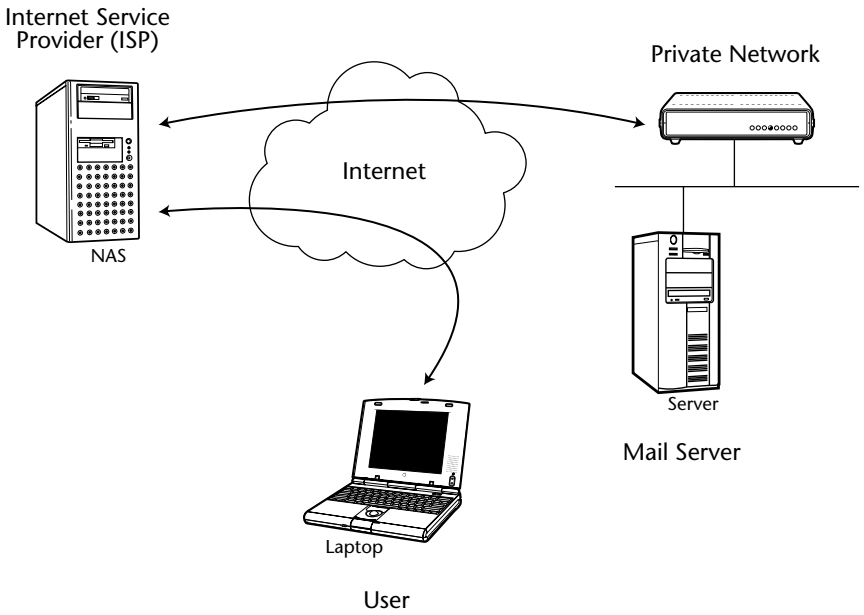


Figure 9-1: L2F tunneling environment

The use of L2F tunneling requires an ISP that provides this type of service. Because this service is available on a limited basis only, the selection of an ISP offering Remote Access Server (RAS)–based services is essential. Because the tunneling and encapsulation of the user's packets are performed by the NAS located at the ISP's location, the user is unaware that they are being tunneled to the central site office. So, without the need for special software or the need to encapsulate data at the user's PC, this type of tunneling is transparent to the end user.

A typical session exchange consists of the following:

1. The user connects to the ISP that is providing the L2F service.
2. Upon authentication and domain determination, a tunnel for that user is established between the ISP's NAS and the central site's VPN device.
3. When the user's PC sends a packet to the ISP, it is identified and associated with the session established for that user to the VPN device.
4. The packet is then encapsulated with an IP header containing the source address of the NAS and the destination address of the VPN device, along with the L2F header and the original PPP packet sent by the user's PC.
5. The packet is then sent out over the public network or Internet and is routed to the VPN destination address.
6. When the VPN device receives the packet, it strips off outer headers (called *de-encapsulation*) and places the packet on the private network.
7. The packet is then routed over the private network to its ultimate destination.

Packets being returned to the user PC that generated the original request are routed over the private network to the VPN device where they are encapsulated for the return to the ISP. When the ISP receives the packet, it de-encapsulates it and sends it to the PC over the PPP link that is established with the user PC.

A typical L2F tunnel packet contains the following:

- Destination IP address
- Source IP address
- L2F header
- PPP Payload packet

Because of encapsulation, L2F offers the capability to perform IP address translation. However, L2F does not offer any form of data encryption, so data can be compromised if the packet is intercepted. To understand the ability to perform network translation, refer to Figure 9-1.

A user dials into the ISP providing L2F service. Once connected and a PPP link is established, the user PC is assigned an IP address of 192.168.124.33. This address is in the range of addresses that are not routable over the Internet. The user wants to obtain mail from the mail server located at the central site office. The private network has an IP address range of 10.35.50.X, which is using a Class C subnet mask. The mail server is located at 10.35.50.148. The ISP's NAS is connected to the Internet with an IP address of 199.201.45.29 and the central site office VPN device connects to the Internet at 206.33.12.194.

The user PC sends a packet request destined for the mail server on the central site private network. A representative packet contains the following:

- Media information
- PPP information
- IP header
- Source IP address (192.169.124.33)
- Destination IP address (10.35.50.148)
- Data

The packet is received by the ISP and is associated with a user tunnel to the VPN device at the central site. The packet is then encapsulated with the L2F header, along with the source address and destination addresses. A packet representing the packet as it leaves the NAS contains the following:

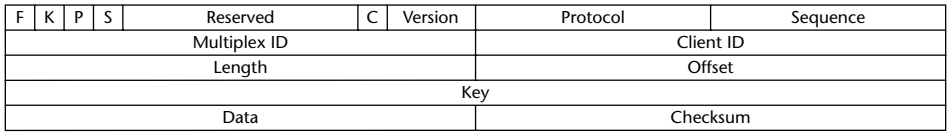
- Media information
- Source IP address (199.201.45.29)
- Destination IP address (206.33.12.194)
- PPP information
- IP header
- Source IP address (192.169.124.33)
- Destination IP address (10.35.50.148)
- Data

The packet it routed over the public network or Internet to the VPN device over the L2F tunnel created for that user. The packet is received by the VPN device, where the encapsulation is removed and the packet is passed through the device to the private network. A packet representing the packet after it has been de-encapsulated contains the following:

- Media information
- PPP information
- IP header
- Source IP address (192.169.124.33)

- Destination IP address (10.35.50.148)
- Data

The packet is received by the mail server and the response is returned to the user PC in reverse order, with the source and destinations IP addresses interchanged. The L2F header has the following form:



This header includes the following:

- *F:* 1 bit in length. If the bit is set to 1, then the Offset field is present.
- *K:* 1 bit in length. If the bit is set to 1, then the Key field is present.
- *P:* 1 bit in length. If this bit is set to 1, then the packet is a Priority packet and should be processed before packets that have been received but not processed, and that do not have the Priority bit set.
- *S:* 1 bit in length. If the bit is set to 1, then the Sequence field is present. This bit must be set for all packets that are management packets.
- *Reserved:* 8 bits in length. This is a reserved field and it always has all 8 bits set to zero.
- *C:* 1 bit in length. If the bit is set to 1, then the 16-bit Checksum field follows the encapsulated payload.
- *Ver:* 3 bits in length. This Version field is always set to 001. The packet it considered invalid if it is set to any other value.
- *Protocol:* 8 bits in length. The Protocol value specifies the protocol that is encapsulated within the L2F packet, as follows:
  - 0—Illegal
  - 1—L2F management packet
  - 2—PPP tunneling
  - 3—SLIP tunneling
- *Sequence:* 8 bits in length. This field is present only if the S bit has been set to 1. This field is set to all zeros for the first sequenced L2F packet.
- *Multiplex ID:* 16 bits in length. This field identifies a particular connection within the tunnel. Each new connection is assigned a Multiplex ID (MID) that is currently unused. The MID of zero is reserved and is only used to indicate the state of the tunnel.

- *Client ID:* 16 bits in length. This field is used to aid the endpoint devices in the de-multiplexing of tunnels. The Client ID (CLID) field contains a unique nonzero value.
- *Length:* 16 bits in length. This field indicates the length of the packet in the number of bytes contained within the packet, but excluding the number of bytes contained within the Checksum field.
- *Offset:* 16 bits in length. This field is only present if the F bit has been set to 1. This field contains the number of bytes beyond the L2F header that the Data field is expected to begin.
- *Key*: 32 bits in length. This field is only present if the K bit has been set to a 1. This field contains a Key that is based upon the authentication response last given to the peer during creation of the tunnel. The Key assists in resisting attacks based on spoofing. This Key is used only for the life of the session.
- *Data*: Variable in its length. This field contains the data payload and will vary in length, depending on the amount of data that is being transmitted.
- *Checksum*: 16 bits in length. This field is present only if the C bit has been set to 1. This field contains a 16-bit CRC value that has been applied over the entire packet from the first byte through the last byte of the data payload. The checksum field is then appended to the packet following the last byte of the data payload.

The Nortel VPN Router supports only L2F tunneling protocol for user tunnels.

Point-to-Point Tunneling Protocol

The Point-to-Point Tunneling Protocol (PPTP) was developed to allow PPP to be tunneled through an IP network. It does not modify any part of the PPP protocol, but provides a transport for that traffic. It is based on client/server architecture and, thus, eliminates the need for an NAS, which L2F relies on. PPTP allows for the direct connection to VPN devices to gain access to the private network. Figure 9-2 shows the client/server relationship with a user utilizing a PPTP-based client to gain access to the private network.

For a user to create a VPN tunnel to a central office utilizing PPTP requires that PPTP client software be loaded on the computer being used. PPTP clients are available for all Microsoft Windows operating systems and various versions of Linux, as well as Mac OS X.

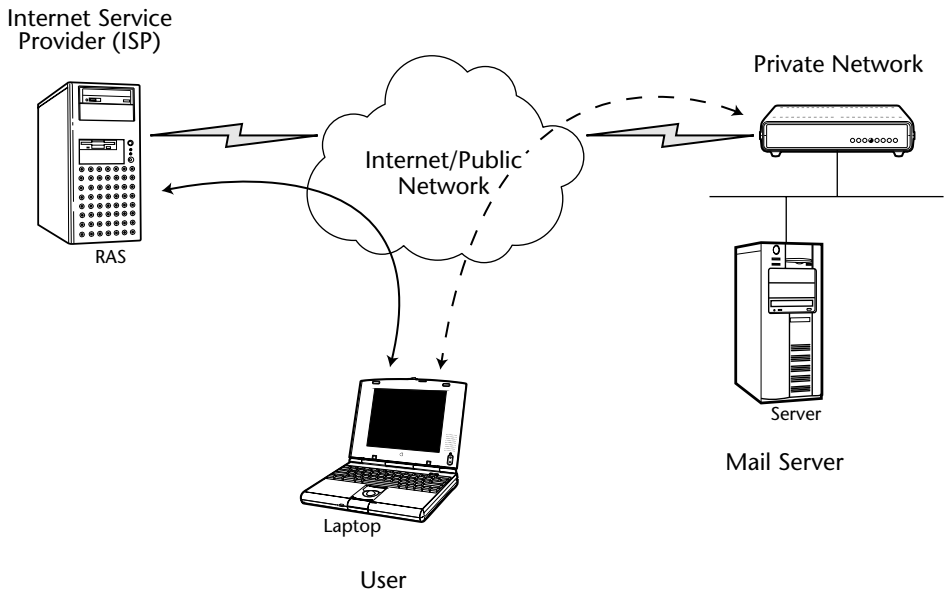


Figure 9-2: PPTP tunneling environment

A user makes a PPP connection to the ISP using either dialup services or another means of communications. Once authorized by the ISP, the user can gain access to the Internet using IP. The user can then launch the configured PPTP client to make a tunnel connection to the central office's VPN device. Once the user is authenticated on the VPN devices, the user is allowed access to the central site network and is permitted access to services and servers on that network.

The advantages of using a PPTP tunneling client is that it allows for flexible IP address management and it offers support for non-IP protocols such as IPX and Appletalk. This allows for a wide range of use covering various client computer operating systems, as well permitting support of non-IP-based private networks. The main advantage that PPTP has over L2F is that user tunnels can be created from a wide range of clients and do not require any special servers from an ISP. This allows the user to be more flexible in the choice of an ISP and also allows for a degree of mobility because ISPs providing services in support of L2F tunneling may not be available in all areas.

A typical session exchange is as follows:

1. A user dials up or connects to the ISP.
2. The user is authenticated and assigned an IP address, which allows for traffic to be routed to the Internet.
3. The user then launches a PPTP client to connect to a VPN device at the Central Office site.

4. The user's PPTP client negotiates a connection with the VPN device.
5. PPTP client authentication is accomplished with Microsoft Challenge Handshake Protocol (MS-CHAP).
6. Once a PPTP tunnel has been negotiated and established, the user is able to communicate with services and servers available on the central site office's private network.

A PPTP tunnel consists of two components: control and data. The *control* portion of a PPTP tunnel uses protocol 6 (TCP) using port 1723, while the *data* component uses protocol 47 (GRE). So, PPTP requires the use of two network sessions to control the tunnel and to pass user data. So in the event that a PPTP session must be established through a firewall to terminate the tunnel on a VPN device, special considerations are required to allow for port 1723 and protocols 6 and 47 to pass traffic through the firewall unaltered.

Once a PPTP tunnel has been established, data is sent over the tunnel using IP-in-IP encapsulation. The outside header of the encapsulated packet contains the source address of the client as it was assigned by the ISP, with a destination address being the public interface IP address of the VPN device.

Within the packet is a Generic Routing Encapsulation (GRE) header used to indicate to the receiving device that the message is a PPTP encapsulated message and to provide sequencing and acknowledgment for the packet. The encapsulated packet is then routed over the public network or Internet to the VPN device. Upon reception of the packet, the VPN device strips off the outer headers and forwards the packet to the private network.

Packets that are to be returned to the user client are similarly encapsulated by the VPN device to allow for routing of those packets back to the client that originally established the tunnel session.

The basic structure of a data packet used with a PPTP tunnel contains the following:

- Media information
- IP header
- GRE header
- PPP payload

Using Figure 9-2, a representative PPTP session would be as follows. A user dials into the ISP providing remote access services. Once connected and a PPP link is established, the user PC is assigned an IP address of 192.168.124.33. This address is in the range of addresses that are not routable over the Internet. The user wants to obtain mail from the mail server located at the central site office.

The private network has an IP address range of 10.35.50.X, which is using a Class C subnet mask. The mail server is located at 10.35.50.148. The ISP's RAS is connected to the Internet with an IP address of 199.201.45.29, and the central site office VPN device connects to the Internet at 206.33.12.194.

Once connected to the ISP's network, the user launches a PPTP client to connect to the Central Office's private network and to gain access to the mail server on that network. A packet is created and routed over the Internet to the VPN device.

The packet received by the VPN device contains the following:

- Media information
- IP header
- Source address IP (199.201.45.29)
- Destination address IP (206.33.12.194)
- GRE
- PPP information
- IP header
- Source address IP (192.168.124.33)
- Destination address IP (10.35.50.148)
- Data

The packet is placed on the public network by the ISP and is routed over the Internet to the VPN device, which receives it. The VPN device then strips the outside headers off, places the packet on the private network, and is routed to the mail server.

The representative packet that the mail server receives contains the following:

- Media information
- IP header
- Source address IP (192.168.124.33)
- Destination address IP (10.35.50.148)
- Data

The mail server receives the packet and processes the request. Response packets to the request are returned to the VPN device, where the packet is properly encapsulated for the return trip back to the ISP and to the requesting client.

The structure of the enhanced GRE header is as follows:

C	R	K	S	s	Recur	Flags	Version	Protocol	Sequence
Key (HW) Payload Length								Key (LW) Call ID	
Sequence Number (Optional)									
Acknowledgment Number (Optional)									

This header includes the following:

- *C:* 1 bit in length. Used to indicate if checksum is present. This bit is set to zero.
- *R:* 1 bit in length. Used to indicate if routing is present. This bit is set to zero.
- *K:* 1 bit in length. Used to indicate if key is present. This bit is set to 1.
- *S:* 1 bit in length. Used to indicate if the Sequence number is present. If the value of this bit is 1, then the packet is a data payload packet. If the value of this bit is zero, then there is no data payload present and the GRE packet is only an acknowledgment packet.
- *s:* 1 bit in length. Used to indicate that strict source route is present. This bit is set to zero.
- *Rec:* 3 bits in length. Used to indicate recursion control. This field is set to a value of zero.
- *A:* 1 bit in length. Used to indicate that an acknowledgment sequence number is present. This bit is set to 1 if the packet contains an acknowledgment number used for acknowledging previously transmitted data packets.
- *Flags:* 4 bits in length. This field must be set to a value of zero.
- *Ver:* 3 bits in length. This field must be set to a value of 1 to indicate that this is enhanced GRE.
- *Protocol Type:* 16 bits in length. This field is used to indicate the protocol ID. This field is set to a value of 6 to indicate PPTP.
- *Key fields:* Two 16-bit length segments whose usage is dependent upon the implementation being used. PPTP uses them as follows:
  - *Payload Length:* High Word (higher two octets of the key field) contains the size of the payload not including the GRE header.
  - *Call ID:* Low Word (lower two octets of the key field) contains the Peer's call ID for the session to which this packet belongs to.
- *Sequence Number:* 32 bits in length. This field contains the sequence number of the packet if the S bit has been set to 1.
- *Acknowledgment Number:* 32 bits in length. This field contains the sequence number of the highest numbered GRE packet received by the sending peer for this particular user session if the A bit has been set to 1.

The data portion of the packet contains the PPP data packet without any specific packet framing elements contained within the media information fields. Assigned sequence numbers are on a per-packet basis. At the start of a session, the sequence numbers for the user session is set to zero. Sequence numbers increment by 1 for each packet sent for a particular user session that contains a data payload and for which the sequence S bit has been set to 1. Because the protocol allows for acknowledgments to be transmitted with the data, this makes it more efficient and thus requires less buffering of packets.

PPTP uses a number of control messages to initiate, manage, and end a user session between the client and the server. Table 9-1 provides a listing of these control messages.

Table 9-1: PPTP Control Messages

CONTROL MESSAGE	CODE
Control Connection Management	
Start-Control-Connection-Request	1
Start-Control-Connection-Reply	2
Stop-Control-Connection-Request	3
Stop-Control-Connection- Reply	4
Echo-Request	5
Echo-Reply	6
Call Management	
Outgoing-Call-Request	7
Outgoing-Call-Reply	8
Incoming-Call-Request	9
Incoming-Call-Reply	10
Incoming-Call-Connected	11
Call-Clear-Request	12
Call-Disconnect-Notify	13
Error Reporting	
WAN-Error-Notify	14
PPP Session Control	
Set-Link-Info	15

The Nortel VPN Router is capable of establishing both user tunnels and Branch Office Tunnels (BOTs) using the PPTP protocol.

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) combines the features found in both the L2F and PPTP tunneling protocols. It may be implemented as either a provider-based service that requires a Layer 2 Access Controller (LAC), or through the use of client software utilizing a client/server relationship between the user PC and the VPN device to establish the tunnel. Figure 9-3 illustrates both implementations.

In Figure 9-3, two users are accessing an ISP that provides both RAS and L2TP capabilities. One user is using dialup services to connect to the ISP forming a PPP connection utilizing the L2TP services that the ISP is providing to access services, and servers that are located on the central site private network.

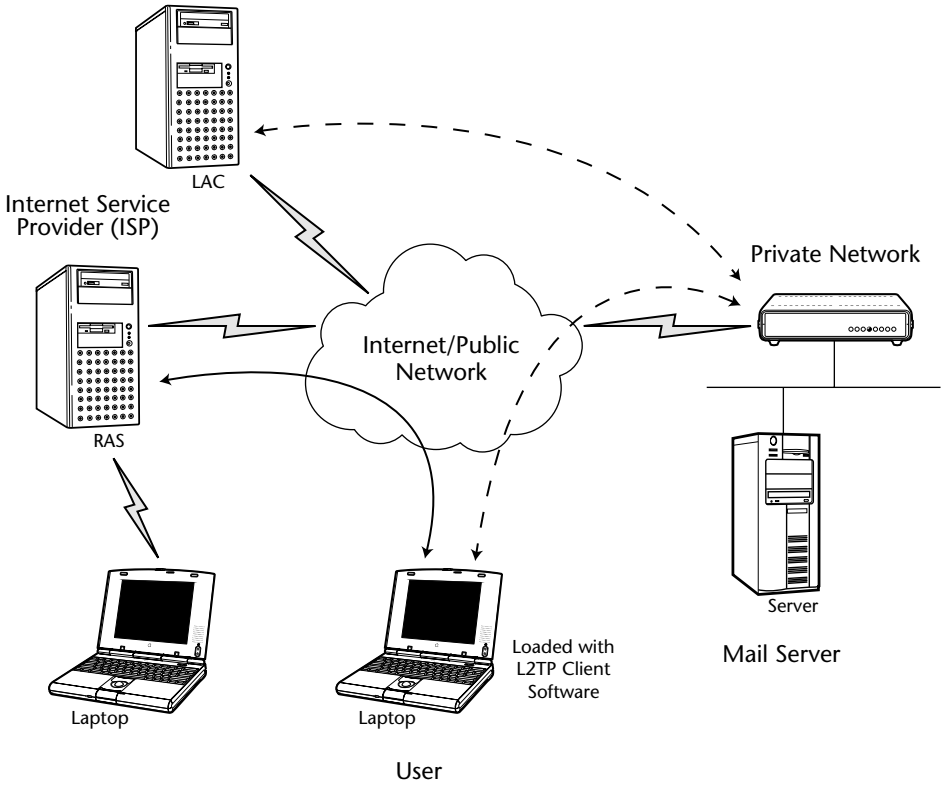


Figure 9-3: L2TP tunneling environment

The user is authenticated by the ISP and a determination is made that this user requires L2TP services. Once the connection is established, the user connection is routed to the LAC to establish an L2TP tunnel session with the VPN device that is performing the functions of the L2 Network Server (LNS). Once the tunnel is established between the LAC and LNS, bi-directional traffic is able to traverse the tunnel between the user and the services and servers that are residing on the central site office's private network. Tunnel traffic is encapsulated by the LAC and LNS and routed over the public network or Internet as long as the session is valid.

When the user sends a packet that is destined for the L2TP tunnel, the LAC identifies the session that it is associated with and adds headers to the user packet consisting of an IP header with the source address of the LAC, the destination address of the VPN device performing the LNS function, and the L2TP header, along with the original PPP packet. The encapsulated packet it routed over the public network or Internet to its destination LNS where the headers are stripped and the packet is placed on the private network.

A user dials into the ISP providing L2TP services. Once connected and a PPP link established, the user PC is assigned an IP address of 192.168.124.33. This address is in the range of addresses that are not routable over the Internet. The user wants to obtain mail from the mail server located at the central site office. The private network has an IP address range of 10.35.50.X, which is using a Class C subnet mask. The mail server is located at 10.35.50.148. The ISP's LAC is connected to the Internet with an IP address of 199.201.45.29 and the central site office VPN device acting as an LNS connects to the Internet at 206.33.12.194.

The user PC sends a packet request destined for the mail server on the central site private network.

A representative packet contains the following:

- Media information
- PPP information
- IP header
- Source IP address (192.168.124.33)
- Destination IP address (10.35.50.148)
- Data

The packet is received by the ISP and forwarded to the LAC, where it is associated with the user session and encapsulated with an L2TP header and an IP header before being routed over the Internet. The LAC places the encapsulated packet on the public network, where it is received by the VPN device. A representative L2TP encapsulated packet contains the following:

- Media information
- IP header
- Source IP address (199.201.45.29)
- Destination IP address (206.33.12.194)
- L2TP header
- PPP information
- IP header
- Source IP address (192.168.124.33)
- Destination IP address (10.35.50.148)
- Data

The received packet is stripped of its outer headers by the VPN device and placed on its private network to be routed to the mail server. The packet that arrives at the mail server contains the following:

- Media information
- IP header
- Source IP address (192.168.124.33)
- Destination IP address (10.35.50.148)
- Data

The mail server sends responses for the received packet back to the VPN device that is acting as the LNS to have it encapsulated and routed back over the Internet to the user who made the original request.

The user who uses ISP-based L2TP services is required to use the services of the ISP that the user is subscribed to in order to tunnel into the central site office's private network using L2TP tunneling protocol (restricting that user's mobility). However, a user with an L2TP client loaded directly on a PC is able to establish L2TP tunnels to the central office VPN device using any ISP to access the Internet. When a user connects to the ISP, the user then launches the L2TP client software installed on the PC. The software enables the PC to act as the LAC to establish a PPTP session with the VPN device acting as an LNS. The VPN device is responsible for authenticating the user, in most cases by utilizing MS-CHAP. Once authenticated, the user is assigned an IP address that will allow it to route data from the PC to the private network behind the VPN device. The L2TP tunnel is maintained directly between the user PC and the VPN device. L2TP uses UDP port 1701, so if users need to connect to a VPN device behind a firewall, then these ports must be made accessible through the firewall.

Because L2TP is not strong in the security area, there have been developments that allow L2TP to be used over IPSec, making it more robust in the

security and authentication areas. IPSec is used to create a tunnel using its security abilities to allow L2TP tunnels to be established between Security Association (SA) endpoints. This allows the L2TP packets to be encapsulated within IPSec, thus preventing the exposure of information concerning the internal private networks.

NOTE **IPSec is discussed in more detail later in this chapter.**

The basic structure of an L2TP packet contains the following:

- Media information
- IP header
- UDP header
- L2TP header
- Data

The basic structure of the L2TP version 2 header is as follows:

T	L	0	S	0	O	P	0	Version	Length
Tunnel ID									Session ID
Ns									Nr
Offset Size									Offset Pad
Data									

This header includes the following:

- *T:* 1 bit in length. Message type. If the bit is zero, then this is a data message; if it is set to 1, then it is a control message.
- *L:* 1 bit in length. Length present. If the message is a control message, then this bit must be set to 1.
- *Bit positions 2 and 3 are set to zero.*
- *S:* 1 bit in length. Sequence present. If the bit is set to 1, then the Ns and Nr fields are present. This bit must be set for control messages.
- *Bit position 5 is set to zero.*
- *O:* 1 bit in length. Offset present. If this bit is set to 1, then the offset size field is present. This bit must be set to zero for control messages.
- *P:* 1 bit in length. Priority. If set, the data message should receive preferential treatment for local queuing and transmission. This bit must be set to zero for all control messages.
- *Bit positions 8 through 11 are set to zero.*

- *Ver:* 4 bits in length. This field contains the total length of the message in bytes. This field exists only if the L bit has been set to 1.
- *Length:* This field specifies the length of the message. This is present only if the L bit is set.
- *Tunnel ID:* 16 bits in length. This field indicates the tunnel ID for the control connection. A tunnel will have different identifiers on each end of the tunnel. The message contains the tunnel ID of the intended recipient.
- *Session ID:* 16 bits in length. This field indicates the session within a tunnel. A session will have different identifiers on each end of the session. The message contains the session ID of the intended recipient.
- *Ns:* 16 bits in length. This optional field indicates the sequence number of the data or control message. This field is zero at startup and is increased by 1 with each message that is sent.
- *Nr:* 16 bits in length. This optional field indicates the expected sequence number that is to be received with the next control message. So, this field is set to the last value of Ns received plus 1. With a data message, the Nr field is reserved and must be ignored upon receipt if it is present.
- *Offset size:* 16 bits in length. This optional field specifies the number of bytes past the L2TP header where a payload is expected to start. If the offset pad field is present, then the L2TP header ends after the last byte of the offset padding. This field exists only if the O bit has been set to 1.
- *Offset pad:* This is an optional variable-length field.
- *Data:* This field is variable in its length.

The Nortel VPN Router is capable of establishing both User tunnels and BOTs using the L2TP protocol.

IP Security Tunneling Protocol

IP security (IPSec) tunneling protocol is a network layer (layer 3) of the OSI Reference Model–based tunneling protocol. It is the standard for securing IP traffic by encryption and authentication of all packets. Unlike L2F, PPTP, and L2TP, whose first concern is connectivity and then security, the primary goal of IPSec is security.

IPSec uses a set of cryptographic protocols for securing packets and key exchange. IPSec uses the strong encryption provided by Data Encryption Standard (DES) and Triple DES encryption. DES encryption has an effective 56-bit key length, although it uses 64 bits to encrypt and decrypt data. The reason for it being only effectively 56 bits is that the least-significant bit in each byte is used to indicate parity.

Triple DES uses the same encryption scheme as DES, but it is repeated three times. The data is first encrypted with the first key, then decrypted with a second key, and then once again encrypted with a third key. Thus, the name Triple DES was given for this encryption method. Integrity protection is provided by Message Digest algorithm 5 (MD5), Secure Hash Algorithm (SHA1), Internet Security Association and Key Management Protocol (ISAKMP), and Internet Key Exchange (IKE) Diffie-Hellman Group.

IP-in-IP encapsulation is used to send data over an IPSec tunnel. The outside header contains the source IP address of the client, and the destination address is the public IP address of the VPN device that the tunnel is to be terminated on. Figure 9-4 shows a user connecting to an ISP and launching an IPSec client to connect to and from an IPSec tunnel with the central office site's VPN device.

In this scenario, the user dials into the ISP providing remote access services. Once connected and a PPP link is established, the user PC is assigned an IP address of 192.168.124.33. This address is in the range of addresses that are not routable over the Internet. The user wants to obtain mail from the mail server located at the central site office.

The private network has an IP address range of 10.35.50.X, which is using a Class C subnet mask. The mail server is located at 10.35.50.148. The ISP's RAS is connected to the Internet with an IP address of 199.201.45.29, and the central site office VPN device connects to the Internet at 206.33.12.194.

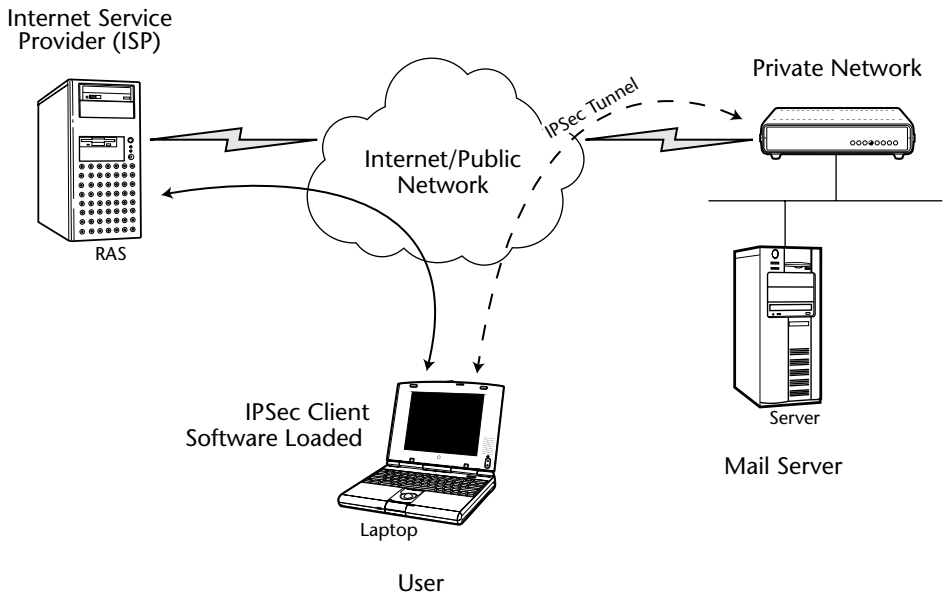


Figure 9-4: IPSec tunneling environment

Once connected to the ISP's network, the user launches the IPSec client to connect to the central office's private network and to gain access to the mail server on that network. The virtual network interface card that is created on the PC using the IPSec client software receives an IP address of 10.35.50.200 assigned to it by the VPN device on tunnel establishment. A packet is created and routed over the Internet to the VPN device.

The packet received by the VPN device contains the following:

- Media information
- IP header
- Source IP address (10.35.50.200)
- Destination IP address (206.33.12.194)
- Encapsulating security header
- Authentication header
- PPP information
- IP header
- Source IP address (10.35.50.200)
- Destination IP address (10.35.50.148)
- Data

When the packet is received by the VPN device, it strips the outer headers and decrypts the encrypted payload, reassembles the packet destined for the mail server, and places it on the private network. The packet received by the mail server contains the following:

- Media Information
- IP header
- Source IP address (10.35.50.200)
- Destination IP address (10.35.50.148)
- Data

IPSec uses Protocol 17 (UDP) port 500 for the tunnel creation. So, if a user is passing through a firewall, it must allow for passage of traffic on that port as well as allowing Protocol 50 (ESP) and Protocol 51 (AH) information to also pass. With a number of users using NAT-enabled routing devices to connect to the Internet, provisions have been made to allow for port translation in the establishment of an IPSec tunnel.

The initial contact from the client must be made on UDP port 500 on the VPN device. The VPN device determines that the source is coming from behind a NAT-enabled device. The VPN device and the client negotiate a port

that is to be used for tunnel creation. The feature of allowing IPSec tunnels to be able to traverse a NAT-enabled device is often referred to as *NAT Traversal* (*NAT-T*).

IPSec operates at the IP level. Because of this, it is able to offer protection for IP traffic as well as the upper layer protocols of the OSI Reference Model. This is accomplished through the use of the security protocols of Authentication Header (AH) and Encapsulating Security Payload (ESP), along with the use of cryptographic key management protocols. This allows it to provide security services that include access control, connectionless integrity, data origin, authentication, and encryption.

The AH is used to provide connectionless integrity and the authentication of IP datagrams. It also provides the optional service of anti-replay to help in countering denial of service attacks.

The basic packet structure using an Authentication header contains the following:

- Media information
- IP header
- Authentication header (AH)
- Data

The structure of the AH is as follows:

Next Header	Length	0
Security Parameters Index		
Sequence Number		
Authentication Data		

This header contains the following:

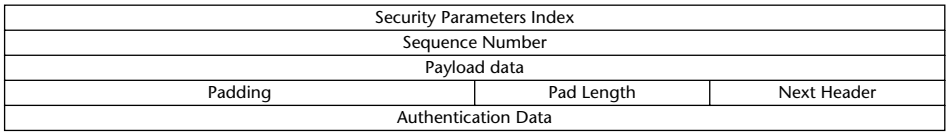
- *Next Header:* 8 bits in length. Specifies the next encapsulated protocol.
- *Length:* 8 bits in length. Specifies the size of the Authentication Data payload in 32-bit words minus 2. This field may be cleared to all zeros.
- *Bits 16 through 31 are set to all zeros*.
- *Security Parameters Index (SPI):* 32 bits in length. This field contains a pseudo-random number value used to identify the datagram's security association. If this field contains all zeros, then a security association does not exist. The values 1 to 255 are reserved.
- *Sequence Number:* 32 bits in length. This field increases by 1 with each sent packet, and is used in the prevention of replay attacks.
- *Authentication Data:* Variable in length, but must contain multiples of 32-bit words. This data is necessary for the authentication of the packet.

The ESP header is used to provide security services either alone or in combination with the AH. ESP offers a set of services that negotiate with the establishment of a Security Association (SA). These services provide confidentiality, data origin authentication, connectionless integrity, and an anti-replay ability. The ESP header is inserted after the IP header and the next protocol layer in transport mode, or before an encapsulated IP header in tunnel mode.

The basic structure of a packet containing an ESP header includes the following:

- Media information
- IP header
- ESP header
- Data

The structure of an ESP header is as follows:



This header contains the following:

- *Security Parameters Index (SPI):* 32 bits in length. This field contains the value used to uniquely identify the SA associated with the datagram. It is determined by an arbitrary number in combination with the destination IP address and the security protocol. The values 1 through 255 are reserved.
- *Sequence Number:* 32 bits in length. This field increases by 1 with each sent packet and is used in the prevention of replay attacks. This field is mandatory and must be sent even if the receiver does not elect to enable the anti-replay service.
- *Payload Data:* Variable-length field. This field contains the data described by the Next Header field and is mandatory.
- *Padding:* Variable-length field. This field may contain from 0 to 255 bytes used to align the packet to have it terminate on a 4-byte boundary.
- *Pad Length:* 8 bits in length. This field specifies the size of the Padding field in the number of bytes it contains.
- *Next Header:* 8 bits in length. This field contains a protocol number that describes the format of the Payload Data field.

- *Authentication Data:* Variable-length field. This field contains the Integrity Check Value (ICV) that is computed using the ESP packet minus the Authentication Data. This field is optional and is included only when an authentication service has been selected for the SA associated with the datagram.

The Nortel VPN Router supports both user and BOTs using the IPSec protocol.

This section primarily covered the use of IPSec with a user and client. However, IPSec may be used for the creation of tunnels between two VPN devices. These tunnels are normally point-to-point, where the endpoint IP address on the public interface of each device is know by the other. These tunnels may be also referred to as *Peer-to-Peer* or *Main Mode* tunnels.

However, IPSec has the ability to form tunnels where only one endpoint address is fixed and known publicly. These tunnels are referred to as *Initiator/Responder* or *Aggressive Mode* tunnels. These tunnels are suitable for the Small Office/Home Office (SOHO) environment where the ISP services that are available provide only dynamically assigned public IP addresses. However, where Main Mode BOTs may be initiated for either endpoint, Initiator/Responder or Aggressive Mode tunnels may be initiated only from the dynamically assigned IP address endpoint because its address is unknown to the fixed IP address endpoint. However, some VPN devices have added features where these types of tunnels may be maintained with the use of ICMP pings to initiate and maintain an Aggressive Mode tunnel, allowing traffic to be routed from the fixed IP address endpoint without the need for tunnel creation with traffic that requires user interaction.

Quality of Service

When the Internet was first established, it was a best-effort delivery service. Although each packet contained fields designated as type of service and precedence, they were, for the most part, unused. This really did not affect quality of service (QoS) greatly because the services utilizing the Internet were tolerant of dropped packets or slowness of delivery.

For a Web page, for example, a user would initiate a request by typing a site's URL and wait for the requested page to paint on the screen. There are many factors that affect the quickness of the screen, including network congestion, dropped packets, retransmission requests, and overall network reliability. The level of acceptability of the QoS was largely dependent upon the user's tolerance level for receiving a slow response. If the user's PC was able to communicate with the Web server over the Internet, the page would eventually be painted on the user's screen.

However, now that services requiring real-time response are using the Internet to carry their information between endpoints, QoS-capable devices to handle that traffic are required. Services that are coming into wide use are IP-based telephony, video conferencing, and multimedia. These services have a much lower fault tolerance, and require quick and reliable delivery of their data.

As packets traverse over networks, both on the organization's internal network (intranet) and the public network (Internet), their reliable delivery can be affected by many factors. The following is a list of problems that could occur between sender and receiver:

- *Dropped packets:* The cause is varied, but may include that a router in the path between sender and receiver may have its buffers already full before the packet arrived, thus causing that router to drop the packet. This will cause the requestor (receiver) to retransmit the request, affecting the overall performance of the application making the request.
- *Delay:* Packet delivery over the Internet is unpredictable because of different paths between endpoints and congestion at a router in the path with a long queue.
- *Jitter:* Packets from a sender may be routed over different paths, causing packets to be delivered with varying delays. The difference in delivery times is know as *jitter,* and it adversely affects services such as streaming audio or video.
- *Out-of-order delivery:* When an application sends an amount of packets out on the public network, it has no control over how those packets are to be routed. Packets may be sent on different routes and, dependent on the delays on those routes, packets may arrive at the receiver out of order. This requires that the packets be re-ordered by the receiver, which causes additional overhead in processing those packets.
- *Error:* While packets are being transmitted across the public network, it is possible that they can become corrupted. The receiver must be able to detect a corrupted packet, which it will drop, and once again request it from the sender.

To combat the problems of packet delivery between endpoints QoS mechanisms are being used to provide provisioning over the network in support of applications that require timely and reliable delivery.

To accomplish this, the Internet Engineering Task Force (IETF) developed *Differentiated Services* (*DS*), which is also referred to as *DiffServ*. DiffServ provides for the classification and possible conditioning of traffic at the boundaries of a network. Devices and routers at the edges of the network utilize multiple queues to support DiffServ in the processing of packets.

These queues are assigned a priority and are allocated a set bandwidth. Packets not having these requirements are delivered on a best-effort basis. Besides queuing, QoS devices may provide buffer tuning, congestion avoidance, policing, and traffic shaping. QoS is currently effective only in a DS domain because routers on the Internet (for the most part) are still using only best-effort delivery mechanisms. Figure 9-5 shows a DS domain.

Within the DS domain, traffic is received and classified for QoS as it enters and is routed about the domain. Traffic exiting the domain may also be treated for QoS. However, once it has left the domain, traffic may be routed only as a best effort service. Large organizations may opt to have several DS domains to provide QoS delivery of traffic.

To ensure timely delivery between domains, they may opt for high-speed point-to-point circuits and not use the public network or Internet. This type of connectivity is expensive and is not suitable for small organizations.

Within a DS domain, the edge or boundary node routers are responsible for traffic classification and conditioning. Figure 9-6 shows how packets that are received by these routers are handled.

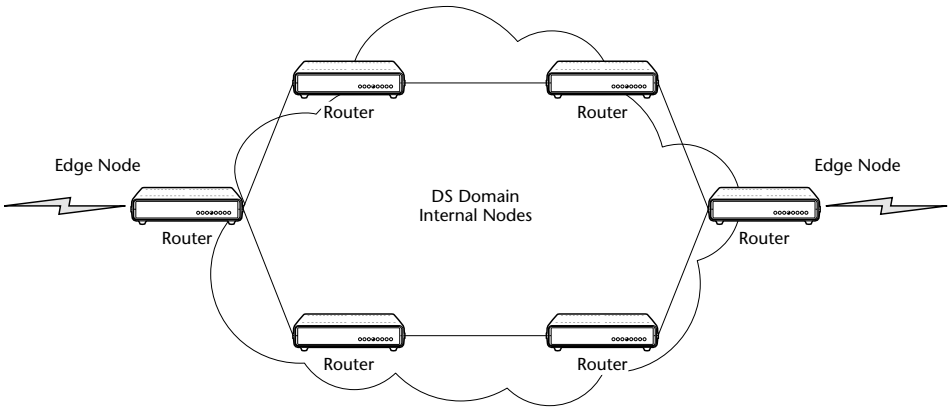


Figure 9-5: Differentiated Services (DS) domain

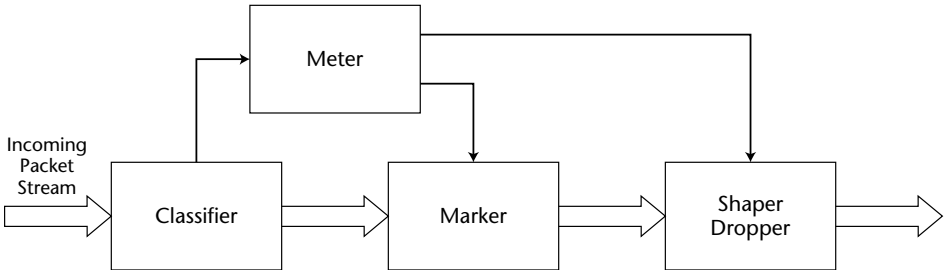
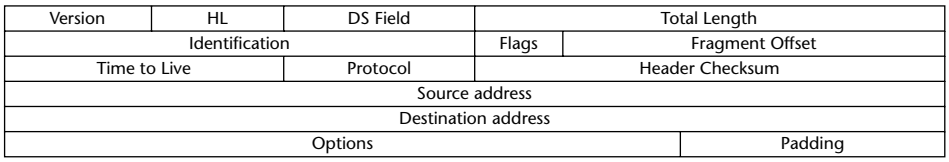


Figure 9-6: DiffServ traffic classification and conditioning

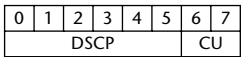
As packets enter DiffServ-enabled device, the classifier divides the packet stream into forwarding classes based upon predefined rules. The packets are then presented to the traffic policing functions to enforce the Service Level Agreement (SLA) requirements. Traffic conditioning is handled by the Meter, Marker, Shaper, and Dropper.

The *Meter* monitors and measures the traffic streams. Packets that are not conforming may undergo marking, shaping, and dropping. The *Marker* sets the DS field of the packet to that of a particular Differentiated Services Code Point (DSCP). The *Shaper* employs a strong form of policing to ensure that excess packets are not introduced into the network. It delays nonconforming packets to maintain set traffic profiles within compliance. The *Dropper* drops the packets that do not meet with the set profile.

The original IPv4 datagram defined a Type of Service (TOS) field that was mostly unused. However, this field has been replaced by the DS field per RFC 2474. The structure of the IPv4 packet with the DS field is as follows:



The DS field is 8 bits in length, where the first 6 bits are used to define the DSCP that sets the Per Hop Behavior (PHB) for how the packet is to be treated. The remaining 2 bits of the DS field are Currently Unused (CU), and the value that is set in these bits is ignored by DS-compliant nodes. The DS field is as follows:



Note the following:

- Bits 0–5 are Differentiated Services Code Point (DSCP)
- Bits 6–7 are Currently Unused (CU) and must be ignored

The PHB describes how a packet is to be treated at a DS node. The IETF has standardized on four PHB groups, as shown in Table 9-2.

Table 9-2: IETF PHB Groups and RFCs

PHB	RFC
Default best effort PHB	RFC 2474
Class Selector (CS) PHB	RFC 2474
Assured Forwarding (AF) PHB	RFC 2597
Expedited Forwarding (EF) PHB	RFC 3246

The entire 6 bits of the DSCP field is used by DS nodes as an index into a table to select how a packet is to be handled. The IETF has standardized on three pools for DSCP assignment management. The notation that is used for the 6 DSCP bits is xxxxxx. The DSCP pools are shown in Table 9-3.

Table 9-3: DSCP Pools

POOL	NOTATION	DESCRIPTION
Pool 1	xxxxx0	32 codepoints standardized by the IETF.
Pool 2	xxxx11	16 codepoints reserved for local and experimental use.
Pool 3	xxxx01	16 codepoints currently available for local and experimental use. This pool may be used in the future if the pool 1 codepoints have been exhausted.

The default best-effort PHB is mapped to a codepoint of 000000. This default codepoint must be supported by each DS node. The behavior is the standard best effort that is found on all routers. If a packet is received with an unrecognized codepoint, the DS node may just treat it as best effort. The DS router may or may not modify the DSCP before forwarding the packet.

The Class Selector (CS) PHB ensures backward compatibility with routers and networks that had used IPv4 Precedence classification and forwarding. Table 9-4 shows the relationship between the DSCP field and the Precedence field.

The Assured Forwarding (AF) PHB is standardized and its intent is to provide predictable services, even in the event of network congestion. The AF standard defines four classes, each with an allocated amount of buffers and bandwidth. The minimum resources that are allocated are guaranteed to be available at all times. Packets in different AF classes are forwarded independently of one another. Table 9-5 shows the recommended AF values.

Table 9-4: DSCP Field and Precedence Field

FIELD VALUE	IP PRECEDENCE	CS DSCP
111 000	Network Control	CS 7
110 000	Internet Work Control	CS 6
101 000	CRITIC/ECP	CS 5
100 000	Flash Override	CS 4
011 000	Flash	CS 3
010 000	Immediate	CS 2
001 000	Priority	CS 1
000 000	Routine	CS 0

Table 9-5: Recommended AF Values

DROP PRECEDENCE	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low	010000	011000	100000	101000
Medium	010010	011010	100010	101010
High	010100	011100	100100	101100

The Expedited Forwarding (EF) PHB with its priority can be used to build a low-loss, low-latency, low-jitter, assured-bandwidth path through DS domains. This is useful for IP telephony, video conferencing, and for providing a virtual point-to-point leased line. With enough resources on the network, EF PHB–designated packets should be treated with strict priority.

The Nortel VPN Router has been designed for the support of QoS protocols. It is highly configurable and is easily tailored to fit most network QoS requirements.

Voice over IP

Voice over IP (VoIP) is the ability to transfer voice conversations over a network, whether it be an internal or public network. Analog voice data is digitized and then placed within a packet to be routed to its destination. These packets are able to traverse the local network for voice communication within that network, or routed over a larger network such as the Internet. Figure 9-7 illustrates what a VoIP installation may look like.

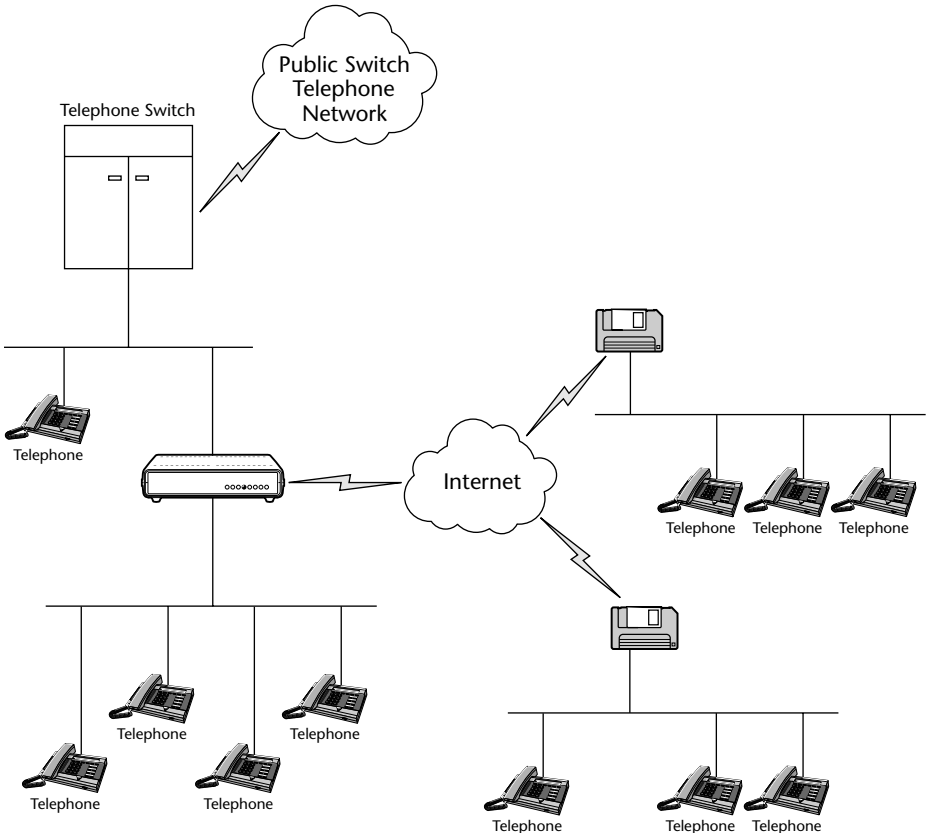


Figure 9-7: Voice over IP network example

In Figure 9-7, an organization with a central office and two Remote Offices is using VoIP to form the organization's telephone network. Figure 9-7 shows telephone handsets that are IP-enabled. However, these can be PC-based soft phones. Although this figure does not show any computers, there is the ability to send computer-based data over the same network, thus converging both data and voice networks.

The central office has a telephone switch that terminates conventional telephone service from the Public Switched Telephone Network (PSTN) and connects to the internal VoIP network.

The offices are connected over the Internet with the use of VPN devices to form an extended intranet (private network). With the use of VPN tunnels, the IP-enabled phones are able to have assigned IP addresses that are in the private domain and are not routable over the Internet. Each IP-enabled telephone has its assigned IP address registered with the telephone switch. The switch associates the IP address to an internal extension number.

The VPN devices are QoS-enabled devices utilizing DiffServ to give priority to the VoIP packets so that voice data may be delivered with the quality that telephone users are accustomed to. VoIP has advantages over existing PTSN telephone service in the areas of cost, functionality, and mobility. The use of VPN tunnels for sending VoIP packets over the Internet increases security of the conversation because the packets are encrypted, making eavesdropping impossible.

VoIP telephone service may be deployed at a lower cost because it is able to use the existing data network within an organization. If it is a new facility, it is a lower cost alternative because it does not need a separate network of its own, but rather is able to share the same infrastructure with the data network. With multiple offices, VoIP eliminates the need for multiple trunk lines for each office, thus reducing telephone charges for use of the PSTN telephone network. Users in the remote office will place all calls to the PSTN through the telephone switch at the central office. These are the only calls that will have a charge associated with them. Calls between extensions within the same office or between office facilities are made at no charge.

An organization's incoming calls are received by the PSTN telephone switch at the central office and routed to the appropriate extension. If an incoming call is intended for an extension at a remote office, the packets associated with the call are routed over the private network to the VPN device, which then routes it to the remote office over a VPN tunnel that is reliable and secure.

VoIP has functionality that is difficult to achieve with a conventional PSTN. Users do not need to be sitting in a given location to receive phone calls to their extensions. They are able to use any telephone within the network. Users may move to another facility and still be able to retain their existing extension numbers.

VoIP has increased the mobility of users in that, as long as they can register with the telephone switch at the central office, they will have their telephone calls routed to them. An example of this is a user who has a laptop with a VPN client software, as well as software in support of VoIP, which allows the user to utilize the sound capabilities built into the laptop to send and receive voice information. As long as the user has a laptop, the user is able to answer calls to his or her extension anywhere in the world.

To accomplish this, a user will need access to a broadband Internet service and then must launch the VPN client to establish a tunnel to the central office VPN device. Once connected, the user then launches a VoIP software application to register to the telephone switch so that calls made to the user's extension may be routed properly. The user is then able to make calls through the central office telephone switch to telephones that are located on the PSTN, which are local to the central office, without incurring long-distance charges.

The challenges for a VoIP implementation are network delivery quality and the ability to traverse firewalls. VoIP is heavily dependent on QoS capability of the devices within the data path between the ends of a particular conversation. An organization may have control over its premises and can ensure that each facility operates within a DS domain. However, when using the Internet to carry VoIP data there is no guarantee that packets will be transmitted with any sort of priority, because (for the most part) the Internet is a best-effort delivery network. So, although an organization carefully designs QoS into its local networks, it does not have control over the entire path of a conversation.

For low call volume facilities, this may not be a problem. However, larger organizations with high call volumes between DS domains may opt to invest in direct point-to-point, high-speed lines between them.

Currently, the most popular standardized VoIP-based solutions use either H.323 or Session Initiation Protocol (SIP) protocols. Initially, H.323 was the most popular protocol, but it has lost its attractiveness because of its poor ability to traverse NAT-enabled devices or firewalls. Although SIP has been more widely adopted for use in home environments, H.323 remains the protocol of choice of network operators and telephone service providers. H.323 is used by a number of large carriers on the core backbones of their networks.

Currently, many Plain Old Telephone Service (POTS) subscribers are unaware that their calls are being terminated on VoIP networks. Although SIP currently is the leader in the local loop arena, there have been changes made to H.323 that now allow it to easily traverse NAT devices and firewalls. This makes H.323 a viable candidate once again for use in the local loop environment.

The Nortel VPN Router with its built-in QoS functionality, along with its ability to provide secure paths over public networks using VPN tunneling, is an excellent choice as an entry or boundary node for a telephony DS domain.

Point-to-Point Protocol over Ethernet

The Point-to-Point Protocol over Ethernet (PPPoE) is a standard that combines the Point-to Point-Protocol (PPP) standard with the Ethernet standard for the purpose of providing a way to connect Ethernet users over a broadband connection. Following are examples of broadband connection types:

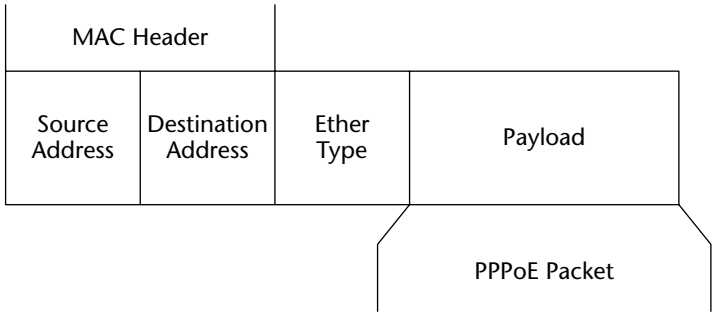
- Cable modem
- Wireless
- Data Subscription Line (DSL)

Because so many LANs utilize the Ethernet standard for data communication, and because of the need to provide a cost effective manner to transmit data remotely, a function needed to be created to allow for such transfer of

data. PPPoE provides just this function. It allows multiple nodes to communicate with one another over existing infrastructure with little (if any) configuration concerns. To provide the service, each remote node needs to learn the Ethernet MAC address of remote peers. PPPoE provides a discovery mechanism that accommodates for this need.

There are two stages of operation for PPPoE. The first stage is the *discovery stage* where a node that wishes to communicate over a PPPoE session will use a discovery protocol to learn the Ethernet MAC address of a peer and to set up a PPPoE session ID. The second stage of operation is the PPP *session stage* and it deals with the remainder of the session until the session is completed and is brought down.

Point-to-Point Protocol (PPP) is a standard that is used to allow two nodes to communicate with one another using a serial interface. Often, this is nothing more than a computer that is using the telephone line to connect to a server. When using PPPoE, the PPP information is encapsulated within the Ethernet frame. Following is an example of the Ethernet frame:



Contained within the Ethernet frame are the following four fields of information:

- *The Source Address:* This is the MAC address of the *source node,* or the node that is originating the session.
- *The Destination Address:* This is either the MAC address of the destination node or it is the Ethernet broadcast address.
- *Ether Type:* This will be coded with the type of frame. The type will either be x8863 if this is a frame for the discovery stage, or it will be x8864 if it is a frame used during the session stage.
- *Payload:* This portion of the Ethernet frame contains the PPP packet of information.

The PPPoE packet is encapsulated in the payload section of the Ethernet frame. Following is an example of the field of information that is contained in the PPP packet of the payload section of the Ethernet frame.

Version	Type	Code	Session ID
Length			Payload

Contained within the PPP portion is the following information:

- *Version:* The version of the PPPoE specification. Currently it is always set to 0x1.
- *Type:* The type of PPPoE. Currently this is always set to 0x1.
- *Code:* This value identifies the type of packet. Following are the packet types:
  - *0x00*—Session data
  - *0x07*—PPPoE Active Discovery Offer (PADO)
  - *0x09*—PPPoE Active Discovery Initiation (PADI)
  - *0x19*—PPPoE Active Discovery Request (PADR)
  - *0x65*—PPPoE Active Discovery Session-confirmation (PADS)
  - *0xa7*—PPPoE Active Discovery Termination (PADT)
- *Session ID:* A fixed value used to identify the session
- *Length:* Used to indicate the length of the PPPoE payload
- *Payload:* Data

When a node wants to set up a PPPoE session, it will send a packet type of PADI to the broadcast address of the destination subnet. When a concentrator on the destination subnet receives a PADI packet type, it will respond to the originating address with a packet type set to PADO.

It is possible that the originating node will receive multiple PADO type packets in response to the broadcast PADI type that it originated. The node will then review the PADO packets that it received until it finds the one it is expecting.

Once it selects a packet, the node then sends out a packet with the type of PADR. The destination of this packet will be the concentrator's Ethernet MAC address.

Once the destination concentrator has received the PADO, it will set up the session. It will create a session ID and will respond to the originating node with a PADS.

When either node determines that it wants to terminate a session, it will send out a PADT packet type. Once a node receives a PADT packet type, it can no longer pass data over that PPP session.

Client Address Redistribution

When a VPN remote user establishes a user tunnel to the corporate VPN Router, the VPN Router assigns a local subnet IP address to the users' session. The assigned address is often referred to as the *inner address*. There are various methods that can be deployed for the assignment of IP addresses to user tunnels. These are determined by the local administration when the VPN Router is first configured. Following are the methods of IP address assignment that can be used:

- An address that is provided by the client
- An address pool configured on the VPN Router that contains addresses that are of the same subnet as the LAN
- An address pool configured on the VPN Router that contains addresses that are not of the same subnet as the LAN
- An address that is configured statically on the VPN Router
- An address that is assigned by a RADIUS server
- An address that is assigned by a DHCP server

The feature known as Client Address Redistribution (CAR) is used to assign IP addresses to user tunnels when the IP subnet that is on the user's network is not found anywhere else on the private network. In order for CAR to operate, a dynamic routing protocol (RIP or OSPF) must be enabled on the VPN Router. The subnet of the user is added to the routing table and is advertised using whichever routing protocol is being used. When the last user using the advertised subnet disconnects from the VPN Router, the subnet is removed from the routing table and the route removal is advertised by RIP and OSPF.

When a client IP address is not an address that would be a member of the networks that are local to the VPN Router, CAR must be enabled to guarantee that the client IP addresses will be advertised in routing updates, as shown in Figure 9-8.

In the example, the private IP of the VPN client is 10.10.10.1. There is only one subnet that is local to the VPN Router and that is 192.168.1.0. In order for Router A to know how to route data to the client, CAR will have to be enabled. This will provide a route to the VPN Router to ensure that data can be sent to the client.

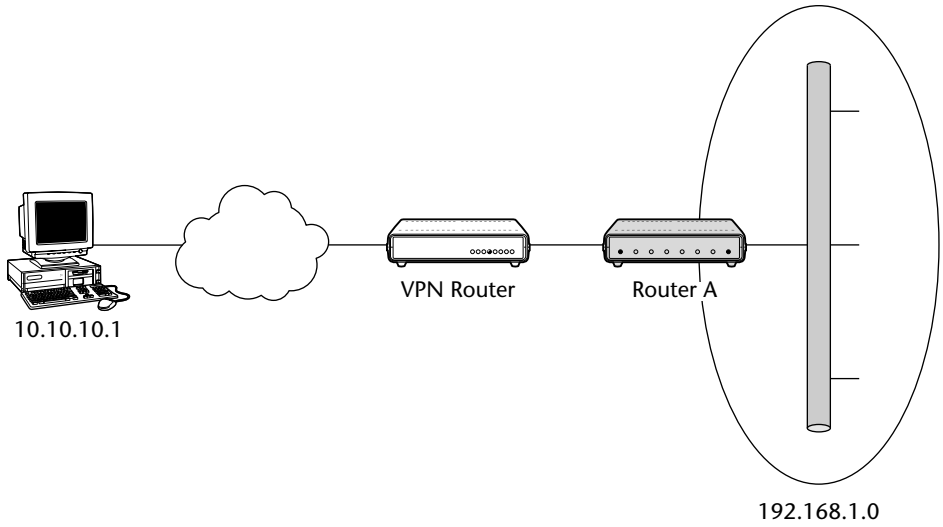


Figure 9-8: An example of CAR

Routing updates are accomplished with a dynamic route update advertisement, which is generated by the Nortel VPN Router. Advertisements can be host routes or subnets using either dynamic or static aggregation of routes. CAR uses one of two route types:

- *Host routes:* When routes are advertised by the VPN Router using host mode, the VPN Router advertises a user tunnel host address that is not an address local to the VPN Router.
- *Network route:* When routes are advertised by the VPN Router using network mode, then the VPN Router will advertise a user tunnel network route. The network address can be an address that is part of one of the locally assigned networks, or not. It is dependent upon the type of address pool that is configured upon and is assigned by the VPN Router.

When operating in host route mode, when the tunnel session is completed and the tunnel is brought down, the host route address will be removed from the routing table. When operating in network route mode, when the tunnel session is completed and the tunnel is brought down, the routes may not necessarily be removed immediately. This will all depend upon whether or not aggregation is configured and enabled.

If the inner address assigned to the user tunnel is allocated from an address pool that contains addresses that are not part of a local network, then route aggregation should be enabled. The purpose of aggregation is to reduce the

number of entries that are in the routing table of the VPN Router. Two types of aggregation modes are supported:

- Dynamic aggregation
- Static aggregation

If *dynamic aggregation* is enabled, then when the last user tunnel that is assigned an address from the pool is shut down, the routing table will remove the summary address from the routing table. If the aggregation mode is *static*, then the route is simply a static entry in the routing table and it will remain in the routing table until the address pool is removed from the VPN Router's configuration.

Circuitless IP

A Circuitless IP (CLIP) address is a logical IP address that is assigned to a router that stays up as long as its interface running IP is up. Also known as a "Virtual IP" address, CLIP is an address on a node that is not related to a specific configured interface. The name "CLIP" originated with the Nortel BayRS routers and has propagated to other Nortel equipment.

In a CLIP environment, all packets are sent to the CLIP address through the configured real IP address interfaces on the node. The CLIP is primarily available for redundancy purposes. The CLIP is always available as long as the node using CLIP has at least one active interface.

As shown in the example in Figure 9-9, there are two BOTs to the corporate VPN Router A. There are two interfaces configured on VPN Router A, one of which is link A and connects to Branch Office (BO) VPN Router 1 and the other is link B that connects to BO VPN Router 2. If Link A fails, then the users in the branch office that connects to BO Router 1 will no longer have connectivity to the corporate LAN (assuming no redundancy has been provided).

If CLIP was being used in this example, the users who are in Branch Office 1 would still have connectivity to the VPN Router. The CLIP address is not tied to any physical interface, so the users in Branch Office 1 would simply be redirected to the link that still could access the VPN Router A. As long as there is an active interface on the VPN Router, then the CLIP address is accessible.

CLIP uses the loopback address of 127.0.0.1 as the next hop address, with a subnet mask of 255.255.255.255. When CLIP is configured, it will enter the CLIP address routing information in the routing table of the VPN Router. This route entry will be a routing type "C," which stands for CLIP.

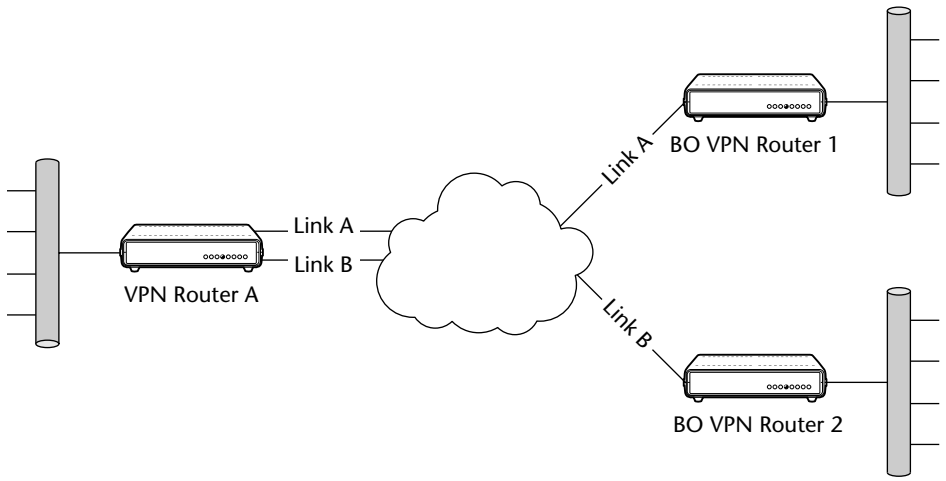


Figure 9-9: An example of a link interface failure in an environment where CLIP is not being used

CLIP is a feature that the Nortel VPN Router supports to ensure that users are able to connect to the VPN Router without any interface restrictions. CLIP is introduced by pointing an IP address to the loopback address of the VPN Router. By doing so, this ensures that the CLIP address is reachable, regardless of the status of the physical interfaces. As long as there is one reachable, active interface, the CLIP address can be reached.

One of the new features of version 6.00 software code for the Nortel VPN Router is support for a virtual management IP address. The management IP address can now be a unique CLIP address that will allow reachability to the management interface through any active interface.

Backup Interface Services

The Nortel VPN Router solution offers remote users the ability to connect to a corporate LAN to perform data communications as if they were local to the LAN. This is done through VPN tunnels. This is a connectivity solution that a lot of system administrators are being tasked to introduce into the networks that they manage.

A VPN solution is nice to have available, but the VPN solution is only a good solution when it is available. Data networking does experience problems and, with those problems, connectivity issues are introduced. Traffic congestion can cause problems with network connectivity. Hardware fails and may take time to correct. Figure 9-10 shows an example of a primary link failure.

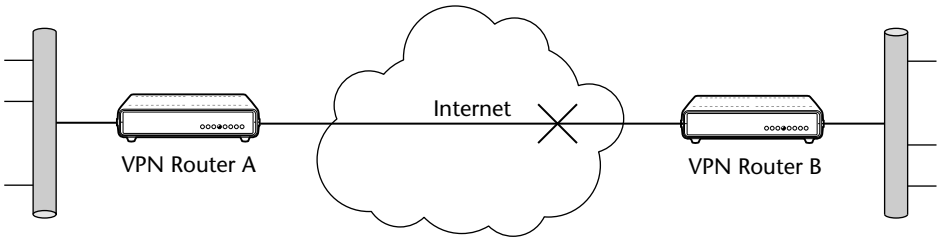


Figure 9-10: A primary link failure

So, what happens when the primary link to the VPN solution fails? Do end users wait until the connection comes up again before continuing their work? Do users continue to try alternate connectivity solutions when a primary link fails? Imagine the loss of productivity and revenue that can occur if a primary link fails with no alternate path into the corporate LAN.

Nortel VPN Routers support a feature called *Backup Interface Services* (*BIS*). BIS allows the system administrator the ability to configure an alternate link that will take over if the primary link fails. Figure 9-13 shows an example of a backup link replacing a primary link that has failed.

The concept of BIS is simple. BIS allows for the configuration of a backup link to automatically take over when a primary link fails. BIS can back up a primary interface, a route to a named destination, or a link to a named destination. Any interface type available on the Nortel VPN Router can back up any other interface type.

BIS is configured by setting up BIS profiles within the VPN Router. A BIS profile contains information about the following:

- The primary connection information
- The backup connection information
- Failover action

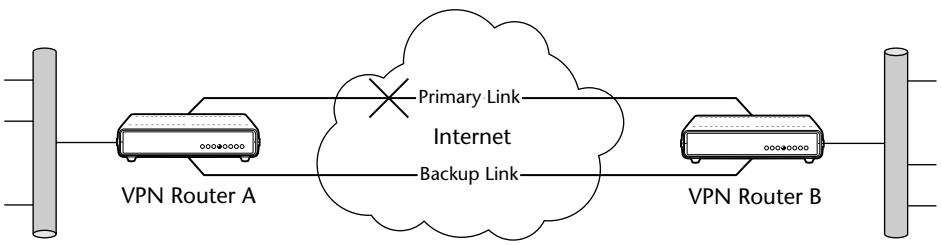


Figure 9-11: A backup link failover example

When a BIS primary interface fails, the configured BIS backup interface will initialize. Any BIS-related configurations on the backup interface profile will take effect as soon as the backup interface takes over for the primary. The backup interface will remain the acting primary until the BIS primary interface reinitializes. When this occurs, the backup BIS interface will be disabled and the primary BIS interface will resume operation.

There are several reasons that a BIS backup interface will assume the role of a primary interface. The actions that will cause BIS to initialize a backup interface are known as *triggers*. In other words, a trigger is a configured event that occurs that will cause a BIS backup interface to initialize. Here are some triggers that can cause a backup interface to initialize:

- *Time of day:* This trigger can be configured to cause the BIS backup interface to become active during specific times of the day.
- *Specific days of the week:* This trigger can be configured to cause the BIS backup interface to initialize during specific days of the week.
- *Loss of ping:* This trigger will cause the BIS backup interface to become active if there is a loss of ping to the destination that it is configured to recover.
- *Destination route unreachable:* This trigger will cause BIS to initialize the backup interface when routers to a configured destination become unreachable.
- *Interface group failure:* This trigger will cause the BIS backup interface to initialize when a configured interface group connection fails. An interface group can be any configured combination of tunnels and interfaces that are supported by the primary BIS profile.

Summary

This chapter provided an overview of VPN tunneling protocols, as well as an overview of VoIP, BIS, CAR, and a few other supported features within the Nortel VPN Router. As with Chapter 8, the information in this chapter is simply an overview to provide you with an understanding of each of these technologies. It is very important to have a basic understanding of the features that are discussed within this chapter. The concepts covered here are integral to the VPN Router family.

Chapter 10 provides a discussion of the Nortel VPN Client, which is the software that allows remote users to communicate with the corporate VPN Router.

CHAPTER 10

The Nortel VPN Client

In networking, a *client* is a node that accesses a remote node known as a *server*. The client is also the software application that gives the client node instructions on how to access a server. Computer clients were developed in the early days of networking, where client nodes did not have the capability of running their own programs. These clients were nothing more than "dumb terminals," or input devices that communicated with a server. The server device handled all of the software computations based on commands received from the client. In other words, the clients relied on a server node to handle the access and storage of data and applications within a network. Following are examples of some well-known client applications:

- Email client applications
- Internet Web browser applications
- Internet chat applications

Today, client applications allow computers to act as clients to various servers. The client can serve multiple functions, all dependent on the needs of the users and the rights that are granted to them. The wonderful thing about client applications is that they reduce overhead by providing the capability to store data applications on servers. A user simply has to load the software necessary for a computer to use to communicate with the server in order to access the requested applications and data.

For the remote users to access the corporate LAN through the Nortel VPN Router, the user's workstation must have the Nortel VPN Client installed. This chapter takes a look at the Nortel VPN Client and some of the features that are provided within the application.

Overview of the Nortel VPN Client

The Nortel VPN Client, which is also known as the Contivity VPN Client (CVC) or the Extranet Access Client (EAC), allows remote users to establish a secure user tunnel over the Internet to the corporate VPN Router. The client software is installed on the remote user's PC. It is this installed software that provides the PC with instructions on how to connect to the remote VPN Router, handles user authentication, provides event logging, and more. Without the VPN Client, remote users would not have a way to connect to the remote network through a user's tunnel.

Because the VPN Client is installed on the PC, it can be used from any place that the PC can establish a connection to the Internet. This is really helpful for professions that depend on traveling to multiple locations for work. Instant remote LAN connectivity ensures that data communications are available at all times for email, order processing, corporate updates, and so on. Figure 10-1 shows an example of a VPN Client that has established a user tunnel to the corporate LAN.

There have been a few changes to the Nortel VPN Client through the years. Each update provided support from upstart protocols to technologies. Most of the VPN Client versions are backward-compatible, although it is recommended that the VPN Client version number match the version number of the software running on the VPN Router. Failure to do so means that some of the features and functionalities may not work as they should.

Operating System Compatibility

The Nortel VPN Client supports most major releases of Microsoft Windows software. There are other versions of the VPN Client that run on other operating systems, but this section is more geared for Windows-based PC users, as this is the predominate operating system used in most VPN environments.

As VPN Router customers began standardization of Windows-based user PCs, the functionality of the VPN Client was geared toward the operating systems most in use at the time of the VPN Client software release.

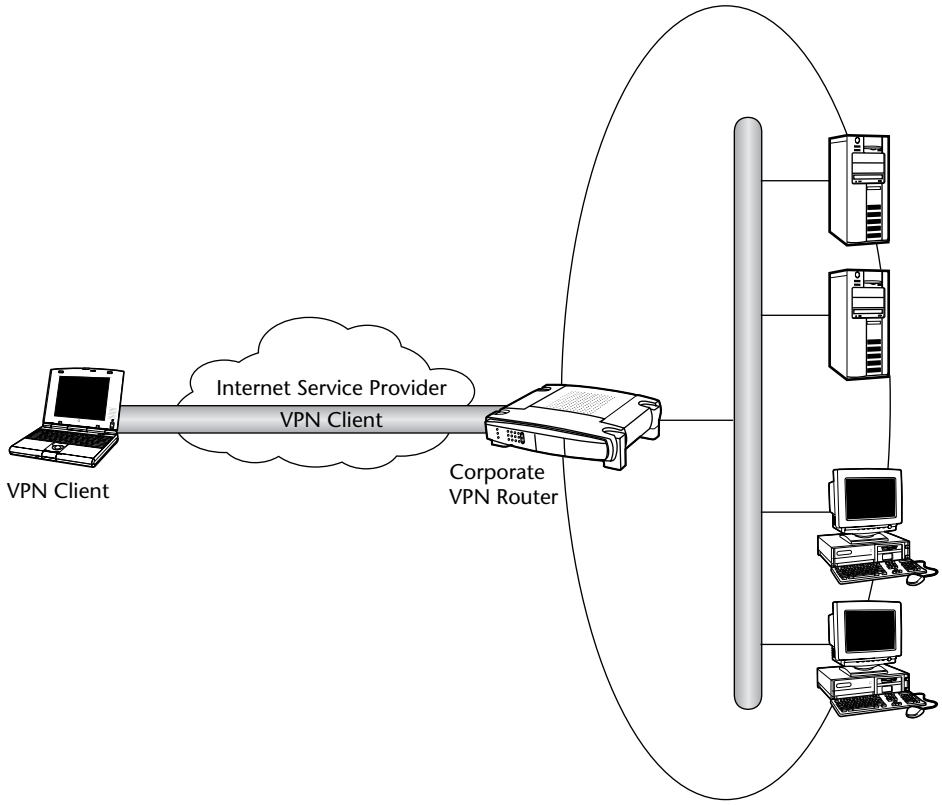


Figure 10-1: An example of a VPN Client–established user tunnel

Supported Operating Systems

A computer operating system (OS) is the computer system application, or software, that handles the control and management for the hardware that is installed in the PC, as well as the PC systems operations. A PC is virtually worthless without an OS. Without an OS, a PC could not perform any basic tasks; not to mention that the PC would not be able to understand how to run applications that include word processing, email, Internet browsers, and so on.

Because different operating structures may include instructions that handle application software differently, the requirement for a software version that differs is a necessity. Let's take a moment to see what versions of Windows OS are supported by the Nortel VPN Client.

Operating Systems Supported Prior to the Nortel VPN Client Version 4.91

Prior to version 4.91 of the Nortel VPN Client, the following OS software versions were supported:

- Windows 98
- Windows ME
- Windows XP
- Windows 2000

Operating Systems Supported in the Nortel VPN Client Version 6.01

The Nortel VPN Client software supports the following versions of Windows OS platforms:

- Windows XP Home Edition
- Windows XP Professional Edition
- Windows XP Tablet Edition
- Windows 2000

Optional Licensing Operating Systems Supported

In addition to the Windows-based operating systems, optional VPN licenses can be purchased for the following operating systems:

- IBM-AIX
- HP-UX
- Linux
- Macintosh
- Palm OS
- Windows CE

Installing the Nortel VPN Client

The Nortel VPN Client software is included with the CD that is shipped with the Nortel VPN Router. If you have a valid support contract, or want to purchase software, a software upgrade can either be downloaded from the Nortel Web site (`www.nortel.com`), or it can be ordered in CD form from the Nortel site as well.

NOTE **Before installing any version of VPN Client software, ensure that you read the release notes that accompany the software. Failure to read the notes may cause you some pain later if you find that you are using an unsupported OS or OS configuration.**

To install the VPN Client, you will need to first copy the VPN Client executable file to a directory on your PC. The filename for the VPN Client will begin with "EAC," which stands for Extranet Access Client. The net portion of the application name is the major and minor revision number. For example, if you are loading the version 6.01 software, the number to the left of the decimal is the major revision number and the number to the right would be the minor revision number. For example, the application filename for the Nortel VPN Client version 6.01 would be:

```
EAC601.exe
```

Once you have loaded the application software onto your computer, you will double-click the application software icon and it will launch the VPN Client installation wizard. Simply read through each of the windows during the install process and follow the instructions. Figure 10-2 is an example of the VPN Client installation wizard's window that you will first see.

In the next step of the installation process, the Nortel software License Agreement is provided to you. As with all software, the License Agreement is legally binding. Therefore, it is important that you read and understand the agreement prior to installing it on your PC.

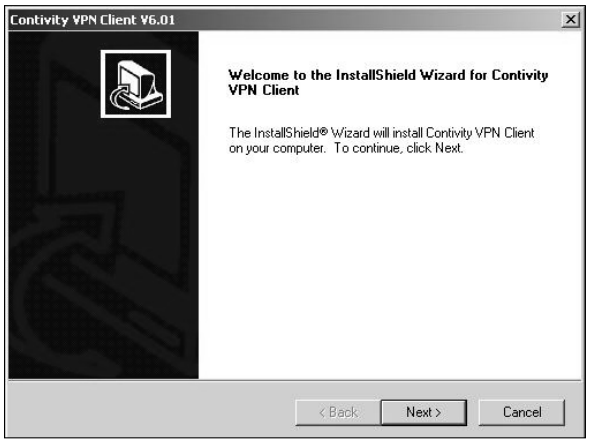


Figure 10-2: The Install Wizard's Welcome screen

The License Agreement is presented in a window that has a scrollbar that allows you to scroll through the agreement from top to bottom. It informs you that you are giving consent to be bound by all of the information within the agreement. That is, it is a legal agreement between you and Nortel as to the intentions of the VPN Client software, and exactly how that software can be used.

NOTE **You can use the Nortel VPN Client only if you agree to the information contained within the License Agreement.**

The License Agreement will define what materials are approved for use within the VPN Client. These materials will include such things as the related documentation, the VPN Client, on-line help, and Nortel Web access.

The License Agreement will define what authority the user has to use the VPN Client. It will list what is and is not allowed as far as sharing of information and will define licensing authority. It informs the user that Nortel owns the rights to the software and can enforce the rules that are outlined in the agreement. It also will list any warranty information and copyright information. Figure 10-3 shows an example of the VPN Client License Agreement window.

Once you have read and accepted the License Agreement, you can begin installing the VPN Client software onto your PC. If you have not yet read the release notes, do so now. The installation of the VPN Client will write files onto your PC, and you want to ensure that there are no known compatibility issues with any other software that may be loaded on your PC.

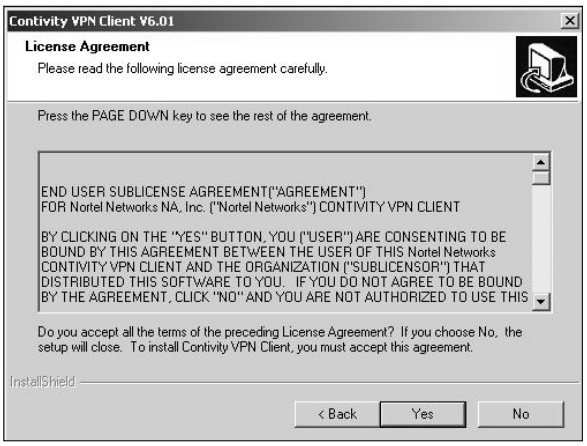


Figure 10-3: The Nortel VPN Client License Agreement

If you are certain that you are ready to install the VPN Client software onto your PC, you will now continue with the installation. The next step is for you to choose the directory into which you would like to install the software. The VPN Client install wizard will default to the following directory (see Figure 10-4):

```
C:\Program Files\Nortel Networks
```

If you want to go with the default setting (recommended), you simply click Next to continue the installation process. If you want to select another directory on your PC in which to install to, then you need to select the Browse button in the installation wizard window. Clicking Browse will allow you the option to specify into which directory you would like to install your VPN Client software. Figure 10-5 shows an example of the directory specification window.

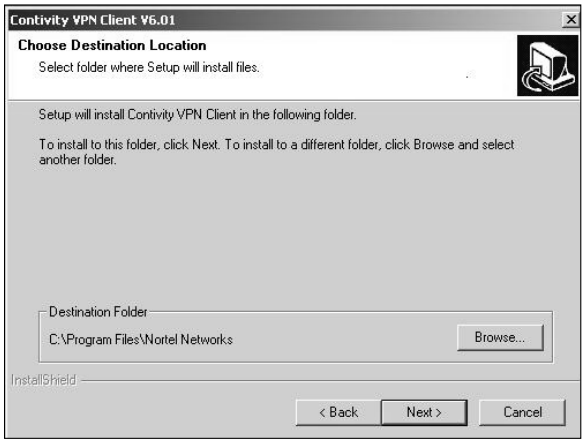


Figure 10-4: The Choose Destination Location window

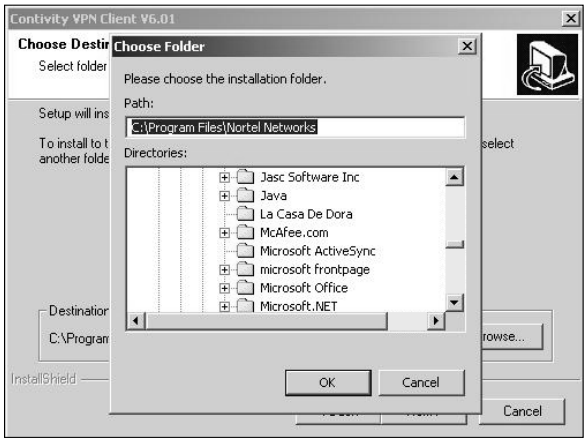


Figure 10-5: Selecting a directory to install your software into

Select the directory that you would like your VPN Client to be installed into and then click OK. You will then be brought back to the installation screen and can now click Next. You will need to specify the program folder that you would like the VPN Client shortcut icons installed into. This will be the Start menu folder that you will use to locate the icon that you will be using in the Windows environment to launch the VPN Client. As you can see in Figure 10-6, the default directory that the icons will be loaded into is Program Files → Nortel Networks.

NOTE **You can specify an alternate directory to have these icons loaded.**

The VPN Client installation software will now ask you what type of service that you would like the VPN Client to support. Following are the choices that you have to select from:

- As a application (default choice)
- As a Windows default service
- As a Windows GINA service

There is a warning message at the top of this installation window that informs you of the importance of reading and reviewing the VPN Client documentation if you are selecting a service other than the default (an application) service. Figure 10-7 shows an example.

The default choice is the most-often used choice and it requires that you launch the VPN Client to connect to your corporate LAN. Once connected, you will have access to the applications and services that you would normally have if you were physically connected to the corporate LAN.

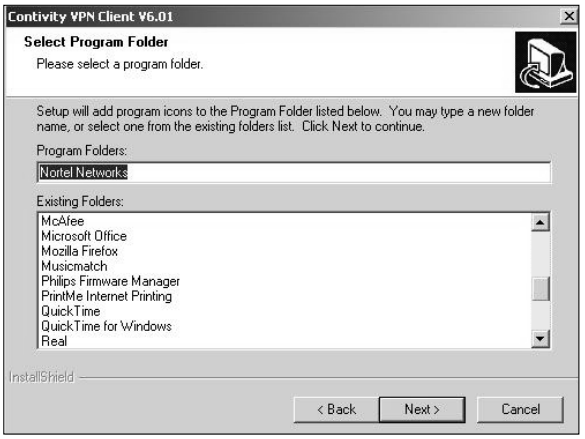


Figure 10-6: Selecting your icon folder

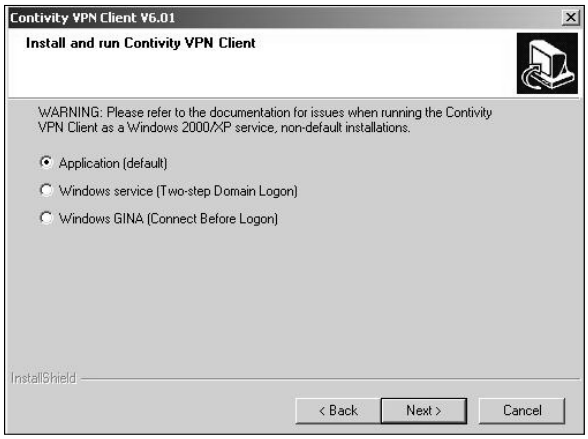


Figure 10-7: The VPN Client install service choice window

NOTE **In this chapter it is assumed that the VPN Client installation that we are referring to is the default application service choice. If a reference is made to any of the other choices, it will be noted as such.**

The Windows service requires you to make a connection to the VPN Router, but before you are able to access LAN applications and services, you will be required to log onto the corporate domain.

The Windows Graphical Identification and Authentication (GINA) service provides the user with secure login services. The Nortel GINA allows the user the ability to log on to the LAN domain prior to launching the VPN Client.

The service that is chosen will be determined by your network administrator and is decided based on the environment in which the network resides. Most installations will simply be the default, but you can check with your network administrator if you are unsure.

Next, you will be presented with a summary window that informs you that the installation process is about to begin. You will review what software and drivers will now be installed onto your PC. If you need to make any changes, you can click Back or Cancel here. Otherwise, you will click on Next. Figure 10-8 shows an example.

The installation process has now begun. The VPN Client installation application will load all necessary files for the correct and proper operation of the VPN Client. This process may take a few minutes. During this time, a status bar informs you of the progress of the installation. Occasionally, you will see a smaller window pop up that informs you some of the files that are being written to your PC and some of the files that are being adjusted.

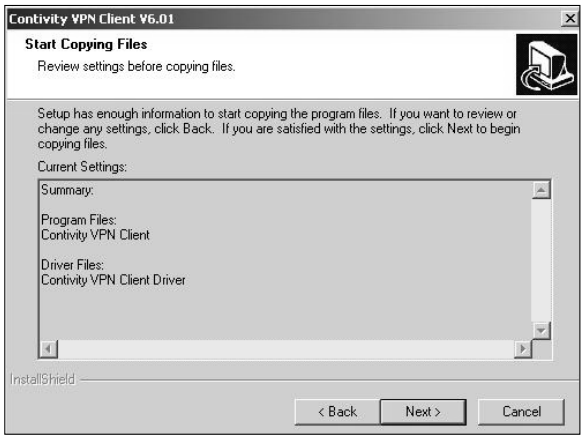


Figure 10-8: Start Copying Files window

The `readme.txt` file is presented in the next window. It is a help file that provides information to you about the VPN Client you are about to install. The following table of contents provides the topics that are contained within the `readme.txt` file.

- I. Introduction
- II. New Features
- III. Known Issues
- IV. Getting Help
- V. How to use Control Panel settings to prevent driver signing warning Messages from appearing

NOTE Beginning with version 6.01, a reboot is no longer required when installing the VPN Client. It is recommended to reboot, but not required.

Once the installation process is complete, a window appears, notifying you that it is done (see Figure 10-9). You can now use your VPN Client. Refer to all technical documentation prior to doing so to ensure that you comply with configuration recommendations. If you are unsure of any configuration or VPN connection parameters, contact you system administrator. If you are a system administrator and have a valid support contract with Nortel, you can find assistance and documentation on the Nortel support site (`www.nortel.com`).

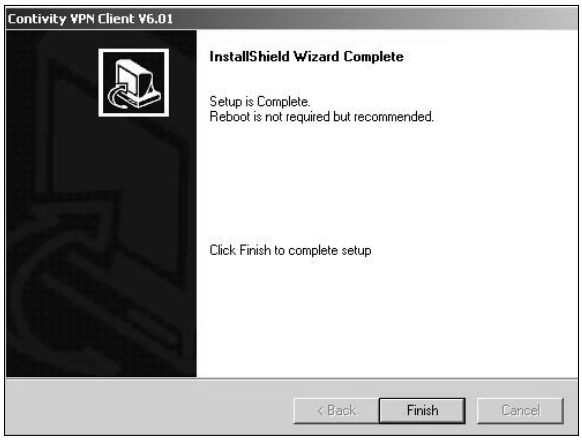


Figure 10-9: Client installation complete notification

Using the Nortel VPN Client

As with any other computer program, the only way to truly become proficient with a program is knowledge and experience. For most of us, reading and studying is the only way to obtain knowledge and learn the capabilities of the application. Putting the knowledge that you have learned to use is the only way that you gain experience in using the application. The Nortel VPN Client application is no different. It is one thing to understand how to enter a username and a password, but understanding some of the other tools available not only helps you in understanding what the program is doing, it can also assist in obtaining information in case you ever have problems.

This section discusses the VPN Client as an application. Covered in this section are some of the tools and services that are available to you in a standard windows installation.

The Nortel VPN Client is a standard Windows-based application and is as easy to use as any other Windows application. There are several different ways to launch the application, and most Windows users are already set in the way that they launch applications on their PCs. We will discuss one of the more common methods of launching applications. Once your Windows PC is up and running, you click the Start menu button on the Windows taskbar, and then go to the following directory: START → PROGRAMS → NORTEL NETWORKS → CONTIVITY VPN CLIENT.

Click once on the Contivity VPN Client icon and your VPN Client application will now load (see Figure 10-10).

Status and Monitoring

Chapter 3 discussed setting up a new VPN connection. Most often, the VPN connection information will be loaded into a corporate install, so to connect you would simply choose the site name that you want to connect to. Once connected, you will see a VPN icon in the Windows taskbar. If you place your mouse over the icon, it will inform you of your connection status. Figure 10-11 shows an example of the icon and the information window.

In the example, you can see that there is an active connection. Not only does the information bubble inform you of that, but there is a green light in the icon. The green light will remain in the icon as long as there is an active connection. If you need to close your VPN connection, you can do so by using the icon in the taskbar. By right-clicking on your mouse, a window appears that will allow you to select an option to shut down and log off the VPN Client.

If you double-click the VPN Client icon, the VPN Client Monitor window appears, and it contains status information about the VPN connection that you have established (see Figure 10-12).

The VPN Client Monitor window can assist you in monitoring your VPN Router connection. It can also be helpful in troubleshooting when you have a bad connection or are unable to bring up a connection. Following is some of the information that you can read on the screen:

- Total Bytes received
- Total Bytes sent
- Total Frames received
- Total Frames sent
- Destination IP address
- The tunneled assigned IP address
- Compression type
- Security Key type
- Duration of the connection
- Optional configuration choices

If you refer back to Figure 10-12, you can see the button options that are available to you on the right-hand side of the window. You can edit your profile, close the window, disconnect the session, and more. The VPN Client Monitor window is very helpful in obtaining quick and useful information about a current tunneled connection.

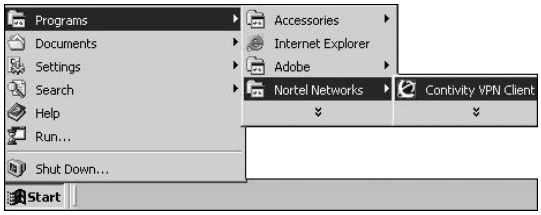


Figure 10-10: Starting the Nortel VPN Client via the Start menu



Figure 10-11: The VPN Client taskbar status icon

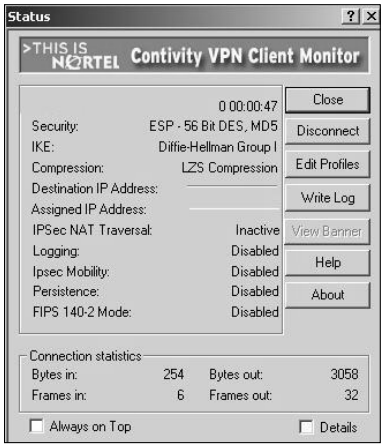


Figure 10-12: The VPN Client Monitor window

VPN Client Main Menu Items

The VPN Client main menu interface is the window that comes up when you first start your VPN Client. Not only is this the main menu you will use to set up and launch your VPN connections, there are also a few Windows menu options that you should get to know. This section discusses some of the options that are available to you. Following are the main menu options:

- File
- Edit

- Options
- Help

The File Menu Option

The File menu option provides you with menu items that you can select to help you set up your VPN Client. The following are submenu items that you can select within the File menu option:

- New
- Connection Wizard
- Save
- Delete
- Create Shortcut
- Exit

Figure 10-13 shows an example of the File menu screen that is in the VPN Client main menu.

The New menu item is used to set up a new VPN connection. It can be used in lieu of the Connection Wizard. The New menu item can be used only if you are sure of all the parameters needed to set up your new connection.

The Connection Wizard is used to assist in setting up the VPN connection for the first time. It is a step-by-step assistant that can help you set up your connection. The Connection Wizard is helpful if you are unsure of any of the parameters needed for your VPN connection.

The Save menu item is used to save a newly configured or modified connection. You do not have to use this unless you are setting up a connection, or are making changes to a connection.

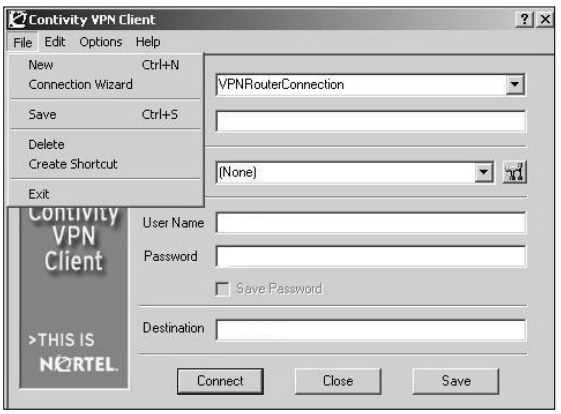


Figure 10-13: The File menu choices

The Delete menu item is used to delete a connection.

The Create Shortcut option will create an icon to allow you to launch the connection from the desktop, the Start menu, or whatever directory you would like to launch the VPN connection from.

Finally, the Exit menu item is used to exit the VPN Client.

The Edit Menu Option

The Edit menu option provides you with menu items that you can select to help you set up your VPN Client. The following are submenu items that you can select within the Edit menu option:

- Cut
- Copy
- Paste

Figure 10-14 shows an example of the Edit menu screen that is in the VPN Client main menu.

All of the options that are submenu picks in the Edit menu are standard Windows menu commands. They are used to either cut, copy, or paste text wherever the cursor is placed.

The Options Menu Option

The Options menu option provides you with menu items that you can select to help you set up your VPN Client. The following are submenu items that you can select within the Options menu option:

- Authentication Options
- Name Server Options
- Disable Keepalives
- Silent Keepalives
- Disable Auto Connect
- Install Auto Connect
- Connect before Logon
- Logoff to Connect
- Logoff Warning
- Log Session to File

Figure 10-15 shows an example of the Options menu screen that is in the VPN Client main menu.

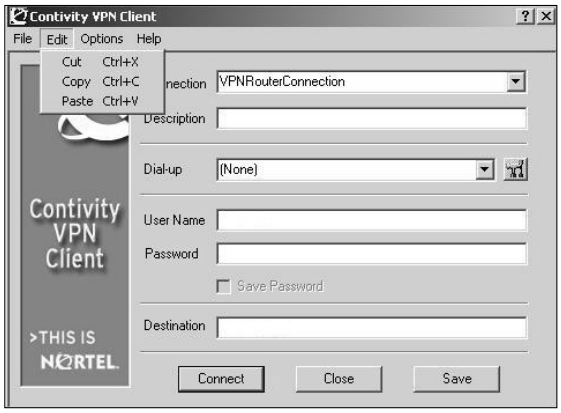


Figure 10-14: The VPN Client Edit menu choices

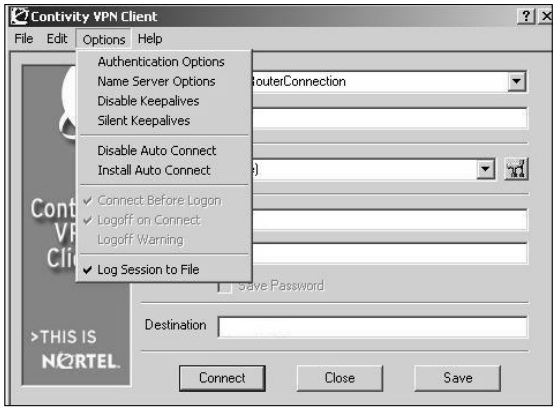


Figure 10-15: The VPN Client Options menu choices

The Authentication Options menu pick is very helpful in changing the authentication options that are already configured for the connection that you have brought up in your VPN Client. Within the Authentication Options, you have a choice of selecting any one of the following:

- Username and password authentication
- Digital certificate authentication
- Groups Security authentication

NOTE **If group authentication is chosen, then you will need to provide the necessary Group Security and Group Authentication Credentials and Options.**

The Name Server Options menu pick allows you to statically enter the Primary and Secondary DNS Server IP Addresses. You are also able to enter the WINS primary and secondary server addresses. Finally, there is a section to enter the Domain name into.

The Disable Keepalives menu pick is used to disable any configured keepalives, while the Silent Keepalives menu pick is used to evoke silent keepalives. Clicking these menu items places a checkmark or takes it away. If there is a checkmark next to either of these menu picks, then that means that particular pick was selected.

NOTE **Keepalives are discussed in more detail later in this chapter.**

The Disable Auto Connect menu pick will remove auto connect if it has been configured. The Install Auto Connect menu pick will install that feature.

The next features perform the action defined by the name of the menu pick. These options may or may not exist, depending on the service (GINA, Windows service) you are running. If the option is grayed out, then that menu item is not available as a choice, based on the configuration of the client. Each of these menu picks is self-explanatory:

- Connect before Logon
- Logoff to Connect
- Logoff Warning

The final menu pick in the Options section is Log Session to File. Selecting this enables client event logging on your PC. This is very helpful in troubleshooting connection issues for the client. It will create and write information about your connection into a file on your PC. The event log is discussed in more detail later in this chapter.

The Help Menu Option

The Help menu option provides you with menu items that you can select to help you set up your VPN Client. The following are submenu items that you can select within the Help menu option:

- Contents
- Search
- About Contivity Client

Figure 10-16 shows an example of the Help menu screen that is in the VPN Client main menu.



Figure 10-16: The VPN Client Help menu choices

The Contents menu option and the Search menu pick will bring up the help dictionary that enables you to search for help with your VPN Client through an index, and provides an in-depth search feature. If you ever have a question about the use of the VPN Client, you can find it through one of these two menu picks.

The About Contivity Client menu pick will provide you with information about the VPN Client. It will specify the version of software that you are running. It will also specify what services were installed, whether logging is on or not, and if Federal Information Processing Standard (FIPS) mode is enabled. FIPS is a U.S. Federal Government standard that enhances security. Finally, copyright information is contained on this screen

Nortel VPN Client Customization

Every private LAN is configured to best meet the needs for the function that the LAN supports. Because of this, network node software is configurable to allow the LAN administrators the capability to utilize services that are needed and exclude services that are not.

The Nortel VPN Client software is configurable and can be adjusted to meet the needs of the network. Not only are the parameters for the users configurable, the VPN Client can be customized so that it represents the supported LAN and ensures that only the necessary parameters are available to the VPN Client user.

You can customize the VPN Client to create icons, bitmaps (to change the user interface), and the customization of user profile parameters. The VPN administrator also has the option of allowing users to install the software themselves, or they can push the software to the client for automatic installation.

User profile parameters are configurable and most administrators utilize the customization options available to enforce network standards and to help reduce the possibility of a bad user installation. Following are some of the user profile parameters that are configurable:

- Advanced Encryption Standard support options
- Client logging support options
- Custom `readme.txt` file support options
- Desktop icon and shortcut installation options
- Dial-up profiles, when used
- Group name
- Keepalive options
- Password retention options
- Radius authentication options
- TokenType, when used
- Username
- VPN Connection Description
- VPN Router IP address or host name entries

VPN Custom Client Installation Modes

The VPN Client installation can be customized to determine what steps in the installation process require input from the user who is installing the VPN Client. The following installation modes are available for customizations within the VPN Client:

- *Reboot Only mode:* Skips most of the installation banner windows, reducing the number of input options the user has for the installation. The user does have to complete the finishing dialog box at the end of the installation.
- *Skip Screens mode:* Skips most of the installation banner windows, reducing the number of input options the user has for the installation. The only message window that will appear to the user during the installation process is the License Agreement.
- *Silent mode:* Skips most of the installation banner windows, reducing the number of input options the user has for the installation. This mode does not display the License Agreement window.

- *Quiet mode:* Skips most of the installation banner windows, reducing the number of input options the user has for the installation. The user does have to click a button to close the License Agreement window and will also have to complete the finishing dialog box at the end of the installation.
- *Verbose mode:* This is the default. This is the mode of the installation when no customization has been configured.

VPN Customer Client Group Profiles Overview

The VPN administrator has the option of creating customer files that can be included in the VPN Client installation process. The group.ini file is one of these types of files. This file allows the distribution of group authentication settings and group profile settings. Following are some of the parameters that are customizable:

- The product name that is displayed on the Start menu is customizable.
- The default program files folder can be customized.
- The installation can be customizable to skip all of the installation screens displayed during the install.

VPN Custom Client Icons and Custom Bitmaps

The Nortel VPN Client icons can be removed and you can put in any other icon that you would like to see displayed on the client node. There are four different icons that can be customized. There are also various areas where the icons reside, and they can all be overwritten with the custom client icons.

The custom bitmap options enable the VPN administrator to change some of the standard Nortel bitmaps. These bitmaps reside in the following client windows:

- The Client status message window
- The Extranet connection manager window
- The main Client window

VPN Client Event Logging and Keepalives Overview

Because a VPN Client connection is so important, the tools used to assist with maintaining and monitoring those connections is very important. The ability to gather important information on the VPN Router side of the tunnel is very convenient to have. However, there is a lot of Internet between the VPN Client

and the VPN Router, so there is a need to have information pertaining to tunnel connections captured on the client side as well.

The VPN Client also supports keepalives that assist in ensuring that the VPN tunnel remains in an up status for the users who need to reach the network at a moment's notice.

This section examines the Nortel VPN Client event log and the keepalives that it supports.

VPN Client Event Log

The Nortel VPN Client supports event logging on the machine that the VPN Client is installed on. The VPN Client logging is helpful in troubleshooting any issues pertaining to the initialization and maintenance of a VPN tunnel. These client event logs can be used with the event logs that are captured on the VPN Router to compare and assist in determining where the problem resides.

The client event log will normally be written if there is tunnel disconnect. It can be manually evoked by going to the following menu directory (see Figure 10-17): OPTIONS → LOG SESSION TO FILE.

The event logging within the VPN Client will initially write information to a space saved in memory for that purpose. Once the memory is full, it will write the information to a text file on the PC's hard drive. The file is written into the directory in which the VPN Client is installed, in the `log` directory.

The filename for the event log will be the name of the connection, followed by the name of the file `.log`. For example, the connection name that you have saved is called `myworkVPN`, and then the filename will be:

```
myworkVPN.log
```

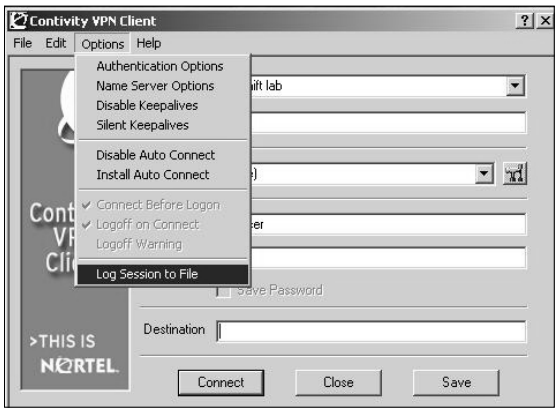


Figure 10-17: Initializing the VPN Client event log

If you stay connected and keep the VPN event logging parameter enabled, the memory will write a new event log each time the memory buffers are full. All subsequent files will be saved with the same connection name, followed by the number of the log. In the previous example, the first file was named `myworkVPN.log`. The following event logs will be named:

```
myworkVPN_001.log
myworkVPN_002.log
myworkVPN_003.log
etc.
```

Figure 10-18 shows an example of event logs saved in the `log` directory.

Event log messages are written in a standard format. The date and time of the event log message is written at the very beginning of the message. The date and time is written from the current time that is on your PC. The following event log entry was written at 01:49 on Dec. 11, 2005:

```
Sun Dec 11 01:49:23 2005 | Isakmpd      | I | Connection initiated to
10.10.10.10 [10.10.10.10] using Diffie-Hellman group 8.
```

Next, the activity that generated the message is written. In the following example, the activity that generated the message was Internet Security Association and Key Management Protocol (ISAKMP):

```
Sun Dec 11 01:49:41 2005 | Isakmpd      | I | NotifyControlApp() - Send
message to SC Application.
```

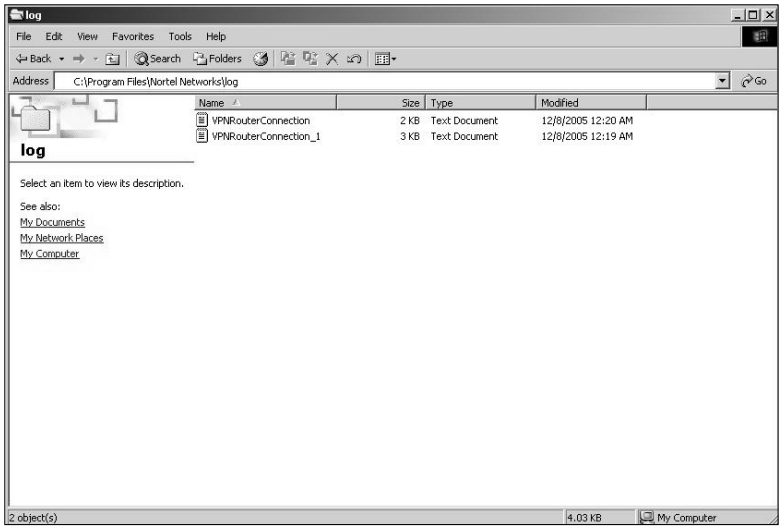


Figure 10-18: The Windows event `log` directory contents

The severity of the message is the third portion of the event log message. The severity will help you prioritize entries when reading the event log. Some event log messages are informational, while others annotate faults and warnings that have occurred. Following is a list of the severity codes for the VPN Clients' event log:

- *Fatal message (F):* This is considered a critical error and has caused a halt in operations.
- *Error message (E):* This is a message that is considered minor in importance, but it does need attention. This message may indicate a problem in the VPN Clients operation.
- *Warning message (W):* This is a message that may need attention. The message informs you that the action that is occurring may hamper other activities.
- *Informational message (I):* This message usually provides information as to the status of the VPN Client and its connection.
- *Success message (S):* This message indicates that there was success in the action that was being taken.

In the following example, the severity code is an `I`, which indicates that this message is an informational message. No action needs to be taken, but the information may be helpful in troubleshooting a problem.

```
Wed Dec 14 01:49:57 2005 | Isakmpd      | I | Connection initiated to
10.10.10.10 [10.10.10.10] using Diffie-Hellman group 8.
```

Finally, the message itself is written. It is written in a way that it can be read without having knowledge of the coding involved in the development of the VPN Client. The following message indicates that there was a login failure because the remote host (the VPN Router) did not respond to a request to connect:

```
Wed Dec 14 01:50:46 2005 | Isakmpd      | F | Login Failure due to:
Remote host not responding
```

VPN Client Keepalive

A VPN tunnel keepalive message is a way of ensuring that a tunnel remains up, even during periods of inactivity. Simply put, a *keepalive* is a message that is sent between end nodes to ensure the link between them is functional. Most of the time, a keepalive message is transmitted at predefined time periods. If a message is sent and a reply is not received, then the link is assumed to have been dropped.

In VPN routing, some user tunnels require a higher priority of connectivity and may require that keepalive messages be transmitted to keep the tunnel from disconnecting. An example of someone who would need to ensure instant connectivity would be a corporate director.

The Nortel VPN Router supports multiple variations of the keepalive message. Each of the different types serves a different purpose than the other. Following are the three types that are supported:

- Internet Security Association and Key Management Protocol (ISAKMP) keepalives
- Network Address Translation (NAT) Traversal keepalives
- Silent keepalives

Internet Security Association and Key Management Protocol Keepalive

ISAKMP is a cryptographic networking protocol that is used as a foundation for the rules defined in the Internet Key Exchange (IKE) protocol.

Considered a traditional keepalive type, the ISAKMP keepalive is sent only during the times that there is no activity within the tunnel. This type of keepalive message is originated by both the VPN Router and the VPN Client. The keepalive packets are sent on UDP port 500.

Each time a keepalive packet is sent, the originating side will expect to receive an acknowledgment of receipt from the other node. If it does not receive that acknowledgment, the tunnel session will be brought down. Remember that this type of keepalive is used only during periods of inactivity and is not generated if there is activity within the tunnel.

NOTE The ISAKMP keepalive is the only type of keepalive that will drop a tunnel session.

Network Address Translation Traversal Keepalive

Network Address Translation (NAT) is a protocol that, when implemented, allows a NAT device to remove the private IP address of an originator and change it to a public address for the NAT device. The packet is then sent across a WAN to a destination.

The NAT device maintains a NAT table so that it knows what the IP address-to-NAT address conversion is. NAT makes adjustments to the original IP header of a packet, so it also makes it hard to use NAT in an environment that is running L2TP over IPSec tunneling protocols.

Because of the security implications of running NAT in an L2TP/IPSec environment, the Internet Engineering Task Force (IETF) created the NAT Transversal (NAT-T) method.

The NAT-T keepalive is configured on the VPN Router and is passed by the VPN Router to the VPN Client when the user tunnel is first established. Once a VPN tunnel session is established, the VPN Client will generate the keepalive packets and will send them constantly while the tunnel is up. The main purpose of this type of keepalive is to maintain an active state within the NAT device for the NAT transversal port for which it is was configured.

Silent Keepalive

The Silent keepalive is the final keepalive type that is supported by the Nortel VPN Router. This type of keepalive is generated by the VPN Client and is constantly generated for the purpose of ensuring that the VPN tunnel remains up and active. The client forwards these packets on UDP port 500.

The Silent keepalives do not expect any acknowledgment to the originating message. Because there is not an acknowledgment to the original keepalive packet, during inactive periods within the tunnel, the client does not recognize if the other side of the tunnel has dropped. This creates a problem in that the tunnel will remain up even if one side is no longer active. The tunnel will not drop until the inactivity time has expired.

Silent keepalives are sent at the ISAKMP or NAT-T interval that is set on the VPN Router. Silent keepalives must be enabled and the ISAKMP keepalive must be disabled in order for the Silent keepalive to become active.

IPSec Mobility

As mentioned several times in this book, VPN networking has a huge number of advantages over traditional remote-access networking. Most companies today employ some type of a VPN solution as a standard for the company and its employees.

IPSec provides the capability for remote users to connect to the corporate LAN from remote locations in a secure manner, over what could be considered an insecure public networking infrastructure.

As technology is constantly evolving, more and more users are using wireless solutions as a method of connecting to the Internet. This provided the users the ability to be mobile while working and to no longer be "hard-wired" to a specific location (the location where your physical connection to the Internet happens to be).

The problem with wireless connectivity in a secure IPSec VPN solution is that it is difficult to ensure that the tunnel does not get torn down as the user is moving between multiple networks in a wireless LAN environment. Traditional IPSec handles the movement between networks by tearing down a connection and then re-establishing it from the network to which the user has moved. This could disrupt whatever the user is doing and could potentially create problems for the user, as well as the company.

For example, refer to Figure 10-19. Here you can see that a wireless user has moved within a building. The connection has changed from access point A to access point B. In making this move, the user will lose the secure VPN connection and will have to re-establish it from the new area. This is because the VPN Router will recognize that the user is no longer accessible through the secure tunnel via access point A and will drop the tunnel.

NOTE **This same concept will hold true if access point A goes down or loses a link. The user does not have to be physically moving to cause the change from one access point to another.**

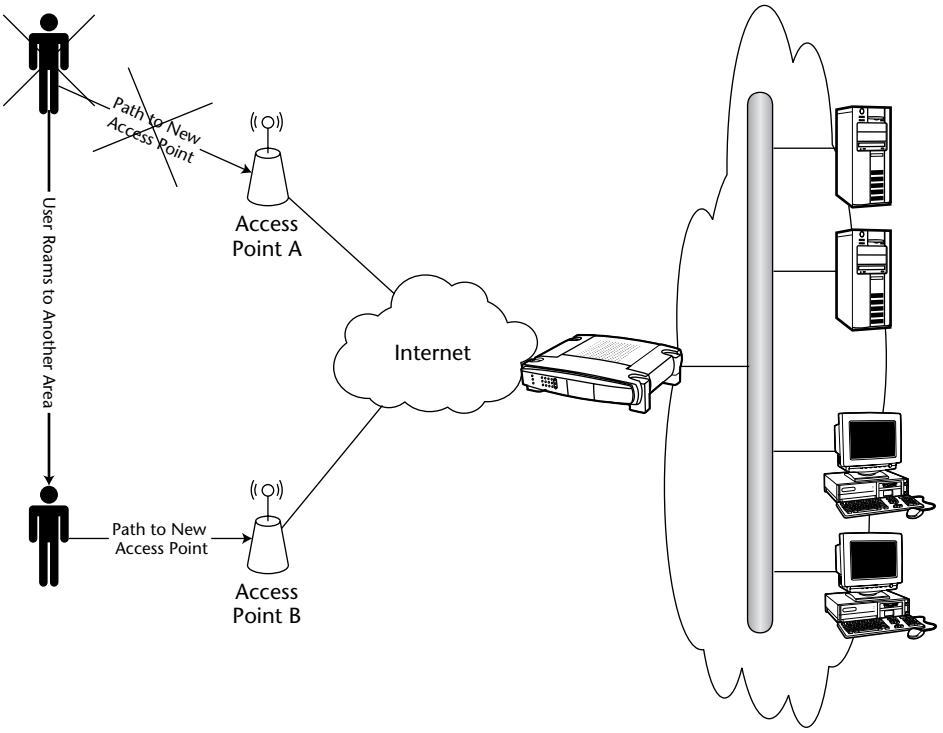


Figure 10-19: Example of an IPSec tunnel dropping because a user moves from one access point to another access point

In the previous example, consider that the remote user may have been a salesperson sending in the order confirmations for the day. Or, it may have been a bank branch manager transmitting financial transaction data for the day. You can see some of the problems that may occur should the tunnel drop down during these crucial periods of time.

There have been a few solution suggestions to the traditional IPSec protocol to allow for mobility within the IP and the IPSec environment. Some of these solutions are considered inefficient because they can cause a duplicate tunnel to be established by a mobile user. Nortel has enhanced the traditional approach to the mobile user within an IPSec tunnel by proposing the IPSec mobility implementation within the Nortel VPN Router environment.

The Nortel VPN Router IPSec solution allows VPN Clients the capability to roam from access point to access point while maintaining the integrity of the tunneled connection. The Nortel solution ensures that TCP application communication remains intact, and it also ensures that UDP applications experience very little (if any) disruption.

If implemented, the Nortel VPN Router will pass the IPSec mobility configuration parameters to the VPN Client, upon the establishment of a VPN user tunnel. Once the VPN Client has received these configuration parameters, it will be instructed to monitor any changes to the IP address that it has been assigned. The PC OS will report any changes of IP addresses to the VPN Client; the VPN Client will then report the changes to the VPN Router. The router will make the appropriate security and routing changes within the maintained databases and will send an acknowledgment to the VPN Client that it recognizes the change.

NOTE **The VPN Client will make four attempts to notify the VPN Router of an address change. If the VPN Client is not able to contact the VPN Router, then the tunnel will be brought down.**

Security Banner

The security banner is configured on the VPN Router and is displayed when a user attempts to make a VPN user tunnel connection to the VPN Router. The message in the banner is developed by the VPN Router administrator and normally contains informational notices about the access rights relating to the VPN connection. Figure 10-20 shows an example of the security banner.



Figure 10-20: The VPN security banner

The security banner changed with VPN Client software version 6.01. The banner developed a new look, and with that new look came some additional features that were not included in previous versions. These features include the following:

- URLs that are included in the security banner now act like hyperlinks and are clickable.
- The buttons that are in the bottom of the security banner in Figure 10-20 (Accept/Close, Accept, and Cancel) were added.

When the security banner is configured on the VPN Router, the banner will come up on the client side when the user attempts to make a connection to the VPN Router. The banner displays whatever message has been configured and all traffic is blocked until the banner has been acknowledged and accepted by the user.

The buttons that are available to the user are at the bottom of the security banner window. When clicked, the buttons perform the following actions:

- *Accept:* This button allows the connection to complete and allows the user access to the LAN. All services that the user is assigned are available. The security banner remains up on the user's desktop.

- *Accept/Close:* This button allows the connection to complete and allows the user access to the LAN. All services that the user is assigned are available. The Security Banner will close when the user clicks on this button.
- *Cancel:* This button cancels the VPN connection and drops the user tunnel.

NOTE **If the user cancels the VPN connection, an event is logged in the event log on the VPN Router.**

Split Tunneling

A VPN tunnel is a secure method of allowing remote users access to a private network over the Internet. The protocols and technologies used in VPN tunneling allow data (normally from a corporate LAN) to flow over the Internet through various routing nodes to a remote destination without any of the public nodes becoming aware that the data is information that is private and secure. Simply put, VPN tunneling utilizes and authorizes the Internet to transmit private data securely to its destination.

When a VPN tunnel is established by a remote user, all traffic sent to and received from the end user's workstation is directed over the tunnel, to/from a VPN Router. Each and every packet that is received and sent over the tunnel is inspected by the VPN Router, and all security policies are applied to that data.

Consider for a moment an end user who is connected through a VPN tunnel to the corporate private LAN. The user takes care of all business data transmissions over that LAN. As a matter of fact, the default gateway for the end user during a VPN tunneling session is the VPN Router, and no other public routes will be applied to the user. If the user has a need to establish a connection outside of the corporate LAN, the VPN Router will handle all of the routing to ensure that the end-user traffic reaches its destination. However, all VPN security parameters are applied to the end-user traffic. This causes the utilization of bandwidth where it really isn't necessary and takes VPN resources to enforce, where they could be used to handle traffic destined to the LAN.

Refer to Figure 10-21. In a traditional VPN tunnel configuration, all traffic to and from the VPN Client goes to the VPN Router and then is inspected and forwarded to its destination. This includes all traffic to and from the client. For example, if the VPN Client has an established VPN connection, and sends a request to connect to the Web site of a supplier, the request goes through the

VPN tunnel, through the VPN Router, and is forwarded back to the Internet hosting service to reach its destination. The return traffic follows a reverse path. You can see how this can consume VPN tunnel bandwidth, as well as VPN Router resources that really should not be involved in servicing traffic destined to a source other than the private LAN resources.

So, to allow a user to connect to the Internet while also being able to send and receive secure private traffic from the private LAN, split tunneling is used.

Split tunneling is a process that allows a VPN Client user to connect to a private LAN from a remote location, and also have the capability to have concurrent public sessions to the Internet. This allows the user to have access to public devices (such as a public email server or HTTP sessions), while also being able to have private LAN data flow to and from the private network.

The main advantage to split tunneling is that is conserves bandwidth and VPN Router resources because Internet traffic does not have to flow through the tunnel and the VPN Router. One disadvantage to consider is that split tunneling may make the VPN Client vulnerable to attacks because it is now accessible through the Internet while a VPN tunnel is established.

In a split tunneling configuration such as the one shown in Figure 10-22, all traffic destined to/from the private network goes through the tunnel to/from the VPN Router and then is inspected and forwarded to its destination. All other traffic is sent over the Internet to the Internet host service, and then is forwarded to its public destination. For example, if the VPN Client has an established VPN connection and sends a request to connect to the Web site of a supplier, the request no longer goes through the VPN tunnel. Rather, it is directed to the Internet host service, which handles the request and subsequent data-flow activity. You can see how this can resolve the problem of the additional VPN tunnel bandwidth, as well as VPN Router resources, because the VPN Router now only has to handle requests to/from the private LAN.

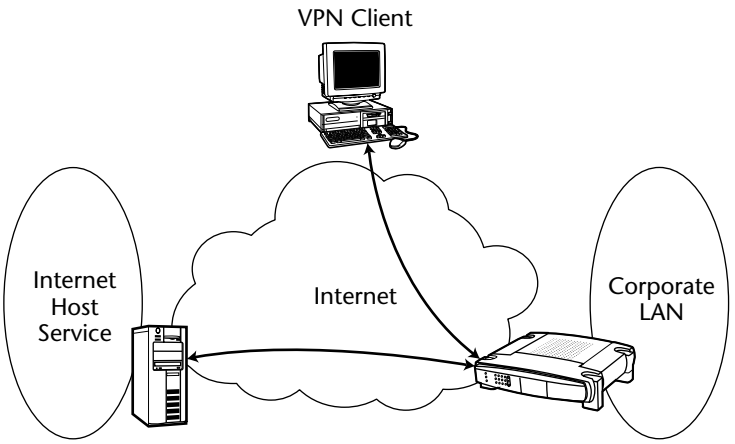


Figure 10-21: Traffic flow in a mandatory VPN tunnel

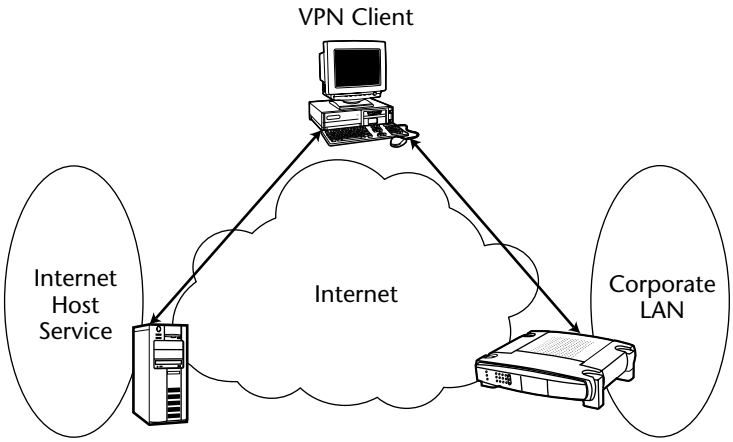


Figure 10-22: Traffic flow when split tunneling is enabled

Considerations

When deciding whether to enable a VPN Client to support split tunneling, there are a number of considerations. Following are some of the advantages of split tunneling:

- Split tunneling conserves bandwidth and VPN Router resources.
- Split tunneling gives the remote user access to LAN services, as well as open access to the Internet.
- Split tunneling ensures that the VPN Client station is able to contact its ISP's DHCP server while in a VPN tunneling session. This ensures that the lease for the client station's IP address does not expire.

While safeguards are in place, there is a consideration that needs to be addressed when applying split tunneling services on a client. The main disadvantage is that with split tunneling enabled, the client's PC is vulnerable to receiving adverse traffic from the Internet. This adverse traffic could cause an application on the client node to forward that adverse data over the tunnel to the private LAN.

This does not mean that private data is forwarded from the VPN tunnel to the Internet, but an application can retrieve information, and then can process and send it to a public destination without the VPN Client user even being aware.

The Nortel VPN Router has safeguards in place that will help to alleviate the potential for such an occurrence. The VPN Router inspects packets that are destined to the private LAN, and will drop any packets that have a source address other than the IP address that is assigned to the VPN tunnel connection. Additionally, the VPN administrator can determine what ports are

active for the VPN Client user, and can limit the applications that are accessible by the client when split tunneling is enabled. Finally, firewall and interface traffic filters can be put in place to put limits on the type of data that can be sent over the user tunnel.

The safeguards that have been put in place for the Nortel VPN solution assist in preventing unnecessary hack attacks. As technology changes, and hackers change with it, there will probably be other changes in the future. As with any other data technology, processes continually change.

Inverse Split Tunneling

Inverse split tunneling can be configured on a VPN Client to limit the traffic destined to other services while the VPN tunnel connection is up. This is helpful in allowing the VPN Client node access to certain subnets outside of the private network, while blocking subnets that may be potentially harmful to the client and the private network.

In an inverse split tunneling configuration such as the one shown in Figure 10-23, all traffic destined to/from the private network goes through the tunnel to/from the VPN Router, and then is inspected and forwarded to its destination. All other traffic destined to/from approved subnets is sent to its public destination. All public traffic destined for subnets that are not defined as approved are then dropped. In Figure 10-23, you can see a VPN Client that has access to a printer and a scanner on its local network. A VPN tunnel is established and inverse split tunneling rules have been configured to allow the user to utilize the print and scanner services on its local LAN, while being able to use services over the tunnel for the private LAN. All other public traffic is blocked.

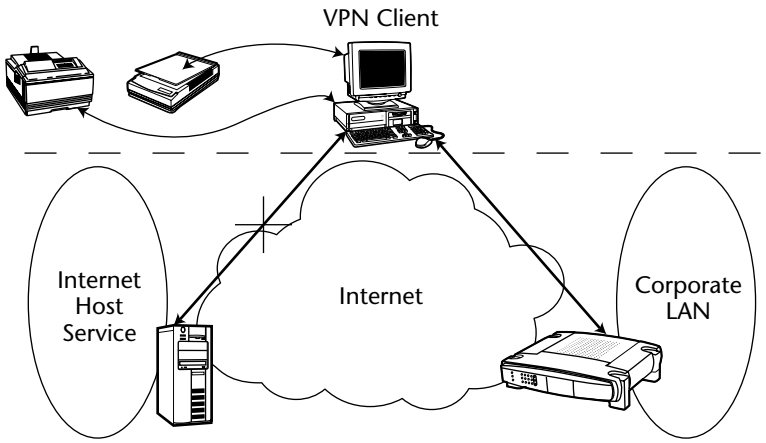


Figure 10-23: An inverse split tunneling solution

Support for All Zeros Addressing in Inverse Split Mode

Beginning with VPN Client software release v6.01, the VPN Client supports inverse split on network wildcard address of 0.0.0.0 with a subnet of 0.0.0.0. This allows the administrator to define the rules of access for the VPN Client without knowing the local subnets defined for the VPN Client user.

When the VPN Client receives a list of inverse split authorized subnets, it will recognize the wildcard IP address and subnet address as the subnets that are local to the user.

TunnelGuard

Nortel's *TunnelGuard* is an application that allows for checking of the VPN Client remote station. TunnelGuard performs system compliance checks in the areas of disk content, digital certificates, and current running processes. As of this writing, TunnelGuard does not perform checks on system registry information and application version information.

Although TunnelGuard is configurable on the VPN Router, it is a software application and is not part of the VPN Client software package. It is mentioned in this chapter because it is part of the VPN Client node when it is installed and in operation. It is important to have an understanding of the TunnelGuard application, not only from an administrator's point of view, but also from a remote user's point of view.

TunnelGuard allows the VPN networks security policy to be applied to the remote user's PC when the user has a VPN Client tunnel up and is connected to the private LAN. TunnelGuard ensures that the valid Software Requirement Set (SRS) is installed, activated, and maintained on the VPN Client node when the VPN user is connected to the private LAN via the VPN Router.

TunnelGuard performs three main functions, each enveloped into a function separate from one another. Following are the three functions that make up TunnelGuard:

- TunnelGuard Agent
- TunnelGuard Daemon
- System Requirement Set (SRS) builder

TunnelGuard Daemon

The *TunnelGuard Daemon* is system software application that runs on the VPN Router. The job of the TunnelGuard Daemon is to communicate the rules of service to the TunnelGuard Agent. The rules are applied to the VPN Client node and are monitored by the TunnelGuard Agent. The Daemon receives the

status information that is provided by the Agent, and it takes appropriate action for non-compliance.

Software Requirement Set Builder

The *Software Requirement Set* (*SRS*) Builder provides the administrator with an easy-to-understand application interface to generate and maintain the SRS rules that have been created. The rules that are created by the SRS Builder are applied to VPN Client users, and are maintained by the Daemon and the Agent.

TunnelGuard Agent

The *TunnelGuard Agent* is a software application that runs on the VPN client's PC. It receives instructions from the TunnelGuard Daemon and it is the job of the TunnelGuard Agent to monitor rules that are assigned to the PC, as well as to monitor the status of those rules.

NOTE The rules that are monitored by the TunnelGuard Agents are known as the System Requirement Set (SRS) rules.

The TunnelGuard Agent provides a status of its findings in the checks and system monitoring information back to the TunnelGuard Daemon, which runs on the VPN Router.

The TunnelGuard Agent does not run all of the time on the end user's PC. It does start when the PC is first booted, but remains inactive and initializes only when a User VPN tunnel is initiated. After the tunnel session is complete and the client disconnects from the tunnel, the Agent remains inactive until the tunnel is brought up again.

NOTE The TunnelGuard application is not part of the VPN Client. It is a separate entity.

So, what does the TunnelGuard agent do while it is in an inactive state? It simply waits until it gets a message from the TunnelGuard Daemon, letting it know that a tunnel is up and that it's time for the Agent to start monitoring the SRS rules. The Agent will then initiate a connection to the daemon, with authentication information. The Daemon will provide the SRS rules to the Agent, which then authenticates personal firewall information. Finally, the Agent begins its checking, and will continue checking and sending status updates to the Daemon until it receives a message that the tunnel has been brought down.

TunnelGuard Features Overview

Like any other software package, the TunnelGuard application has a few standard and a few configurable options that are important to know and to understand. This section provides an overview of most of these features.

TunnelGuard Icon Information

TunnelGuard is supported on the major versions of Windows software. When it is enabled, TunnelGuard displays a status icon on the taskbar of the Windows PC on which it is running. The state of the TunnelGuard Agent is represented within the icon by the following colors:

- *Gray*: TunnelGuard is inactive.
- *Green*: TunnelGuard is active and is in compliance with the rules specified by the Daemon.
- *Red*: The user's PC has failed.

TunnelGuard Installation Considerations

When deploying the TunnelGuard application, it is important to note some of the installation considerations. Ensuring that your network infrastructure can support the TunnelGuard application is important. It is equally important to understand what options are available to you so that you can ensure you are able to maintain the deployment and maintenance of the TunnelGuard application.

The TunnelGuard application can be purchased by CD or can be downloaded from the Nortel Web site. Java Runtime Environment (JRE) version 1.4.1_02 is required on the user's PC in order for TunnelGuard to run. There are two different kits that are available for the TunnelGuard application. One of these is the VM kit, which contains the JRE software, and the other is a non-VM kit, which is smaller and better for downloading.

Within the kits are two versions. One is the standard version and the other is the customizable version. Much like the VPN Client software, the standard version is installed with the standard features, while the customizable version can be changed by the VPN administrator to meet the needs of the private LAN.

TunnelGuard Event Logs

The TunnelGuard event logs will maintain the same status information that the Agent is monitoring. This logging is enabled by default, but may be disabled with the custom install version. It can optionally be disabled through the

system registry on the VPN client's PC. The TunnelGuard event logs are maintained by default in the following directory:

```
C:\Program Files\Nortel Networks\TunnelGuard\logs
```

The logs available to you in the Nortel VPN solution do keep some information pertaining to TunnelGuard. The Nortel VPN Router will log TunnelGuard information that is received from the Agent. The VPN Client log will not log any information pertaining to the TunnelGuard application.

Banner Messages

When the TunnelGuard Agent receives a tunnel failure notification, it will display a pop-up banner on the client PC. The banner message will notify the user that the tunnel has disconnected. If the disconnection occurred because of an SRS check failure, then the banner will notify the user of this. This feature can be disabled.

VPN Client Failover

Several mentions have been made in this book about the benefits of the VPN Router. The time saved and the production values that are now available are priceless compared with what could be done from home prior to VPN technology.

However, for a moment, consider what may occur if you must connect to the network at a particular time and the VPN Router that you are configured to connect to goes down. There are a few alternatives that can be instituted within the corporate LAN. You may have an alternate VPN Router to connect to, or you may have a dialup connection to a modem bank that can be established. Both of these would appear to be viable alternatives if the primary connection fails, but both would require additional steps and may even cause a degradation of service. You just cannot afford to not be able to log in when you need to. Because of this, the Nortel VPN Client and Router software support VPN Client failover.

In data communications, the term "failover" means that if the main node that you would normally connect to goes down, there is an alternate (or standby) node ready to take over operations over the link. Failover occurs without any type of intervention taking place. Additionally, failover is transparent to the end user.

Suppose you are a Nortel VPN Client user connecting to your corporate LAN. You input a destination IP and a username and password, and then try

to connect. The VPN Router has failed, but you are not aware of this. The VPN Client failover feature recognizes that the main link to the LAN is down and will direct your request to an alternate VPN Router. You will be connected and will not even realize the main (or primary) VPN Router had gone down. Figure 10-24 shows a graphical representation of VPN Client failover.

Nortel VPN Client failover is configured on the VPN Router, and it provides the VPN Client with a list of alternate VPN Routers to connect to if the main VPN Router is not reachable. The Nortel VPN Client will continue to try to connect until it exhausts all destination IP addresses that are in its failover list. If none of the VPN Routers in the list are responsive, then the VPN Client will declare the router unreachable and will no longer attempt to connect to a VPN Router.

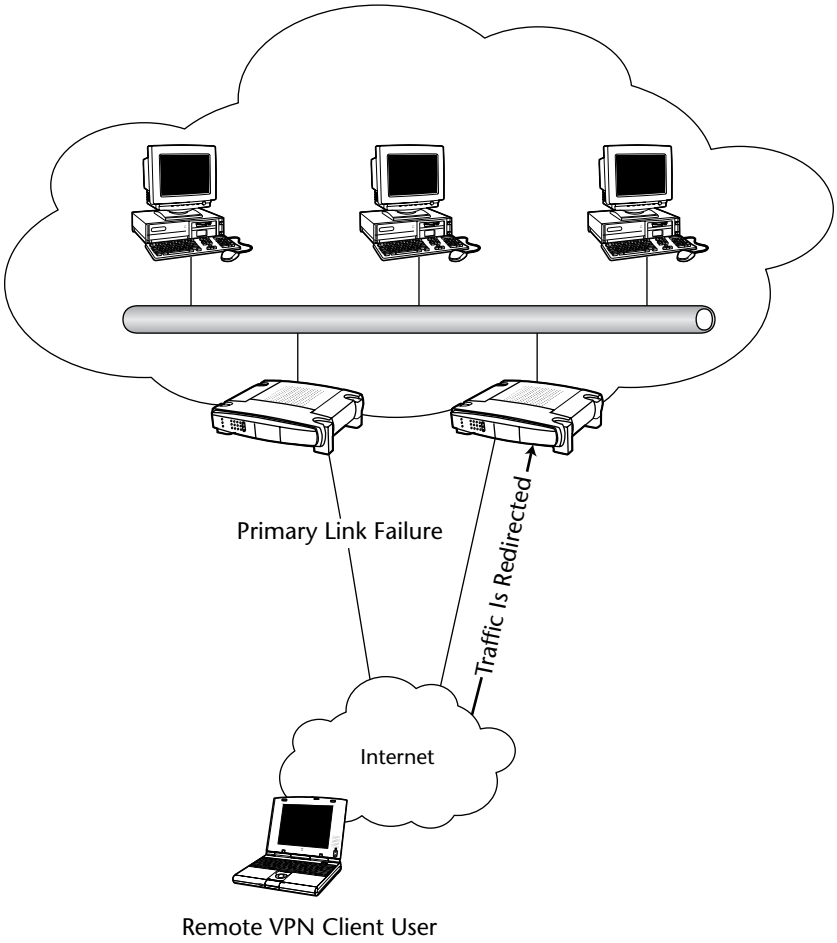


Figure 10-24: An example of VPN Client tunnel failover

When the VPN Client makes its first connection to the VPN Router, it receives a client failover list that provides the destination IPs of all of the VPN Routers that a connection can be made to, in the event that the primary router is inaccessible. The failover listing is written to the Windows OS system registry in the following path:

```
HKEY_CURRENT_USER/Software/Bay Networks/Extranet Access Client/Profile
```

In this directory of the Windows-based OS system, you will find information that is written by the VPN Client that instructs the OS on how to handle certain functions of the VPN Client application.

NOTE **If you do not enable the option to allow for password storage on the VPN Client PC, the client user will be required to enter a password upon connection establishment to a failover router.**

In Figure 10-25, you can see the failover list and the list of IP destinations that can be attempted if the previous one fails. Each destination IP is separated from the next one by a space. Therefore, in the example, the VPN Client will connect to each of the following destination IP VPN Routers and will failover to the next IP if that one fails:

1. Try destination 10.10.10.1.
2. If it fails, then try destination 10.10.10.3.
3. If it fails, then try destination 10.10.20.1.
4. If it fails, then try destination IP 10.10.20.3.
5. If it fails, then the VPN Client will report the connection failure and will stop all attempts to connect.

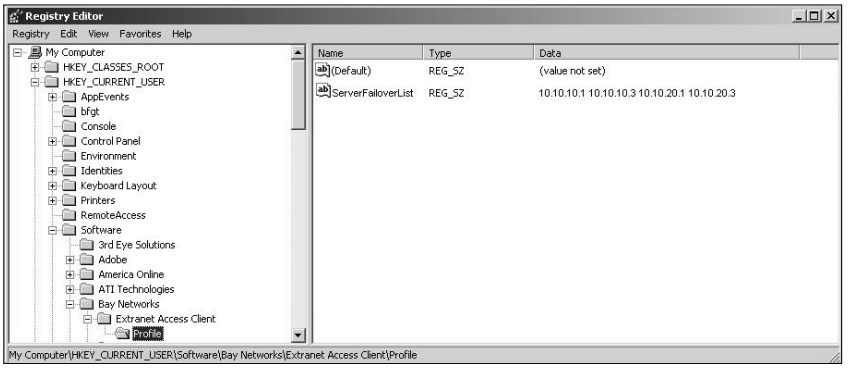


Figure 10-25: The VPN Client failover list in the system registry

For the VPN Client failover to operate correctly, the configuration settings of all of the VPN Routers in the failover list must be the same. If the information is not the same, then the VPN Client will not be able to log onto the failover VPN Router and the connection attempt process will be halted.

VPN Client failover is configured on the VPN Router and is configurable through the browser GUI interface, or through the CLI. In Chapter 11, there is a lab that will walk you through configuring client failover.

Summary

This chapter has covered the Nortel VPN Client software, including supported platforms, installation information, configuration information, and basic concepts. Most of what was discussed in this chapter will be put to practical use in Chapter 11, which covers labs.

In Chapter 11, you will configure many of the options that were discussed in this chapter and, therefore, you will be given some hands-on experience implementing the concepts that were covered.

This chapter also discussed VPN TunnelGuard and how it interfaces with the Nortel VPN Client. Although this is a separate software application, it was important to mention it in this chapter.

CHAPTER

11

VPN Router Administration Lab Exercises

Nortel provides documentation and help-menu selection tools within the VPN Router software. There is also some helpful information contained on the Nortel Web site. Having documentation to refer to is very helpful in administering your VPN Router, but an integral part of learning to use the VPN Router is by doing just that—using the VPN Router.

This chapter should serve as both a learning vehicle and a reference tool. The 18 labs in this chapter walk you through a step-by-step configuration of some of the basics on the VPN Router. Each lab is broken down into sections. The lab will begin with a brief explanation of the lab, followed by a list of requirements for the lab. The "Lab Setup" portion of the lab contains the steps necessary to complete the lab. Finally, the "Lab Summary" contains information and discussion points about the lab.

Installing the VPN Router into your LAN will be very specific to your LAN. The technologies and protocols that you are using are not necessarily the same as those being used by others. The labs in this chapter do not cover every possible administrative task within the VPN Router, but by doing each lab, you should gain a firm understanding of the VPN Router. Take notes as you go through the lab. They may be helpful in the future.

The labs will cover the configuration of some of the services, technologies, or protocols that are supported by the Nortel VPN Router. Advanced configurations and testing are left to you.

Installing the VPN Client Software

As a network administrator, one of tasks that you will be involved with is working with others in completing the installation of the VPN Client software on the remote workstations. The administrator decides how best to handle this procedure. Although there are options in how the rollout of client software is handled, this lab covers how to install this from the remote PC. This lab discusses the steps required to load the Nortel VPN Client software onto a user's PC.

Lab Requirements

- Windows-based PC with Internet Explorer
- Pencil and paper for notes
- VPN Client software V6_01 or higher

Lab Setup

1. Locate the VPN Client installation application and double-click the icon.

NOTE The installation software is an executable (`.exe`) application and the filename begins with "EAC". It can be downloaded from the Nortel Web site, or you can locate the application with the software package that came with your VPN Router.

2. At the Install Shield Wizard window, click Next.
3. Read through the License Agreement and then click Yes.
4. Accept the Default destination, and click Next.
5. Accept the default program folder, and click Next.
6. Ensure that the Application radio button is selected, and click Next.
7. Click Next again.
8. Read the contents of the `Readme.txt` file, and click Next.
9. Click Finish.

Lab Summary

This lab exercise assumed and accepted the default values for the installation of the VPN Client. Additionally, it assumed that the PC that you are using does not have the Nortel VPN Client installed on it. If there is a previous version of the Nortel VPN Client, the steps taken to install will be different than what is in this lab.

This lab explained the deployment of the VPN Client via an executable software load in the remote PC. What other options could be considered for deploying the VPN Client to the remote nodes within your LAN? What are the advantages and disadvantages of each?

As with any configuration change within the nodes on your network, it is important that all related documentation is reviewed before installing and enabling any advanced features on the Nortel VPN Router and/or the Client user PC.

Initial Setup of the Nortel VPN Router

All VPN Router administrators need to understand how to set up and configure the VPN Router. Events may occur that will require this knowledge. One of the most important tasks that you can learn how to do is establishing an initial connection to the VPN Router as well as assigning IP addresses to allow you to access, configure, and manage the VPN Router.

In this lab exercise, you perform the initial setup for your VPN Router. You connect the router and assign the Private IP addresses, as well as the management IP. Finally, you test the setup.

Lab Requirements

- VPN Router
- Windows-based PC with Internet Explorer
- Pencil and paper for notes
- Console cable
- Crossover cable
- Lab diagram (see Figure 11-1)

NOTE **Be sure to refer to the lab diagrams within each lab. The diagrams will contain information that you will need to refer to, including IP addressing for the lab.**

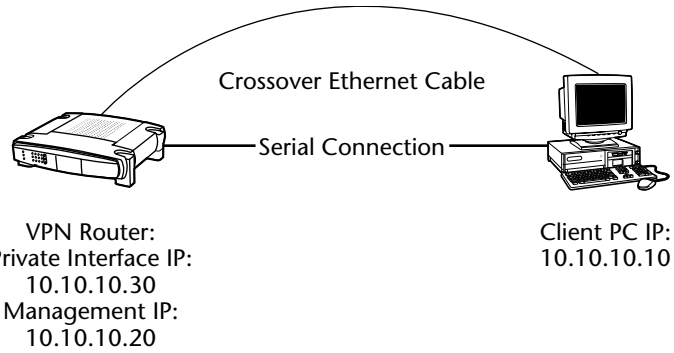


Figure 11-1: VPN Router setup lab diagram

Lab Setup

1. Connect a serial cable to the serial interface on your VPN Router.
2. Establish a HyperTerminal session to the VPN Router. The HyperTerminal settings are as follows:
   - *Bits per second:* 9600
   - *Data bits:* 8
   - *Parity:* None
   - *Stop bits:* 1
   - *Flow control:* Hardware
3. Once connected, press the Enter key on your keyboard. You will be prompted for a username and a password. They are as follows:
   - Username: admin
   - Password: setup
4. You will now assign IP addresses to the private interface on the VPN Router. You will also be assigning a management IP address to the VPN Router. At the CLI menu, you will select option number 1 (Interfaces).
5. You are now at the Interface Menu screen. Because you are configuring the Private LAN interface IP, you will select option number 0 and press Enter.
6. Notice that you are prompted now to enter the Management IP address. The Management IP address for this lab is **10.10.10.20**. Enter this IP address and then press Enter.
7. You are now prompted to enter the Interface IP address. The Interface IP address for this lab is **10.10.10.30**. Enter this IP address and then press Enter.

8. Enter the subnet mask of **255.255.255.0**.
9. Select the default Speed/Duplex of Auto Negotiate.
10. Verify your entries and then select R to return to the main menu.
11. Select E to save your changes and to exit the main menu.
12. Assign the static IP of **10.10.10.10** to your PC.
13. Connect your PC to the LAN interface on the VPN Router with a crossover cable.
14. Ping the interface IP address. If you get a response, then you know that the interface has been configured correctly.
15. Ping the management IP address. If you get a response, then you know that the management IP has been configured and is working.
16. Open your Web browser and enter the management IP into the address field of the browser. If you connect to the VPN Router and see the Welcome screen of the VPN Router, you know that you have successfully completed this lab. Figure 11-2 shows an example of the VPN Router welcome screen.

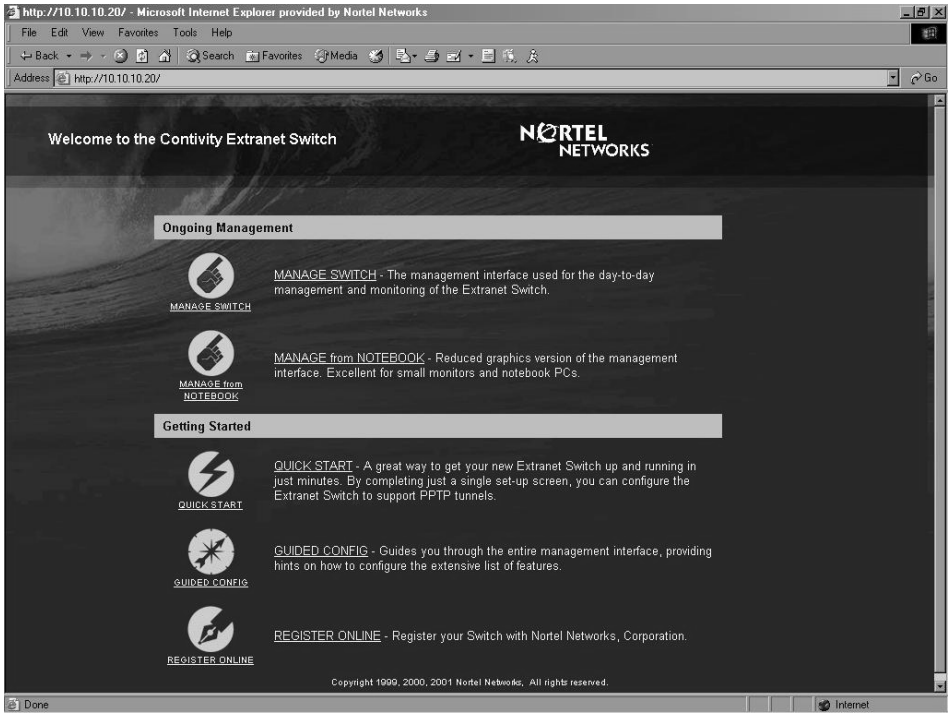


Figure 11-2: The VPN Router Internet Browser Welcome screen

Lab Summary

Much like many of the configuration options on the VPN Router, this lab shows how easy the VPN Router is to configure. Although this lab covered one of the most basic exercises, it is an important exercise to learn and to know. You will need to be able to follow the steps in this lab to connect to the Web browser interface for the configuration of the VPN Router, as well as to be able to use the tools that are available to you for troubleshooting and VPN Router management.

Enabling and Using VPN Client Logging

Troubleshooting VPN Client issues can be a cumbersome activity at times. The Nortel VPN Client software contains a few tools that can assist in determining the cause of VPN Client issues. This lab discusses how to enable VPN Client logging and how to access these logs for review.

Lab Requirements

- Windows-based PC with the Nortel VPN Client installed
- Pencil and paper for notes

Lab Setup

1. Start your VPN Client.
2. Look at the top of the VPN Client window, and select Options.
3. From the drop-down menu, select Log Session to File.

NOTE **If you ever need to disable logging on the client PC, then repeat the preceding process.**

4. Next you will test logging. Create a connection within the VPN Client. It does not have to be a valid connection because you only want to force a log activity. Try to connect and wait for the VPN Client to time out. You will receive a window stating that the remote host is not responding. Select OK to close this error window.
5. Locate the directory that you have loaded the VPN Client into. Within this directory, you will find a directory called `Log`. Open this directory

and locate a file that is named for the client connection that you created. This is the event log that was generated for the error that you received.

6. Open the file. Verify that you are able to see an error notifying you that the remote host is not responding. If you are able to see this, then you know that your client logging has been configured and enabled.

Lab Summary

You can see how easy it is to turn on logging within the VPN Client. Take some time to familiarize yourself with the VPN Client logging tool. Continue using logging and refer to the event log regularly. Use the log when you create a user tunnel and break the user tunnel connection. Refer to the log to see what information it contains. When used in conjunction with the Nortel VPN Router event logging, client logging may provide a lot of assistance in troubleshooting user tunnel connection issues.

Configuring Groups

Configuring groups is a good way to organize the users of your VPN Router. Users will inherit any permission that is assigned to the group. There are multiple options in configuring groups, so in this lab, you learn the basics of how to configure a group on the VPN Router.

Lab Requirements

- VPN Router
- Windows-based PC with Internet Explorer and the Nortel VPN Client
- Pencil and paper for notes
- Crossover cable
- Lab diagram (see Figure 11-3)

Lab Setup

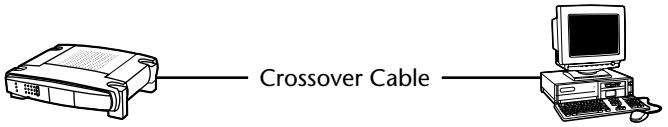
1. Connect to the management IP of your VPN Router via your Internet browser.
2. On the main Welcome page of the VPN Router, select Manage Switch.
3. Provide the login credentials for managing the VPN Router.

4. From the main menu, select PROFILES → GROUPS.
5. Select Add.
6. Enter the Group name of **Sales**. The parent group will be /Base. Select OK.
7. Congratulations, you have configured your new VPN Router group. Now, click the Edit button next to the group that you just created (/Base/Sales), as shown in Figure 11-4.
8. Review the group configuration screen. Click on Configure within each category and familiarize yourself with some of the options.
9. Click Close.

Lab Summary

In this lab, you configured a VPN Router group. You reviewed the options available to you. We highly recommend that you take a good look at all of these options so you know what options are available to you to assign to your user groups.

Consider reasons why you would want to assign remote users to different groups. What benefits can come from using multiple groups within the VPN Router?



VPN Router:
Private Interface IP:
10.10.10.30
Management IP:
10.10.10.20

Client PC IP:
10.10.10.10

Figure 11-3: The Configuring Groups lab diagram



Figure 11-4: Editing the group

Configuring Users

To log on to the LAN from a remote location through a user tunnel, remote users must be configured on the VPN Router for authentication and authorization purposes. In this lab, you will perform the steps necessary to configure a user's access to your LAN through a user tunnel.

NOTE **The remote user must have a supported version of the VPN Client installed on a PC.**

Lab Requirements

- VPN Router
- Windows-based PC with Internet Explorer and the Nortel VPN Client
- Pencil and paper for notes
- Crossover cable
- Lab diagram (see Figure 11-5)

Lab Setup

1. Connect to the management IP of your VPN Router via your Internet browser.
2. On the main Welcome page of the VPN Router, select Manage Switch.
3. Provide the login credentials for managing the VPN Router.
4. From the main menu, select PROFILES → USERS.
5. You are now at the User Management screen (see Figure 11-6).

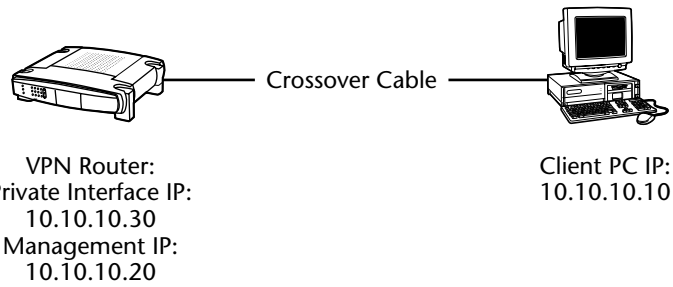


Figure 11-5: The Configuring Users lab diagram

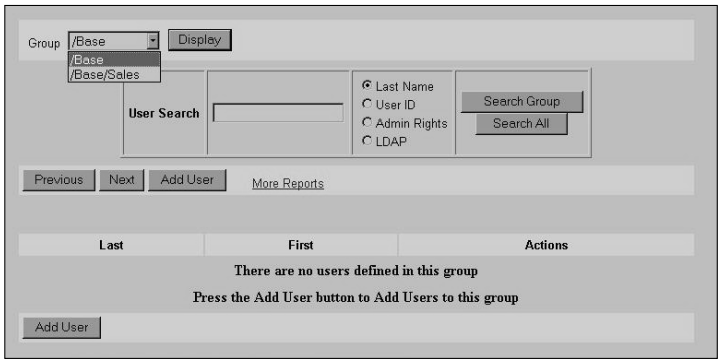


Figure 11-6: The User Management screen

6. Select the Add User button on the bottom of the User Management screen.
7. In the Name field, enter **Jamie** for a first name.
8. In the Name field, enter **Turbyne** for a last name.
9. Select the group name that you configured in the previous lab exercise (/Base/Sales).
10. Enter the IPSec credentials that you would like for this individual. For simplicity, choose the following:
    - *User ID:* User
    - *Password:* password
11. Review the remainder of this page for additional options that can be assigned to this individual.
12. Click OK at the bottom of the page.
13. Verify that the user has been added (see Figure 11-7). You can see that there is a message at the top of the page that informs you that the user has been added. You can also see the user listed in the group list at the bottom of the page.

Lab Summary

Congratulations. You have learned the basics for adding a user to the VPN Router. By performing this, you are well on your way to enabling users to access your LAN via your VPN Router. The group configuration provided several options that can be applied; the same holds true when configuring and assigning users to these groups. There are a lot of options for the users as well. Take some time to learn what these options are to see if they apply to your LAN.

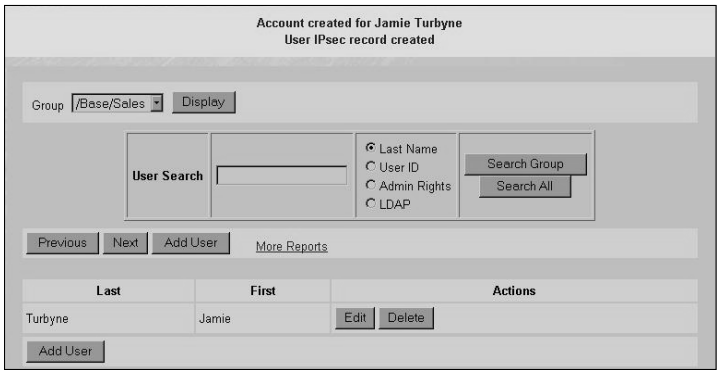


Figure 11-7: Verifying that the user has been added

Configuring Client Failover

VPN Client failover provides continued VPN connectivity to a LAN, should the primary link fail. This lab provides the steps necessary to configure and apply VPN Client failover. Once you have completed this lab, you will know how to configure this very important service.

Lab Requirements

- Two VPN Routers
- Windows-based PC with the Nortel VPN Client installed
- Pencil and paper for notes
- Network cables
- Network hub
- Lab diagram (see Figure 11-8)

Lab Setup

1. Connect to the management IP of your VPN Router via your Internet browser.
2. On the main Welcome page of the VPN Router, select Manage Switch.
3. Provide the login credentials for managing the VPN Router.
4. From the main menu, select SERVICES → IPSEC.
5. Scroll down the page to the section that contains the header "Fail-Over" (see Figure 11-9).

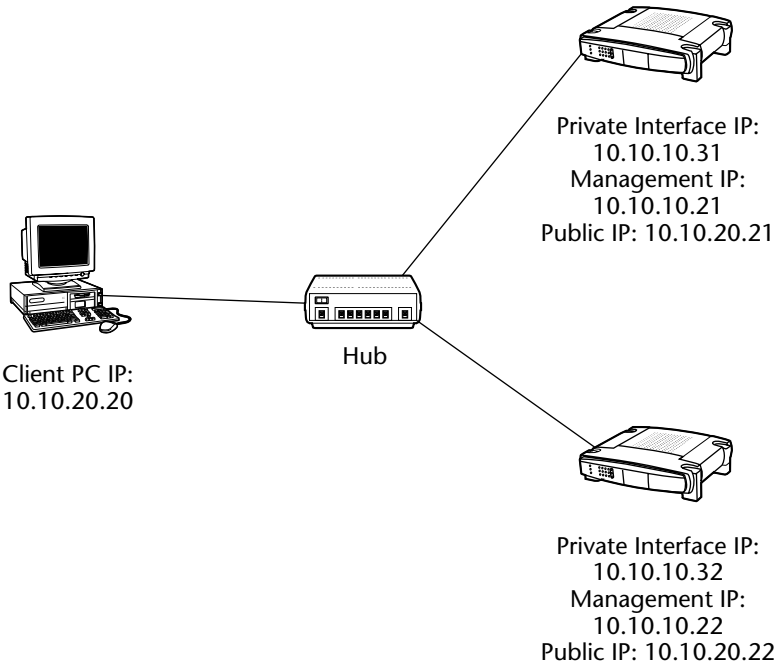


Figure 11-8: Client Failover lab diagram

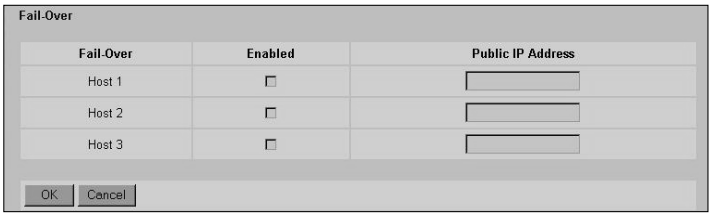


Figure 11-9: The "Fail-Over" section of the IPSec configuration window

6. Select Enabled in the Host 1 field and enter the public IP address of the first VPN Router. This IP address is **10.10.20.21.**
7. Select Enabled in the Host 2 field and enter the public IP address of the second VPN Router. This IP address is **10.10.20.22**.
8. Click OK.
9. From the main menu, select PROFILES → GROUPS.
10. Select the group that the user that you are setting up failover for is assigned to. In this lab, the group will be /Base/Sales. Select Edit.
11. Scroll down the page to the IPSec section and click Configure.
12. Scroll down the page to "Client Failover Tuning" (see Figure 11-10). Click Configure.



Figure 11-10: Client Failover Tuning

13. Click OK at the bottom of the page.
14. Repeat these steps for the second VPN Router.

Lab Summary

This completes the lab on configuring VPN Client failover. To test this configuration, you will establish a user tunnel to the public IP address for VPN Router number 1. The Router will share the failover configuration with the VPN client PC. Break the connection to the WAN port to VPN Router number 1, and then verify that you are directed to the public interface on VPN Router number 2.

Configuring IPSec Mobility

The Nortel VPN Router IPSec Mobility solution allows VPN clients the ability to roam from access point to access point, while maintaining the integrity of the tunneled connection. The Nortel solution ensures that TCP application communication remains intact, and it also ensures that UDP applications experience very little (if any) disruption. This lab provides the steps required to implement IPSec Mobility.

Lab Requirements

- VPN Router with private interface IP address and management IP address.
- Windows-based PC with Internet Explorer
- Pencil and paper for notes
- An Advanced Routing License Key

NOTE **If you do not have an Advanced Routing License Key, you can purchase one through Nortel. It is not recommended that you purchase one unless your company has a need for one. If you do not have this key, then you will not be able to participate in this lab.**

Lab Setup

1. Connect to the management IP of your VPN Router via your Internet browser.
2. On the main Welcome page of the VPN Router, select Manage Switch.
3. Provide the login credentials for managing the VPN Router.
4. Install the Advanced Routing License Key. Go to ADMIN → INSTALL KEYS.
5. Enter the Advanced Routing Key (see Figure 11-11).
6. Verify that the Advanced Routing Key is installed (see Figure 11-12), and then click OK.
7. From the main menu, select PROFILES → GROUPS.
8. Select the group that you will be configuring IPSec Mobility for, and click Edit.
9. Scroll down to the IPSec section and click Configure.
10. Scroll down the page to "Mobility Support." Click Configure.
11. The page will refresh. Scroll back down the page to "Mobility Support" and select Enabled (see Figure 11-13).
12. Click OK at the bottom of the page.

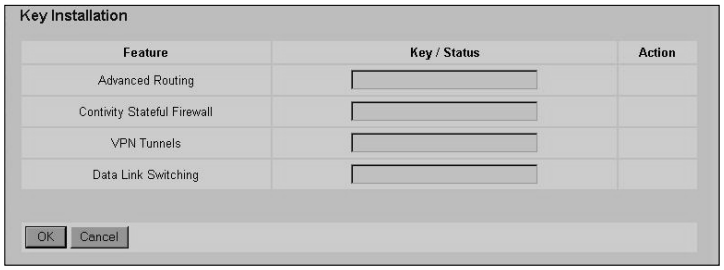


Figure 11-11: The Key Installation screen

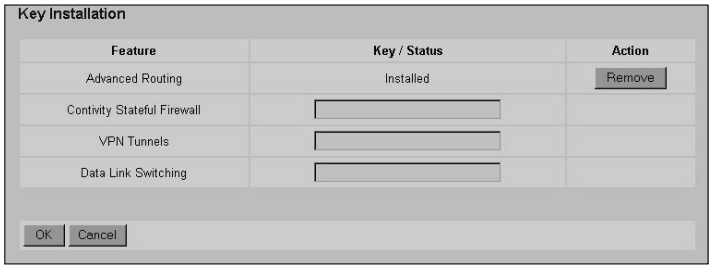


Figure 11-12: The Key Installation screen with key installed verification



Figure 11-13: Selecting Enabled for "Mobility Support"

Lab Summary

IPSec Mobility can greatly improve consistent connectivity through a user tunnel from remote users. Consider the implementation of IPSec Mobility within a LAN. What are the advantages and disadvantages of doing this? What would be an example of a scenario in which you would want to implement IPSec Mobility?

Configuring Automatic Backups

Automatic Backups can be implemented to help ensure that your system files are backed up to a file server at regularly scheduled intervals. It is recommended that you implement this as soon as you get your VPN Router. Automatic backups can assist greatly in system recovery and system management. This lab provides the steps taken to configure and implement automatic backups.

Lab Requirements

- VPN Router with private interface IP address and management IP address
- Windows-based PC with Internet Explorer
- Pencil and paper for notes
- Console cable
- Crossover cable

Lab Setup

1. Connect to the management IP of your VPN Router via your Internet browser.
2. On the main Welcome page of the VPN Router, select Manage Switch.
3. Provide the login credentials for managing the VPN Router.

4. From the main menu, go to ADMIN → AUTO BACKUP (see Figure 11-14).
5. Click the Enabled button.
6. Enter the host name or IP address of the file server that will be storing the backups.
7. In the Path column, enter the directory where the files are to be stored.
8. Enter the specific time that you would like the backup to occur.
9. Enter the time period interval that you would like the backups to occur.

NOTE You have the option of specifying a specific time of day for your automatic backup, or can opt to have multiple backups spread apart by the time period you specify in Step 9.

10. Enter the user ID and the password that are required by the FTP server.

NOTE You can perform a backup to your enabled backup servers at any time by going to the ADMIN → AUTO BACKUP screen and clicking the Backup button (see Figure 11-15).

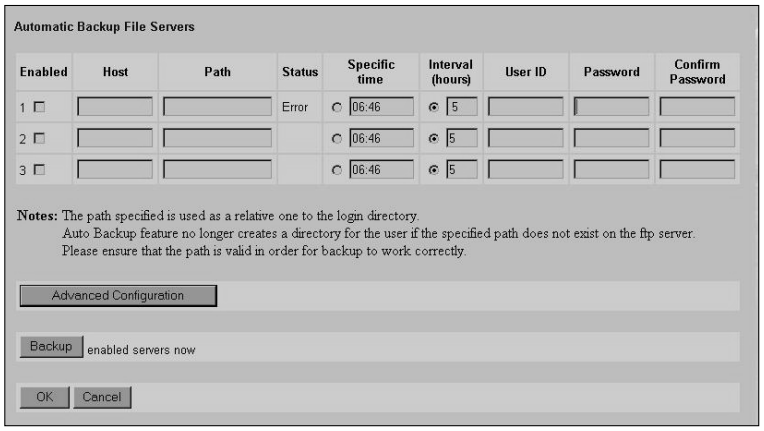


Figure 11-14: The Auto Backup configuration screen



Figure 11-15: Performing a backup to the enabled FTP backup servers

Lab Summary

Automatic backups are a very important tool that can be used to recover and monitor the VPN Router system. You can use the backed up files to monitor configuration changes and to recover from a catastrophic event. In addition to automatic backups, it is highly recommended that you perform a system backup prior to making any configuration changes or system code upgrades to the VPN Router.

Consider what might happen if you do not implement the automatic backup feature. What are the advantages? What are the disadvantages?

Configuring a Peer-to-Peer Branch Office Tunnel

A Branch Office Tunnel (BOT) within your VPN Router is one of the most common (and most important) features that you will be configuring, monitoring, and maintaining for the life of your VPN Router. This lab provides the steps to configure and implement the BOT.

Lab Requirements

- VPN Router: A
  - Mgmt IP: 10.10.10.15
  - Private IP: 10.10.10.11
  - Public IP: 192.168.1.1
- VPN Router: B
  - Mgmt IP: 10.20.20.25
  - Private IP: 10.20.20.21
  - Public IP: 192.168.1.2
- Windows-based PC with Internet Explorer (for configuration purposes)
- Lab PC—A: IP 10.10.10.10
- Lab PC—B: IP 10.20.20.20
- Pencil and paper for notes
- Console cable
- Ethernet cables
- Network diagram (see Figure 11-16)

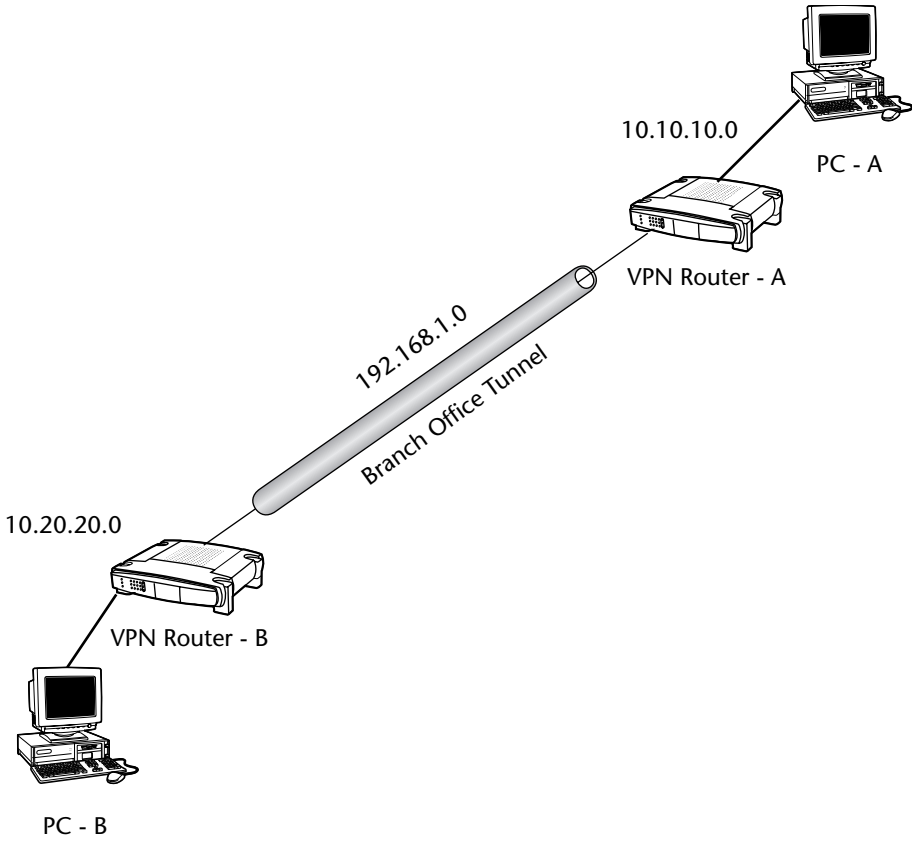


Figure 11-16: Branch Office Tunnel lab diagram

Lab Setup

1. Configure the IP addresses on both of the VPN Routers and both of the Lab PCs. Refer to the Lab requirements section of this lab for the IP addressing scheme.
2. Connect to the management IP of VPN Router A via your Internet browser.
3. On the main Welcome page of the VPN Router, select Manage Switch.
4. Provide the login credentials for managing the VPN Router.
5. From the main menu, go to PROFILES → BRANCH OFFICE.
6. Ensure that the /Base Group is selected.
7. Scroll down to the Connections section of the page and click Add.

8. Enter a name for the BOT connection. This is normally a name that will help you to identify the tunnel. For purposes of this lab, you can call it "VPN A to VPN B."
9. Leave all other fields at the default settings, and click OK.
10. On the Connection Configuration screen, check Enable in the Connection section (see Figure 11-17).
11. In the Endpoints section, select the public IP of the VPN Router A from the drop-down menu.
12. In the Endpoints section, enter the public IP of VPN Router B.
13. Leave the Filters section at the default value.
14. For authentication, select Text Pre-Shared Key. Enter a value of **labtest** for the Pre-Shared key. Confirm by re-entering **labtest**.
15. Leave the IP Configuration section at the value of Static.
16. In the Local Network section, click Create Local Network.
17. Create the Network "VPN Router A Local 10.10.10.X" and click Create.
18. Input the Network As IP address and the subnet mask. Click Add.
19. Click Close.
20. Click the link called Return to Connection Configuration, located in the right corner of the page. You are now redirected to the Connection Configuration screen.
21. Select the network you just created from the Local Networks section.
22. Scroll down to the Remote Networks section. Click Add and enter the remote network information.
23. Click OK.
24. The BOT has now been configured for the VPN Router A. Follow these steps on VPN Router B to complete this lab.
25. Once both VPN Routers have been configured, you can go to PROFILES → BRANCH OFFICE. Ensure that Select is chosen and then click Test (see Figure 11-18). Follow the prompts to complete the test.

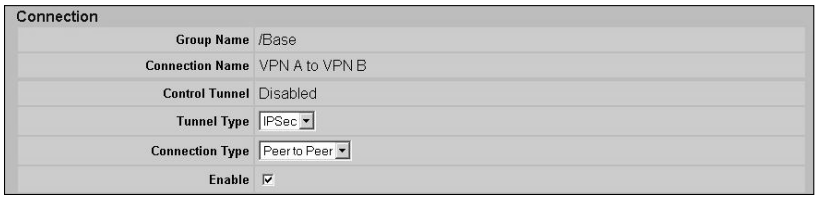


Figure 11-17: Enabling the BOT through the Connection Configuration screen

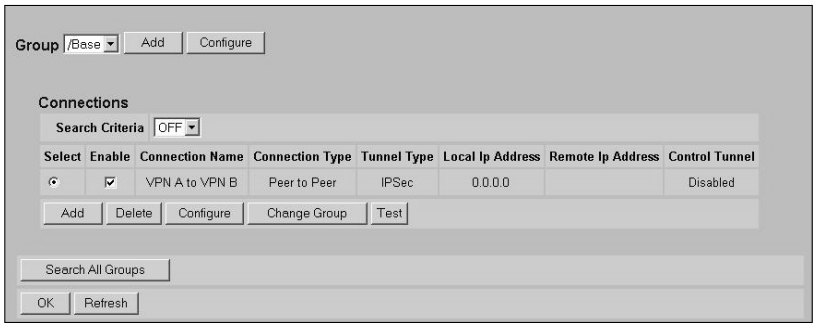


Figure 11-18: Testing the connection through the Connection Configuration section

Lab Summary

Now that you have the BOT configured on your VPN Router, you can test connectivity issues. Perform various tests that cause your tunnel to go down. Refer to the system logs to see what information is provided to you in determining why your connection has gone down.

Configuring RIP Routing

The Routing Information Protocol (RIP) is one of the most common routing protocols in use in LANs today. Knowing how to implement it within the VPN Router is a must for anyone that is managing the Nortel VPN Router. This lab provides the steps required to configure and implement RIP on the VPN Router.

Lab Requirements

- VPN Router
- Windows-based PC with Internet Explorer
- Pencil and paper for notes
- Console cable
- Crossover cable

Lab Setup

1. Connect to the management IP of your VPN Router via your Internet browser.
2. On the main welcome page of the VPN Router, select Manage Switch.

3. Provide the login credentials for managing the VPN Router.
4. From the main menu, go to ROUTING → RIP.
5. Check Enabled. Leave the Update Timer at the default value (see Figure 11-19).
6. RIP is now enabled globally for the VPN Router. To verify and configure the RIP settings at the interface level, you will need to go to ROUTING → INTERFACES.
7. Verify that RIP is enabled on the interfaces that you would like it enabled on (see Figure 11-20).
8. Click Configure.
9. Verify the RIP configuration interface parameters. Adjust them to meet the needs of your LAN.
10. Click OK when you are finished.

Lab Summary

This concludes the lab on establishing and enabling RIP within your VPN Router. There are several optional configuration parameters, and these can be implemented to suit your LAN topology configuration. Take time to get to know and understand these parameters.

For additional testing, set up your VPN Router in a lab with another layer 3 device. Add some PCs and test your optional parameters. See if you are able to run a RIP environment successfully.

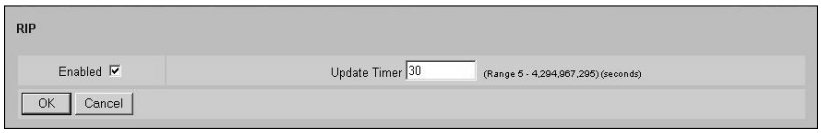


Figure 11-19: Enabling RIP

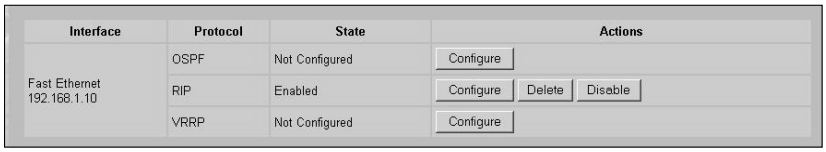


Figure 11-20: Enabling RIP on the interface

Configuring Network Time Protocol

Network Time Protocol (NTP) is essential in maintaining the proper time on the Nortel VPN Router. Each event is logged with an associated time. The correct time is critical for good maintenance and aids in troubleshooting when more than one unit is involved.

An example would be the creation of a BOT between two Nortel VPN Routers. If the tunnel is not being established, then the easiest way to try to determine the reason is the comparison of event logs on both units. Because the log is sequenced using time increments, it may not be overly obvious that you are looking at the same event on both routers if the clock is skewed between them. It is highly recommended that all units in a network that includes the extended intranetwork formed with the use of tunneling be synchronized to a fixed time source.

Lab Requirements

The requirements listed are the minimum essential components required to configure the Nortel VPN Router to use NTP. If the Nortel VPN Router is already residing on a larger network segment, then the unit may be accessed and configured from any PC that is capable of routing to the Management port on the Nortel VPN Router. The following is required:

- Nortel VPN Router with private and management IP addresses preconfigured on the private interface, as well as an IP address preconfigured on the public interface
- The IP address of either a privately accessible NTP server or one that is accessible over the Internet
- Windows-based PC with Internet Explorer
- Routable access from either the private or public interfaces of the Nortel VPN Router
- Network diagram (see Figure 11-21)
- Pencil and paper for notes

Lab Setup

1. Verify that the lab configuration meets the example setup shown in Figure 11-21.
2. At the Windows PC, launch Internet Explorer and HTTP to the management IP address of the Nortel VPN Router.

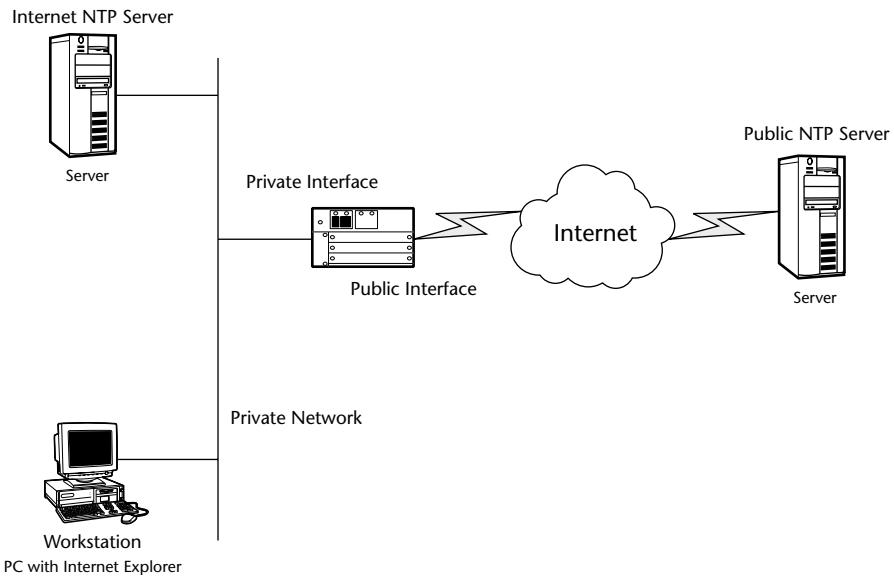


Figure 11-21: The NTP lab diagram

3. Log in with an administrator user ID and password.
4. At the Nortel VPN Router Management screen, select SYSTEM → DATE & TIME to display the Date and Time configuration screen.
5. If NTP has not previously been configured on this unit, the screen will display Date and Time boxes that can be manually configured to set the time and date on the Nortel VPN Router.
6. Click the Configure Network Time Protocol link to display the Network Time Protocol configuration screen (see Figure 11-22).
7. In the Servers area of the screen, click the Add button to display the Add/Edit Server configuration screen.
8. In the Server IP Address field, enter the IP address of the NTP Server that is to be used for the time standard.
9. In the Interface field, click the radio button adjacent to either Private or Public to specify which interface is to be used to access the server.

NOTE **If the Public interface is selected, then a list of public interfaces is used to select the interface being used to route to the NTP Server interface. However, if the Nortel VPN Router's stateful firewall has been enabled, then an interface filter must be added to allow NTP traffic.**

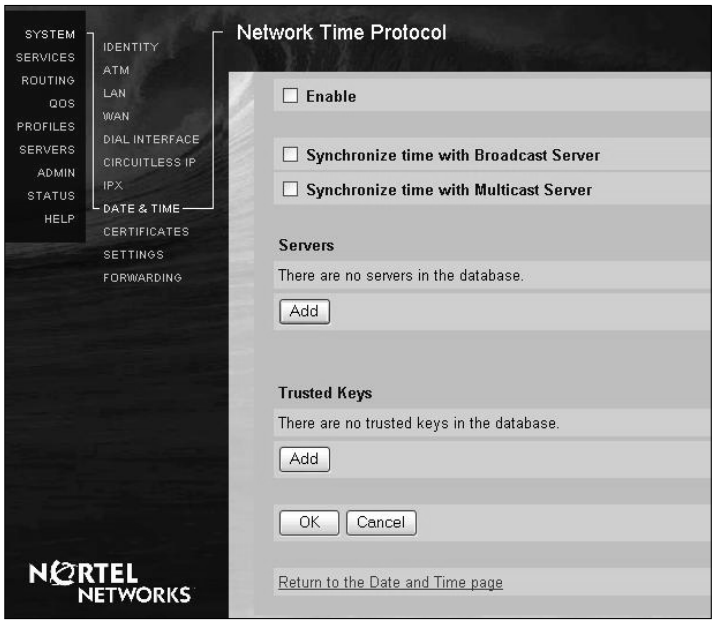


Figure 11-22: The NTP configuration screen

10. The Key ID, Bursting, and Version fields are dependent upon the NTP server that is being used. A brief description of each follows:
    - *Key ID:* Default is set to None. This field is used if Message Digest 5 (MD5) authentication is being used between the NTP Server and the VPN Router.
    - *Bursting:* Default is set to Disable. The selection of Enable specifies to send a burst of eight packets at each poll interval.
    - *Version:* Default is set to Default. This allows for the selection of NTP version numbers 1 through 4 to be selected. The default is set to version 3.
11. When all the appropriate settings for the NTP server have been selected, click OK. The Network Time Protocol configuration screen, where the server was just configured, appears in the Servers area of the screen.
12. Check the Enable check box to enable NTP.
13. Click either of the following check boxes depending on the type of NTP server that is being used:
    - Synchronize time with Broadcast Server
    - Synchronize time with Multicast Server

14. Click OK at the bottom of the screen to accept these settings and then click the Return to the Date and Time page link to return to the Date and Time configuration screen.
15. Notice that the Date and Time fields are no longer able to be edited. Use the Time Zone drop-down menu to select the appropriate local time zone for the Nortel VPN Router.

NOTE Although the time on the unit will be the local time where it is located, on very large intranets that traverse many time zones, a consideration may be to set all the units to one zone such as Greenwich Mean Time (GMT). Selecting one time zone for all units would facilitate troubleshooting where log comparisons may need to be made, and would eliminate the need to interpolate times for varying time zones, or, in the case of units traversing the International Date Line, the need to interpolate both time and date.

16. Click OK to accept all the NTP settings to enable the Nortel VPN Router to use an NTP server to set and control its internal clock.
17. To verify that NTP has indeed been enabled and configured properly, select STATUS → EVENT LOG to display the event log screen.
18. Use the Edit → Find (on this Page) option of Internet Explorer to search on NTP. If none has been found, click the Refresh button on the Event Log screen.
19. When the event log lines with the NTP status are found, verify that error messages are not being displayed. Time set, clock update, and clock synchronized messages are displayed if NTP has been configured properly.

Lab Summary

This lab demonstrates the necessity of proper time maintenance and the ease in which it may be configured on the Nortel VPN Router. It is essential to have prior knowledge of the NTP server that is to be used so that the router may be configured properly to synchronize its internal clock to that time standard. Also, a special consideration is necessary if the NTP server is located on the Public network and the Nortel VPN Router's stateful firewall has been enabled.

Once configured, NTP is maintenance-free. However, it is recommended to monitor STATUS → HEALTH CHECK to verify that Network Time Protocol has an OK status being displayed on that screen. If an alert condition is displayed, then action is required to diagnose the reason for the alert.

Configuring DHCP Server

The use of the Nortel VPN Router's DHCP Server functionality is beneficial to a smaller network installation where there is no centralized DHCP server on the network. If there is an existent DHCP server on the network, then DHCP server functionality on the Nortel VPN Router should be disabled, and DHCP Relay should be enabled to allow the router to forward DHCP requests to that DHCP server.

The usefulness of DHCP is beneficial in offices where the PCs are not static (for example, a salesperson with a laptop). When the salesperson is out of the office, a laptop may reside on other networks with the use of DHCP. When the salesperson returns to the office and connects the laptop back into the network, the salesperson will obtain an IP address, as well as other DHCP-provided information.

Lab Requirements

The minimum requirements that are needed to configure and test the DHCP Relay and DHCP server functionality of the Nortel VPN Router may be larger than that shown as the lab setup, but will not affect the performance of this lab. The following components are required:

- Nortel VPN Router with private and management IP addresses preconfigured on the physical private interface
- The IP address of a privately accessible DHCP server and DHCP Relay Agent (only required for the DHCP Relay portion of this Lab)
- Windows-based PC with Internet Explorer
- Network diagram (see Figure 11-23)
- Pencil and paper for notes

Lab Setup

If a DHCP server already exists on the network, it must reside on a network subnet different from the one the Nortel VPN Router is resident on. There must be a router or other device that is acting as the DHCP Relay agent for the subnet that the Nortel VPN Router is residing on. If this is the case, then perform only the DHCP Relay section of this lab.

If no DHCP server exists for the network subnet that the Nortel VPN Router is resident on, then perform the DHCP Server section of this lab.

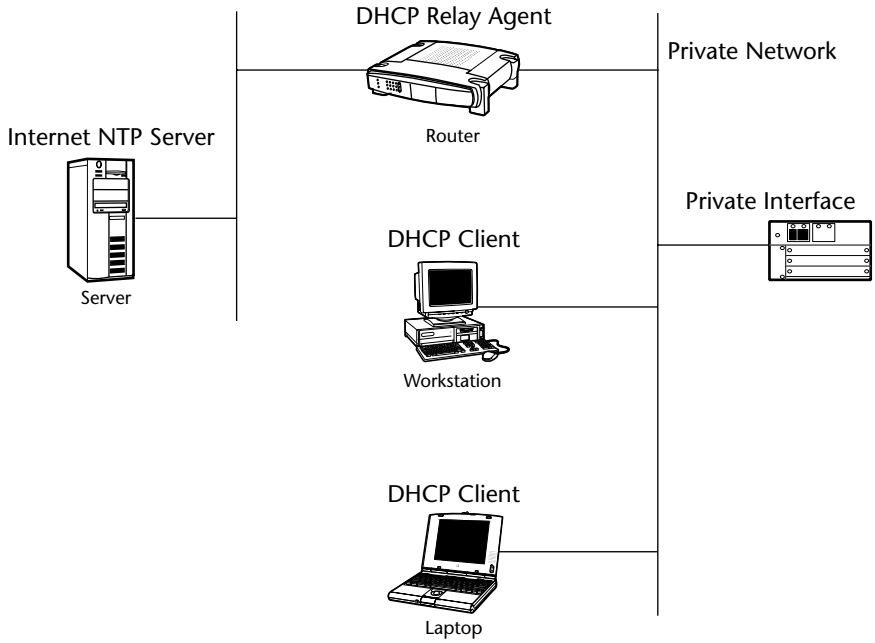


Figure 11-23: The DHCP lab diagram

DHCP Relay Lab

1. Verify that the lab configuration meets the example setup shown in Figure 11-23 for the DHCP Relay portion of the lab.
2. At the Windows PC, launch Internet Explorer and HTTP to the management IP address of the Nortel VPN Router.
3. Log in with an administrator user ID and password.
4. At the Nortel VPN Router Management screen, select SERVERS → DHCP RELAY to display the DHCP Relay screen (see Figure 11-24).
5. In the DHCP Relay Interfaces portion of the screen, click the Add button to display the DHCP Relay Interface configuration screen.
6. In the Add New DHCP Relay Interface section, use the drop-down menu to make a selection for the Physical Interface (private) from the adjacent drop-down menu. The Nortel VPN Router listens only to DHCP Requests on its Private physical interfaces and tunnels.
7. In the State drop-down menu, ensure that Enabled is selected.
8. In the DHCP Server Helper 1 dialog box, enter the IP address of the DHCP Relay Agent that is serving the subnet that the Nortel VPN Router is resident on.

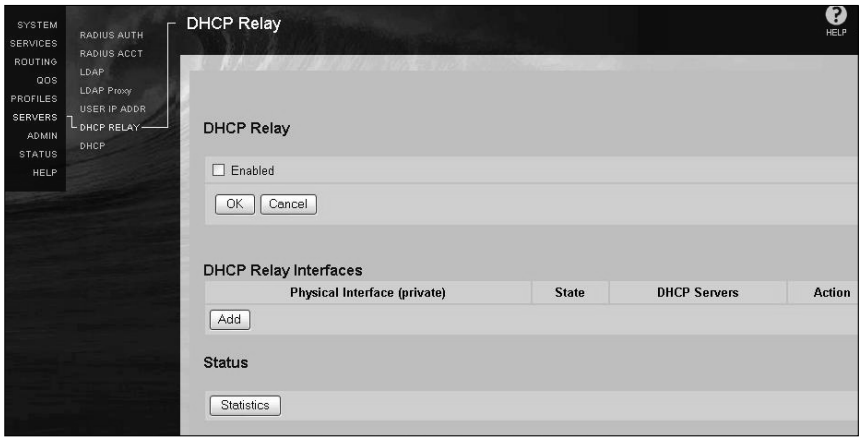


Figure 11-24: The DHCP Relay configuration screen

NOTE **The DHCP Relay Agent must have an interface that is connected to the same subnet as the Nortel VPN Routers Management Interface.**

9. If additional DHCP Relay Agents are available on the same subnet as the Nortel VPN Router is residing on, they also may be configured at this time. Up to three DHCP Relay Agents may be configured.
10. Click the Enabled check boxes for all configured DHCP Server Helper IP addresses and click OK.
11. When the DHCP Relay screen appears, verify that the configured DHCP Relay Interfaces are displayed.
12. In the DHCP Relay portion of the screen, click the Enabled check box and then click OK.
13. To verify that DHCP Relay is working properly, use a PC that is configured to use DHCP to obtain an IP address and connect it to the same subnet the Nortel VPN Router Management Interface is connected to.
14. If the PC is already powered on, perform a release and renew request from the PC using the command `ipconfig /release` and then issue an `ipconfig /renew` command. Did the PC receive an IP address? If not, verify your settings and repeat this step.
15. To aid in troubleshooting on the DHCP Relay screen, click the Statistics button to display the DHCP Relay Statistics. This screen displays the In, Out, Discarded, Relayed to Server, and Relayed to Client statistics. This can be used to determine if the Nortel VPN Router is detecting the DHCP request broadcast from the PC, and if it had been sent on to the DHCP Relay Agent. It will also display if there were any DHCP responses sent from the DHCP Relay Agent, and if those responses were passed to the

client. If further troubleshooting is required, a network packet sniffer may be required to trace where the requests and responses are being dropped.

16. This lab is completed successfully when the requesting PC is able to receive an IP address from the DHCP Relay Agent.

DHCP Server Lab

Verify that the lab configuration meets the requirements of the example network shown in Figure 11-23. For this lab only, the Nortel VPN Router and a DHCP client PC are required, along with a PC that is performing the configuration of the Nortel VPN Router.

1. At the Windows PC being used to configure the Nortel VPN Router, launch Internet Explorer and HTTP to the management IP address of the Nortel VPN Router.
2. Log in using an administrator user ID and password.
3. At the Nortel VPN Router Management screen, select SERVERS → DHCP.
4. On the DHCP Server configuration screen (see Figure 11-25), first add an IP pool to use for the distribution of IP addresses. Scroll down to the Pool area and click the Add button to display the Add Pool configuration screen. Enter the network IP address that is to be used for the pool and the subnet mask that defines this network segment. The number of addresses that must be specified is the number of anticipated user tunnels that are to be supported. Enter a name that matches the name assigned to the user group in the DHCP settings within the group profiles Address Pool Name. There are other options that may be configured, but, for the purposes of this lab, accept the default values.

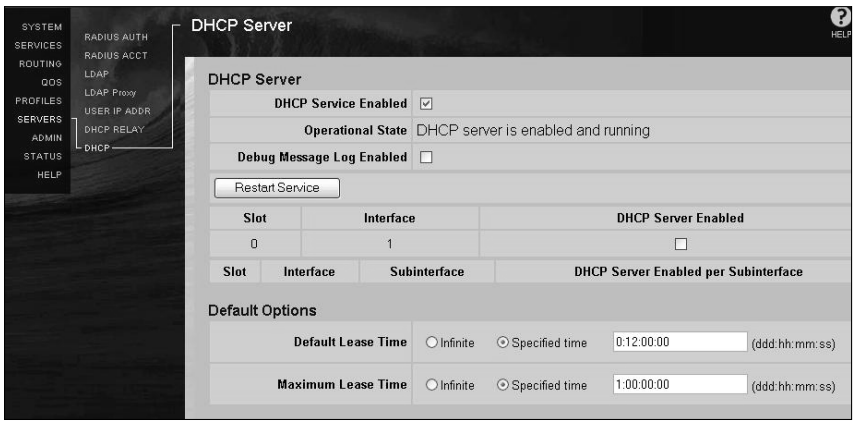


Figure 11-25: The DHCP Server configuration screen

5. Verify that, in the DHCP Server area of the DHCP configuration screen, the DHCP Service Enabled check box is selected, and select the Debug Message Log Enabled check box to allow the recording of DHCP events to be logged in the event log for troubleshooting purposes. If not selected, check the DHCP Server Enabled check box on the interface that will be running the DHCP service, and then click the Restart Service button to start the DHCP server to respond to DHCP requests on that interface.
6. To test that the DHCP server is configured properly to assign IP addresses to incoming clients, use a PC with the Nortel VPN Router to connect to with the client. Verify that, on connection, the client receives an IP address that is within the pool addresses assigned to the DHCP server. If needed, view the event log to aid in troubleshooting.
7. This lab is complete when the Nortel VPN Client receives an address from the DHCP Server running on the Nortel VPN Router.

Lab Summary

In this lab both the DHCP Relay and DHCP server features of the Nortel VPN Router were configured for use by the DHCP client on the private internal network, and by clients connecting to the Nortel VPN Router from over the Internet. The use of DHCP allows for the ease in management of clients, whether they reside on the local private network or at a remote site.

The DHCP server is flexible and highly configurable. For the purpose of this lab, only the distribution of IP addresses was discussed. However there are many configurable options that you may want to take advantage of, and you are encouraged to configure and test to become familiar with those options.

Configuring the Nortel 100 VPN Router

The Nortel VPN Router 100 has its own configuration tools and screens that are different from the other units within the Nortel VPN Router suite. This lab describes the process of basic configuration and tunneling of the unit, along with some insights into the available tools associated with it for configuration, maintenance, and troubleshooting of the unit.

Lab Requirements

- Nortel VPN Router 100
- A second Nortel VPN Router 100 or other VPN Router to perform the tunneling portion of the lab
- Nortel VPN Router 100 configuration software

- Windows-based PC
- Ethernet cables (patch and crossover)
- PC for testing of tunnel
- Network diagram (see Figure 11-26)
- Nortel 100 VPN Router documentation
- Pencil and paper for notes

Lab Setup

This lab is divided into two sections: basic configuration and configuration of tunnels. The Nortel VPN Router 100 is used in many installations in the small office environment for providing Internet access without the use of the tunneling functionality of the unit. The tunneling portion of the lab is used in environments where VPN capabilities are used to connect to a central office while still allowing users to connect to resources on the Internet.

Basic Configuration Lab

1. Install the Nortel VPN Router 100 administrative tools on the PCs that are to be used to configure the unit.
2. Power on the Nortel VPN Router 100 and observe the LEDs on the front panel.
3. If LED 2 glows amber, the unit is in a factory default condition. If the LED glows green, then the unit has been previously configured. For the purposes of this lab, an unconfigured unit is needed. If the unit is not part of an existing installation and restoring the factory defaults is not a problem, then this can be accomplished by using the DIP switches on the back of the unit. Power off the Nortel VPN Router 100. On the DIP switch, place switches 1, 2, 3, 5, 6, and 7 in the down position, while switches 4 and 8 remain in the up position. Power the unit on and observe the LEDs. The LEDs will cycle and, after a brief period of time, LEDs 1, 2, 3, 5, 6, and 7 will glow amber while LEDs 4 and 8 will remain off. The unit is now in a factory default condition. Power the Nortel 100 VPN Router off and place all the DIP switches in the up position.
4. Install the Nortel VPN Router 100 administrative utilities software on the PC that is to be used to configure the unit.
5. With the Nortel VPN Router 100 powered on, connect the PC with the administrative tools to the Ethernet interface on the front of the router. It appears as a seven-port hub. Any port may be used for this interface. Either a patch (straight through) or crossover Ethernet cable may be

used. The PC should be configured with an IP address that will be used on the network subnet that the Nortel 100 VPN Router is to reside on. For this lab, enter on the PC a static IP address of **10.0.0.254** with a subnet mask of **24** bits.

6. On the PC, launch the Setup application within the administrative tools. A window appears stating that an unconfigured unit has been found. Click OK. Select the unit and click OK to proceed with the installation.
7. A dialog window appears to add an IP address to the Eth1 interface. Enter the IP address **10.0.0.1** and click OK. A window appears requesting if a DHCP is to be run. For this lab, click No. A registration screen appears and, for this lab, just click the Register Later button.
8. A dialog box appears to assign a name and password on the unit. These may be modified as desired, or, to accept the default, just click OK. If no password was assigned, another dialog box will be displayed asking if the password is to be blank. Just click Yes to accept no password.
9. For the interface, select Eth2 and add the IP address and subnet mask to be used. For the purposes of this lab, enter the IP address **100.100.100.100** and subnet mask of **255.255.255.252**. Click OK.
10. A dialog window appears where the Router address of **100.100.100.101** may be entered. Click OK.
11. A dialog window appears to enter a DNS server. For the purposes of this lab, click Cancel.
12. A dialog window appears. Click Accept settings.
13. This completes the basic configuration. To test the setup, use a crossover Ethernet cable from the Eth2 interface to the other PC used in this lab setup. Assign an IP address of the Router address of **100.100.100.101** with a subnet mask of **255.255.255.252**.
14. From the PC used to configure the Nortel VPN Router 100, open a command window and ping the 100.100.100.101 IP address. If there is a response, then the lab is completed. If no ping response was received then verify all settings and test once again.
15. If further troubleshooting is required, ping 100.100.100.100 from the PC connected to the Eth2 interface. If a response is received, then the PC and the Eth2 interface are able to communicate. If no response is received, verify cabling and setup of the PC IP configuration. If a ping is received from the PC connected to the Eth2 interface and you are still unable to ping it from the PC connected to the Eth1 interface, Telnet to the Nortel VPN Router by using the DOS command Telnet `10.0.0.1`. At the ping prompt enter **100.100.100.1**. If a response ID is received, then the Nortel VPN Router is able to ping the PC, so the issue is that NAT is not configured on the Eth2 interface. Verify that NAT is enabled on the Eth2 interface. Ping should now be able to perform requests and receive responses.

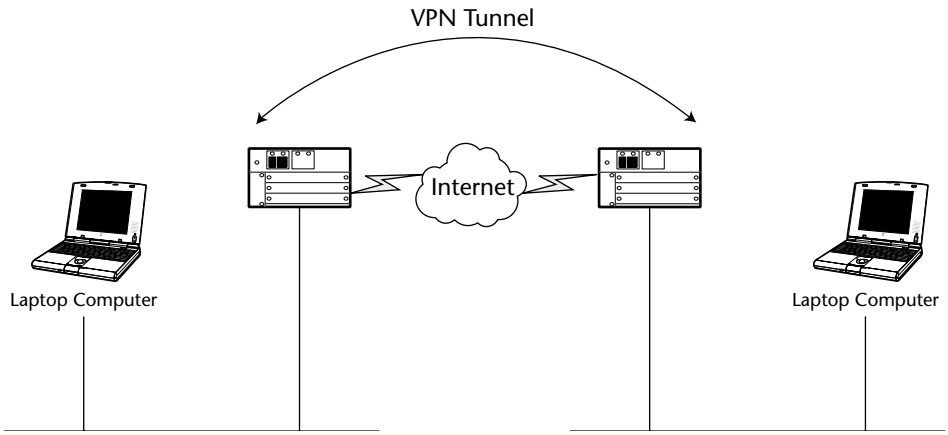


Figure 11-26: The VPN 100 Configuration lab diagram

Tunneling Lab

The Nortel VPN Router 100 is capable of creating and maintaining IPSec BOTs between itself and another Nortel VPN Router 100 or other member of the Nortel VPN Router family. It is capable of establishing peer-to-peer (main mode), Initiator/Responder (ABOT), and client mode tunnels. This lab is broad-based and is dependent on the device being used to terminate the remote end of the tunnel.

To configure BOT on the Nortel VPN Router 100, on the PC used to configure the unit, launch the setup program once again. On the Interfaces configuration screen, click the Add button to bring up the Connection Type screen. Click the IPSec button to bring up the Connection Device selection screen. Following are the three buttons that may be selected:

- *Contivity:* The selection for creating a BOT to another model within the Nortel VPN Router family
- *Instant Internet:* The selection for creating a BOT to another Nortel VPN Router 100
- *Other:* The selection for creating a BOT to an IPSec-compatible device that is capable of supporting IPSec tunneling protocols

Tunneling to Another Nortel VPN Router 100

1. Click the Instant Internet button to display the Type of Connections selection screen with the following options:
   - *Responder:* For tunnels initiated from the remote endpoint only.
   - *Initiator:* For tunnels being initiated by the unit to another Nortel VPN Router 100 configured as a responder.

- *Peer-to-Peer:* For BOTs that are main mode tunnels that may be initiated from either endpoint. The requirement is that both endpoints must have static IP addresses.

2. Click the Responder button to display its IPSec Configuration screen.
   a. Enter the name to be given the tunnel in the Name entry box.

NOTE The name must be the same on both devices that the tunnel is to be established between.

   b. In the Key entry box, enter the pre-shared secret that will be used by both units that the tunnel is being established between.
   c. In the Local Addresses box, the default displayed is 0.0.0.0/0, which indicates mandatory tunneling. This means that all traffic on the remote end that is not intended for that local network will be routed up the tunnel to the private network on the remote end. If this is not to be the case and split tunneling is enabled, then select this subnet and click the Remove button. To add the subnets that the remote traffic is allowed to be routed to, click the Add button to display the Enter IP Address dialog box. Enter a subnet address and the number of bits that are used to define the subnet, and click OK. This process may be repeated as many times as needed to define all the local subnets that the remote users on the other private network will be permitted to access. For the purposes of this lab, enter the network address **10.0.0.0** and **24** bits.
   d. Click OK to accept all the Responder Tunnel settings. The tunnel will now be displayed in the Interfaces by assigned tunnel name.
   e. Click Save and Exit. The Nortel VPN Router 100 will reboot with the new configuration.
3. On the Remote Nortel VPN Router being used to terminate that end of the tunnel, the device must be configured as an Initiator. Select Interfaces Add → Connection Type IPsec → Connection Device Instant Internet. At the Type of Connections screen, click the Initiator button to display its IPSec configuration screen.
4. Enter the tunnel name exactly as it was entered on the Responder Nortel VPN Router 100 unit.
5. Enter the same preshared secret that is being used for the Key.
6. Enter the Destination address. This is the publicly routable IP address that has been assigned to the interface on the Responder unit being used to connect to the Internet. In this lab, enter the IP address of **100.100.100.100**.

7. Notice in the Local Addresses box that the subnet that the Initiator Nortel VPN Router 100 is connected to is displayed by default. If other subnets are to participate in the tunnel, they may be added by clicking the Add button and then on the Enter IP Address screen.
8. In the Remote Addresses click the Add button to enter the remote networks that the local users may access through the tunnel. For the example of this lab, enter the remote accessible network of **10.0.0.0/0** with **24** bits. Click OK.
9. Click OK on the IPSec configuration screen to display the Interfaces screen. The created tunnel will appear in the Interfaces box by its assigned name.
10. Click the Save and Exit button to save the configuration. The Nortel VPN Router 100 will reboot with the new configuration.
11. To test the tunnel configuration, start a continuous ping to the PC that is behind the Nortel VPN Router 100 that is the Responder. The first initial responses will ping timeouts, but when the tunnel is established, ping replies should be displayed.
12. If the tunnel does not establish, verify configurations on both the Responder and Initiator Nortel VPN Router 100 units. If the tunnel still will not establish, then further troubleshooting steps will be required. An IPSec log can be run on both devices by using Telnet to start a command-line session. As an example, on the Responder side, if that PC issues a `telnet 10.0.0.1` command, and then, at the command line issued a command `ipsec`, the current state of all IPSec tunnels would be displayed. To capture a log of the IPSec tunnel negotiation between two units, enter the command **ipsec log 9** to start logging the IPSec sessions as they are being established or torn down. To view the log, enter a Telnet command **cat ipsec.log** to page out the results of the captured tunnel negotiation. The IPSec log may also be viewed from the Windows-based configuration program. To view the log, select the View drop-down menu and select Ipsec Log.

Although this lab setup was for a Responder/Initiator BOT, the steps are similar for those of a Peer-to-Peer tunnel configuration. In the Peer-to-Peer Branch Tunnel configuration, both endpoint public addresses must be known. This will require that the devices be assigned static IP addresses for the Nortel VPN Router 100 Internet IP address. Responder/Initiator BOTs are useful where the ISP is unable to provide a static Internet IP address.

If you want to try a Peer-to-Peer branch office lab setup, use the already assigned public interface IP address of **100.100.100.100** for one endpoint address and **100.100.100.101** for the other endpoint address.

Tunneling to a Nortel VPN Router

Tunneling from the Nortel VPN Router 100 to another member of the Nortel VPN Router family is the same for every model, excluding the Nortel VPN Router 100, 221, and 251 models. This portion of the lab will deal with models within the 600, 10XX, 2XXX, 4XXX, and 5000 ranges. The configuration is the same for each of these models.

1. On the PC used to configure the Nortel VPN Router 100, launch the Windows-based setup program and navigate to the Setup screen with Interfaces being displayed.
2. Click the Add button to add another interface.
3. At the Select Connection Type screen, click the IPsec button.
4. At the Select Connection Device screen, click the Contivity button.

   Following are the button selections presented:

   - *Branch-Peer to Peer:* This selection is for a main mode tunnel where the public interface IP address is statically assigned.
   - *Branch-Initiator:* This selection is for an aggressive mode tunnel where the remote end of the branch office has a statically assigned public interface IP address, and the Nortel VPN Router 100 public interface IP address is dynamically assigned.
   - *Client:* This selection is for an aggressive mode tunnel where the remote end of the tunnel has a statically assigned public interface IP address, and the Nortel VPN Router 100 public IP address is dynamically assigned. This tunnel differs from the Branch selections in that it is a client mode tunnel, and user sessions can be established only from the client end of the tunnel. In the Branch selections, peers on either end of the tunnel may establish sessions with each other. However, in the Client selection, the Nortel VPN Router 100 end of the tunnel is assigned an address, or has one statically assigned that is used to NAT all sessions through from the Nortel VPN Router 100 end of the tunnel. Users on the Nortel VPN Router end of the tunnel are unable to establish sessions with users on the Nortel VPN Router 100 end of the tunnel.
5. Click the Branch-Peer to Peer button to display the IPsec Configuration screen.
6. By default, the Name dialog box has "vpn" within it. This may be changed to whatever name you choose for the tunnel.

NOTE This name must be identical on both the Nortel VPN Router 100 and the Nortel VPN Router being used to establish the tunnel. Enter a name for this tunnel in the dialog box referred to in Step 6.

7. In the Key dialog box, enter a preshared key that is to be used on both ends of the tunnel.
8. Because this is a peer-to-peer BOT, both ends of the tunnel have statically assigned public interface IP addresses. For the Destination address, enter **100.100.100.101**.
9. Local Addresses by default will display the subnet assigned to Eth1, which is 10.0.0.0/24. Click the Add button to add any additional subnets on the Nortel VPN Router 100 side that are to participate in the tunnel. Remember that, in a peer-to-peer BOT, you must have the local- and remote-accessible networks mirroring themselves. In other words, the local subnets on one unit must match the remote subnets on the other.
10. The Remote Addresses are the accessible networks that are on the private network of the other Nortel VPN Router. If this is to be a mandatory tunneling situation, then the remote address should be specified at 0.0.0.0/0, which means that all non-local traffic is to be sent up the tunnel. For the purpose of this lab, enter **10.10.0.0/24** for the remote accessible network. Click the Add button for Remote Addresses. For Address, add **10.10.0.0** and for bits enter **24**, and then click OK to return to the IPsec Configuration screen.
11. On the IPsec Configuration screen, click OK to return to the Interfaces configuration screen. The tunnel that was just created will be listed in the list of available interfaces. Click the Save and Exit button to save and reboot the Nortel VPN Router 100 with the new settings. This concludes the configuration of the Nortel VPN Router 100 and its end of the peer-to-peer BOT.

This portion of this lab will deal with the configuration of the Nortel VPN Router that is being used to terminate the remote end of the peer-to-peer BOT. For this lab, the Nortel VPN Router will be previously configured with a Public Interface IP address of 100.100.100.101 with a 255.255.255.252 subnet mask. The Private Interface IP address will be set to 10.10.0.1 with a 255.255.255.0 subnet mask. The Nortel VPN Router Management Interface IP address will be set to 10.10.0.2. If the Nortel VPN Router remains to be configured with its initial IP, refer to other portions of this chapter dealing with the initial configuration of the Nortel VPN Router.

1. With the PC that is located on the Nortel VPN Router private network, launch a browser and enter the Management IP address of **10.10.0.2**. Log in using the administrator user ID and password that are, by default, admin for the user ID and setup for the password.
2. Select PROFILES → BRANCH OFFICE to display the Branch Office configuration screen.

3. The Group setting by default is /Base. For the purposes of this lab, keep that setting. However, if you want to add a new group for this tunnel, then clicking the Add displays a group configuration screen where the parameters of the new group may be selected.
4. In the Connections section of the Branch Office configuration screen, click the Add button to display the Add Connection screen.
5. Add the Connection Name just as it was entered on the Nortel VPN Router 100 to name this tunnel. The Group Name that is displayed should be /Base, Control Tunnel should be Disabled, Tunnel Type should be IPSec, and Connection Type should be Peer to Peer.
6. Click OK to accept these settings and return to the Connection Configuration screen.
7. In the Connection area of the Connection Configuration screen, click the Enable check box.
8. In the endpoints area of the Connection Configuration screen, add the Local IPAddress of **100.100.100.101** and the Remote Ip Address of **100.100.100.100**.
9. In the Filters area of the Connection Configuration screen, ensure that the Filter is set to permit all. If not, click the down arrow to open the drop-down menu and select the permit all filter.
10. In the Authentication area of the Connection Configurations screen, ensure that Authentication is set to Test Pre-Shared Key. If not, click the down arrow to open the drop-down menu and select Text Pre-Shared Key. In the Test Pre-Shared Key box, enter the Key that was entered on the Nortel VPN Router 100. Enter it once again in the Confirm box.
11. In the MTU area of the Connection Configuration screen, the default settings should be Enable for Tunnel MTU and 1788 for the MTU Value. These settings will remain unchanged.
12. In the NAT area of the Connection Configuration screen, the default setting should be (None) for NAT. This setting will remain unchanged.
13. In the IP Configuration area of the Connection Configuration screen, the default setting for IP Configuration is Static. This setting will remain unchanged.
14. In the Local Networks area of the Connection configuration screen, a Local Network must be specified. If one has not been previously created, click the Create Local Network button to display the Networks configuration screen.
15. On the Networks configuration screen, enter a network name such as **local_net** and click the Create button to display the Networks Edit configuration screen.

16. In the "New /subnet area" in the IP Address field, add the subnet for the local network. Enter the value of **10.10.0.0**. In the Mask field, add **255.255.255.0** and click the Add button. The subnet will be displayed in the Current Subnets for Network box. Click the Close button to return to the Networks configuration screen
17. Click the Return to Connection Configuration link to return to the Connection Configuration screen and, in the Local Networks area, select the named local network that was just created. The Connection Configuration display screen will refresh and the IP subnet (or, if more than one, subnets) will be displayed.
18. In the Remote Networks area of the Connection Configuration screen, click the Add button to display the Add Remote Network Configuration screen. In the connection Area, the Group Name will appear along with the Connection Name for this peer-to-peer BOT.
19. In the Remote Network area of the Add Remote Network configuration screen, enter the IP Address **10.0.0.0** in the provided field and the IP Mask **255.255.255.0** in that field. Click OK to return to the Connection Configuration screen.
20. In the Remote Networks area of the Connection Configuration screen, the entered remote network is displayed with the default cost of 10 and the Enabled check box is checked. If there are additional remote networks to be added, repeat the previous two steps as many times as necessary.

NOTE **Although many subnets may be added, the proper use of IP ranges and subnet masks will prevent this field or the Local Networks field from being cluttered with unnecessary subnets. Careful planning and design of the network provides the ability for it to be easily understood and managed.**

21. Click OK at the bottom of the Connection Configuration screen to add the defined tunnel to the list of BOTs. If any of the parameters are improperly configured in the Connection Configuration screen, a pink banner will be displayed at the top of the page with suggestions for the corrections that need to be made.
22. On the Branch Office configuration screen, click the Select radio button and check the Enable check box for the tunnel just created. Click OK at the bottom of the screen to accept the list of tunnels. Click the Test button to test the newly created tunnel.

NOTE **It is assumed that the Nortel VPN Router 100 and the Nortel VPN Router being used to terminate the remote end of the tunnel are connected in a manner that will enable them to communicate with each other. This can be accomplished over an already existing network, with the use of a crossover cable directly connected between the units, or with a hub and patch cables. The method selected is dependent on the initial lab setup and user preferences.**

23. On the Test Connection screen, ensure that the correct Group and Connection are displayed. Check the Clear Event Log Before Test check box, which will allow the event log to be more easily read. Click the Test OK button.
24. After clicking the Test OK button, it may take a few minutes for the test to complete. Wait until the test results are displayed on a banner at the top of the screen.
25. If the tunnel test completes successfully, then you may want to ping from the PCs used to configure each Nortel VPN Router unit. If ping is successful in both directions, then the tunnel is configured properly and this lab is completed.
26. If the tunnel test fails then consult the event log on this Nortel VPN Router to see where the failure occurred. Verify the settings on both Nortel VPN Router units and repeat the previous two steps. Pay close attention to Tunnel Name, Pre-Shared Keys, Endpoint Addresses, Local Networks, and Remote networks. Any variation in these configuration parameters will cause the tunnel to fail and is the most common reason for tunnel creation and test failure.

Lab Summary

This lab extensively covered the configuration of the Nortel VPN Router 100, tunneling between two Nortel VPN Router 100 units, and tunneling between the Nortel VPN Router 100 and another member of the Nortel VPN Router family. It also contained hints on good networking practices and basic troubleshooting. There was also discussion on the different tunneling modes and the benefit of using each in the networking environment.

Configuring CLIP for Management IP Address

A new feature in the version 6 release of VPN Router code for the Nortel VPN Router is the ability to use Circuitless IP (CLIP) as an IP address for the Management Interface. What this means is that the IP address assigned to the Management Interface does not have to be on a subnet that is used on any physical interface of the Nortel VPN Router.

In previous version releases of VPN Router code for the Nortel VPN Router, the Private Interface and the Management Interface IP addresses had IP addresses that were resident within the same subnet. With the use of CLIP for the Management Interface, this relationship is no longer necessary. The beauty of using a CLIP IP Address for the Management Interface is that it adds an additional layer of security because its address is not deterministic from the IP addresses assigned to any of the physical addresses. This lab configures CLIP and demonstrates its use.

Lab Requirements

- Nortel VPN Router with version 6.00 VPN Router code loaded
- Serial console cable for the Nortel VPN Router being used for this lab
- Crossover Ethernet cable, or hub and patch Ethernet cables
- Windows-based PC with HyperTerminal and the Nortel VPN Client loaded
- Pencil and paper for notes

Lab Setup

1. Connect the console serial cable to the Console Port on the Nortel VPN Router and the PC serial port.
2. On the PC, launch the HyperTerminal program and if necessary press the Enter key to bring up the login prompt.
3. Log in to the console with the primary administrator user ID and password to bring up the Console Interface screen.
4. Select menu option 0 to bring up the Management IP Address menu.
5. Select option M to enter the management IP address of **8.8.8.8.**
6. Select option R to Return to the main menu.
7. Select option 1 to bring up the Interface menu.
8. Select option 0 to enter the Private LAN IP address of **10.10.0.1** with a subnet mask of **255.255.255.0**. Leave Speed/Duplex at the default setting of AutoNegotiate.
9. Select option 1 to enter the Public LAN IP address of **100.100.100.100** with a subnet mask of **255.255.255.0**. Leave Speed/Duplex at the default setting of AutoNegotiate.
10. Select option R to Return to the main menu.
11. Select option E to Exit, Save, and Invoke Changes.

12. On the PC, enter the network setting of the internal network card for an IP address that is on the **10.10.0.0** network with a subnet mask of **255.255.255.0** and a default gateway set to **10.10.0.1**. Save the network settings.
13. Using the Ethernet crossover cable, or the hub and Ethernet patch cables, connect the PC to the Private LAN of the Nortel VPN Router.
14. Ping the Management IP Address of 8.8.8.8. If ping replies are received, continue with the lab. If not, verify the settings of the previous steps and continue with the lab.
15. On the PC, launch a browser window and HTTP to 8.8.8.8.
16. At the Management screen, select PROFILES → USERS to configure a user with management rights on the Nortel VPN Router with a statically assigned IP address of **10.10.0.20**. If you are unfamiliar with how to accomplish this, the following lab covers configuring a user tunnel for managing the Nortel VPN Router.
17. After the user has been created, log off the Nortel VPN Router and disconnect your PC from the Nortel VPN Router.
18. Using the same cabling arrangement that was used to connect to the Private LAN, connect to the Public LAN of the Nortel VPN Router.
19. On the PC, set the network settings on the internal network card to have an IP address of **100.100.100.200** with a subnet mask of **255.255.255.0** and a default gateway of **100.100.100.100**. Save the network settings.
20. From the PC, ping the Public LAN interface at 100.100.100.100. If ping replies are received, continue with the lab. If no ping replies are received verify the settings on the PC and, if they appear correct, verify the Nortel VPN Router Public LAN settings with the use of the console cable and the HyperTerminal program.
21. On the PC, launch the Nortel VPN Client application. Configure a Connection name, add the User Name and Password for the user with administrator rights that was previously configured, and enter the Destination address of **100.100.100.100**.
22. On the Nortel VPN Client dialog window, click the Connect button. A dialog to save the configuration will appear. Click the Yes button to proceed with the client connection to the Nortel VPN Router.
23. The client should successfully connect to the Nortel VPN Router with a Nortel VPN Client icon appearing in the system tray of Windows.
24. Open a Command/DOS window and type the command **ipconfig**. Within the DOS window, the settings for the virtual NIC used for the Nortel User connection should have the IP address of 10.10.0.20, which was statically assigned to that user.

25. Launch a browser window and HTTP to 8.8.8.8. Verify that the Nortel VPN Router Management screen appears. Log in with the user that was created with the management rights. For the purposes of this lab, it will be the same user that was used to connect with the Nortel VPN Client. However, any user with administrator rights may be used, including the primary administrator user ID and password. Verify that the user is able to navigate the different configuration screens without a denial.
26. If the user is capable of navigating the configuration screens without being denied, then this will conclude this lab. If the user has an issue, then log in with an administrator user ID and password, which will be used to verify this user's profile to ensure that administrator privileges have been granted to that user.

Lab Summary

This lab showed how a CLIP address may be assigned to the Management Interface. Although the unit is not bound to any physical interface, the administrators of the Nortel VPN Router are still able to manage the unit. Although it was not mentioned within the context of this lab, there are obvious routing and networking considerations that would come into play in order for the administrators remote from the unit to manage the unit.

Using the example of this lab, you can see that if an administrator on a remote network needed to manage this particular Nortel VPN Router, then the management session would need to be capable of being routed to the management address of 8.8.8.8. However, an administrator would be capable of using the Nortel VPN Client to manage the unit from anywhere, as long the administrator is able to establish a successful user tunnel to the Nortel VPN Router.

Configuring Administrator User Tunnels

Administrators of the Nortel VPN Router require the ability to manage the unit in a number of ways. This lab covers the use of the Nortel VPN Client to allow remote user administrators to configure, control, and manage the unit. Administrators may be given only certain privileges, depending upon their level of responsibility for the unit. Where applicable throughout this lab, discussion of privilege options will be noted.

Lab Requirements

- Nortel VPN Router with version 6.00 VPN Router code loaded
- Serial console cable for the Nortel VPN Router being used for this lab
- Crossover Ethernet cable, or hub and patch Ethernet cables

- Windows-based PC with HyperTerminal and the Nortel VPN Client loaded
- Pencil and paper for notes

Lab Setup

For the purposes of this lab, assume that the Nortel VPN Router has been previously configured with the following settings:

- Private LAN IP address of 10.10.0.10 with a 255.255.255.0 subnet mask and Speed/Duplex set to AutoNegotiate
- Public LAN IP address of 100.100.100.100 with a 255.255.255.0 subnet mask and Speed/Duplex set to AutoNegotiate
- Management Interface IP address set to 8.8.8.8

1. If the Nortel VPN Router has not been previously set to these addresses, then with the use of the console cable and the administrator's user ID and password, set the interfaces with these values.
2. Set the Windows-based PC network settings to have an IP address of **10.10.0.20** with a subnet mask of **255.255.255.0,** and with the default gateway set to **10.10.0.10**. Save the network settings.
3. Connect the PC to the Private LAN Interface of the Nortel VPN Router using either Ethernet crossover cable, or hub and Ethernet patch cables.
4. From the PC, ping the Management Interface IP address at 8.8.8.8. If ping replies are received, continue with the lab. If no ping replies are received, go back to verify settings on the PC and then the Nortel VPN Router.
5. From the Windows-based PC, launch a browser and HTTP to 8.8.8.8.
6. On the Nortel VPN Router Management screen, click the Manage Switch link and use either the default user ID of admin and the password of setup, or another administrator user ID/password combination that has full management privileges on the Nortel VPN Router.
7. From the main menu, select PROFILES → GROUPS to display the Groups configuration screen. Click the Add button to add a new group. At the Add screen for group add a Group Name of Admins and leave the Parent Group at /Base. Click the OK button, which will return you to the Groups configuration screen.
8. Select PROFILES → USERS to display the User Management screen. On Group, click the down arrow to select the group /Base/Admins and click the Add User button to display the Add User configuration screen.
9. To add a new group, perform the following:

a. Add a First and Last Name in the supplied boxes (for example, First Name = **NVR** Last Name = **Admin_user**).

b. Ensure that the group /Base/Admins is displayed. If not, then it may once again be selected by clicking the down arrow.

c. In the Remote User area, add a Static IP Address of **10.10.0.30** and a Static Subnet Mask of **255.255.255.0**.

NOTE **This address may be dynamically assigned if an address pool has been defined or if DHCP has been configured to allocate addresses for user tunnels. For the purposes of this lab, the User Tunnel address is statically assigned.**

d. In the User Accounts area for an IPSec user, enter the user ID of **NVR_Admin** and, for the purposes of this lab, a password of **12345678**. Re-enter the password in Confirm Password.

NOTE **The User Accounts area provides for the addition of users with different tunneling clients if needed or desired. For this lab, because the Nortel VPN Client will be used to establish the user tunnel, utilize the IPSec User Account.**

e. Because the user being created will be utilizing local authentication (Internal LDAP), scroll past the various authentication methods to the Administration Privileges area. In the Administrative Authentication Method, ensure that the radio button for Local Authentication is selected.

f. In the Admin area, add the User ID **NVR_Admin** with a password of **12345678** and re-enter the password in the Confirm Password box.

g. In the /admin Rights area for Manage Switch, click the down arrow and select Manage. For Manage Users, click the down arrow and select Manage.

NOTE **Administrators may be given different levels of responsibility. It is possible to limit the abilities of administrators, from only being able to view different screens of the Nortel VPN Router without the ability to change any parameters to full management rights to change a wide range of configurations with the right to add and delete users. However, there are a few rights that are permitted to be exercised only by the Primary Administrator of the Nortel VPN Router. For the purpose of this lab, the administrator has been given a wide range of management rights on the Nortel VPN Router.**

h. Click OK to accept the parameters set for this user. The User Management screen will be displayed with a banner at the top that the user has been successfully created. If there is an error in a parameter,

the banner lists the reason for the exception. Correct any errors and click on the OK button until the user has been correctly added.

10. With the administrator user created, close down the browser and move the PC connection from the Private LAN Interface to the Public LAN Interface.
11. Reconfigure the PC network settings to have an IP address of **100.100.100.200** with a subnet mask of **255.255.255.0** and a default gateway of **100.100.100.100**.
12. On the Windows-based PC, launch the Nortel VPN Client and set the Connection to Lab Setup; enter the username **NVR_Admin** and a password of **12345678**. Enter the destination of the Nortel VPN Router Public LAN Interface IP address of **100.100.100.100**. Click the Connect button. A dialog box appears asking if you want to save changes to the current connection. Click Yes to establish a user tunnel to the Nortel VPN Router.
13. If the connection attempt is successful and the user tunnel is established, the Nortel VPN Client icon will appear in the system tray. Continue with the lab with a successful tunnel connection. If the tunnel fails to establish, verify that the settings on the client match the settings that were configured for this user. Repeat the preceding steps until a successful user tunnel has been established.
14. With the user tunnel established, launch a Command/DOS window and enter the command **ipconfig**. Notice that the Nortel VPN Client virtual Network Interface Card is displaying the address of 10.10.0.30.
15. Launch a browser and HTTP to 8.8.8.8. The Nortel VPN Router management screen will be displayed. Click the Manage Switch link and enter the user ID **NVR_Admin** and the password **12345678** to log in to the Nortel VPN Router.
16. Navigate through a few configuration screens to ensure that you are able to navigate the menu system without restriction.

NOTE **Although this administrative user has been given full rights, restrictions are placed on that user by the fact that a user tunnel is being utilized to manage the Nortel VPN Router. To have full access to all management functions on the Nortel VPN Router, you must add a tunnel filter in this user's group settings to allow for functions such as Telnet and FTP.**

17. From the main menu, select PROFILES → FILTERS to display the Filters configuration screen. In the Current Contivity Tunnel Filters area (see Figure 11-27), add the name **NVR_Admin** in the box adjacent to the Create button and click the Create button after the name has been entered.

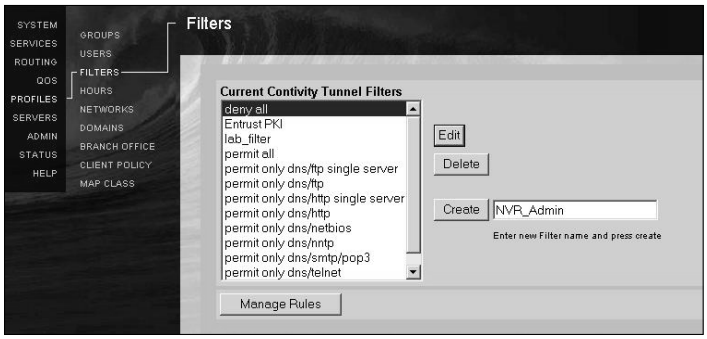


Figure 11-27: The filters configuration screen

18. The Tunnel Filters Edit screen will be displayed for the Tunnel Filter Set: NVR_Admin. From the Available Rules, select "permit all/in" and click the double left arrow button to move the rule to the Rules in Set column. Do this also for the "permit all/out" rule. Notice the Allow Management Traffic area is divided into a "For these Local Services" grouping and a "For these Remote Servers" grouping. Select the following by checking the appropriate check box:
    - *HTTP:* Allow the management of the Nortel VPN Router using the GUI screen.
    - *SNMP:* Allow SNMP gets from the Nortel VPN Router, which may be used to monitor the operation of the unit.
    - *FTP:* Allow the movement of files to and from the Nortel VPN Router with the use of an FTP client.
    - *Telnet:* Allow the ability to Telnet to the Management Interface to perform Command Line Interface (CLI) commands on the unit.
    - *PING:* Allow the pinging of the Management Interface to receive ping echo replies.

    In the "For these Servers" area, check the FTP check box. This permits the fetching of VPN Router code upgrades from the tunneled PC while it is running an FTP server. Although this may be accomplished in this manner, it is more efficient to perform upgrades to the Nortel VPN Router from an FTP server that is located on the local Private LAN.
19. Once the filter is configured as shown in Figure 11-28, click OK at the bottom of the screen to accept these settings and return to the Filters configuration screen. The NVR_Admin filter should now be displayed in the Current Contivity Tunnel Filters selection box.

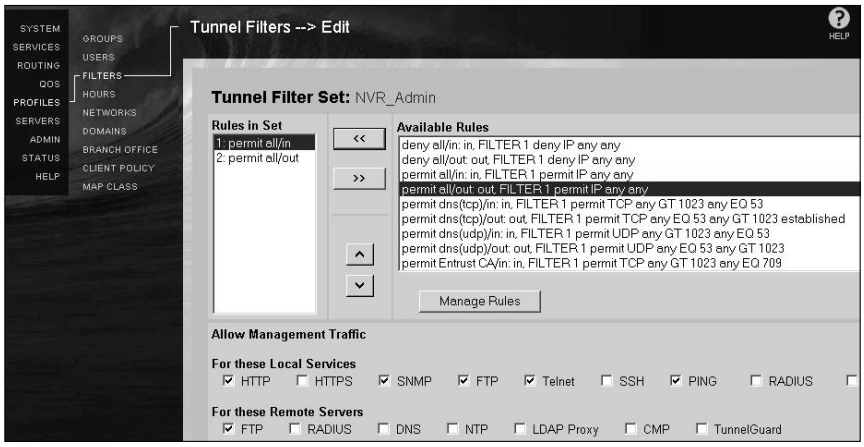


Figure 11-28: Verifying the filter via the Tunnel Filters edit screen

20. From the main menu, select PROFILES → GROUPS to display the Groups configuration screen. Click the Edit button for the group /Base/Admins to display the Groups Edit configuration screen.
21. In the Connectivity area, click the Configure button to open this section for modification.
22. Scroll down to the Filters line and click its Configure button, which will cause the Groups Edit Connectivity screen to refresh.
23. Once again, scroll down to the Filters line and notice that there is a filters selection drop-down menu displayed. Click the down arrow and select the NVR_Admin filter set.
24. Scroll to the bottom of the screen and click OK to display the Groups Edit screen.
25. Scroll to the bottom of the screen and click the Close button to return to the Groups selection screen. This completes the filter configuration and applies it to the appropriate group. However, because this tunnel is established already, the filters have not been applied to this particular tunnel. Close the browser window and disconnect from the Nortel VPN Router by clicking the Nortel VPN Client icon to display the client status window and by clicking the Disconnect button.
26. Once the user tunnel has been totally disconnected, launch the Nortel VPN Client again to establish a new tunnel to the Nortel VPN Router.

27. Once the tunnel is established, launch a browser window and HTTP to the Management Interface IP address of 8.8.8.8. Log in using the **NVR_Admin** user ID and the password **12345678**.
28. Verify that it is possible to navigate the different configuration screens.
29. Open a Command/DOS window and Telnet to 8.8.8.8. A login prompt is presented. Log in using the **NVR_Admin** user ID and the password **12345678**. On successful login, a command-line prompt will be displayed. Issue a **dir** command to display the directory structure of the Nortel VPN Router.
30. Open another Command/DOS window and FTP to 8.8.8.8. A login screen is presented. Log in using **NVR_Admin** with the password **12345678**. On successful login an `ftp` prompt will be displayed. Issue a **dir** command to display the directory structure of the Nortel VPN Router.

NOTE **Each service that is called performs a login query. Each service is capable of being run simultaneously with the other services. This capability is essential for the ongoing maintenance and service of the Nortel VPN Router.**

31. This concludes this lab. We recommend (and encourage) that you further explore the capabilities that are granted to an administrator to develop the required profiles for users who will be responsible for the administering of the Nortel VPN Router.

Lab Summary

In this lab, an administrator user was created and the different capabilities provided to that administrator were discussed. In creating this user, we touched upon the use and configuration of group settings and tunnel filters. Administrative users with the proper privileges are essential in the maintenance and ongoing support of the Nortel VPN Router.

Careful consideration of the capability granted to users is required. Within the scope of this lab, however, not all possible combinations of administrative capabilities were explored. We encourage you to examine and carefully plan the levels of administrator involvement upon completion of this lab.

Configuring Syslog Server

The Nortel VPN Router has local logging on the unit that may be viewed and used to monitor different aspects on the Nortel VPN Router, such as events in the security and configuration of the Nortel VPN Router. However, because these logs utilize local storage, they are limited in their ability to store historical data, which, in certain organizations, is recorded and archived for extensive periods of time.

You can take advantage of the Nortel VPN Routers' logging ability and monitor storage of those logs over long periods of times by using an external Syslog server. This lab covers the simple configuration and discusses some points of logging on the Nortel VPN Router at the same time.

Lab Requirements

- Nortel VPN Router with version 6.00 VPN Router code loaded
- Crossover Ethernet cable, or hub and patch Ethernet cables
- Windows-based PC with Syslog server program
- Windows-based PC with browser software
- Network diagram (see Figure 11-29)
- Pencil and paper for notes

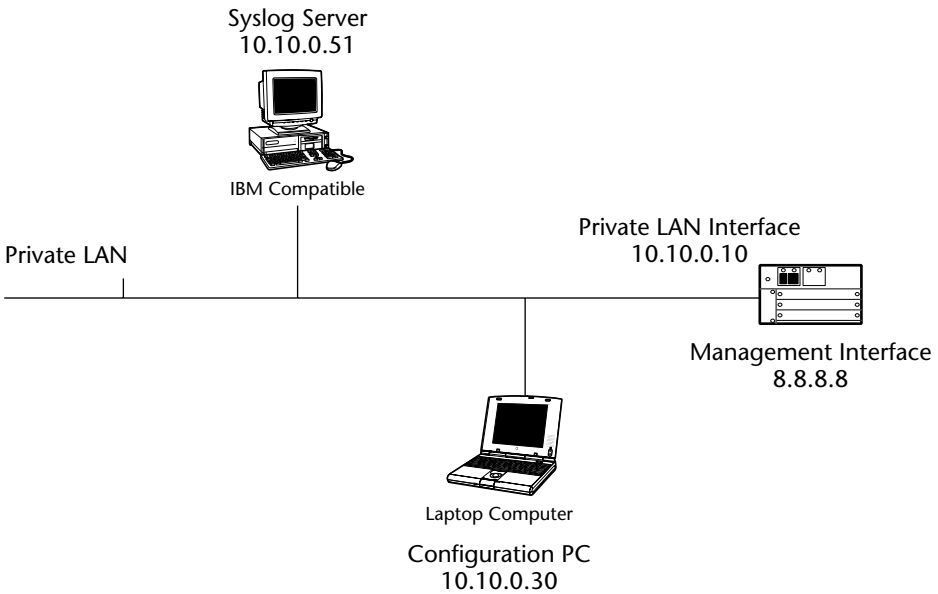


Figure 11-29: The Syslog configuration lab diagram

Lab Setup

For purposes of this lab, it is assumed that the Nortel VPN Router has been previously configured with the following IP addresses:

- Private LAN Interface 10.10.0.10 with a subnet mask of 255.255.255.0
- Management IP address of 8.8.8.8

1. The Windows-based PC used for the configuration of the Nortel VPN Router should have its network interface set to an IP address of 10.10.0.30 with a subnet mask of 255.255.255.0, and a default gateway set to 10.10.0.10. The Syslog server does not necessarily have to be another PC. It can be combined within the same PC that is being used to configure the Nortel VPN Router. However, for this lab, it is another standalone PC that has its network interface configured with an IP address of 10.10.0.51 with a subnet mask of 255.255.255.0 and a default gateway set to 10.10.0.10.
2. Ensure that the network is connected as shown on the network diagram illustrated in Figure 11-29.
3. At the PC being used to configure the Nortel VPN Router, launch a browser window and HTTP to 8.8.8.8.
4. Click the Manage Switch link and log in using an administrator's user ID and password.
5. On the main menu, select SERVICES → SYSLOG to display the Syslog Forwarding configuration screen, as shown in Figure 11-30.
6. Enter the IP address of the Syslog server in the Host Name or IP Address field and click the Enabled check box.
7. Filter Level is by default set to All. Click the down arrow and notice that there are different levels of severity that may be selected. For the purposes of this lab, leave it set to All.

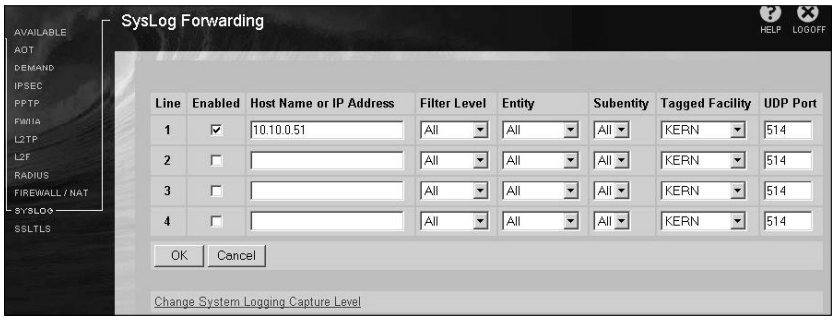


Figure 11-30: The Syslog Forwarding configuration screen

8. Entity Level is by default set to All. Click the down arrow and notice that there are different selections for various components of the Nortel VPN Router. If a component is selected, the screen will refresh and the Subentity will have other selections than the present default setting of All. For the purposes of this lab, leave both the Entity and Subentity settings set on the default of All.
9. Tagged Facility is by default set to KERN, which is the main kernel of the operating system that will record all events that occur on the Nortel VPN Router. Click the down arrow to view the other selections that may be selected. For the purposes of this lab, the default setting of KERN will be used.
10. UDP Port, by default, is set to 514, which is a common listening port for Syslog servers. This may be adjusted if needed. For the purposes of this lab, leave the default setting of 514 for the UDP port to communicate with the Syslog server. Click OK to accept these settings for the Syslog server.
11. Click the Change System Logging Capture Level link, which is just below the OK button, to display the System Log screen.
12. Capture Level is, by default, set to All. Click the down arrow to view the other selections. For now, leave the default setting of All and click the link Change SYSLOG Forwarding Details to return to the SysLog Forwarding screen.
13. This completes the configuration of the Nortel VPN Router to store system logs to an external Syslog server.
14. On the PC that is acting as the Syslog server, if it has been previously configured and is listening on UDP port 514 for Syslog updates, then check the logging on the unit to verify it is receiving updates from the Nortel VPN Router. If updates are not received, then check all settings and, in particular, assigned IP addresses on both the PC and the Nortel VPN Router.

NOTE **For testing purposes, there is freeware Syslog server software available for download from various organizations. There are also demo programs and shareware (which may have a limited usage license) available for download. For the purposes of this lab, no particular Syslog server is specified or recommended. All Syslog server software should be able to record and display the logs generated by the Nortel VPN Router.**

Lab Summary

In this lab, you configured an external Syslog server for use in recording system logging information from the Nortel VPN Router. The external Syslog server will allow for the storage and archiving of all system logs reported to it from the Nortel VPN Router. Also, this lab included a discussion on the customization of logs to set the severity of events, the selection of what entities will be logged, as well the use of the common UDP port. The amount of logging that is accomplished is dependent on the organization that the Nortel VPN Router is situated in.

Different organizations have various requirements. With the Syslog server logs that are archived, it is possible to gather historical data on user usage patterns, as well as alarms that may have been triggered for a number of reasons. The use of the external Syslog server should be strongly considered a good practice for maintaining and monitoring the Nortel VPN Router, along with the traffic that is passing through the unit.

Configuring User IP Address Pools

As users establish user tunnels to the Nortel VPN Router, they require an assigned IP address to allow them to be able to route IP traffic to and from their PC to the Private LAN behind the Nortel VPN Router. Depending on the size of the user base, using a VPN Client to tunnel to the Nortel VPN Router makes dynamic address allocation more desirable than statically assigning a user to a particular IP address.

Although static IP address assignment is easy to accomplish, it can become a tedious task to keep track of addresses as they are assigned and retired.

There two methods of dynamically assigning user IP address on the Nortel VPN Router: DHCP and Address Pool.

Lab Requirements

- Nortel VPN Router with version 6.00 VPN Router code loaded
- Crossover Ethernet cable, or hub and patch Ethernet cables
- Windows-based PC with the Nortel VPN Client loaded
- Windows-based PC server capable of acting as a DHCP server
- Network diagram (see Figure 11-31)
- Pencil and paper for notes

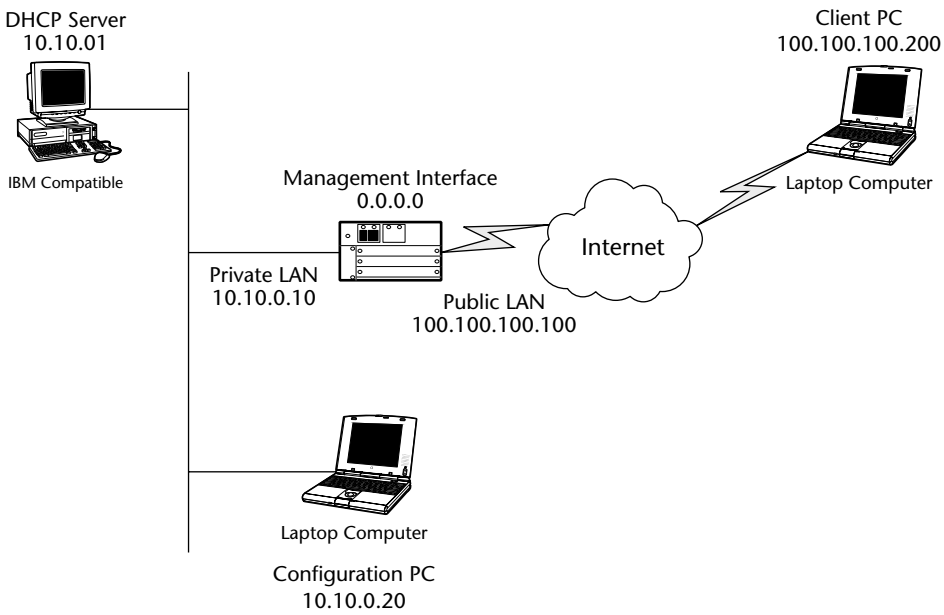


Figure 11-31: The configuring User IP Address Pools lab diagram

Lab Setup

This lab is divided into two parts. You may choose to do either or both to learn to use each method to dynamically assign IP addresses to user tunnels. The first lab deals with DHCP and the second deals with Address Pool.

Configuring User IP Address Assignment Using DHCP Lab

For the purpose of this lab, we assume that the Nortel VPN Router has been previously configured with the following IP addresses:

- Private LAN Interface IP address is set to 10.10.0.10 with a subnet of 255.255.255.0.
- Public LAN Interface address is set to 100.100.100.100 with a subnet of 255.255.255.0.
- The Management Interface IP address is set to 8.8.8.8.

1. On the PC set up to perform the Nortel VPN Router configuration, set the internal Network Interface Card to the IP address of **10.10.0.20** with a subnet mask set to **255.255.255.0** and the default gateway set to **10.10.0.10**.

2. On the PC being used for the configuration of the Nortel VPN Router, launch a browser and HTTP to 8.8.8.8. Log in to the Nortel VPN Router using an administrator's user ID and password.
3. At the main menu, select SERVERS → USER IP ADDR to display the Remote User IP Address Pool, which is shown in Figure 11-32.
4. Select the radio button for DHCP.
5. In the DHCP Server area there are three radio button selections:
   - *Any External DHCP Server:* Uses a broadcast to find a DHCP on the local Private LAN Network.
   - *Internal DHCP Server:* Uses the DHCP server that is contained within the Nortel VPN Router. Configuration of this server was performed in the DHCP lab earlier in this chapter.
   - *Specified DHCP Server:* Is routed to a particular DHCP server. For the purposes of this lab, select this radio button and enter the IP address assigned to the DHCP server for this lab, which is **10.10.0.1**.
6. DHCP Cache Size value is the number of IP addresses the Nortel VPN Router will request and store internally for use to assign to user tunnels as they connect to the Nortel VPN Router. If the Nortel VPN Router has many users that would tunnel to it in a relatively short time, then a number higher than 1 would allow the Nortel VPN Router to make fewer requests to the DHCP for addresses it will allocate out to user tunnels. For purposes of this lab, set this value to 1. There is a balance to the value that would be inserted in this field. Too high of a number would cause the Nortel VPN Router to hoard addresses, thus not allowing the external DHCP server to uses those addresses for other devices on its network.

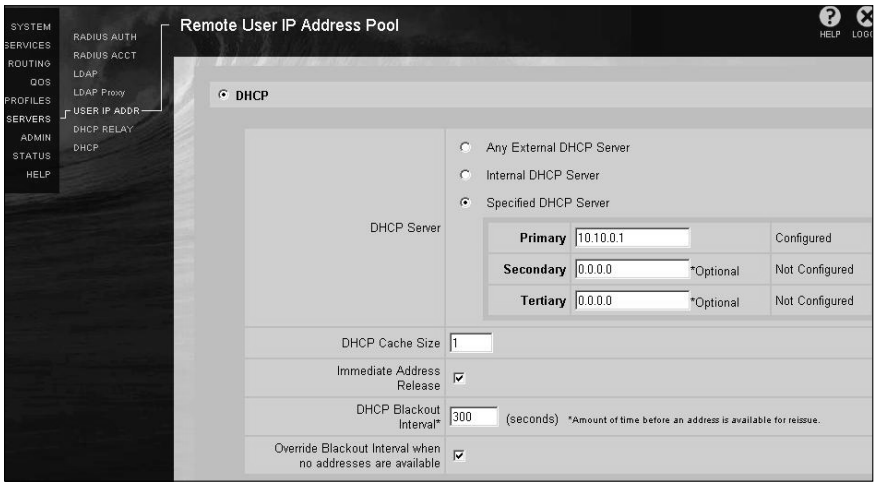


Figure 11-32: The Remote User IP Address Pool DHCP screen

7. Select the check box for Immediate Address Release, which will immediately return IP addresses to the DHCP server as they are freed up when a user tunnel disconnects from the Nortel VPN Router.
8. The value for DHCP Blackout Interval is the amount of time in seconds that the Nortel VPN Router will wait before it will reuse an IP address that it has cached. Because you are caching only one IP address and the Immediate Address Release check box has been selected, this value will have no effect on how IP addresses are handled in this lab. For the purposes of this lab, just allow the default value of 300 to remain.
9. The "Override Blackout Interval when no addresses are available" check box allows the Nortel VPN Router to use an IP address sooner than the set DHCP Blackout Interval if there are no more addresses in its cache that are beyond the blackout interval that it can allocate. For the purposes of this lab, this box may remain either checked or unchecked because there is no caching of more than a single address at a time.
10. Scroll to the bottom of the screen and click OK to accept the DHCP settings. The Nortel VPN Router is now ready to request IP addresses from a DHCP server for allocation to user tunnels as they connect.
11. Verify that the DHCP server has a scope of addresses it will allocate within the subnet range of the Private LAN (for example, an address range of 10.10.0.100 to 10.10.0.150).
12. If no users are currently configured on the Nortel VPN Router, configure one to test the ability of the Nortel VPN Router to allocate an address to the connecting user tunnel.
13. Connect a Windows-based PC with the Nortel VPN Client installed to the Public LAN Interface. This can be accomplished with either an Ethernet crossover cable, or a hub and Ethernet patch cables.
14. Set the PC Network Interface IP address to **100.100.100.200** with a subnet of **255.255.255.0** and with the default gateway set to **100.100.100.100**.
15. On the PC, launch the Nortel VPN Client and set the connection with the user ID and password that is assigned to the user that was created for this test. Set the destination address to **100.100.100.100** and then click the Connect button. If prompted to save the current connection settings click Yes.
16. On a successful connection, the Nortel VPN Client icon will appear in the system tray. Double-clicking the icon will open a connection dialog screen. Verify that the assigned address is within the range of the IP addresses that are being allocated by the DHCP server. If the address is not within the range, or the connection fails, verify all configuration settings and repeat until the connection provides the desired result.

This concludes this portion of the lab. Continue with the Address Pool portion.

Configuring User IP Address Assignment Using Address Pool Lab

For the purpose of this lab, it is assumed that the Nortel VPN Router has been previously configured with the following IP addresses:

- Private LAN Interface IP address is set to 10.10.0.10 with a subnet of 255.255.255.0.
- Public LAN Interface address is set to 100.100.100.100 with a subnet of 255.255.255.0.
- The Management Interface IP address is set to 8.8.8.8.

1. On the PC setup to perform the Nortel VPN Router configuration, set the internal Network Interface Card to the IP address of **10.10.0.20** with a subnet mask set to **255.255.255.0** and the default gateway set to **10.10.0.10**.
2. On the PC being used for the configuration of the Nortel VPN Router, launch a browser and HTTP to 8.8.8.8. Log in to the Nortel VPN Router using an administrator's user ID and password.
3. At the main menu, select SERVERS → USER IP ADDR to display the Remote User IP Address Pool, which is shown in Figure 11-33.
4. Select the Radio button for Address Pool.
5. To add an address pool, click the Add button to display the Enter Address Pool Information screen.
6. In the Starting IP Address field, add the address **10.10.0.75.**
7. In the Ending IP Address field, add the address **10.10.0.85.**
8. In the Subnet Mask field, add **255.255.255.0.**
9. Because this is the first pool that is added, leave the Pool selection radio button set to Default.

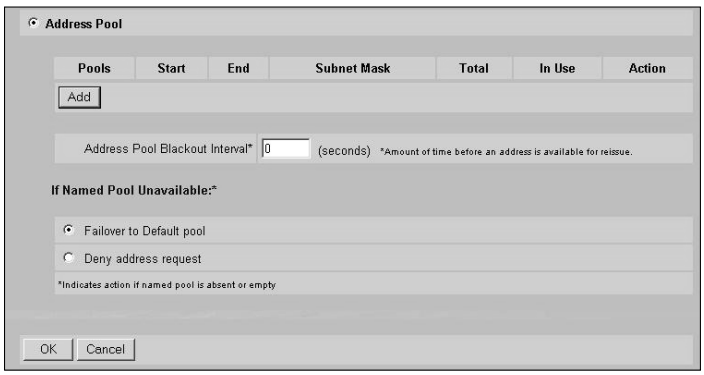


Figure 11-33: The Remote User IP Address Pool configuration main screen

NOTE **Named pools may be created to allocate different address pools to different groups. This is accomplished by setting the GROUP PROFILE → CONNECTIVITY → ADDRESS POOL NAME to the name that was given to that address pool. Users that are members of this group are given an address from that address pool.**

10. Click OK to accept the address pool settings and return to the Remote User IP Address Pool screen.
11. For the Address Pool Blackout Interval, insert the value of **300** seconds. This is the time the IP address will not be available when a user tunnel disconnects.
12. In the If Named Pool Unavailable area, the selections are "Failover to Default pool" and "Deny address request." Leave "Failover to Default pool" selected.

NOTE **If users of a particular group are to be restricted to a given address pool and not permitted to use addresses from the default pool, the "Deny address request" selection will cause the Nortel VPN Client to fail to connect successfully until an IP address for that named pool is released back to the pool.**

13. Verify that the Address Pool radio button is selected and click OK at the bottom of the screen. This concludes configuration of the Nortel VPN Router for allocating IP addresses to user tunnels.
14. If no users are currently configured on the Nortel VPN Router, configure one to test the ability of the Nortel VPN Router to allocate an address to the connecting user tunnel.
15. Connect a Windows-based PC with the Nortel VPN Client installed to the Public LAN Interface. This can be accomplished with either an Ethernet crossover cable, or a hub and Ethernet patch cables.
16. Set the PC Network Interface IP address to **100.100.100.200** with a subnet of **255.255.255.0** and with the default gateway set to **100.100.100.100**.
17. On the PC, launch the Nortel VPN Client and set the connection with the user ID and password that is assigned to the user that was created for this test. Set the destination address to **100.100.100.100** and then click the Connect button. If prompted to save the current connection settings, click Yes.
18. On a successful connection, the Nortel VPN Client icon appears in the system tray. Double-clicking the icon will open a connection dialog box. Verify that the assigned address is within the range of the IP addresses that are being allocated by the address pool. If the address is not within

the range, or the connection fails, verify all configuration settings and repeat until the connection provides the desired result.

19. Once a successful connection is made and the assigned IP address is in the range of the addresses allocated by the address pool, click the Disconnect button to terminate this connection session.
20. The Address Pool Blackout Interval has been set to 300 seconds, or 5 minutes. Reconnect to the Nortel VPN Router with the Nortel VPN Client within that interval and verify that, on the next successful connection, the new assigned IP address is not the same as the one that was received in the previous connection session.
21. As an optional addition to this lab, you may want to return to the SERVERS → USER IP ADDR configuration screen and edit the default address pool to have only two addresses (such as 10.10.0.75 and 10.10.0.76) and reduce the Address Pool Blackout Interval to 180 seconds.
22. Within the three-minute interval period for Address Pool Blackout, connect to the Nortel VPN Router using the Nortel VPN Client three times. Note the assigned IP address each time before clicking the Disconnect button. On the third attempt, if still within the Address Pool Blackout Interval, the connection will fail because no addresses are available in the default pool that are not within the interval. This can be verified by using the Management Screen main menu by selecting STATUS → EVENT LOG to display the log. Scroll down to the third attempt to connect with the Nortel VPN Client and notice that the event log shows that the tunnel didn't establish because the IP address assignment failed.

This concludes this portion of the lab.

Lab Summary

This lab showed two methods for dynamically allocating IP addresses to remote users. We discussed various options and testing of the principles used to familiarize you with the methods available for user tunnel IP address assignment. Management of IP addresses can also be used to control access for users and groups, which was described in the discussion on named address pools. You are encouraged to try variations of this lab to further your knowledge of IP address allocation with the Nortel VPN Router.

Client Address Redistribution Configuration

Client Address Redistribution (CAR) is a feature that can be used to allocate IP addresses to user tunnels that are not bound to any physical entity on the

Private LAN network. It uses an address pool of addresses, which can be allocated from internal address pools or by using DHCP internal/external servers. The Nortel VPN Router controls the routing of these user tunnels and proxies all requests to the Private LAN for the clients that are using a CAR IP address.

The feature also adds additional security because the IP address on the client is a virtual address and the user has no reference to the IP addressing that is being used on the Private LAN.

Lab Requirements

- Nortel VPN Router with version 6.00 VPN Router code loaded
- Crossover Ethernet cable, or hub and patch Ethernet cables
- Two Windows-based PCs, one with the Nortel VPN Client loaded
- Network diagram (see Figure 11-34)
- Pencil and paper for notes

Lab Setup

For the purpose of this lab, it is assumed that the Nortel VPN Router has been previously configured with the following IP addresses:

- Private LAN Interface IP address is set to 10.10.0.10 with a subnet of 255.255.255.0.
- Public LAN Interface address is set to 100.100.100.100 with a subnet of 255.255.255.0.
- The Management Interface IP address is set to 8.8.8.8.

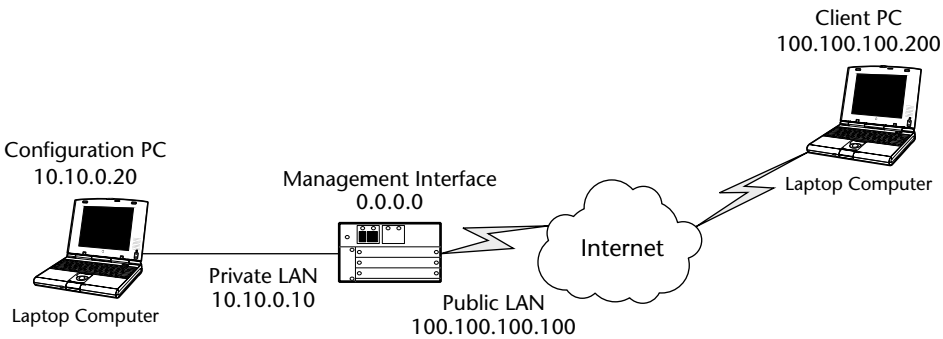


Figure 11-34: The Client Address Redistribution configuration lab diagram

1. On the PC setup to perform the Nortel VPN Router configuration, set the internal Network Interface Card to the IP address of **10.10.0.20** with a subnet mask set to **255.255.255.0** and the default gateway set to **10.10.0.10**.
2. On the PC being used for the configuration of the Nortel VPN Router, launch a browser and HTTP to 8.8.8.8. Log in to the Nortel VPN Router using an administrator's user ID and password.
3. At the main menu, select SERVERS → USER IP ADDR to display the Remote User IP Address Pool configuration screen.
4. Select the Radio button for Address Pool.
5. To add an address pool, click the Add button to display the Enter Address Pool Information screen.
6. In the Starting IP Address field, add the address **20.20.0.30**.
7. In the Ending IP Address field, add the address **20.20.0.40**.
8. In the Subnet Mask field, add **255.255.255.0**.
9. Because this is to be a named pool, click the New radio button and add a name for this pool in the box provided. For the purposes of this lab, enter **sup_grp**.
10. Click OK to accept the Address Pool settings and return to the Remote User IP Address Pool screen.
11. For the Address Pool Blackout Interval, insert the value of **300** seconds. This is the time the IP address will not be available when a user tunnel disconnects.
12. In the If Named Pool Unavailable area, the selections are "Failover to Default pool" and "Deny address request." Click the radio button next to "Deny address request."

NOTE **If users of a particular group are to be restricted to a given address pool and not permitted to use addresses from the default pool, the "Deny address request" selection will cause the Nortel VPN Client to fail to connect successfully until an IP address for that named pool is released back to the pool.**

13. Verify that the Address Pool radio button is selected and click OK at the bottom of the screen. This concludes configuration of the Nortel VPN Router for creating a named IP address pool to allocate IP addresses to user tunnels.

14. If no users are currently configured on the Nortel VPN Router, configure one to test the ability of the Nortel VPN Router to allocate an address to the connecting user tunnel.
15. After the user is created and assigned to a group, the group must be configured to use the newly created named Address Pool for all users within that group. From the main menu, select PROFILES → GROUPS.
16. Click the Edit button for the group to which the user who will be used for testing of the CAR feature is assigned. This will display the Groups Edit configuration screen.
17. In the Connectivity area, click the Configure button to allow modification of these parameters.
18. Scroll down to the Address Pool Name area and click the Configure button.
19. The screen will refresh and a drop-down menu will appear adjacent to Address Pool Name.
20. Click the down arrow for the drop-down menu and select the named address pool to be used. For the purposes of this lab, enter **sup_grp**.
21. After the group has been selected, scroll to the bottom of the screen and click OK.
22. This concludes the assigning of the named address pool to the group the user is a member of. However, CAR still remains to be configured to allow the assigned address pool to route user traffic onto the Private LAN.
23. From the main menu, select ROUTING → CLIENT-ADDR-DIS to display the Client Address Redistribution configuration screen.
24. In the Client Address Redistribution area, click the down arrow for CAR options. The options presented are:
    - *Host Only*: A route for each user tunnel is added to the route table. These entries are established each time a user tunnel is established using a CAR-assigned address. The route is removed upon client Disconnect.
    - *Dynamic Aggregation*: A subnet route is added when the first client connects and remains until the last user using an assigned IP address from the subnet disconnects.
    - *Static Aggregation*: A subnet route is added when the first client connects and the route remains as long as the address pool remains valid.

25. For the purposes of this lab, select Host Only.
26. Leave the Maximum Number of U Tunnel Host Routes set to the default value of 200 and click OK to accept these configuration settings and enable CAR.
27. Connect a Windows-based PC with the Nortel VPN Client installed to the Public LAN Interface. This can be accomplished with either an Ethernet crossover cable, or a hub and Ethernet patch cables.
28. Set the PC Network Interface IP address to **100.100.100.200** with a subnet of **255.255.255.0** and with the default gateway set to **100.100.100.100**.
29. On the PC, launch the Nortel VPN Client and set the connection with the user ID and password that are assigned to the user created for this test. Set the destination address to **100.100.100.100** and then click the Connect button. If prompted to save the current connection settings, click Yes.
30. On a successful connection, the Nortel VPN Client icon will appear in the system tray. Double-clicking the icon opens a connection dialog screen. Verify that the assigned address is within the range of the IP addresses that are being allocated by the address pool (20.20.0.30–20.20.0.40). If the address is not within the range, or the connection fails, verify all configuration settings and repeat until the connection provides the desired result.
31. Once a successful connection is made and the assigned IP address is in the range of the addresses allocated by the address pool, return to the PC that is being used to configure the Nortel VPN Router.
32. Launch a browser window and HTTP to 8.8.8.8.
33. Click on the Manage Switch link and log in to the Nortel VPN Router using an administrator's user ID and password.
34. From the main menu, select ROUTING → CLIENT-ADDR-DIS to display the Client Address Redistribution configuration screen.
35. Click the Show User Tunnel Routes button. The Client Addr Redist → User Tunnel Routes will be displayed.
36. Verify that the IP address assigned to the user tunnel is displayed.
37. On the PC that is making the user tunnel, double-click the Nortel VPN Client icon that is displayed in the system tray.
38. In the connection dialog box that is displayed, click the Disconnect button to terminate the user tunnel session.

39. Return to the PC that is displaying the Client Addr Redist → User Tunnel Routes screen, and click the Refresh button. The user address that was assigned to the client should now be removed.
40. On the PC that is being used for establishing the user tunnel, once again launch the Nortel VPN Client to establish a user tunnel.
41. On a successful connection, verify that the assigned address is from the named Address Pool that was created. This address will be different from the one that was previously assigned if the connection attempt was made within the Address Pool Blackout Interval.
42. Return to the PC that is displaying the Client Addr Redist → User Tunnel Routes screen, and click the Refresh button. The user address that was assigned to the client should now be displayed.
43. From the main menu, select ROUTING → ROUTE TABLE to display the Route Table screen.
44. Click the IP Forward Table button to display the Route Table → IP Forward Table.
45. Verify that the IP address that is assigned to the client user tunnel is displayed on the table.
46. After the display of the IP address on the table has been confirmed, click the Close button to return to the Route Table screen.
47. Click the Route Table button to display the Route Table.
48. Verify that the IP address that is assigned to the client user tunnel is displayed on the table as a host route (for example, 20.20.0.40/24).

We encourage you to further explore the named Address Pool and Client Address Redistribution features. A suggestion would be to terminate the user tunnel and verify that the IP address that had been assigned to the user tunnel has been removed from the IP Forward Table and Route Table.

Lab Summary

This lab demonstrated the configuration and use of Client Address Distribution (CAR), as well as its various options. Also demonstrated was the use of named Address Pools and their use in controlling users who are members of a group that is using an assigned address pool. The chapter covered the ability of the Nortel VPN Router to route and control traffic flow from a group of addresses that were not bound to any of its physical interfaces, and discussed the possible increase of security for the Private LAN by utilizing these addresses.

Summary

This chapter has provided you with basic instructions on configuring your VPN Router. Upon successful completion of this chapter, you should have a much better understanding of the capabilities of your Nortel VPN Router. The completion of this chapter should also help you build confidence in the browser-based interface and its use.

Now that you have a greater understanding of the VPN Router and its capabilities, you must understand how to troubleshoot network problems. Chapter 12 discusses not only troubleshooting general network data flow issues, but also troubleshooting VPN Router–specific issues.

CHAPTER 12

Troubleshooting Overview

In data communications, one thing is guaranteed: Problems do occur in data networks. Sometimes these problems are created by an individual or group of individuals. Sometimes these problems occur because of environmental issues. Regardless of *why* problems occur, they *do* occur. Being able to effectively diagnose a problem and reach a resolution is paramount.

When performing network troubleshooting, it is very easy to follow a single path and to forget some of the other contributors to the problem. Quite often, the problem is more in-depth than it appears from the beginning.

Knowing what tools are available to the network administrator can greatly increase the effectiveness in diagnosing problems in a network. Additionally, several proactive steps can be taken to reduce some of the pain when a network problem occurs.

Because other issues may arise that are causing issues with the VPN Router and its performance, it is important to understand some basics of network troubleshooting. This chapter discusses some of these basics, and provides an overview of troubleshooting problems with the VPN Router.

NOTE **In several parts of this chapter, some third-party troubleshooting applications and tools are discussed. Several examples are listed for many of these tools and applications. The examples are for reference only and are not an endorsement of those products.**

Overview of Network Troubleshooting

As noted previously, network problems will occur, and they can occur for many reasons. These issues can range from power outages to vendor compatibility issues. Knowing and understanding the tools that are available to you, as well as the answers to a few basic questions, can be instrumental in resolving the network problems as quickly and painlessly as possible. Following are some questions to consider when faced with an operational issue on the network:

- Is the problem related to a change that is occurring (or has recently occurred) on the network?
- Has the problem occurred before?
- Is the problem causing an outage or is redundancy built in place?
- How vital are the applications and users that are affected by the problem?
- Is the problem local to an individual subnet, or is it related to multiple subnets?
- Is the problem related to an individual network node, or multiple nodes?
- Can you localize the source of the problem?
- What are the users complaining about? What applications/services are affected?

Knowing what to ask and getting the answers to your questions will increase your effectiveness in resolving your problem.

Logical Steps

When a networking issue arises and it is brought to your attention, it is very important to take a few logical investigative steps before you start making changes. If you are not careful, you can create even more problems by making changes before you have a good, firm understanding of the problem and its source.

Make Sure You Understand the Problem

When a problem arises within a network, it is an issue because a user or multiple users are having problems reaching a service or an application. It is important to understand, from the user's point of view, what the problem is. Are the users unable to access anything on the network, or is the problem that they cannot access a particular application that resides on the network?

Always remember that most issues within a network result from a problem with the physical connection or with a node that has malfunctioned. Of course, other issues can cause problems within a LAN, but these are the most common causes of problems.

Following are some questions that should be considered when gathering information to understand the problem:

- Are the users normally allowed access to the application or services that they are attempting to connect to?
- Is the user's workstation configured correctly?
- Is the user's workstation experiencing a hardware issue?
- Are the device/devices that are involved in the issue configured correctly?
- Have there been any recent changes?

Diagnosing the Problem

Once you have an understanding of the problem, the next step is to diagnose the problem. Initiate testing to see what layer within the OSI Reference Model is affected. Determine what user, or group of users, is affected. It is important that you determine the level of impact when diagnosing the problem.

It is also important to keep an open mind when diagnosing the problem. Take everything into consideration before formalizing you diagnosis. Far too often, a network administrator heads down the wrong track when diagnosing a problem, causing a delay in the resolution or compounding the issue.

When diagnosing a problem, ensure that you answer some basic questions that will assist you in gathering as much information as possible. Following are some sample questions:

- What do you know about the problem?
- What other factors must be considered?
- What testing can be performed on the affected equipment to help resolve the problem?
- If the devices involved in the problem subnet have logging capabilities, what are you able to determine about the problem from the data contained within the logs?

Testing

Generally, a problem must be proven or be replicated to be an actual problem. If you experience a momentary lapse of connectivity, and then connectivity is restored, the best thing to do is to wait to see if the problem arises again. Of

course, if the device that had the momentary loss has logging capabilities, then the event log can give insight as to whether or not there is an actual problem.

Occasionally, you may experience an intermittent problem, but it is hard to determine when the problem will arise again. In this case, you can utilize a network management station or a network sniffer to try to nail down the problem as it occurs.

When testing a problem within your production network, you will need to ensure that you have some basic equipment with you. Some examples of network troubleshooting equipment include the following:

- A laptop computer
- A network sniffer, or sniffer software
- Appropriate console cables for the affected devices
- Topology diagrams
- Documentation for the devices that are being tested
- Cable tester

Reaching a Resolution

Often, network issues can be fairly simple to resolve. There are times, however, when the symptoms are misleading and problem resolution may take more time. An open mind and a level head are very helpful in quickly determining and resolving network issues. It's also very helpful to engage other professionals to assist. Brainstorming can be a very effective tool.

There are many variables that might cause issues within your network. Understanding the network and historical documentation of network issues can help in reaching a solution to a problem. Solutions are often variable and each problem can present challenges that have may not have been encountered before. Following are some examples of common solutions to network problems:

- Software upgrade
- Hardware upgrade
- Network traffic load-balancing
- Hardware replacement
- Changes introduced by another group
- Problems related to another group
- Network redesign to accommodate traffic pattern changes and network growth

TCP/IP Utilities

The TCP/IP protocol suite is one of the most used protocol suites in networking today. Most data equipment supports the TCP/IP protocol suite. All nodes that support TCP/IP contain a few basic tools that can assist in troubleshooting issues within a network.

This section discusses some of these tools. The examples provided will be from a Windows OS perspective, although any TCP/IP-supported node (including the Nortel VPN Router) has the capability to obtain the same data. All the tools discussed in this section are accessible on a Windows computer via the MS-DOS window. Following are the tools that are discussed:

- Ping
- Traceroute
- Route
- Netstat
- IPconfig

Ping

Developed in 1983, the Ping command utility is probably the most commonly used network troubleshooting diagnostic tool. Most TCP/IP applications support the `ping` command. It was originally designed to troubleshoot issues within a network.

The acronym "Ping" stands for Packet Internet Grouper, but was originally named for the sounds that are made by sonar, which is used in submarines to detect other vessels under water. The name "Packet Internet Grouper" came later on.

The purpose of Ping is to send a message from one TCP/IP system to another TCP/IP system to see if the network layer is functioning as expected. Ping sends an echo request from one node to another. The node that is being "pinged" will send an echo reply to the originating node.

The Ping command is not as useful as it used to be. Beginning in 2003, many Internet service providers (ISPs) started filtering out the ICMP type 8 packets (echo requests) to reduce the probability of an Internet worm virus flooding the ISP's LAN.

To issue the `ping` command from a Windows operating system, you must access an MS-DOS utility. This can be done by going to the Start menu and clicking Run, as shown in Figure 12-1.

Once you have clicked the Run command, the Run dialog box opens. This window can be used to initiate any executable file within your Windows

system. All Windows systems have a Ping utility loaded within its system directly. You can simply issue the command within the Run dialog box, but once the replies have all been received, the Ping utility will complete. Its best to enter **command** in the Run dialog box. This open an MS-DOS session. Figure 12-2 shows an example of the Run dialog box.

Once you have entered the MS-DOS window, you simply have to type **ping** followed by the IP address of the node that you are testing for reachability. For example, if you are testing whether or not a node can reach the IP address 216.109.112.135, you would type **ping 216.109.112.135** from the `C:\` prompt. If you receive a reply, then the connection is good. For example:

```
C:\>ping 216.109.112.135

Pinging 216.109.112.135 with 32 bytes of data:

Reply from 216.109.112.135: bytes=32 time=22ms TTL=48
Reply from 216.109.112.135: bytes=32 time=23ms TTL=48
Reply from 216.109.112.135: bytes=32 time=23ms TTL=48
Reply from 216.109.112.135: bytes=32 time=21ms TTL=48

Ping statistics for 216.109.112.135:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum =  23ms, Average =  22ms
```



Figure 12-1: The Windows Run command

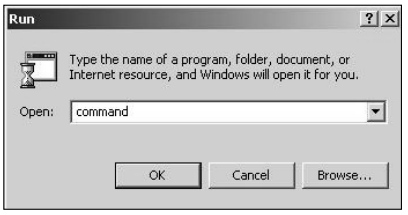


Figure 12-2: Issuing the command to enter the MS-DOS window via the Run dialog box within the Windows OS

In this example, you can see that you are able to reach the node that you were searching for. The tested node has sent back echo replies, which are output to the screen within your MS-DOS session. In the following example, the tested node is not available:

```
C:\>ping 216.249.48.1

Pinging 216.249.48.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 216.249.48.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

In this example, it was determined that you are not able to reach the tested node and you can assume that this is either a non-existent IP address, or that there is a problem or a reason that you are not able to reach this node.

The Ping utility in a Windows environment has a few optional parameters that can be used to gather some additional information. To use one of these optional parameters, you simply add a minus (-) and then the letter for the parameter that you would like to use. These options are shown in Table 12-1.

Table 12-1: Ping Utility Options

OPTION	DESCRIPTION
`-a`	Resolve addresses to host names
`-f`	Set Don't Fragment flag in packet
`-i <TTL>`	Time-to-Live (TTL)
`-j <host-list>`	Loose source route along host-list
`-k <host-list>`	Strict source route along host-list
`-l <size>`	Send buffer size
`-n <count>`	Number of echo requests to send
`-r <count>`	Record route for count hops
`-s <count>`	Timestamp for count hops
`-t`	Continuous
`-v <TOS>`	Type Of Service
`-w <timeout>`	Timeout in milliseconds to wait for each reply

You might use an optional parameter, for example, if you need to issue a continuous `ping` to test when a connection drops or when a node comes up. To issue a continuous `ping`, your syntax would be as follows:

```
C:\Ping 216.249.48.1 -t
```

Traceroute

Traceroute is another helpful tool that is supported by TCP/IP nodes. What the traceroute utility does is trace a packet's path from a source node to a destination node.

In a Windows Command Line Interpreter (CLI) session, the traceroute tool is invoked by typing the command **tracert** followed by the IP address of the node that you are trying to reach. For example, if you want to trace the route from your PC to the IP address 216.109.112.135, you initiate the MS-DOS window and enter the command as follows:

```
  C:\>tracert 216.109.112.135

Tracing route to w2.rc.vip.dcn.yahoo.com [216.109.112.135] over a
maximum of 30 hops:


  1    11 ms     8 ms     7 ms  110.212.208.11
  2     8 ms      9 ms    9 ms  168.187.153.193
  3    10 ms    11 ms     9 ms  168.187.144.161
  4    10 ms     9 ms     9 ms  168.187.144.157
  5    12 ms    10 ms    11 ms  121.118.188.15
  6    25 ms    25 ms    26 ms  121.122.81.118
  7    32 ms    31 ms    31 ms  tbr2-cl16.n54ny.net [121.122.10.221]
  8    26 ms    23 ms    28 ms  tbr1-cl23.n54ny.net [121.122.9.120]
  9    23 ms    25 ms    24 ms  tbr1-cl8.pa.ip.net [121.122.12.118]
 10    24 ms    24 ms    23 ms  tbr2-cl71.pa.ip.net [121.122.9.66]
 11    25 ms    24 ms    23 ms  tbr1-cl9.wswdc.ip.net [121.122.12.8]
 12    22 ms    25 ms    21 ms  gar1-p.ascva.ip.net [121.123.18.149]
 13    36 ms    22 ms    23 ms  msr1.dcn.yahoo.com [216.115.96.181]
 14    23 ms    23 ms    22 ms  msr1.dcn.yahoo.com [216.109.120.207]
 15    21 ms    20 ms    29 ms  vip.dcn.yahoo.com [216.109.112.135]

Trace complete.
```

In this example, the packet passed through 14 nodes before reaching the destination. Each line produced provides information about the roundtrip time between nodes, the DNS name of the node, and the IP address of the node.

All of this information is extremely helpful when troubleshooting. It can provide you information about the time it takes to get to a node, as well as whether or not the node is reachable.

The traceroute utility in a Windows environment has a few optional parameters that can be used to gather some additional information. To use one of these optional parameters, you simply add a minus (–) and then the letter for the parameter that you would like to use. These options are shown in Table 12-2.

Traceroute works by incrementing the TTL value for each successive packet that is sent. When a packet reaches a host node that is in the path to the destination, the host node will reduce the TTL value by 1 before passing the packet to the next node. Once the packet has a TTL value of 1, the host node will send an ICMP time-exceeded packet to the originating node. The originating node will then generate a list showing what hosts the packet reached on its way to a destination.

In other words, the packet destined for the first node will have a TTL of 1. The first node receives the packet, reduces the TTL by 1, and then sends the ICMP time-exceeded message to the originator, which will log this information to the screen. The originator then will send the next packet with a TTL of 2. The first node receives the packet, reduces the TTL by 1, and then forwards it to the second node. The second node now receives the packet with a TTL of 1 and then sends the message to the originator. This process continues until the destination node is reached, or the connection times out.

Although the traceroute utility can be helpful, it is important to realize that there can be a lot of redundancy built into networks, and that just because a packet takes a particular path one time, that does not mean it will take the same path a second time. Usually, when troubleshooting LAN-related issues, the packet will take the same path, but it may take a different path, and this may need to be considered.

Table 12-2: Traceroute Options

OPTION	DESCRIPTION
`-d`	Do not resolve addresses to host names
`-h <maximum_hops>`	Maximum number of hops to search for target
`-j <host-list>`	Loose source route along host-list
`-w <timeout>`	Wait timeout milliseconds for each reply

Routing Tables

The `route` command in MS-DOS allows you to add, remove, and view route information in the routing table. Most layer 3 network nodes also provide you with routing table information. The routing table is very useful when troubleshooting your network

In an MS-DOS window, you can view, add, or delete the route information by using the `route` command, followed by the appropriate subcommand or optional parameter. The syntax for the route command is as follows:

```
C:\>route <-f/-p> <command> <destination> Mask <netmask> <gateway>
<metric> <interface>

<-f/-p>

-f          Clears the Routing table
-p          ensures persistency of the route

<Command>

Print     Used to print the routing table to screen
Add     Used to add a route
Delete     Used to delete a route
Change     Used to modify a route

<destination>     Specifies the host node
<netmask>          Subnet mask
<gateway>          The default gateway
<metric>          Cost to the destination node
<interface>     The interface to the destination
```

One of the most commonly used optional parameters is the `print` command, which is used to view the current routing table information for the PC workstation that you are using. Following is an example of the command and its output:

```
C:\>Route print

===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...44 45 53 54 42 00 ...... NOC Extranet Access Adapter
0x3 ...00 10 b5 65 4d 1a ...... NDIS 5.0 driver
===========================================================================
===========================================================================
```

```
Active Routes:
Ntwk Dest      Netmask          Gateway        Interface       Metric
 0.0.0.0       0.0.0.0          192.168.1.1   192.168.1.100     1
127.0.0.0      255.0.0.0        127.0.0.1     127.0.0.1         1
192.168.1.100  255.255.255.255 127.0.0.1     127.0.0.1         1
Default Gateway:       192.168.1.1
===========================================================================
Persistent Routes:
  None
```

Netstat

The Netstat utility provides you with information about the current operating status for multiple protocols within your network traffic. Like the other commands discussed thus far, the `netstat` command in a Windows environment has a few optional parameters that can be used to gather some additional information. To use one of these optional parameters, you simply add a minus (-) and then the letter for the parameter that you would like to use. These options are shown in Table 12-3.

Probably the most helpful of these optional parameters is the `-s` parameter, which provides you with statistical information for each of the major protocols within TCP/IP. An example of this follows:

```
c:\>netstat -s

IP Statistics

  Packets Received                   = 52045
  Received Header Errors             = 0
  Received Address Errors            = 0
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 0
  Received Packets Delivered         = 52045
  Output Requests                    = 48287
  Routing Discards                   = 0
  Discarded Output Packets           = 4
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMP Statistics
```

```
                          Received    Sent
  Messages                0           0
  Errors                  0           0
  Destination Unreachable 0           0
  Time Exceeded           0           0
  Parameter Problems      0           0
  Source Quenches         0           0
  Redirects               0           0
  Echos                   0           0
  Echo Replies            0           0
  Timestamps              0           0
  Timestamp Replies       0           0
  Address Masks           0           0
  Address Mask Replies    0           0

TCP Statistics

  Active Opens                        = 1508
  Passive Opens                       = 4
  Failed Connection Attempts          = 10
  Reset Connections                   = 376
  Current Connections                 = 0
  Segments Received                   = 45440
  Segments Sent                       = 42352
  Segments Retransmitted              = 14

UDP Statistics

  Datagrams Received    = 6589
  No Ports              = 16
  Receive Errors        = 0
  Datagrams Sent        = 5919
```

Table 12-3: Netstat Options

OPTION	DESCRIPTION
-a	Displays all connections and ports that are listening
-e	Displays all Ethernet statistics
-n	Displays all addresses and port numbers
-p <proto>	Displays connections for the specified protocol
-r	Displays the routing table
-s	Displays statistics for each protocol
<interval>	Reissues the command pausing the specified interval before repeating

IPconfig

The IPconfig utility allows you to see the system's TCP/IP configuration. This is helpful if you are allowing DHCP to assign addresses to nodes, and you must determine the TCP/IP configuration of the workstation that you are on.

The IPconfig utility in a Windows environment has optional parameters that can be used to gather some additional information. To use one of these optional parameters, you simply add a forward slash (/) and then the letter for the parameter that you would like to use. These options are shown in Table 12-4.

To view the TCP/IP configuration of the Windows workstation, you enter the command **IPconfig** at the `C:\` prompt in an MS-DOS window. For example:

```
C:\>IPconfig

Windows 2000 IP Configuration

Ethernet adapter {XXXXXXX8-4XXX-4XXX-XXXX-XXXXXXXXXXXX}:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : hsd1.pqn.net.
        IP Address. . . . . . . . . . . . : 192.168.1.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
```

Other Troubleshooting Tools

In addition to the utilities discussed in the previous section, some optional tools can be used that can save a lot of time and trouble when trying to narrow down the source of a connectivity problem. These tools include the following:

- A *packet sniffer* captures data packets and sorts the information based on user-controlled parameters to allow for the analysis of data that is transmitted in the network.
- A *cable tester* is a tool that allows for the testing of the physical cabling in the network to determine if there are any defects.
- A *network management station* can provide dynamic statistical information about your network, and can alert you to problems as soon as they arise.

Table 12-4: IPconfig Options

OPTION	DESCRIPTION
`/?`	Displays help information
`/all`	Displays full configuration information
`/release`	Releases the IP address for the specified adapter
`/renew`	Renews the IP address for the specified adapter
`/flushdns`	Purges the DNS Resolver cache
`/registerdns`	Refreshes all DHCP leases
`/displaydns`	Display the contents of the DNS Resolver cache
`/showclassid`	Displays all the DHCP class IDs allowed for adapter
`/setclassid`	Modifies the DHCP class ID

Packet Sniffer

A packet *sniffer* (also known as a *network analyzer* or a *protocol analyzer*) is used to capture data that is being transmitted on a network. The sniffer can be hardware- or software-based.

The sniffer captures data that is being transmitted within the area it is configured to capture from. This data will be saved into a file and is normally referred to as a *sniffer trace*. The sniffer then analyzes the data and sorts it based on the appropriate specifications that are set forth. Figure 12-3 shows an example of a sniffer trace that captures DHCP traffic.

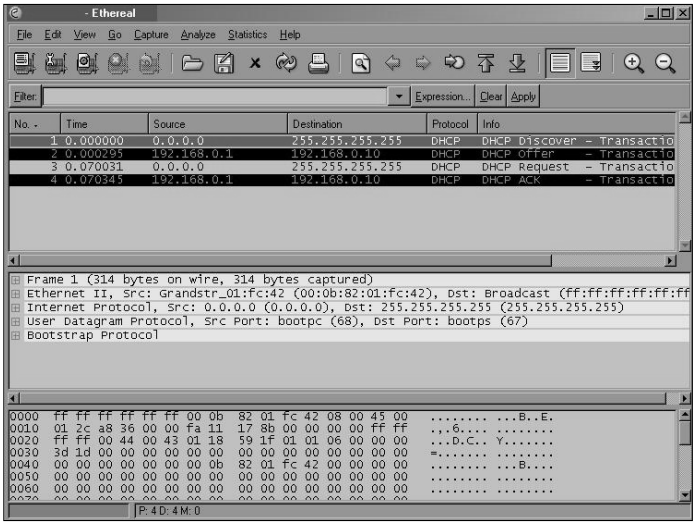


Figure 12-3: Example of a sniffer trace that contains DHCP traffic

The sniffer can be set up to capture all traffic or just portions of traffic that is being transmitted. It can also be set to capture data that meets only specified criteria (based on RFC or other specification). A single workstation can be used throughout the network to capture data. Following are some of the common uses for a packet sniffer:

- Detecting network intrusion attempts
- Troubleshooting data-transmission problems
- Managing network utilization
- Monitoring traffic patterns
- Gathering statistics
- Monitoring network activity

From a troubleshooting perspective, the packet sniffer can determine if a packet is reaching its destination and whether or not the destination is responding. It can also determine if a device or an interface is generating excessive messages, or if the amount of traffic is more than there is available bandwidth for.

Many software-based sniffers are available today. Some of these can be downloaded free of charge. Here are a few of them:

- *Ethereal:* `www.ethereal.com`
- *Tcpdump:* `www.tcpdump.org`
- *Windump:* `www.winpcap.org/windump`

Cable Testing

A *cable tester* is a troubleshooting device that is used to test the cables within a data network. It is able to determine if there is a break or a defect in the cable, as well as monitor the cable for traffic congestion and collisions on the line.

Cable testers vary in price, depending upon the needs of the network. Although not necessarily required to perform network troubleshooting, an investment in one may save problems and headaches later down the road. Having a cable tester for use when troubleshooting allows a network administrator to test cables to determine if they are the root cause of a connectivity issue before you begin troubleshooting other hardware and devices in the problem subnet.

A cable tester can be a standalone hand-held unit, or can be a PC-based peripheral unit. It all depends on the needs of the network and the purpose that the tester will be serving. There are multiple vendors of cable testing equipment and a multitude of options to choose from, so ensure that you research before you buy.

Network Management Station

The *network management station* is the first place to go to verify the health of your network. A network management station is a combination of hardware and software used together to monitor and manage a network. A typical network management station is a PC, with the appropriate network management software, that is dedicated to monitoring the status of the network.

The network management application will provide a graphical representation of the nodes on your network and will notify you if any events occur that are not normal. Figure 12-4 shows just one example of the type of interface you can get through a typical network management station screen.

The network management station should allow you to view network configuration and allow you to obtain various views of the network to simplify the understanding of the physical network. It should also have logging and reporting ability, to assist in managing the network and addressing issues in a more proactive fashion. Many other options are available to meet the needs of most any network manager or administrator. Figure 12-5 shows an example of a reporting statistical graph that is being captured on a network management station's screen.

Most network management stations utilize colors to alert you to problem nodes. IP address information normally resides on the screen, so it is easy to quickly narrow down the problem area, and reach a quick resolution.

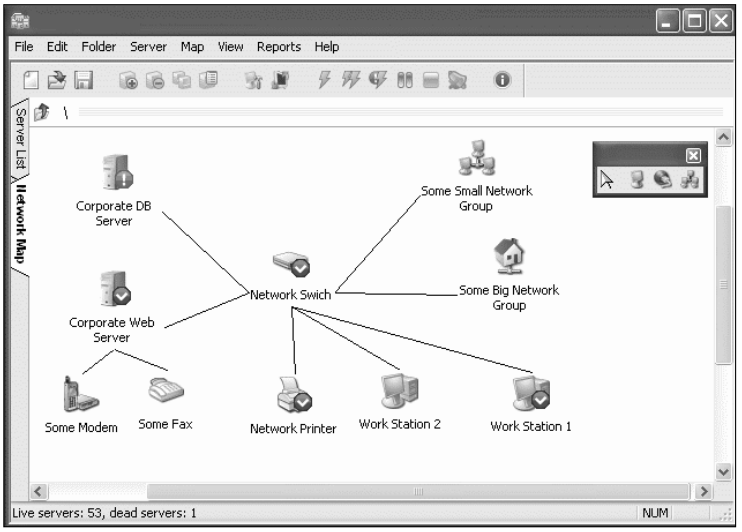


Figure 12-4: Example of a network management screen that shows the monitoring of nodes within the network

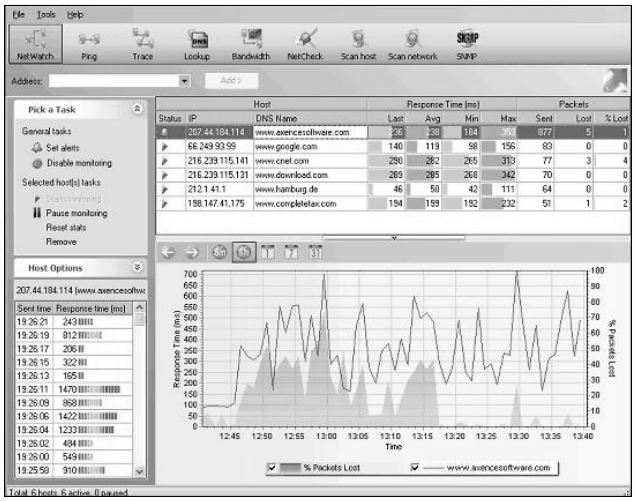


Figure 12-5: Capturing statistics with the network management station and reviewing a graph with the captured information

There are many different network management vendors, each providing several options. Determine what the needs are for your network and purchase a system that can accommodate those needs. In you planning, remember to anticipate future requirements as well.

Following are some common network management systems:

- Alcatel 5620 Network Manager
- Crannog Software Netwatch
- Equator One
- HP Openview
- IBM Tivoli

Nortel VPN Router Troubleshooting

Troubleshooting issues within the Nortel VPN Router can, at times, present a real challenge even for the seasoned professional. Because of all of the features that the router supports, often there are a lot of other variables that may be contributing to, or even causing, the issues that the end users are experiencing.

Fortunately, the Nortel VPN Router contains several tools and utilities that can assist in troubleshooting connectivity issues. There are several log features, as well as TCP/IP utilities and statistical information that can present data helpful to the resolution of data traffic issues.

So far, this chapter has discussed tools to troubleshoot general network communication issues. This section discusses troubleshooting from the VPN Router perspective. This information should greatly improve your ability to reach timely resolution to problems you might encounter when administering the Nortel VPN Router.

Tools

As with general network troubleshooting, several tools and/or utilities are very important to have available when performing troubleshooting and diagnosis of the Nortel VPN Router. Without these, the resolution time for connectivity issues will be severely hampered, if not impossible.

Proactively ensuring that all individuals who are involved in the management of your VPN Router have these tools available to them will guarantee their effectiveness to get connectivity restored for the end users. These tools include the following:

- Console cable
- Crossover Ethernet cable
- System recovery disk
- Laptop
- Nortel VPN Client software
- Terminal emulator (HyperTerminal)
- Access to an FTP server
- FTP client software

Console Cable

A *console cable* is simple a serial cable that is used to obtain a direct connection between your PC and the VPN Router. The console cable uses the RS-232 standard of communication between devices, where data is transferred sequentially one bit at a time over the communications channel. This is known as *serial communication.*

Each end of the console cable has a DB-9 connector (see Figure 12-6).

NOTE Some versions of the VPN Router use a DB-9 to RJ-45 connector. Figure 12-7 shows an example of this cable.



Figure 12-6: The connector at the end of a console cable

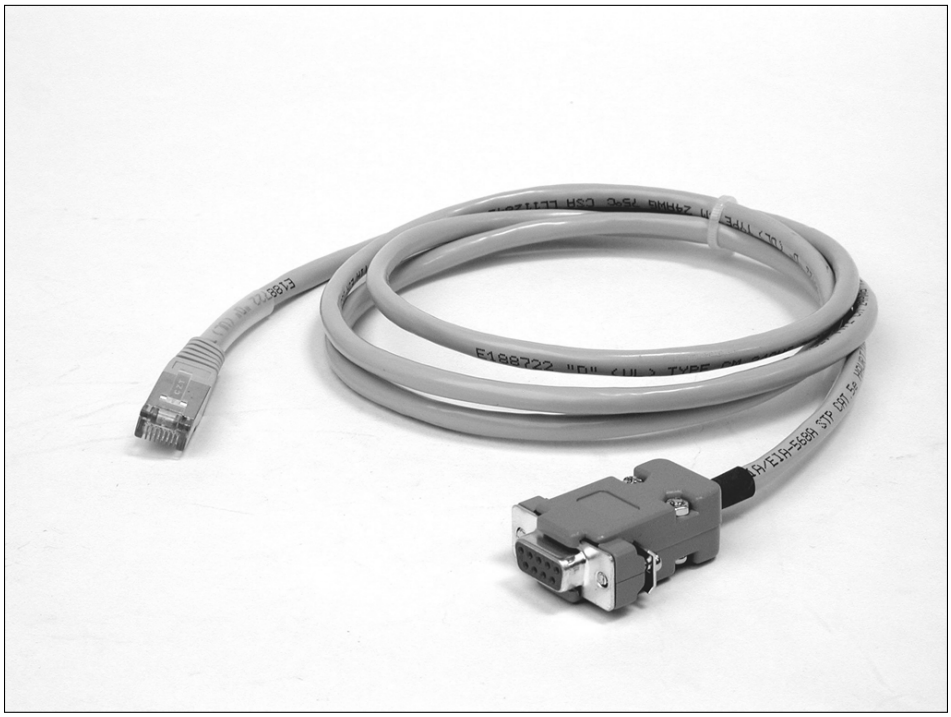


Figure 12-7: Optional console cable connectors

One end of the console cable is connected to the serial port on the PC and the other connects to the serial port on the VPN Router. A connection can then be made via the HyperTerminal application, or any terminal emulator.

Console access to the VPN Router will allow you to troubleshoot through the CLI or serial menu. You can also make necessary configuration changes through the use of the console cable.

Crossover Cable

Ethernet cables follow the 10BASE-T and 100BASE-TX standards for data communication. Each wired pair contained in the cable transmits data in each direction. The standard requires that the RJ-45 connections be placed where the transmit pair on one end of the cable is transformed to the receive pair on the other end of the cable. This is considered a *straight-through cable* where the wiring pin connectors on one end correspond to the wiring pin connectors on the other end of the cable. This is the type of cable that is used when you are connecting two terminal devices together with a hub or a switch in between the devices.

When you are required to connect a terminal device directly to another terminal device, a *crossover cable* is required for communication between the two. The crossover cable basically flips pairs two and three of the wired pairs to the opposite ends, so each end would be an opposite of the other.

NOTE When you are connecting a hub or a switch to another hub or switch, a crossover cable is required.

While troubleshooting VPN Router issues, sometimes it is necessary to isolate the router and obtain a direct connection to your laptop. The crossover cable is used so you can obtain an Ethernet connection to the VPN Router in order to use the browser-based interface for troubleshooting and configuration.

System Recovery Disk

A *system recovery disk* is simply a floppy disk that contains recovery software in case of catastrophic failure of the VPN Router. The recovery disk can be created via the browser interface within your VPN Router software. It is highly recommended that you make a recovery disk as soon as you set up your VPN Router. It is also important to make the recovery disk when you upgrade software on your VPN Router.

NOTE Some versions of the VPN Router do not have a hard drive and, therefore, cannot support the recovery disk option. For these versions, there is a recovery button that will support VPN Router recovery.

To make a recovery disk, place a floppy disk in the floppy disk drive port of your VPN Router. Connect to the management IP of your VPN Router and log in to the browser interface. Once the main menu comes up, go to ADMIN → RECOVERY. This will bring you to the Create Recovery Diskette screen of the Web interface, as shown in Figure 12-8.

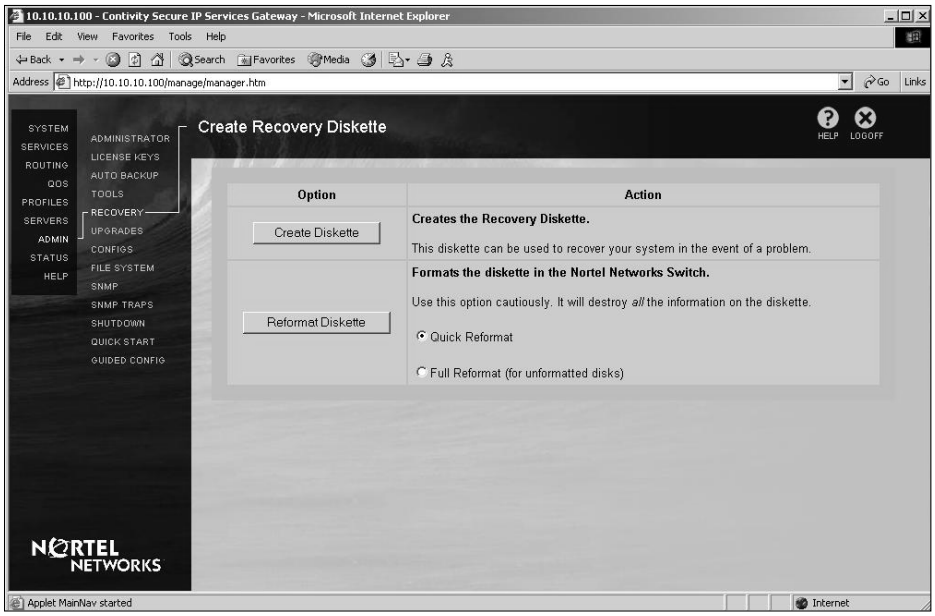


Figure 12-8: The Create Recovery Diskette screen

At the Create Recovery Diskette screen, you have two options. You can create a recovery disk or you can reformat the diskette. We recommend that you reformat the diskette. Reformatting removes all data files from the diskette and presents you with a clean disk to write to. Once you have reformatted, select the Create Diskette option of the menu. Simply follow the prompts to create the recovery disk.

Once you have completed creating your recovery disk, be sure to label it and then put it in a place that is physically local to the VPN Router. Many users prefer to keep it in the disk drive, just not completely inserted. If you have lab security in place, you are more than welcome to choose this option.

For troubleshooting purposes, the recovery diskette is very important. It is required to recover the VPN Router when all other options are exhausted. Therefore, it is important to not only make a recovery disk, but also to ensure it is available to whoever is onsite for troubleshooting.

Laptop

A *laptop computer* (also known as a *notebook computer*) is an extremely helpful tool when troubleshooting within the network. A *desktop computer* or a *dumb terminal* that is physically local to the equipment can also be used. Because a laptop is mobile, it is preferred because it is easy to move from area to area within the LAN for network maintenance and troubleshooting.

Because there are a lot of things that may need to be analyzed when you are troubleshooting VPN issues, it is important to have the laptop loaded with all software that you normally would use when maintaining and configuring your network devices. From a Nortel VPN Router perspective, at a very minimum, it is important to have the following applications:

- A version of the Nortel VPN Client that is compatible to the software running on the router
- A terminal emulator
- Microsoft Internet Explorer or compatible network browser
- TCP/IP support

Because you will be using the laptop for troubleshooting purposes, the laptop should have the appropriate hardware interfaces as well. The following are required:

- Serial interface
- Ethernet interface

Nortel VPN Client

The Nortel VPN Client has been discussed previously in this book. It is a very important troubleshooting tool when testing user connectivity issues.

Ensure that you are running the proper version of VPN Client for the VPN Router software that you are running. If running an incompatible version, ensure that you make the proper adjustments for optimal performance.

When troubleshooting VPN user connectivity issues, it is important that the VPN users are running the correct version of VPN Client as well.

Terminal Emulation (HyperTerminal)

A *terminal emulator* is software that provides an interface that emulates a "dumb" terminal. Most emulation software contains other options that enhance the user's capabilities.

The terminal emulator is an application that allows the user to access the command line of a node. You can use the terminal emulator to access a device via Telnet, SSH, or modem dial-up. When connecting to the Nortel VPN Router, you will use the terminal emulator when accessing the VPN Router via the console interface.

NOTE **Most terminal emulators have the ability to connect to a device via TCP/IP. When choosing this option, you can use the terminal emulator to Telnet to a device. This is very helpful when troubleshooting because it will allow you to log your sessions for data-preservation purposes.**

Standard with a Windows OS PC is an application that was discussed previously in this book. The HyperTerminal emulator is a very useful tool to have available when troubleshooting issues with the VPN Router. Figure 12-9 shows an example of the HyperTerminal application interface.

Following are some well-known terminal emulators available today:

- HyperTerminal
- PuTTy
- SecureCRT

FTP Server

The File Transfer Protocol (FTP) is responsible for exchanging files over a network. The FTP server can be either a PC that is dedicated to the transfer of data files, or it can be a software program that runs as a daemon on a PC.

The *FTP server* simply "serves" files to FTP clients that are requesting the data. It is extremely helpful in data networking when transferring large files. Figure 12-10 shows an example of an FTP Server application running on a PC.

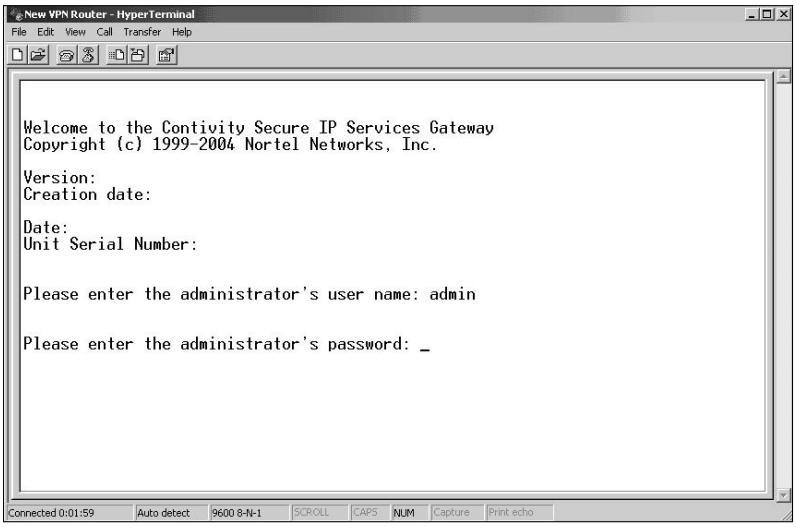


Figure 12-9: The HyperTerminal terminal emulator interface

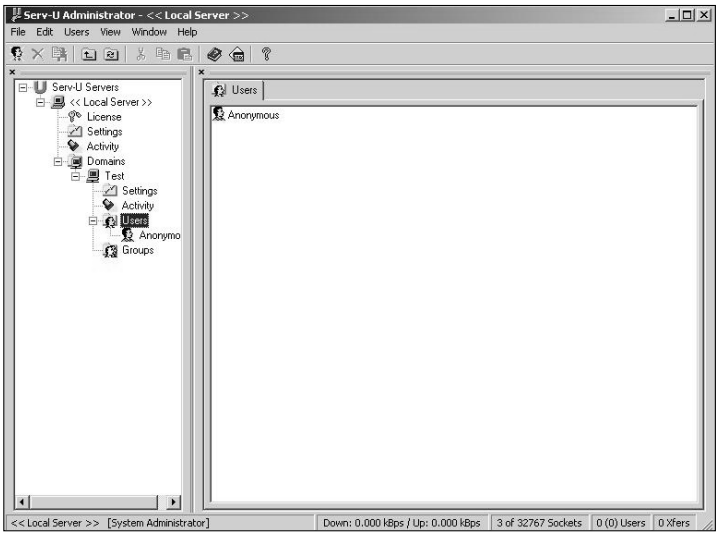


Figure 12-10: An FTP Server application interface on a Windows PC

When troubleshooting issues with your VPN Router, it may be necessary that you have access to an FTP server. This will allow you to retrieve software images, transfer event logs and data core files, and transfer screen captures of data gathered.

Following are some examples of FTP servers:

- Serv-U FTP server
- BulletProof FTP server
- Microsoft FTP server
- FileZilla server

FTP Client

The *FTP client* is required for communication with the FTP server. Most operating systems contain a text-based version of an FTP client as a standard application. Some Web browsers have an FTP client built-in as well. Figure 12-11 shows an example of the Windows/MS-DOS text-based FTP client.

When troubleshooting issues with your VPN Router, it may be necessary for you to receive and send large file transfers between yourself and others, as well as between yourself and the VPN Router. An FTP client application is required to do this. For software retrieval, the Nortel VPN Router will act as a client.

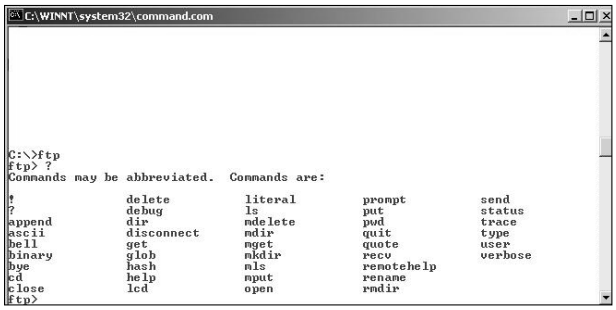


Figure 12-11: Using ftp.exe for file transfer

Following are some examples of FTP clients:

- CuteFTP
- FileZilla
- FTP Surfer
- WS_FTP
- MS-DOS `ftp.exe`

VPN Router System Recovery

Sometimes the VPN Router will have a catastrophic failure and will need to have intervention to recover. The VPN Router supports system recovery in one of two ways:

- *Recovery diskette:* Used by the Nortel VPN Routers that have a hard drive onboard. These are also known as the *disk-based version* of the VPN Router family.
- *Recovery pushbutton:* Used by the Nortel VPN Routers that do not have a hard drive onboard. These VPN Routers are known as the *diskless version* of the VPN Router family.

The previous section discussed how important it is to make and have available a recovery disk for your VPN Router. This section discusses how to use that recovery disk to do the following:

- Restore the VPN Router to factory defaults
- Retrieve system backups to recover to a previous configuration

- Perform a software installation
- Reformat the onboard hard disk drive
- View the files saved on the hard disk drive
- Select and apply a version of code
- View event log entries
- Reboot the VPN Router

System Recovery for Disk-Based Versions

To perform system recovery on a disk-based version of the Nortel VPN Router, you simply have to insert the recovery disk into the floppy drive on the router. Once you have inserted the recovery disk, you boot up the system. The VPN Router boots using the recovery image that is saved on the recovery diskette.

NOTE **Booting to a recovery diskette is a process that takes a while.**

Booting to a recovery diskette does not remove any IP address configurations that you have stored on the VPN Router. Once you have booted to the recovery disk, you can establish a HyperTerminal session to the VPN Router to confirm interface settings. You can also ping the management interface to verify that connectivity has been restored. Figure 12-12 shows an example of the menu options available to you through the serial interface when booted to the recovery image on the recovery diskette.

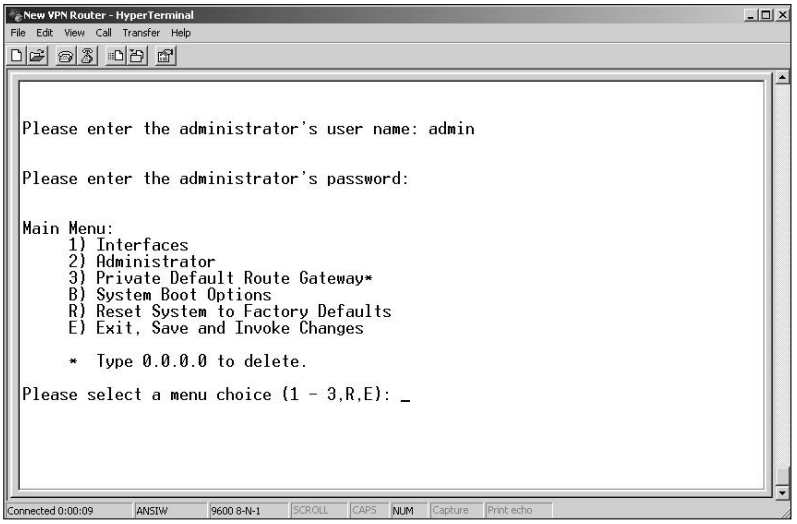


Figure 12-12: The post-recovery serial interface menu

In the example, you can see a limited number of options are available to you in the serial interface menu. This gives you the minimum required configuration parameters for recovering your VPN Router. Following are the options available to you:

- 1) Interfaces
- 2) Administrator
- 3) Private Default Route Gateway
- B) System Boot Options
- R) Reset System to Factory Defaults
- E) Exit, Save, and Invoke Changes

If you have confirmed connectivity with the management IP address (with a successful ping), you do not have to take any action via the serial interface. If you do not have access to the management IP address, then you may need to reconfigure the private addressing schema to connect to the management IP via the browser interface.

Open your Web browser and establish a session with the management IP address. Be patient because it may take a few moments to come up. When the browser interface does come up, you will be presented with several options. Following are the options that you have with the recovery image:

- Restore
- Reformat hard disk
- Apply new version
- Perform File Maintenance
- View event log
- Restart System

System Restore Option

Figure 12-13 shows an example of the top portion of the system recovery image screen. In this section of the screen, you have an option to restore the VPN Router to factory default settings or to restore it using a known good backup of the system configuration and image. You can also use the second option to retrieve an image from disk and load it to a freshly formatted drive.

Once you have selected whether you want to restore to factory defaults or to restore to a backed-up image and configuration, then you simply have to press the Restore button and then follow the instructions that are given on the screen.

Figure 12-14 shows an example of the bottom portion of the system recovery image screen. The remaining options available to you are listed in this example.

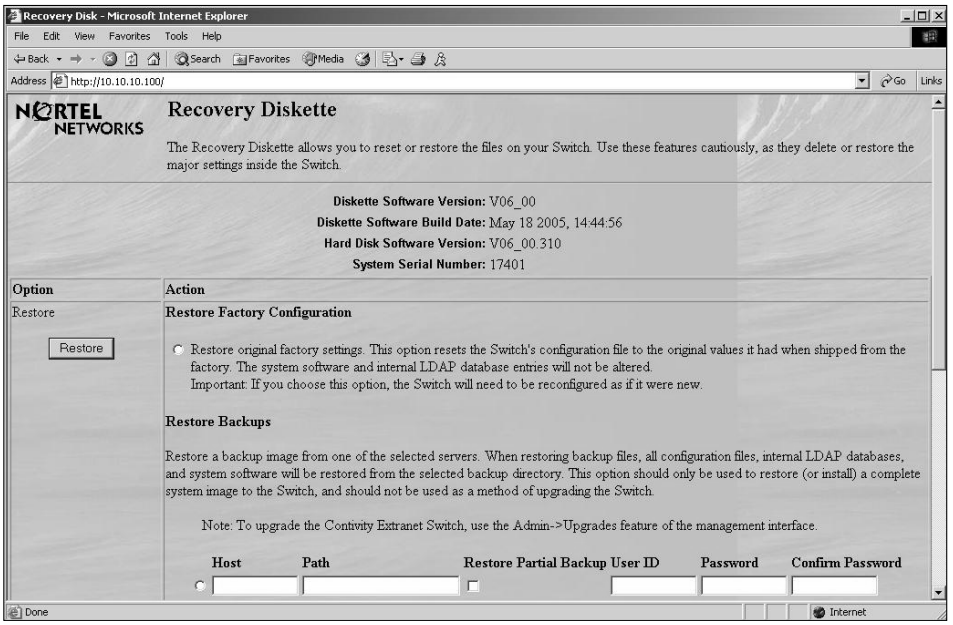


Figure 12-13: The top portion of the system recovery screen

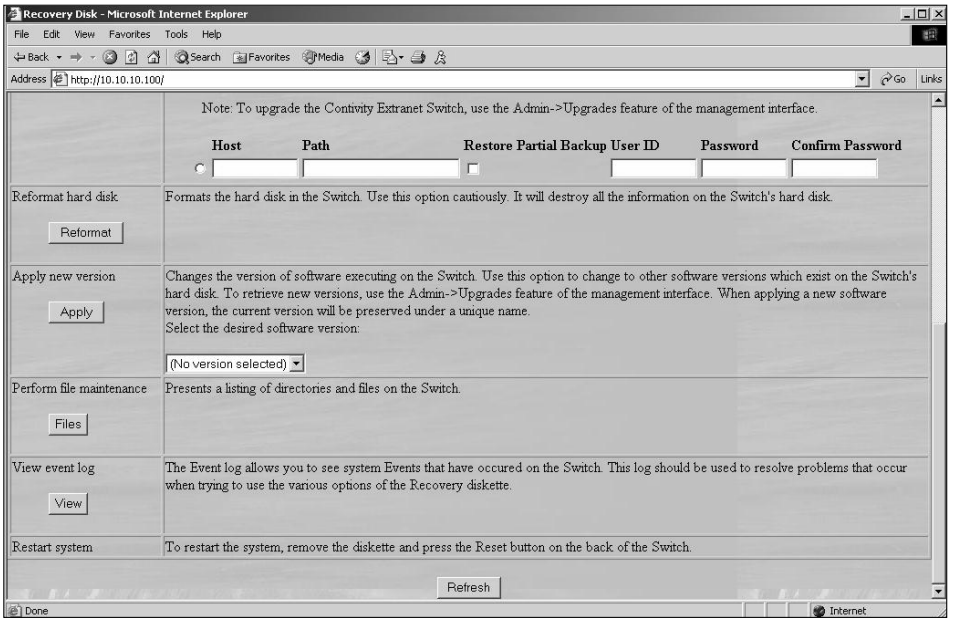


Figure 12-14: The bottom portion of the system recovery screen

Reformat Hard Disk Option

Reformatting the hard disk is an option that will remove all data from the hard disk and will present the user with an empty disk to work with. Reformatting on the Nortel VPN Router means exactly the same thing as reformatting a PC hard disk drive.

Whenever possible, it is a good practice to back up any data information prior to formatting the drive. Of course, there may be instances where this is not possible, but it should be done whenever possible. Following are some examples of instances when a reformat would be necessary:

- You need to configure the VPN Router from scratch.
- You cannot recover the VPN Router by any other means.
- You install a new hard drive.
- You encounter problems retrieving image and/or configuration files.

Apply New Version Option

Selecting this option will allow you to boot the VPN Router with another software version. This option will be available to you only where there is more than one software version loaded on the VPN Router. If there is only one version loaded, there will not be any options to select, and this option will not be available to the user.

This option can be helpful if you have a corrupted software image on the VPN Router. It is also helpful if the router will not boot to the image that it is configured to boot to because of hardware/software compatibility issues.

Perform File Maintenance option

The "Perform file maintenance" option provides the user with the ability to review the data files that are stored on the hard drive of the VPN Router.

This option is helpful when trying to determine if there is any data file corruption, or if there are data files missing. It is also helpful in identifying other files that may have been written and are available to the user.

View Event Log Option

The "View event log" option provides the user with the ability to review the current event log. This option is helpful when troubleshooting system recovery issues.

Restart System

Once you have completed whatever previous option you have chosen, or if you simply want to reboot the VPN Router, you will select this option. Prior to selecting this, you will want to remove the recovery diskette so the VPN Router will boot to the image that is stored within the VPN Router.

This option is helpful because it ensures that all data changes that might be occurring on the VPN Router are completed prior to booting the router. This is the preferred option because turning the unit off and then on may contribute to data corruption. This option is very similar to the Windows shutdown procedures that all Windows users are familiar with.

System Recovery for Diskless Versions

To perform system recovery on a diskless version of the Nortel VPN Router, you simply have to insert a paper clip into the hole on the VPN Router that contains the recovery button. This hole is located on the back of the VPN Router and is labeled "rec." Figure 12-15 shows an example of where the recovery button is located on the VPN Router 1050.

Once you have pressed the recovery button, you will boot up the system. The VPN Router will boot using the recovery image that is stored in Programmable Read Only Memory (PROM) within the VPN Router.

As with the disk-based versions, booting the diskless version to a recovery image will not remove any IP address configurations that you have stored on the VPN Router. Once you have booted to the recovery image, you can establish a HyperTerminal session to the VPN Router to confirm interface settings. You can also ping the management interface to verify connectivity has been restored.

If you have confirmed connectivity with the management IP address (with a successful ping), you do not have to take any action via the serial interface. If you do not have access to the management IP address, then you may need to reconfigure the private addressing schema in order to connect to the management IP via the browser interface.

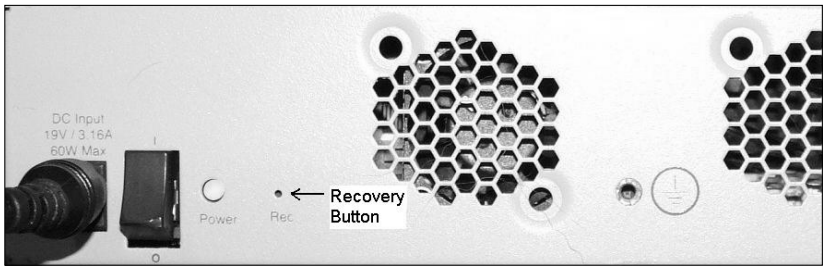


Figure 12-15: The recovery button location on the back of the VPN Router 1050

Open your Web browser and establish a session with the management IP address. When the browser interface does come up, you will be presented with the same options that were available when performing recovery on a disk-based version of the VPN Router. The options are as follows:

- Restore
- Reformat hard disk
- Apply new version
- Perform file maintenance
- View event log

System Restore Option

The restore option provides the ability to restore the VPN Router to factory default settings, or to restore it using a known good backup of the system configuration and image. You can also use the second option to retrieve an image from disk and load it to a freshly formatted drive.

Reformat Hard Disk Option

Reformatting the hard disk removes all data from the hard disk and presents the user with an empty disk to work with. Reformatting on the Nortel VPN Router means exactly the same thing as reformatting a PC hard disk drive.

Apply New Version Option

Selecting this option enables you to boot the VPN Router with another software version. This option will be available to you only where there is more than one software version loaded on the VPN Router. If only one version is loaded, there will not be any options to select, and this option will not be available to the user. Figure 12-16 shows an example of the drop-down menu with code version options.

Perform File Maintenance Option

The "Perform file maintenance" option provides the user with the ability to review the data files that are stored on the hard drive of the VPN Router. Click the Files button to open up the File System Maintenance screen, as shown in Figure 12-17.

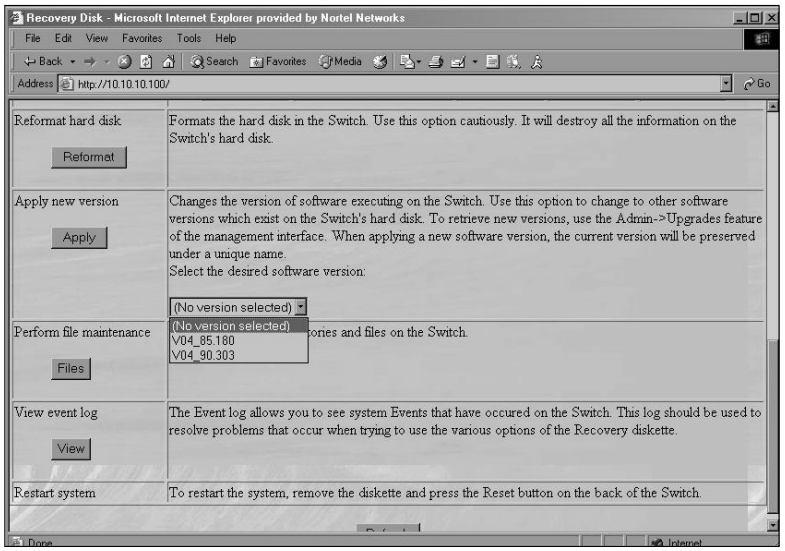


Figure 12-16: Applying a new version of code via the recovery screen

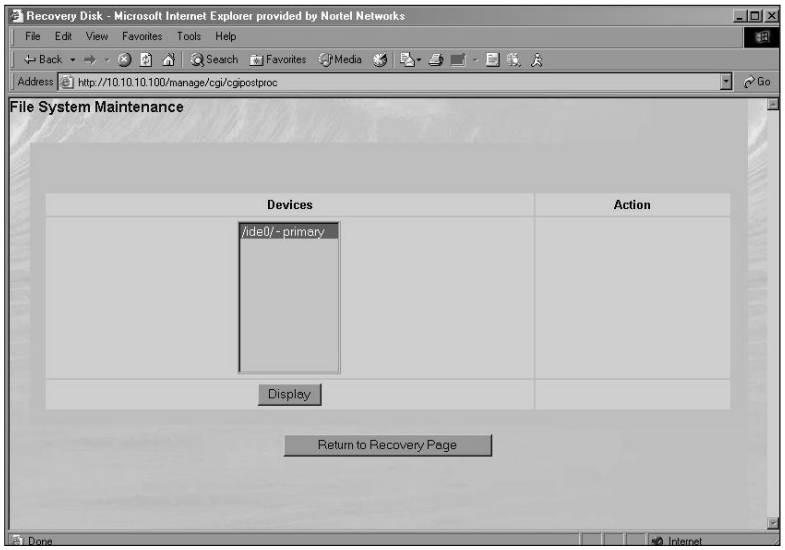


Figure 12-17: The File System Maintenance screen

From the File System Maintenance screen, you will see a list of the storage devices that the VPN Router recognizes. Ide0 will be the only option that is available to you with the diskless versions of the VPN Router.

Ensure that the device that contains the files that you want to view is highlighted. Once highlighted, you click the Display button, and a new window

opens. The new window is still the File System Maintenance screen, but instead of the device listing, there will be a listing of directories that are located on the device that you highlighted previously. Figure 12-18 shows an example of the directory listing in the File System Maintenance screen.

Select the directory you would like to view. Once you have highlighted the directory, you can click the Details button. This provides you with a list of files that are stored within the directory that you have selected. The files will be listed in the column on the right-hand side of the Files System Maintenance screen.

Once you have completed viewing the files that you wanted to view, you can click the Return to Recovery Page button at the bottom of the window. This will return you to the system recovery screen.

View Event Log Option

The "View event log" option provides the user the ability to review the current event log. This option is helpful when troubleshooting system recovery issues. By clicking the View button in the "View event log" section of the recovery screen, you are issuing a command for the VPN Router to produce the latest event log entries that are contained in the VPN Router. The output of this command will be dumped to the bottom of the recovery screen. Figure 12-19 shows an example of this.

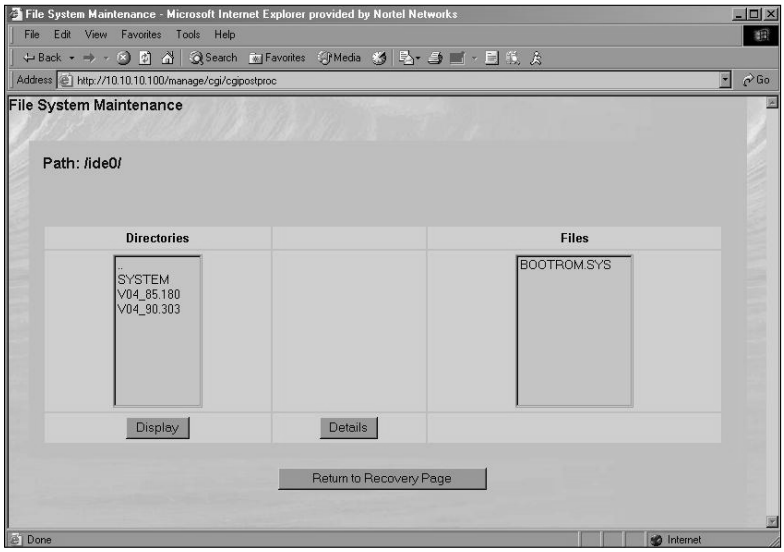


Figure 12-18: Viewing files via the File System Maintenance screen

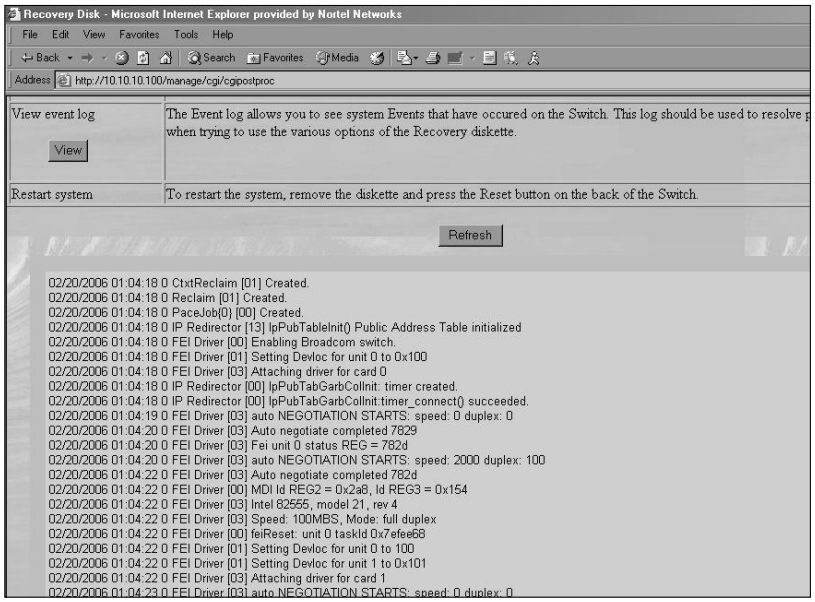


Figure 12-19: Viewing the event log via the recovery screen

Use of the Nortel VPN Router Reporting Utilities

The Nortel VPN Router contains several very helpful tools and utilities that provide statistical data, as well as other important information about the VPN Router and its operations.

The utilities that are available within the VPN Router that can assist you the most when troubleshooting the VPN Router can be accessed through the browser interface. From the main menu, select either the Status directory or the Admin directory.

As shown in Figure 12-20, the following subdirectories are available to you from the "status" directory:

- Sessions
- Reports
- System
- Health Check
- Statistics
- Accounting
- Security Log
- Config Log

- System Log
- Event Log

As shown in Figure 12-21, the following subdirectories are available to you from the Admin directory:

- Administrator
- License Keys
- Auto Backup
- Tools
- Recovery
- Upgrades
- Configs
- File System
- SNMP
- SNMP Traps
- Shutdown
- Quick Start
- Guided Config

Status

The Status menu contains utilities that provide information pertaining to the current status of the VPN Router. From this section of the browser interface, you can view information about who currently has an active session with the VPN Router. You can also gather reporting data, as well as event log data to determine what problems may be occurring (if any).



Figure 12-20: The Status menu directory structure

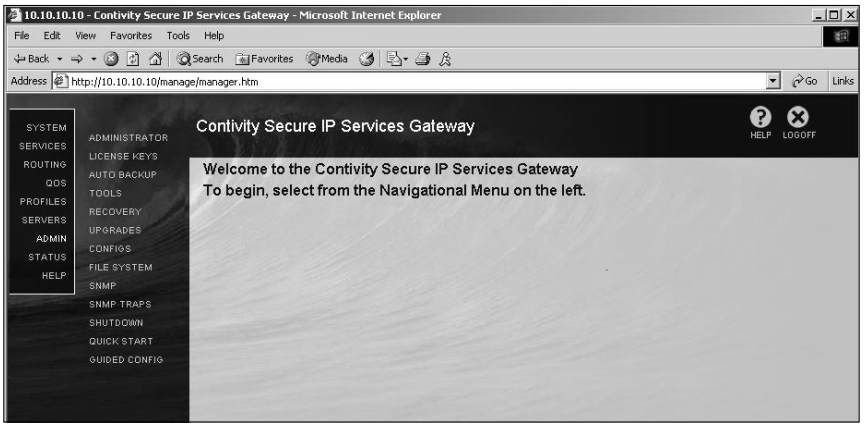


Figure 12-21: The Admin menu directory structure

Sessions

The Sessions subdirectory will provide you with information about the current active sessions within the VPN Router. The following information is included in this screen:

- A summary of user active tunnels
- A summery of active Branch Office Tunnels (BOTs)
- Individual BOT statistical data
- Individual User Tunnel statistical data
- Idle branch office sessions
- Idle user tunnel sessions
- Log-off capabilities

The data contained in this screen can help you analyze information about the current activities through the tunnels that are connected to your VPN Router. Data received and transmitted is recorded here on a per–branch office and per–user tunnel basis.

Assigned local IP address information is recorded on this screen, as well as the date and time that a tunnel was established. Also helpful is the ability to determine exactly who may be affected if there is a requirement to disconnect tunnels for troubleshooting and maintenance. This will provide you with the ability to notify the individuals who will be affected if you have the need to drop their sessions. Figures 12-22 and 12-23 show examples of the Active Sessions screen.

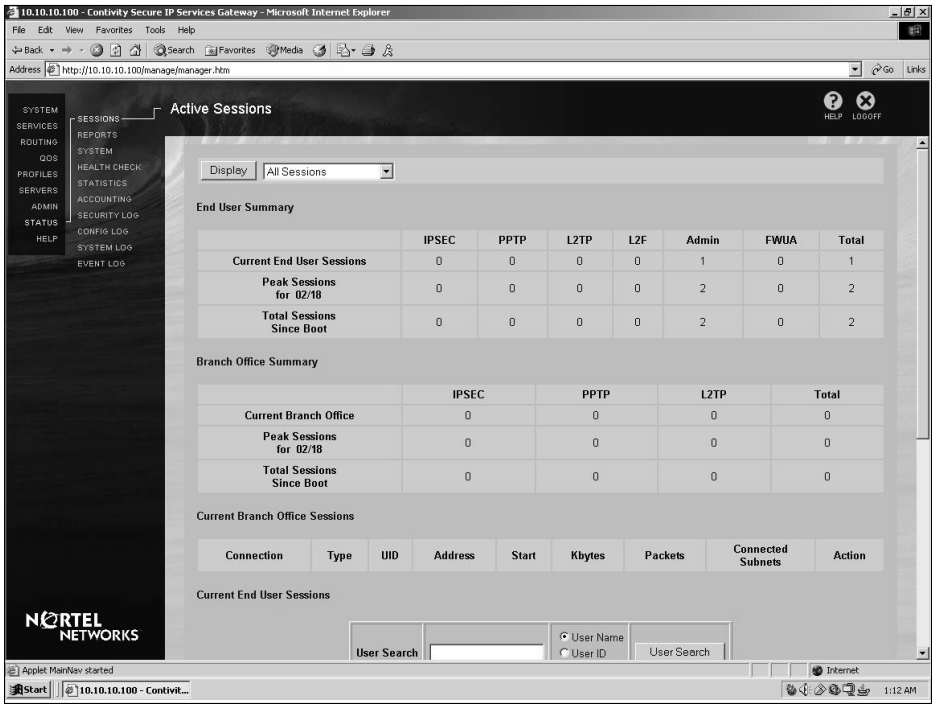


Figure 12-22: The top portion of the Active Sessions screen

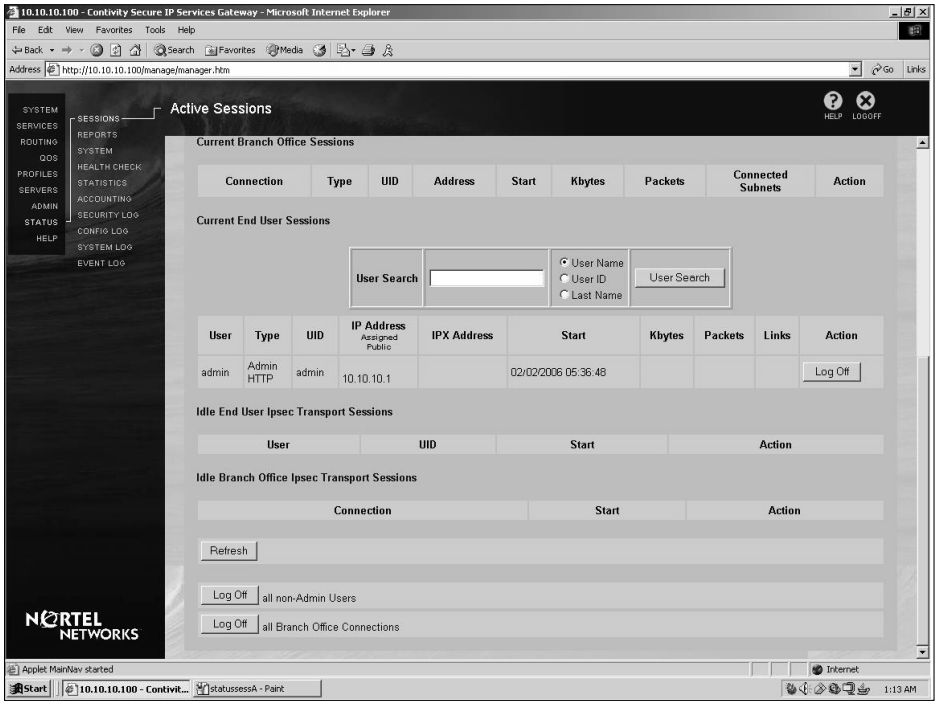


Figure 12-23: The bottom portion of the Active Sessions screen

Reports

The Reports subdirectory will provide you with general system information and system performance data. In this screen, you have the option of viewing the data either in text, as a report, or graphically. Additionally, the text reports can be viewed in a tabular or a comma-delimited format.

NOTE The diskless version of the VPN Router does not provide support for the Reports utility.

Figure 12-24 shows an example of the Reports main screen.
The reports that you are able to run on this screen are as follows:

- *Administration:* This report contains information about the users who have administrative rights and access to the VPN Router.
- *Users*: This report contains information about the configured users for the VPN Router.
- *System Report:* This report contains information about the VPN Router.
- *Sessions Report:* This report contains information about sessions that have been connected to the VPN Router.
- *Failed Authorization Report:* This report contains information about failed authentication attempts with the VPN Router.
- *Expired Password Report:* This report provides a list of users who have expired passwords.
- *RADIUS Diagnostic Report:* This report provides information about RADIUS configuration and whether or not the VPN Router RADIUS settings match those of the RADIUS server.

In addition to the Text reports that can be reviewed within this screen, the user also has an option to generate graphs for this information. Graphs are used to provide a visual baseline of the status of the report you are viewing. Figure 12-25 shows an example of a graph that is outlining the current data flow for traffic passing through the VPN Router.

System

The System subdirectory will provide you with information about the VPN Router. The information contained within this screen is helpful when troubleshooting the VPN Router. Following is the information that you can view on this screen:

- The current system uptime
- The current software version that is running
- The software build date
- Whether the software version is for disk-based or diskless systems
- The serial number of the VPN Router
- The MAC address of the VPN Router
- The system BIOS type
- The maximum number of VPN tunnels that are supported
- The system hardware processor type
- System memory information, including total memory and amount used
- Hard drive information
- Diskette type (if supported)

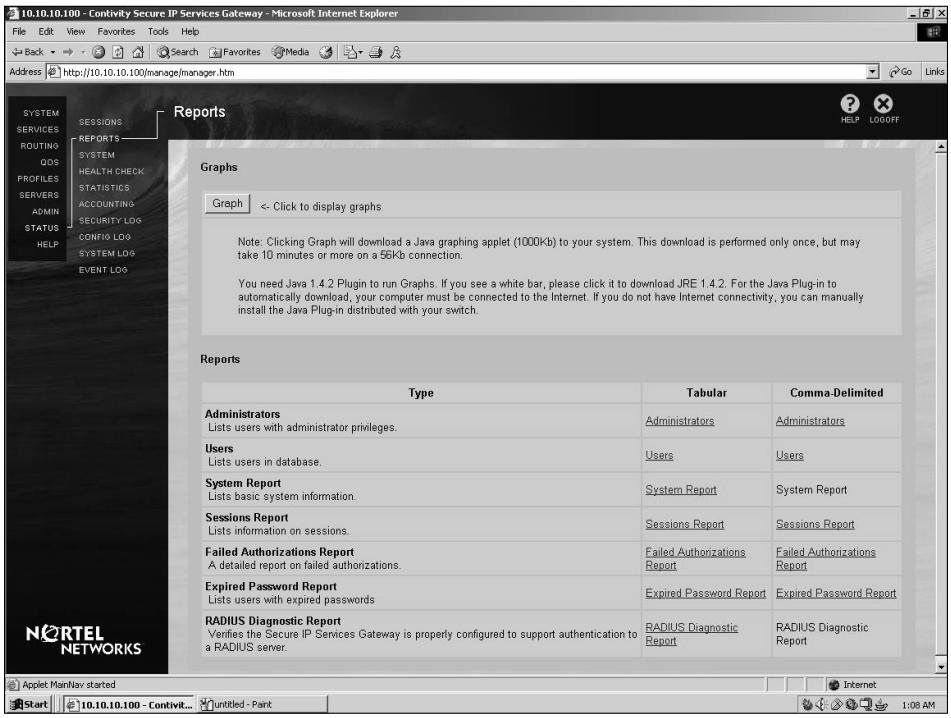


Figure 12-24: The Reports screen

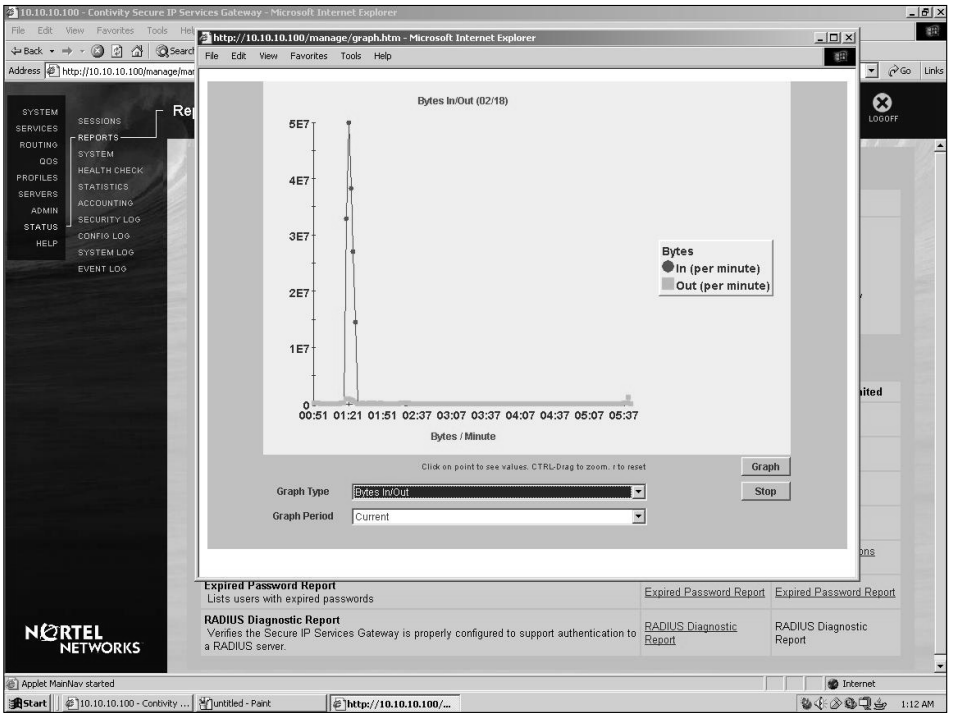


Figure 12-25: The graphing feature within the Reports utility

Health Check

The Health Check subdirectory will provide you with information about the current state of the VPN Router and its configured technologies. Figure 12-26 shows an example of the Health Check screen.

The Health Check screen resembles a spreadsheet and is formatted in a way that is very easy to review. The information reported on the screen appears in four columns. The first column lists the name of the hardware or software feature that it being reported on. The second column lists the current status of that feature. The third column is a description of what the status message is reporting. The last column is a hyperlink to take you to where you can get more information, or can take appropriate action for the feature.

Also on the Health Check screen is an option to turn off or turn on audible alarms. If your VPN Router supports event alarms, then there is a feature on this screen that will allow you to enable and disable the audible alarms.

The status column lists color-coded event severities. These will always be placed in an order where the more severe events will be logged to the top of the page. Following are the severity levels:

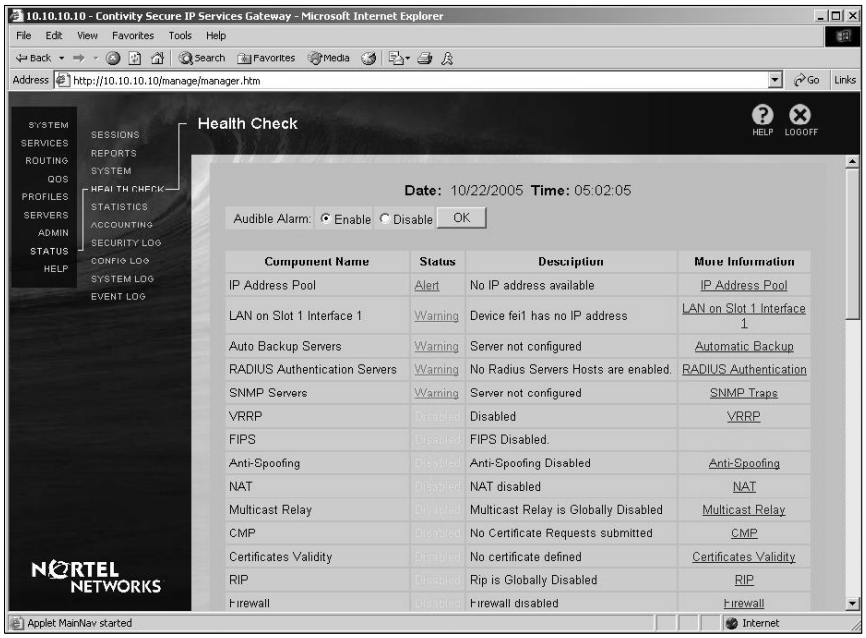


Figure 12-26: The Health Check screen

- *Alert (red):* This status level is the most critical event status. It informs you that action needs to be taken as soon as possible.
- *Warning (yellow):* This status informs you that feature failure is imminent.
- *Warning (purple):* While not as critical as a yellow warning, it is still important that this status is reviewed and verified. The purple warning is informing you that this feature is not yet configured.
- *Disabled (yellow):* This informs you that the feature is currently not enabled.
- *OK (green):* This informs you that everything for this feature is working as it should.

Statistics

The Statistics subdirectory will provide you with statistical information about the VPN Router. This screen provides access to multiple other screens that will outline almost everything you might need to know about historical data for the VPN Router. Not only does this screen allow access to information about the hardware associated with your VPN Router, but a lot of data can be gathered about the software and data traffic associated with the VPN Router as well. Figure 12-27 shows you all of the categories contained within this section.



Figure 12-27: The Statistics screen

The information provided within the sub-screens of this section will provide you with a lot of diagnostic information that can be extremely helpful in reaching a resolution to connectivity issues. The data can also be very helpful should you have to engage a Nortel support engineer for assistance.

The main categories on the Statistics screen are as follows:

- *System:* From this section, the following sub-screens are available: software version, file system data, data stored on Flash (non-volatile memory), Network Time Protocol (NTP) statistics, Object List (for use by Nortel software engineers), configuration file contents, and Active software objects.

- *Interfaces:* From this section, the following sub-screens are available: Interface data, LAN counter information, and WAN statistics.
- *Hardware:* From this section, the following sub-screens are available: Device driver information, Packet Content Engine (PACE) data, and Asynchronous Data Subscriber Line (ADSL) data.
- *Resources:* From this section, the following sub-screens are available: System memory data, Stack information, memory-forwarding information, buffer statistics, current tasks, internal LDAP data, and database optimization status.
- *Network:* From this section, the following sub-screens are available: Routing table, TCP/IP and UDP bound port information, TCP statistics, UDP statistics, Internet Control Message Protocol (ICMP) statistics, DHCP statistics, IP statistics, IP forwarding table, IP address pool data, Internet Packet Exchange (IPX) statistics, IPX routing table, IPX server table.
- *Routing:* From this section, the following sub-screens are available: Address Resolution Protocol (ARP) table, RIP statistics, OSPF statistics, VRRP statistics, and BGP statistics.
- *Admin:* From this section, the following sub-screens are available: Load-balancing data, Session statistics, and Branch Office statistics.
- *Security:* From this section, the following sub-screens are available: security statistics, flow cache (memory used by the firewall) statistics, stateful firewall statistics, Network Address Translation (NAT) statistics, Tunnel Guard statistics.

Accounting

The Accounting subdirectory will provide you with information about tunnel sessions that are running within the VPN Router. On the Accounting Records screen, you have the option to review information relating to all sessions, user tunnel sessions, or BOT sessions. Figure 12-28 shows an example of this screen.

NOTE The diskless version of the VPN Router does not provide support for the Accounting utility.

The Accounting Records screen also provides a search function that will allow you to define your search criteria to narrow down the search for information that you want to get from the VPN Router. The following fields are the available search parameters:

- User last name
- User first name
- Session User ID
- Group name or Branch Office name
- Tunnel type
- Session start date
- Session end date

Security Log

The Security Log subdirectory provides information about the security function of the VPN Router. All security events are logged in the security log. Security successes and failures are logged. Figure 12-29 shows an example of the Security Log screen.

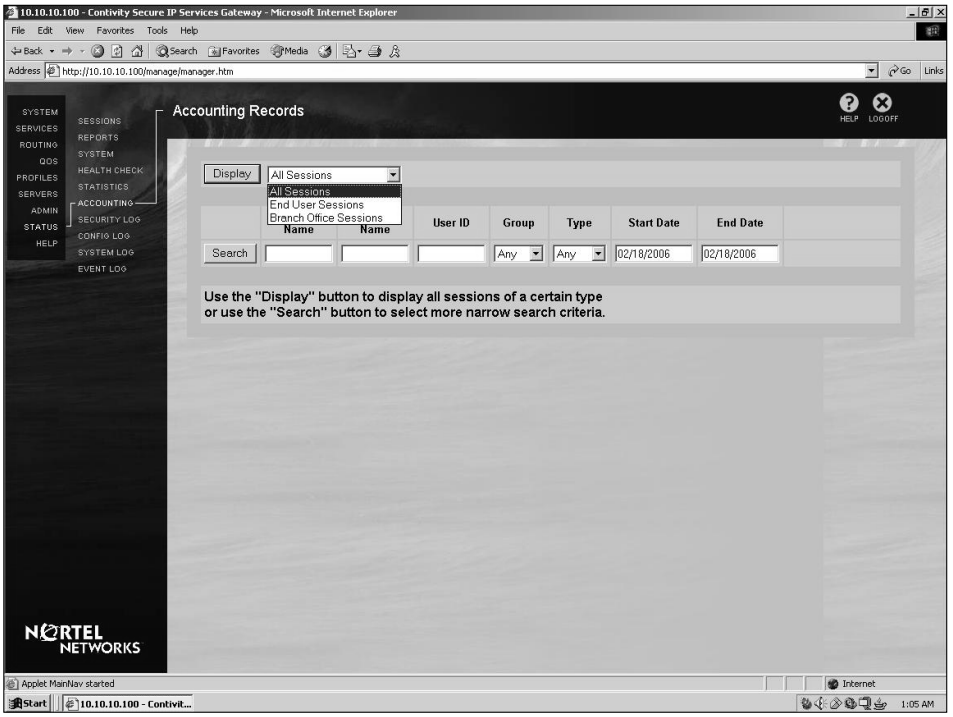


Figure 12-28: The Accounting Records screen

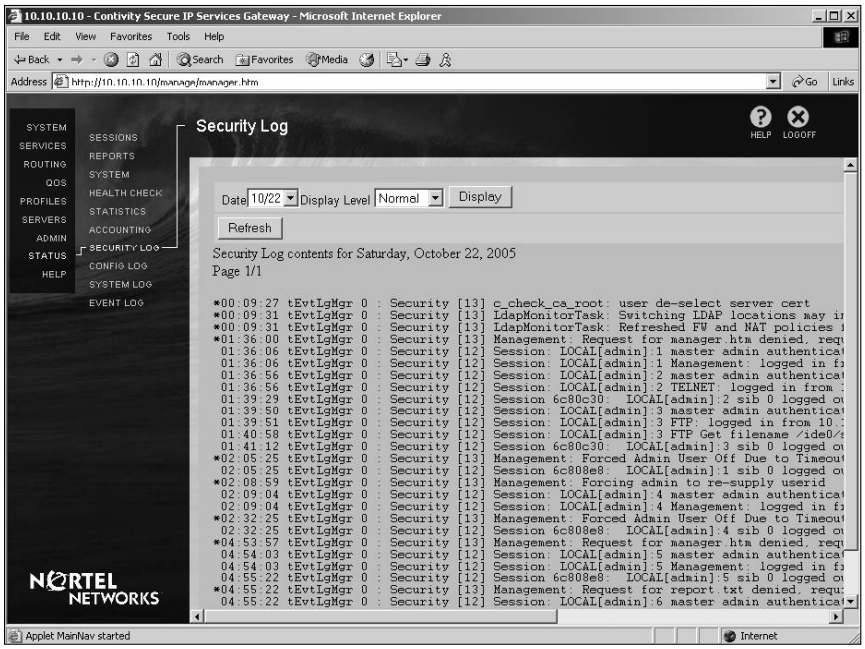


Figure 12-29: The Security Log screen

NOTE Chapter 5 discusses the security log in detail. Refer to Chapter 5 for additional information pertaining to this log.

Following is an example of some security log entries:

```
*00:09:27 tEvtLgMgr 0 : Security [13] c_check_ca_root: user de-select
server cert
*00:09:31 tEvtLgMgr 0 : Security [13] LdapMonitorTask: Switching LDAP
locations may impact SSL certificate identification, a re-load may be
necessary.
*00:09:31 tEvtLgMgr 0 : Security [13] LdapMonitorTask: Refreshed FW and
NAT policies for new LDAP server
*01:36:00 tEvtLgMgr 0 : Security [13] Management: Request for
manager.htm denied, requires login
 01:36:06 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:1 master
admin authenticated
 01:36:06 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:1
Management: logged in from 10.10.10.1 Server Rights: Manage User Rights:
Manage
 01:36:56 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2 master
admin authenticated
 01:36:56 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2 TELNET:
logged in from 10.10.10.1
```

NOTE **The diskless version of the VPN Router does not provide support for the Security Log utility.**

Config Log

The Config Log subdirectory will provide you with information about any additions, deletions, and changes to the configuration of the VPN Router. Figure 12-30 shows an example of the Config Log screen.

NOTE **Chapter 5 discussed the config log in detail. Refer to Chapter 5 for additional information pertaining to this log.**

Following is an example of some config log entries:

```
*00:09:01 tRootTask 0 : cfg file setting warning
'IpxIntfOmCls.IpxPrivateLANS[256].IpxAddress=N/A'
*00:09:01 tRootTask 0 : cfg file setting warning
'IpxIntfOmCls.IPXPublicAddress=N/A'
*00:09:19 tSerialConfig 0 : DirBackup.PrimaryHost changed from '' to ''
by user '' @ ''
*00:09:19 tSerialConfig 0 : DirBackup.PrimaryPath changed from '' to ''
by user '' @ ''
*00:09:19 tSerialConfig 0 : DirBackup.PrimaryUsername changed from '' to
'' by user '' @ ''
*01:39:12 tHttpd 0 : Security.TrustedFTPEnabled changed from 'FALSE' to
'TRUE' by user 'admin' @ '10.10.10.1'
```

NOTE **The diskless version of the VPN Router does not provide support for the Config Log utility.**

System Log

The System Log subdirectory will provide you with information pertaining to significant events that are logged within the VPN Router. These events are significant enough to be written to file and saved for review. Figure 12-31 shows an example of the system log.

NOTE **Chapter 5 discussed the system log in detail. Refer to Chapter 5 for additional information pertaining to this log.**

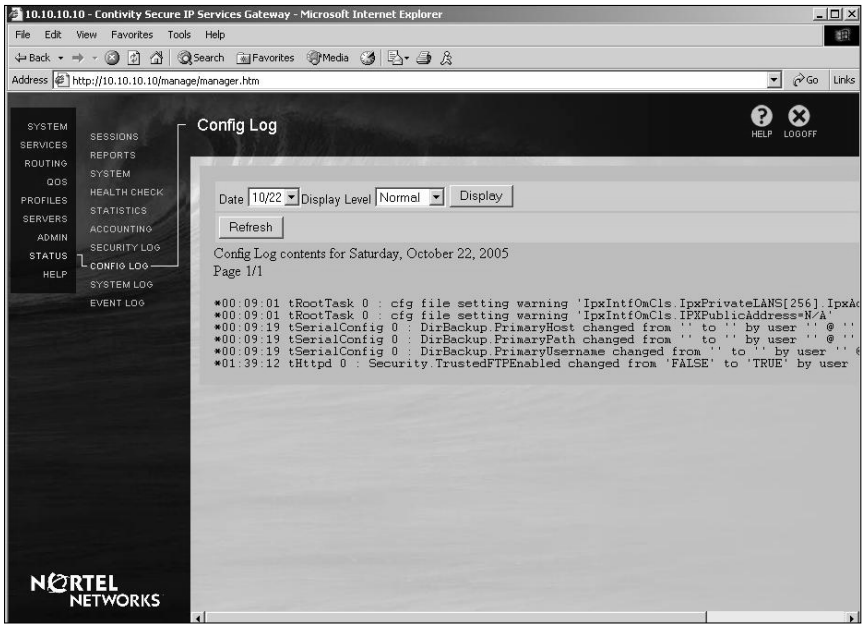


Figure 12-30: The Config Log screen

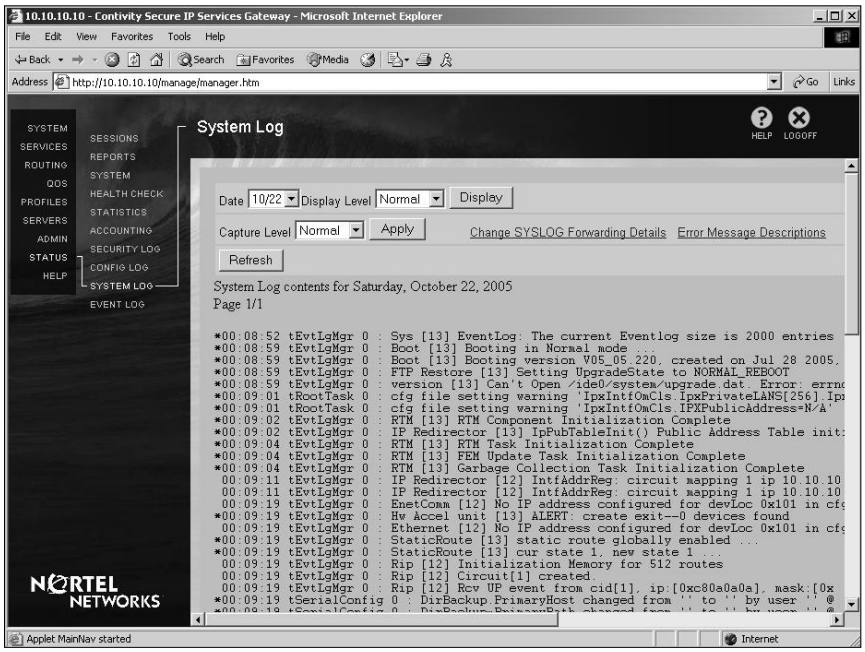


Figure 12-31: The System Log screen

The system log retains data for up to 61 days. All system log data is written to a file and is stored on the disk. The event log will send significant events to the system log to be stored for reference purposes. The config log and the security log will also write significant events to the system log. Following is an example of some system log entries:

```
*00:08:52 tEvtLgMgr 0 : Sys [13] EventLog: The current Eventlog size is
2000 entries
*00:08:59 tEvtLgMgr 0 : Boot [13] Booting in Normal mode ...
*00:08:59 tEvtLgMgr 0 : Boot [13] Booting version V05_05.220, created on
Jul 28 2005, 21:54:53.
*00:08:59 tEvtLgMgr 0 : FTP Restore [13] Setting UpgradeState to
NORMAL_REBOOT
*00:08:59 tEvtLgMgr 0 : version [13] Can't Open
/ide0/system/upgrade.dat. Error: errno = 0x388002
*00:09:01 tRootTask 0 : cfg file setting warning
'IpxIntfOmCls.IpxPrivateLANS[256].IpxAddress=N/A'
*00:09:01 tRootTask 0 : cfg file setting warning
'IpxIntfOmCls.IPXPublicAddress=N/A'
```

Event Log

The Event Log subdirectory will provide you with information about all activities that occur on the VPN Router. The event log retains these events in memory and will write significant events to the system log. Figure 12-32 shows an example of the event log.

NOTE **Chapter 5 discusses the event log in detail. Refer to Chapter 5 for additional information pertaining to this log.**

The event log captures data as it is occurring on the VPN Router. The event log thus provides a running entry of all events that occur on the VPN Router. The event log retains all of these entries in memory and reports significant entries to the system log, to be written to the system log file, and saved on disk. Following is an example of some event log entries:

```
10/22/2005 00:08:52 0 Sys [13] EventLog: The current Eventlog size is
2000 entries
10/22/2005 00:08:59 0 Boot [13] Booting in Normal mode ...
10/22/2005 00:08:59 0 Boot [13] Booting version V05_05.220, created on
Jul 28 2005, 21:54:53.
10/22/2005 00:08:59 0 CtxtReclaim [01] Created.
10/22/2005 00:08:59 0 Reclaim [01] Created.
```

Admin Tools

The Admin section within the browser interface contains a subdirectory labeled Tools. Figure 12-33 shows an example of the Tools subdirectory.

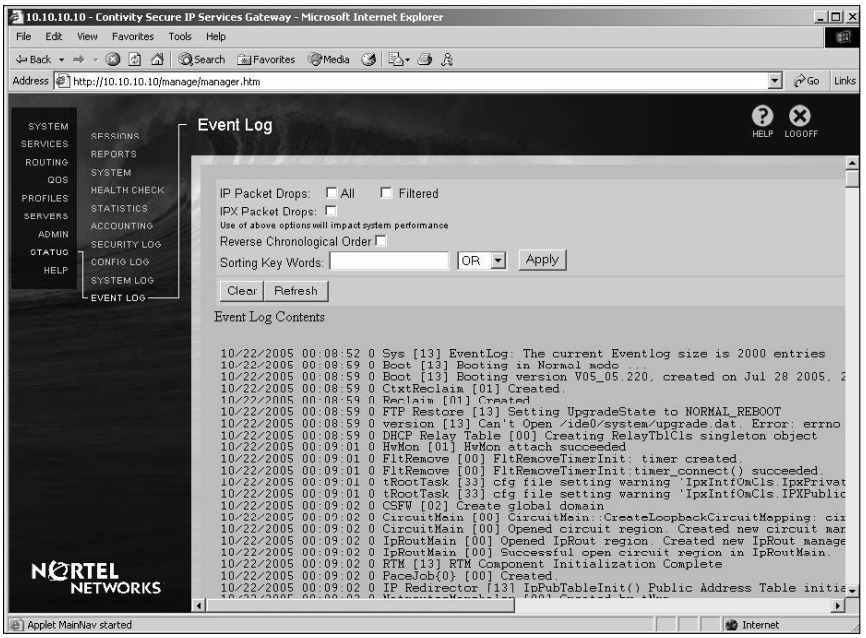


Figure 12-32: The Event Log screen

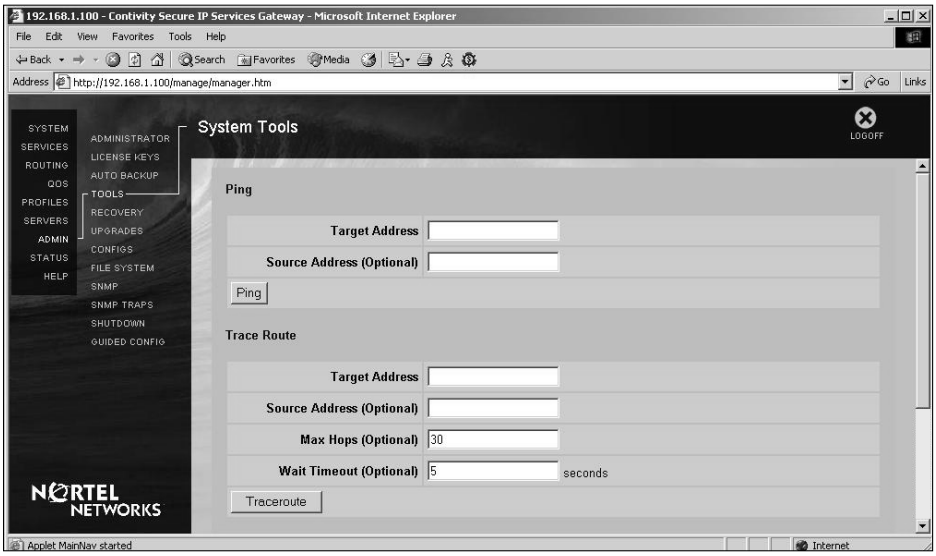


Figure 12-33: The Tools subdirectory of the Web browser interface

The following troubleshooting utilities are available from the browser interface as listed in the Tools subdirectory:

- Ping
- Trace Route
- Arp

Ping

Earlier in this chapter, you learned about the TCP/IP tool known as Ping. The Nortel VPN Router supports the `ping` command and it is one of the tools available within the Web browser interface.

The purpose of the Ping tool is to send a message from one TCP/IP system to another TCP/IP system to see if the network layer is functioning as expected. Ping sends an echo request from one node to another. The node that is being "pinged" will send an echo reply to the originating node.

The Ping utility in the browser interface has two fields where data can be entered:

- *Target Address:* Enter the IP address for the device you are trying to contact.
- *Source Address (Optional):* Specify an IP address that you would like the ping to come from.

Figure 12-34 shows an example of the Ping utility.

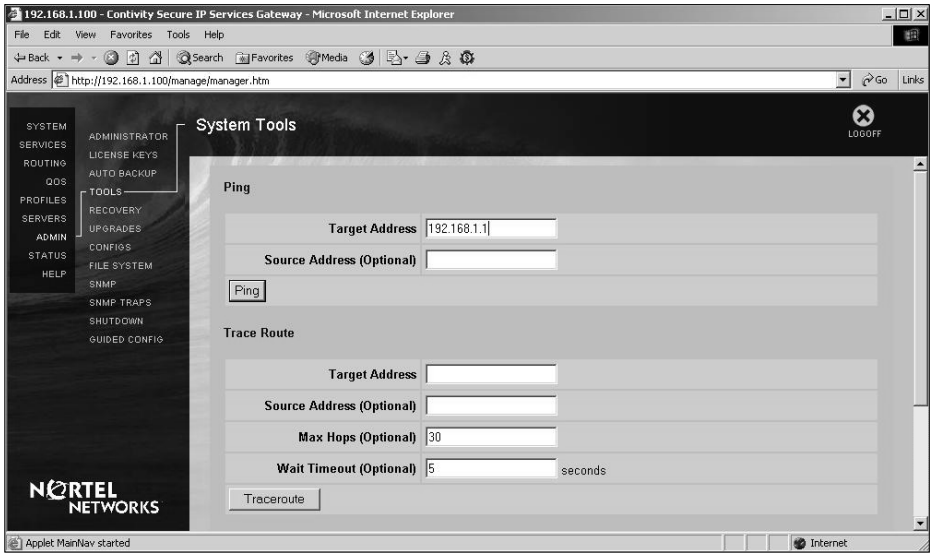


Figure 12-34: Using the Ping utility

The results of the Ping test are output to the bottom of the tools screen. The data contained in the output is the same data that was observed when `ping` was discussed earlier in this chapter. Figure 12-35 shows an example of the output of a successful Ping test.

Trace Route

Previously in this chapter, the `traceroute` command was discussed. The Nortel VPN Router also supports trace routing from within the browser interface.

The Trace Route utility provides information about the data path that a packet will take between a source node and a destination node. Using this utility, you can determine if a packet is taking the correct path in reaching a destination and, if not, help pinpoint where the packet is taking a wrong turn.

Four fields are available for data within the Trace Route section of the Tools screen, and Figure 12-36 shows an example. These sections are as follows:

- *Target Address:* Enter the IP address of the node you are trying to reach.
- *Source Address (Optional):* Specify the IP address of where you want the trace route to begin. This is an optional section.
- *Max Hops (Optional):* Specify the maximum number of hops that you would like to pass through. This is optional.
- *Wait Timeout (Optional):* Specify the timeout value for non-responsiveness. It is also an optional field.

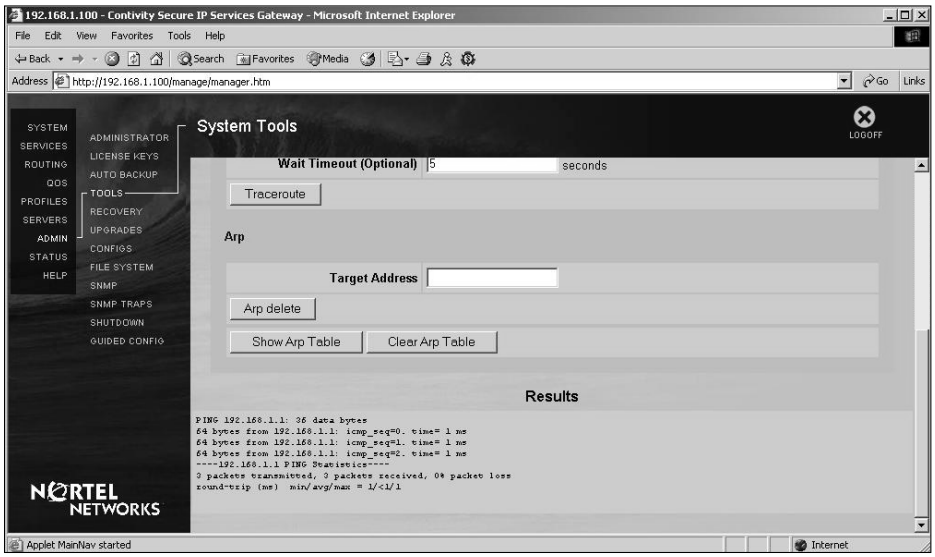


Figure 12-35: The Ping test results

The results of the Trace Route test are output to the bottom of the tools screen. The data contained in the output is the same data that was observed when `traceroute` was discussed earlier in this chapter. Figure 12-37 shows an example of the output of a successful Trace Route test.

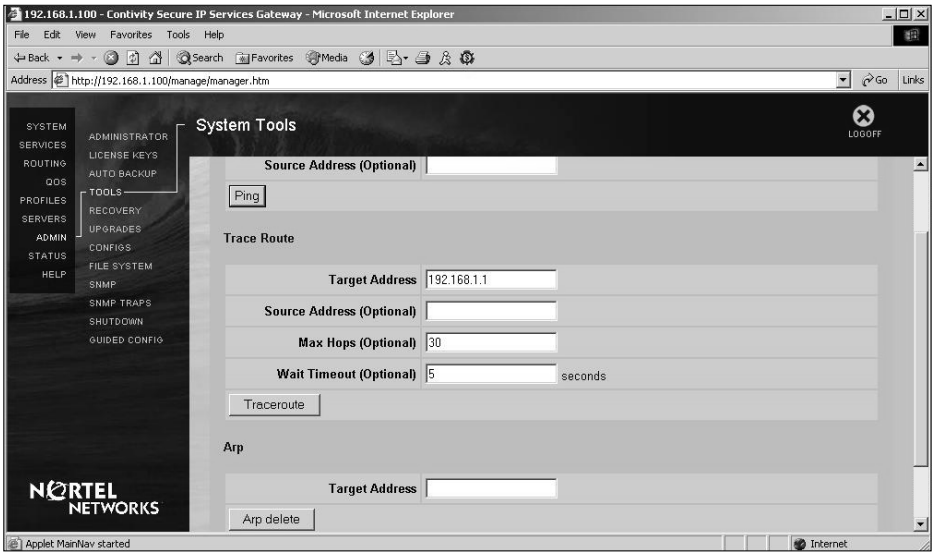


Figure 12-36: The Trace Route utility

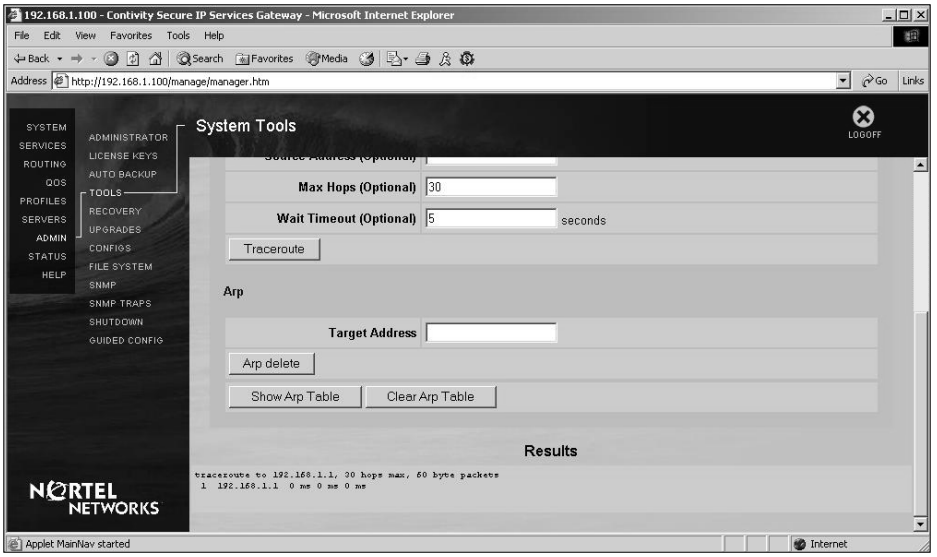


Figure 12-37: The Trace Route test results

ARP

The Address Resolution Protocol (ARP) provides a way to find a node's MAC address when only the IP address is known. The way ARP works is simple. A sending node will send a broadcast through the network with the IP address of the node that it is trying to locate. Once a node recognizes an IP address in an ARP broadcast, it will respond to the originating node with the MAC address that matches the IP address. ARP entries are stored in a cache, known as the *ARP table*.

ARP is limited to the nodes within the network that support broadcasting and will accept a broadcast packet. Other nodes will ignore the broadcasts.

Sometimes a node may be moved or, for some other reason, a node may no longer be able to locate another node within the network. When this occurs, you might want to try to force the node to relearn where the destination node may reside.

The Arp section of the Tools screen provides access to the ARP table and some options that can be used to assist in troubleshooting. This section is located at the bottom of the Tools screen (see Figure 12-38). Within the Arp section is one field that allows you to specify the IP address of a node that you would like to have removed from the ARP cache so the device will resend the ARP broadcast packets. You can enter the IP address and then press the Arp delete button that is in this section.

Two other buttons can be chosen within the Arp section. The first button is the Show Arp Table button. By clicking this button, you will receive an output of the ARP table, which lists the entries contained in the VPN Router's ARP cache. Figure 12-39 shows an example of an ARP table. The other button provides an option to clear the entire ARP table.

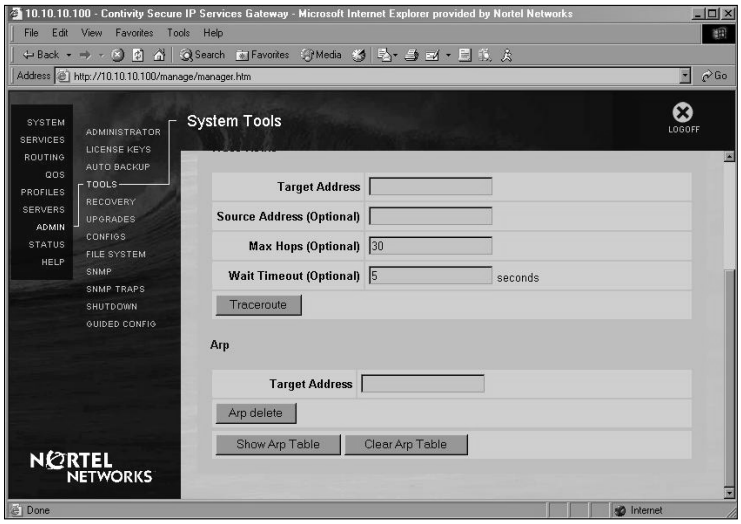


Figure 12-38: The Arp section of the System Tools screen

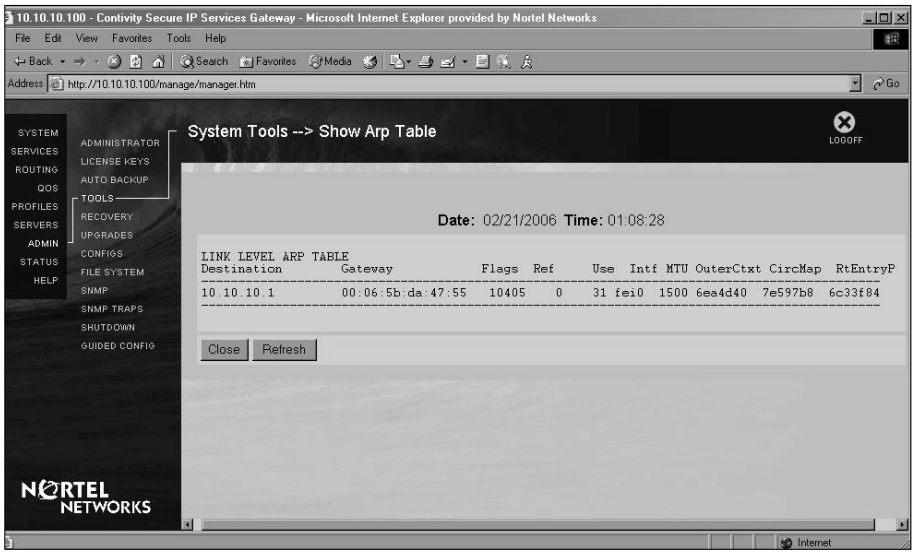


Figure 12-39: The ARP table

Packet Capture

Previously in this chapter, we discussed the use of sniffers as a helpful tool in troubleshooting data connection issues within a network. Often, however, a link must be broken to put a sniffer "in line" before it can be used. Also, some nodes (such as the Nortel VPN Router) use an encryption technology that a sniffer may not understand when capturing packets.

Many data nodes (such as VPN Routers) support what is known as Packet Capture (PCAP) built into the software. This allows the capture of packets that are passing through the node without requiring an external sniffer to be placed in the network segment. PCAP is an application program interface (API) that supports the capture of packets within a network. The captured packets are then stored in a trace (often referred to as a *capture*), which can then be analyzed by a packet sniffer application, such as Ethereal. Figure 12-40 shows an example of a PCAP capture of a client tunnel session that is being viewed in Ethereal.

Beginning with VPN Router code version v04_85, the Nortel VPN Router supports packet capturing by including PCAP support within the software. The Nortel VPN Router PCAP utility allows for the capturing of packets that are passing through all interfaces, tunnels, and even Ethernet segments that are not related to the VPN Router.

Several security events are in place when performing a PCAP on the Nortel VPN Router. Performing a PCAP must be done from the console interface. The administration password must be other than the default password, and a password is assigned to the capture, so that password must be known before the capture can be read.

Performing the PCAP operation on the VPN Router is memory-intensive so it should be performed only when required for troubleshooting purposes. There are filters that can be implemented to reduce the amount of data capture and free up some resources, but the process still requires the use of VPN Router resources.

Most sniffer applications provide a few features that allow you to view different aspects of the PCAP file. This is helpful when you are trying to gather statistics or narrow down the information that you are viewing. These features include the ability to sort by protocol hierarchy (see Figure 12-41) and graph statistics (see Figure 12-42).

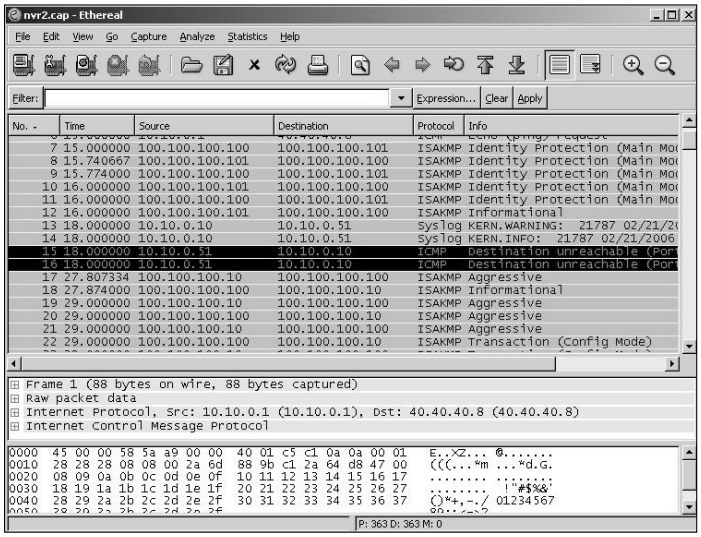


Figure 12-40: Viewing the PCAP capture

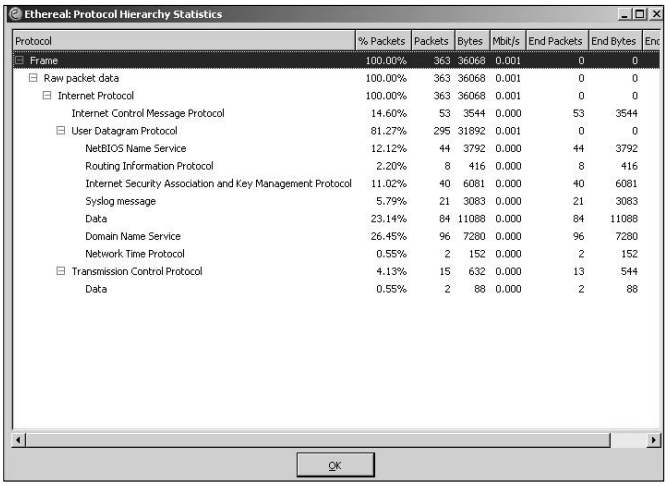


Figure 12-41: Viewing the protocol hierarchy statistics in a client tunnel session PCAP capture

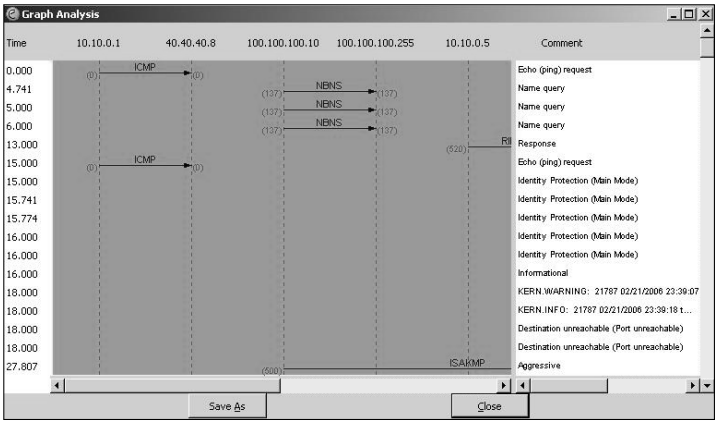


Figure 12-42: Viewing a statistical graph of a client tunnel session PCAP capture

General Network Proactive Measures

As mentioned previously, problems with communication in a data network are going to happen. Hardware failures, compatibility issues, data traffic flow issues, and many other things can contribute to a break in communication. Sometimes these issues are simple to diagnose, and sometimes they can take hours and even days to resolve.

Proactive measures can be taken in anticipation of potential failures. Viewing outages in a proactive manner can truly help the resolution time when a problem arises. Unfortunately, a proactive approach is not always practiced in many LANs.

This section discusses some recommended proactive measures to assist you in considering and in taking a proactive stance toward the maintenance of the VPN Router, as well as other network nodes.

Perform Regular Backups

One of the easiest things that can be done to the VPN Router (as well as other nodes within the network) is to perform system backups regularly. If possible, it is also a good practice to make duplicate backups in case of a backup storage device failure. Anticipate the possible and try to accommodate.

System configurations, databases, images, and other system files do get corrupted and sometimes may even get lost. Having a recent backup for any required file can save you a lot of work in the long run. Many network managers perform daily backups of critical files. This may or may not be a practice that needs to be adhered to in every network, but a regular backup is highly recommended.

Consider what problems may arise if a core network node experiences configuration corruption and the network administrator does not practice regular system backups. That core device's configuration will have to be rebuilt, which will probably contribute to extended downtime for the device. In turn, user productivity will drop because of the lack of network resources. The lack of a recent backup may cost your employer hundreds to thousands of dollars.

Backups are also a necessity when performing system maintenance. Whether it is a hardware replacement or a configuration change, always back up the system-critical files before you begin the scheduled maintenance for the device.

A little time spent up front in backing up these files can save you a lot of time in the long run.

Research

When planning a network design or considering a change to the network, always research before you implement. If tasked to support a certain protocol or application, ensure that you understand how that application and/or protocol works. Ensure that the nodes within the network are compatible with the considered change or implementation. Consider the impact that the change may have on the existing network infrastructure.

Effective planning is paramount in data networks. In addition to planning how the change may affect the current network, it is also prudent to anticipate future growth. What might occur if you need to purchase a VPN Router and you don't consider the number of active tunnels that you may need in your decision? What problems might occur if you purchase a NIC upgrade for a server only to later discover that there are compatibility issues with the brand of NIC and some of the nodes within your network?

Effective planning is always a very important proactive step to take. It's always possible that not all contingencies can be considered up front, but planning for as many as you can think of will help alleviate potential problems in the future.

Always Have a System Recovery Disk Available

Making a system recovery disk and having it available to you are very important, but often ignored. The process of making the recovery disk is very quick and easy and can save you a lot of problems in the future.

If you are running multiple versions of code on the VPN Routers in your network (which, by the way, is *not* recommended), then ensure that you have a recovery disk to match each of those versions of code.

When making a recovery disk, also ensure that you make the recovery disk available. It will not serve any purpose if you are onsite working on a VPN Router issue and need your recovery disk, which happens to be in another state.

We recommend that you keep the recovery disk available in an area that is local to the VPN Router. In addition to making one local to the router, ensure that it is accessible to anyone who may be performing troubleshooting and/or maintenance on the VPN Router.

Another practice that is followed by some VPN administrators is to provide a copy of the recovery disk to all personnel who may need to have it. The problem with this practice it that a procedure would need to be set up to allow for recovery disk upgrades.

Consider the impact that the users would feel if you had a catastrophic failure on the VPN Router and you did not have a recovery disk available. The system downtime would then be increased until a recovery disk was obtained, or a VPN Router replacement would have to be ordered.

Whatever policy you choose to implement, the main thing is to ensure that the recovery disk is made and is made available to anyone who may be working on the VPN Router.

Dial Access for Support Personnel

Providing access to the network for the support personnel within the network is a very important proactive step to take. If the network provides for an on-call person for potential outages, then it is very important that that person be able to access the network from a remote area.

Ensuring that all support personnel have remote access can assist in clearing up outages in a timely manner. Of course, remote access is not always going to be the resolution to a problem, and personnel will have to go to the site where the equipment resides, but it may help in certain instances.

Knowledge Sharing

Because of security concerns and some other factors, some networks provide critical information about the network and the nodes within the network to only a few personnel. Far too often, this information resides with only one person.

Knowledge management is a very important factor when running a network. The sharing of knowledge can also make the resolution to network problems much easier to contend with. Ensure not only that as many people as possible are involved in the administration of basic network duties, but also that at least two or three trusted individuals have access to all of the documentation pertaining to the network.

Consider what problems may arise if you entrust only one person to retain the management login information for all of the VPN Routers in the network. What may occur if that person is on vacation or has left the company and you need to access the VPN Router for troubleshooting purposes? Because of the security considerations for the VPN Router, there is no default or back-door password. In the event of system failure when login access is denied, the unit will have to be replaced.

Also consider the extended time it may take to troubleshoot a problem within a subnet when the only person who is aware of the nodes within the subnet is not available. Tracing down problem areas can be very time consuming (if not impossible) at times.

Knowledge sharing is very important and it can make a tremendous difference in resolving issues that occur in the network. Follow this very important proactive step to help ensure that network connectivity timelines stay up and to reduce recovery time when network troubleshooting is required.

Documentation

Using a system of developing and retaining effective documentation that relates to your network can be very rewarding in not only troubleshooting the network, but also in future growth and development. Effective documentation can also provide a wealth of information for training and reference.

Among the most important documents that should be developed are network topology diagrams. These diagrams can provide a lot of help when you are troubleshooting a network. They also make great reference documents when you are training new personnel, or planning for network changes and/or growth. Following are some examples of other helpful documentation to have available:

- Network change control documents
- Contractual support documents
- IP schemes
- Topology diagrams
- List of support centers
- List of contacts
- Information about network nodes
- Training documentation

Retaining documentation relating to the nodes within your network, as well as the network itself, is very effective for the overall support of the network. There is really no such thing as too much documentation.

Upgrades and Configuration Changes

Data communications are always changing. New products are always being introduced to the marketplace. New technologies and protocols are developed on a fairly constant basis. Keeping up with these changes is a time-consuming process, but one that is required to meet the demands of customers and employees within the corporate LAN.

Technology that was cutting-edge just 5 to 10 years ago is being replaced with the technology of today. Data equipment upgrades and replacements are fairly common with most large corporations and, with that, the need to analyze and plan for that growth is a requirement and not a luxury.

In addition to keeping up with the ever-expanding data communications market, there are times when an upgrade or a change is required to resolve an issue, or simply to meet internal growth.

You have already learned that planning to meet the current needs of the network is important. When cost is a factor, planning for the future is also important. So, now that the planning is complete and the hardware and software that are needed to implement the change are available, it's time to take the plan and put it into action.

Because most planned events on the network do require some network downtime, it makes sense to reduce the downtime as much as possible and to make the transition run as simply as possible. This section contains a few proactive steps that can be taken to help ensure that the implementation of the plan runs more smoothly than it would if the changes were put into place "on the fly."

Research

When planning for a network change event, it is important to ensure that you research what you are trying to accomplish. If you are introducing new hardware or support of a new protocol or technology, research to ensure that the existing infrastructure can support what you want to introduce. Following are some questions to consider when introducing a technology change or hardware change:

- Will the new hardware or change accomplish what you need?
- Are there any interoperability issues with the new change and the existing equipment within the network?
- Are any code upgrades required to support the new hardware/change?
- Are any other changes or hardware upgrades required to support the new change?

If you are performing a software upgrade, then research the release notes for the software to ensure that you are aware of new changes and implementations within the new code version, as well as any known issues. When upgrading your VPN Router, ensure that you read the code version release notes. Following are examples of things to check and verify:

- Will the new code accomplish what you need?
- Are there any known issues in the new code that may affect the network?
- Are any hardware upgrades required to support the new code?
- Are any higher versions of code that may need to be considered?
- Are there any interim upgrades required to upgrade to the version that you need?
- If upgrading VPN Router code, will a Client upgrade be required as well?

Knowing the answers to these questions is important. Consider what problems may occur if you upgrade to a version that is not compatible with technologies that are supported within your network? What is the impact of the upgrade to the end user? Knowing what to expect and planning for it will help the transition run smoothly.

Pre-Testing

Whenever practical, it is always a good practice to pre-test the change that you will be making in a lab environment. Not only will this give you an opportunity to document the steps required to complete the change, but it will also give you practice in doing the change.

Pre-testing should be accomplished as far in advance as possible. This will give you ample time to walk through and document the process, and will also provide time to let the setup run in the lab for a while. If the setup runs smoothly in the lab, chances are it will run fine when implemented in your production network.

As with upgrades and changes to existing equipment, pre-staging new equipment can be a tremendous help in implementing a change in the network. Pre-staging new equipment gives you an opportunity to "burn" the equipment in and also test to ensure that the equipment is functional. If pre-staged correctly, you can also simply move the new equipment into place with very little configuration required. This process greatly reduces network downtime during the change.

Action Plan

A detailed action plan is a tremendous help when implementing a network change. Not only does the action plan outline all steps to be taken during the duration of the change, but it can provide a lot of insight if technical support is required at some point during the change.

A network change action plan should be as detailed as possible. Following are some of the things that should be included within the action plan:

- Exact time and date of the change
- Equipment that will be affected
- What the purpose of the change is
- Individuals to be involved
- Anticipated duration
- List of required tools (software, configurations, hardware, and so on)
- Login information

- Topology diagram(s)
- Pre-change testing information
- Post-change testing information
- White space for notes

Once you have developed an action plan, ensure that all individuals who will be involved in the change receive a copy of the action plan and review it. Whenever possible, have a "dry run" for the action plan to ensure that no details have been left out. If you have pre-tested or pre-staged the equipment that will be involved in the change, get someone to test the action plan in the lab. Finally, save a copy of the action plan and have it available in case you need to involve a support person from one of your vendors at some point during the change.

Nortel Support

Nortel provides technical support 24/7 for most of its products. The Nortel VPN Router is included in this support. To access Nortel technical support, you will need to have a valid support contract or provide a valid credit card number. Nortel telephone support can be reached at 1-800-4NORTEL.

The Nortel Web site also contains a lot of support information that can assist the users of Nortel equipment in troubleshooting and/or configuring the equipment. The Nortel Web site is located at: `www.Nortel.com`.

If you must call the Nortel support center for help with a problem with your Nortel VPN Router, there is some basic information that you should have available to provide to the support engineer. Although not required, this basic information will help the support engineer understand your network and the problem that you are calling for assistance on. This information is as follows:

- An exact description of the problem
- Code version of the VPN Router
- Code version of the VPN Client
- Personnel affected
- List of recent changes
- Baseline the criticality of your issue
- Configuration, logs, dumps, and any other supporting system files (when applicable)
- IP address of the public interface
- IP address for the management interface

- An admin user account to be used by the Nortel support engineer
- Topology diagrams
- Unit serial number and model number
- Remote access for support personnel
- Action plan (if applicable)
- Outline of troubleshooting performed

Because all networks are different, this information can assist in a speedy recovery. Even if you cannot get all of the information on this list, the more you can get the more helpful it is to the support engineer.

Summary

This chapter provided an overview on network troubleshooting, as well as an overview of troubleshooting the Nortel VPN Router. Many of the utilities that are available were introduced. Also, third-party tools were discussed and examples were provided of each of these.

This chapter completes the introduction to the Nortel VPN Router. Using and understanding the information in this book will greatly improve your understanding and effectiveness when working with your Nortel VPN Router.

APPENDIX

A

Abbreviation and Acronym Reference Listing

This appendix contains abbreviations and acronyms for VPN terminology, as well as other abbreviations and acronyms that you will come across occasionally as the VPN router administrator.

A

AAA Authentication, Authorization, and Accounting

AAL ATM Adaptation Layer

AAL1 ATM Adaptation Layer 1

AAL2 ATM Adaptation Layer 2

AAL3/4 ATM Adaptation Layer 3/4

AAL5 ATM Adaptation Layer 5

AARP AppleTalk Address Resolution Protocol

ABM Asynchronous Balanced Mode

ABR Available Bit Rate

ABR Area Border Router

ABRD Automatic Baud Rate Detection

AC Alternating Current

ACK Acknowledgment

ADSL Asymmetric Digital Subscriber Line

AH Authentication Header

AIM Asynchronous Interface Module

ANSI American National Standards Institute

APPN Advanced Peer-to-Peer Networking

ARIN American Registry for Internet Numbers

ARM Asynchronous Response Mode

ARP Address Resolution Protocol

ARPA Advanced Research Projects Agency

ARPANET Advanced Research Projects Agency Network

ARQ Automatic Repeat Request

ARU Alarm Relay Unit

AS Autonomous System

ASAM ATM Subscriber Access Multiplexer

ASBR Autonomous System Boundary Router

ASCII American Standard Code for Information Interchange

ASIC Application-Specific Integrated Circuit

ASN Auxiliary Signal Network

ATM Asynchronous Transfer Mode

ATM NIC ATM Network Interface Card

AU Access Unit

AUI Attachment Unit Interface

B

BAP Bandwidth Allocation Protocol

BACP Bandwidth Allocation Control Protocol

BAMM Bidirectional Asymmetric Multipoint-to-Multipoint

BAP Bandwidth Allocation Protocol

BAPM Bidirectional Asymmetric Point-to-Multipoint

BAPP Bidirectional Asymmetric Point-to-Point

BER Bit Error Rate

BERT Bit Error Rate Test

BG Border Gateway

BGP Border Gateway Protocol

BIOS Basic Input/Output System

B-ISDN Broadband ISDN

B-ISSI Broadband Inter-Switching System Interface

BIT Binary Digit

BMS Bandwidth Management Services

BN Boundary Node

BNI Broadband-to-Narrowband Interface

BOM Beginning of Message

BOOTP Bootstrap Protocol

BPDU Bridge Protocol Data Unit

Bps Bits per second

BRI Basic Rate Interface

C

CA Collision Avoidance

CAU Controlled Access Unit

CBR Constant Bit Rate

CBS Committed Burst Size

CCP Compression Control Protocol

CCU Communications Control Unit

CD Carrier Detect

CDMA Code Division Multiple Access

CDRAM Cache DRAM

CD-ROM Compact Disk Read Only Memory

CD-RW CD Rewritable

CDS Current Directory Structure

CDSA Common Data Security Architecture

CGI Common Gateway Interface

CGM Computer Graphics Metafile

CHAP Challenge-Handshake Authentication Protocol

CIDR Classless Inter-Domain Routing

CIF Cells in Frames

CIR Committed Information Rate

CLI Command Line Interface

CLK Clock

CLNP Connectionless Network Protocol

CLNS Connectionless Network Service Protocol

CO Central Office

COM Continuation of Message

CONS Connection-Oriented Network Services

CPS Characters Per Second

CPU Central Processing Unit

CRC Cyclic Redundancy Check

CRM Connection Request Mode

CRMI Committed Rate Measurement Interval

CSMA Carrier Sense Multiple Access

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD Carrier Sense Multiple Access with Collision Detection

CSP Cryptographic Service Provider

CSU Channel Service Unit

CTCP Client to Client Protocol

CTS Clear-to-Send

D

DAP Directory Access Protocol

DAP Data Access Protocol

DARPA Defense Advanced Research Projects Agency

DBA Data Base Administrator

DBCS Double-Byte Character Set

DC Direct Current

DCAP Data Link Switching Client Access Protocol

DCC Data Communication Channel

DCD Data Carrier Detect

DCE Data Carrier Equipment

DCP Data Compression Protocol

DCR Direct Connecting Receptacle
DDA Digital Differential Analyzer
DDC Display Data Channel
DDCMP Digital Data Communications Message Protocol
DDE Dynamic Data Exchange
DDNS Dynamic DNS
DDoS Distributed Denial of Service attack
DDP Distributed Data Processing
DDP Datagram Delivery Protocol
DE Discard Eligibility
DES Data Encryption Standard
DET Directory Entry Table
DHCP Dynamic Host Configuration Protocol
DHTML Dynamic HTML
DIMM Dual In-line Memory Module
DISA Data Interchange Standards Association
DLC Data Link Control
DLCI Data Link Connection Identifier
DLL Dynamic Link Library
DLSW Data Link Switching
DMA Direct Memory Access
DN Distinguished Names
DNA Digital Network Architecture
DNS Domain Name Service
DOS Denial of Service attack
DRAM Dynamic Random Access Memory
DS Distribution System
DSE Data Switching Equipment
DSL Digital Subscriber Line
DSMON Differentiated Services Monitoring
DSN Data Source Name
DSO Dynamic Shared Object
DSU Digital Service Unit

DSVD Digital Simultaneous Voice and Data

DTCP Digital Transmission Content Protocol

DTE Data Terminal Equipment

DTP Data Transfer Process

DTR Data-Terminal-Ready

DTS Distributed Time Service

DVMRP Distance-Vector Multicast Routing Protocol

DWDM Dense Wavelength Division Multiplexing

E

EBS Excess Burst Size

EC Error Checking

ECC Error Checking and Correction

ECF Echo Frame

ECP Encryption Control Protocol

ED Ending Delimiter

EDAC Error Detecting and Correcting

EGP Exterior Gateway Protocol

EISA Extended Industry Standard Architecture

EN End Node

EOF End of File

EOI End of Interrupt

EOL End of Line

EOR End of Record

EOT End of Transmission

EPROM Erasable Programmable Read-Only Memory

EPS Encapsulated PostScript

ESD Electro-Static Discharge

ESDI Enhanced Small Device Interface

ESDRAM Enhanced SDRAM

ESP Encapsulating Security Payload

F

FATMA Frequency and Time Multiple Access

FC Frame Control

FCAPS Faults, Configuration, Accounting, Performance, Security

FCC Federal Communications Commission

FCRAM Fast Cycle RAM

FCS Frame Check Sequence

FDDI Fiber Distributed Data Interface

FDM Frequency Division Multiplexing

FDX Full Duplex operation

FEBE Far-End Bit Error

FEC Front-End Controller

FECN Forward Explicit Congestion Notification

FERF Far-End Receive Failure

FIFO First-In First-Out

FIPS Federal Information Processing Standard

FIR Fast Infrared

FLAG Fiber-optic Link Around the Globe

FLOPS Floating Point Operations Per Second

FM Frequency Modulation

FO Fragment Offset

FPS Fast Packet Switching

FRU Field Replaceable Unit

FS Frame Status

FTAM File Transfer Access and Management

FTP File Transfer Protocol

G

GLAN Global LAN

GMM GPRS Mobility Management

GMT Greenwich Mean Time

GSM Global System for Mobile Communications

GSMP General Switch Management Protocol
GUI Graphical User Interface
GUID Global Unique Identifier (128-bit code)

H

HDLC High-level Data Link Control
HDSL High bit rate Digital Subscriber Line
HDSL-RA HDSL Rate Adaptive
HDTP Handheld Device Transport Protocol
HDX Half Duplex
HEC Header Error Control
HEL Hardware Emulation Layer
HERF High Energy Radio Frequency
HSSI High-Speed Serial Interface
HTA HTML Application
HTML Hyper Text Markup Language
HTTP Hyper Text Transport Protocol
HTTPR Reliable HTTP
HTTPS Secure HTTP
Hz Hertz

I

IAB Internet Architecture Board
IACR International Association for Cryptologic Research
IANA Internet Assigned Number Authority
IAS Information Access Service
IASIW Institute for the Advanced Study of Information Warfare
IBR Intermediate Bit Rate
IC Integrated Circuit
ICA International Communications Association
ICH I/O Controller Hub
ICMP Internet Control Message Protocol
ICMPv6 Version 6 revision of ICMP

ICP Initial Connection Protocol
IDEA International Data Encryption Algorithm
IDN Integrated Data Network
IDRP Interdomain Routing Protocol
IEEE Institute of Electrical and Electronics Engineers
IESG Internet Engineering Steering Group
IETF Internet Engineering Task Force
IGMP Internet Group Management Protocol
IGP Interior Gateway Protocol
IGRP Interior Gateway Routing Protocol
IHL Internet Header Length
IIS Internet Information Server
ILMI Interim Local Management Interface
INMS Integrated Network Management System
InterNIC Internet Network Information Center
IO Input/Output
IP Internet Protocol
IPCP Internet Protocol Control Protocol
IPES Improved Proposed Encryption Standard
IPHC IP Header Compression
IPSec IP Security
IPSO Internet Protocol Security Options
IPX Internet Packet Exchange
IPXCP Internet Packet Exchange Control Protocol
IPV6 Revised version of IP
IPV6CP IPv6 PPP Control Protocol
IRC Internet Relay Chat
IrDA Infrared Data Association
IrLAP Infrared Link Access Protocol
IrLMP Infrared Link Management Protocol
IrOBEX Infrared Object Exchange protocol
IRQ Interrupt Request
IRTF Internet Research Task Force

IS Intermediate System
ISA Industry Standard Architecture
ISDN Integrated Services Digital Network
ISI Information Sciences Institute
ISO International Organization for Standardization
ISOC Internet Society
ISSA Information Systems Security Association
IT Information Technology
IVD Integrated Voice Data

K

KB Kilobyte
Kbps Kilobits per Second
KEA Key Exchange Algorithm

L

L2F Layer 2 Forwarding
L2TP Layer 2 Tunneling Protocol
LAI Location Area Identity
LAN Local Area Network
LANA Local Area Network Adapter
LANE LAN Emulation
LAP Link-Access Procedure
LAPB Link-Access Procedure (Balanced)
LAPD Link-Access Procedure, D channel
LAPF Link-Access Procedure F (Frame Relay)
LAT Local Area Terminal
LCP Link Control Protocol
LCR Least Cost Router
LDAP Lightweight Directory Access Protocol
LDIF LDAP Data Interchange Format
LDM Local Domain Manager
LDSL Low bit rate Digital Subscriber Line

LLC Link Layer Control
LLC Logical Link Control
LLP Lower-Level Protocol
LMI Layer Management Interface
LSA Link State Algorithms
LSB Least Significant Byte

M

MAC Media Access Control
MAN Metropolitan-Area Network
MAP Management Access Protocol
MAU Medium Attachment Unit
MB Megabyte
Mbps Million bits per second
MBR Master Boot Record
MBS Maximum Burst Size
MDSL Medium bit rate Digital Subscriber Line
MFM Modified Frequency Modulation
MFT Master File Table
MFTP Multicast File Transfer Protocol
MGCP Media Gateway Control Protocol
MHS Message Handling System
MHz Megahertz
MIB Management Information Base
MIC Management Interface Connector
MID Message Identification
MIPS Million Instructions per Second
MIS Management Information System
MO Managed Object
MODEM Modulator / Demodulator
MOF Managed Object Format
MOPS Millions of Operations per Second
MOSPF Multicast Open Shortest Path First

MPDU Message Protocol Data Unit
MPOA Multi-Protocol Over ATM
MRU Maximum Receive Unit
MSB Most Significant Bit
MSB Most Significant Byte
MSS Maximum Segment Size
MTBF Mean Time Between Failures
MTTR Mean Time to Repair
MTU Maximum Transmission Unit

N

NAK Negative Acknowledgment
NANP North American Numbering Plan
NAP Network Access Points
NAS Network Attached Storage
NAT Network Address Translation
NAU Network-Addressable Unit
NBMA Nonbroadcast, Multiaccess
NBS National Bureau of Standards
NC Network Computer
NCC Network Control Center
NCM Network Control and Management
NCSA National Computer Security Association
NCSC National Computer Security Center
NE Network Element
NetBEUI NetBIOS Extended User Interface
NetBIOS Network Basic Input/Output System
NFS Network File System (Sun)
NHC Next Hop Client
NIC Network Interface Card
NIST National Institute for Standards and Technology
NIU Network Interface Unit
NIUF North American ISDN User Forum

NMC Network Management Center
NMIB Network Management Information Base
NMMP Network Management Manager Process
NMP Network Management Protocol
NMPE Network Management Protocol Entry
NMS Network Management System
NMUP Network Management User Process
NN Network Node
NNI Network to Network Interface
NSAP Network Service Access Point
NT Network Termination
NT1 Network Termination 1
NT2 Network Termination 2
NTFS NT File System (NT)
NTP Network Time Protocol
NUA Network User Address
NUI Network User Identification
NVFS Network Virtual File System
NVP Network Voice Protocol
NVRAM Non Volatile RAM

O

OAM Operations, Administration, and Maintenance
OCC Open, Cooperative Computing
OCCA Open, Cooperative Computing Architecture
ODI Open Data-Link Interface
OEM Original Equipment Manufacturer
OLE Object Linking and Embedding
OOF Out of Frame
OS Operating system
OSI Open Systems Interconnection
OSINLCP OSI Network Layer Control Protocol
OSPF Open Shortest Path First
OU Organizational Unit

P

PAD Packet Assembly / Disassembler

PAM Pulse Amplitude Modulation

PAP Password Authentication Protocol

PBX Private Branch Exchange

PC Personal computer

PCI Peripheral Component Interface

PCMCIA Personal Computer Memory Card International Association

PCR Peak Cell Rate

PCSA Personal Computing System Architecture

PCTA Personal Computer Terminal Adapter

PCU Packet Control Unit

PDN Public Data Network

PDP Packet Data Protocol

PDU Protocol Data Unit

PES Proposed Encryption Standard

PHY Physical layer medium independent

PIM Protocol Independent Multicast

PIM-DM Protocol Independent Multicast/Dense Mode

PIM-SM Protocol Independent Multicast/Sparse Mode

PING Packet Internet Groper

PKCS Public Key Cryptography Standards

PKI Public Key Infrastructure

PMP Point to Multipoint

PNNI Private Network to Network Interface

PnP Plug 'n' Play

POP Point of Presence

POST Power-on Self Test

POTS Point of Termination Station

PPP Point-to-Point Protocol

PPPBPDU PPP Bridge Protocol Data Unit

PPPMultilink Multilink Point-to-Point Protocol

PPPoE PPP over Ethernet

PPS Packets per second

PPTP Point-to-Point Tunneling Protocol

PRI Primary Rate Interface

PROM Programmable Read-Only Memory

PSDN Packet-Switched Data Network

PSPDN Packet Switched Public Data Network

PSN Private Switching Networks

PSTN Public Switched Telephone Network

PU Physical Unit

PVC Permanent Virtual Circuit

PVT Permanent Virtual Terminal

Q

QoS Quality of Service

R

RADIUS Remote Authentication Dial-In User Service

RAF Resource Allocation Frame

RAID Redundant Array of Inexpensive Disks

RAM Random Access Memory

RARP Reverse ARP

RAS Remote Access Service

RCP Remote Communications Processor

RDA Remote Database Access protocol

RDF Request Denied Frame

RDP Reliable Datagram protocol

REJ Reject

RF Radio Frequency

RFB Remote Frame Buffer

RFC Request for Comment

RFI Radio Frequency Interference

RFI Request for Information

RFP Request for Proposal

RFS Remote File Service
RIF Routing Information Field
RIP Routing Information Protocol
RISC Reduced Instruction Set Computing
RJE Remote Job Entry
RLOGIN Remote Login
RLP Radio Link Protocol
RMA Return Merchandise Authorization
RMON Remote Monitoring
RNR Receive Not Ready
ROM Read Only Memory
RPC Remote Procedure Call
RPM Rotations per Minute
RR Receive Ready
RRAS Routing and Remote Access Service
RST Reset
RTC Real Time Clock
RTD Round Trip Delay
RTF Rich Text Format
RTM Response Time Monitor
RTMP Routing Table Maintenance Protocol
RTO Retransmission Time Out
RTP Routing Update Protocol
RTS Request to Send
RTSE Reliable Transfer Service Element
RTT Round Trip Time
RUDP Reliable UDP
RW Read/Write

S

SA Security Association
SAA Systems Application Architecture
SABM Set Asynchronous Balanced Mode

SAC Single Attached Concentrator
SAP Service Advertising Protocol
SAR Segmentation And Reassembly sublayer
SARM Set Asynchronous Response Mode
SAS Single Attached Station
SCSI Small Computer System Interface
SD Starting Delimiter
SDRAM Synchronous DRAM
SFD Start Frame Delimiter
SFTP Simple File Transfer Protocol
SID Security ID
SIF Status Information Frame
SIMM Single In-line Memory Module
SIPP Single In-line Pin Package
SLA Service-Level Agreement
SMTP Simple Mail Transfer Protocol
SNA System Network Architecture
SNR Signal to Noise Ratio
SOA Start of Authentication
SOHO Small Office/Home Office
SONET Synchronous Optical Network
STA Spanning Tree Algorithm
STD Standard
STDM Synchronous Time Division Multiplexing
STE Signaling Terminal Equipment
STM Synchronous Transport Module
STP Shielded Twisted Pair
STP Spanning Tree Protocol
STS Synchronous Transport Signal level
SVC Switched Virtual Circuit
SVD Simultaneous Voice over Data
SWAP Shared Wireless Access Protocol

T

TA Terminal Adapter
TAN Transaction Number
TCA Telecommunications Association
TCP Transmission Control Protocol
TCP/IP Transmission Control Protocol/Internet Protocol
TDM Time Division Multiplex
TDMA Time Division Multiple Access
TE Terminal Equipment
TEI Terminal Endpoint Identifier
TELNET Telecommunications Network
TFTP Trivial File Transfer Protocol
TIA Telecommunications Industry Association
TL Total Length
TMN Telecommunications Management Network
TOS Type of Service
TP Transaction Program
TPDU Transport Protocol Data Unit
TPS Transactions per Second (Bus)
TPU Time Processing Unit
TS Time Slot
TSR Terminate and Stay Resident
TTL Time to Live

U

UART Universal Asynchronous Receiver Transmitter
UAWG Universal ADSL Working Group
UBR Unspecified Bit Rate
UCI User Class Identifier
UCP Universal Computer Protocol
UCS Universal Component System
UDC Universal Digital Channel
UDP User Datagram Protocol

UE User Elements
ULP Upper Level Protocol
UMB Upper Memory Block
UME UNI Management Entity
UMM Unidirectional Multipoint-to-Multipoint
UMTS Universal Mobile Telecommunications Systems
UN Unbalanced Normal
UNA Upstream Neighbor Address
UNC Universal Naming Convention
UNI User Network Interface
UPM Unidirectional Point-to-Multipoint
UPnP Universal Plug and Play
UPP Unidirectional Point-to-Point
UPS Uninterruptible Power System
URI Universal Resource Identifier
URL Uniform Resource Locator
USB Universal Serial Bus
USENET User Network
USM User-based Security Model
USTA United States Telephone Association
UTC Universal Coordinated Time
UTP Unshielded Twisted Pair

V

VAC Volts of Alternating Current
VAS Value-added services
VAT Virtual Allocation Table
VAX Virtual Address Extension
VBR Variable Bit Rate
VC Virtual Circuit
VCC Virtual Channel Connection
VCI Virtual Channel Identifier
VCL Virtual Channel Link
VCM Virtual Channel Memory

VCPI Virtual Control Programming Interface
VCSDRAM Virtual Channel SDRAM
VDC Volts of Direct Current
VDSL Very high bit rate Digital Subscriber Line
VDU Visual Display Unit
VESA Video Electronics Standards Association
VF Voice Frequency
VFAT Virtual File Allocation Table
VLAN Virtual LAN
VLSIC Very Large Scale Integrated Circuit
VM Virtual Memory
VMM Virtual Memory Manager
VMS Virtual Memory System
VOIP Voice over IP
VP Virtual Path
VPC Virtual Path Connection
VPI Virtual Path Identifier
VPL Virtual Path Link
VPN Virtual Private Network
VRE Voltage Regulated Extended
VRRP Virtual Router Redundancy Protocol
VRT Voltage Reduction Technology
VSE Virtual Storage Extended
VSIA Virtual Socket Interface Alliance

W

W3C World Wide Web Consortium
WAE Wireless Application Environment
WAIS Wide Area Information Server
WAN Wide Area Network
WAP Wireless Access Protocol
WATS Wide Area Telephone Service
WDM Wavelength Division Multiplexing

APPENDIX

B

Command Line Interpreter Commands

The use of Command Line Interpreter (CLI), also known as Command Line Interface, commands have less intensive bandwidth requirements and may be used for out-of-band management via a low-speed dialup connection connected to the Console Interface. This aids in monitoring the Nortel VPN Router when TCP/IP connectivity over the Internet has been lost and allows a user to communicate with the device to monitor and perform remote diagnostics and troubleshooting.

CLI Command mode may be entered via Telnet or the Console mode. Telnet may be used over the dialup connection if the Console Interface has been configured to accommodate TCP/IP. To use Telnet, simply telnet to the management IP address of the Nortel VPN Router. This also can be done from either the private network or through a user control tunnel established with a VPN Client over the Internet. If using a Console connection, select Command Line Interface from the Console menu choices if the Console Interface has been configured for terminal use.

The Nortel VPN Router has three levels of command mode:

- User EXEC mode
- Privileged EXEC mode
- Global configuration mode

Access via Console Connection

The console connection is an RS232 Serial Port on the unit. It may be accessed locally by connecting a compatible serial cable to a PC running a terminal emulation program such as HyperTerminal in Windows. The default settings for the Console Interface on a Nortel VPN Router is 9600 baud, 8 bits, 1 stop bit, and no parity. Upon connection to the Console Interface, you may need to press the Enter key to display the login screen. The prompt appears as follows:

```
Please enter the administrator's user name: admin <Name of the Primary
Administrator of the unit>
Please enter the administrator's password: setup <Password assigned to
the Primary Administrator Used ID>
```

NOTE **On a new unit, the default user ID for the Primary Administrator is admin with a password of setup. These values may be changed upon initial configuration of the Nortel VPN Router and can be changed only by that administrator. The user ID and password must be safeguarded. Without it, the unit cannot be totally administered or configured because the Primary Administrator has rights that no other administrator has.**

After logging in, the user is presented with the following Console Interface menu:

```
Main Menu:  System is currently in NORMAL mode.

     0) Management Address
     1) Interfaces
     2) Administrator
     3) Default Private Route Menu
     4) Default Public Route Menu
     5) Create A User Control Tunnel(IPsec) Profile
     6) Restricted Management Mode       FALSE
     7) Allow HTTP Management            TRUE
     8) Firewall Options
     9) Shutdown
     B) System Boot Options
     P) Configure Serial Port
     C) Controlled Crash
     L) Command Line Interface
     R) Reset System to Factory Defaults
     E) Exit, Save and Invoke Changes

Please select a menu choice (0 - 9,B,P,C,L,R,E):
```

Select selection `L` to enter the CLI. The user is presented with the following prompt to begin entering commands:

```
CES>
```

Access via Telnet Session

Using any Telnet utility program, a Telnet session may be established with the Nortel VPN Router by connecting to the Management Interface IP address. Once the connection is established, the user is presented with a login prompt. After logging in, the user is presented with the following prompt:

```
CES>
```

The user may now enter commands that will be acted upon by the CLI.

User EXEC Mode

The EXEC mode is a limited-display mode that is established when you Telnet to the Nortel VPN Router. In this mode, the user is unable to view the configuration file or modify configuration settings. However, in this mode, a user has the ability to clear a route.

A list of EXEC mode commands may be displayed by logging in as the administrator and typing a question mark at the command prompt as follows:

```
Login: admin
Password:
CES>?
Exec commands
  Cd       Change current directory
  Clear    Clears the IP routing table (user and admin mode), ARP cache,
           or event log (admin mode)
  dir      To display a list of files in the current directory
  enable   Enables privileged commands
  exit     Enables settings and disables exec mode and enables user level
           mode
  help     Displays information about using commands interactively
  ls       To display a list of files in the current directory
  ping     Sends a ping message to a destination
  pwd      To show the current directory
  reset    Resets a port
  show     Displays running system information
  terminal  Terminal screen configuration
```

```
trace     Enables tracing a route to a destination
verify    Verify the system
who       Displays active Telnet sessions on the CES with what number
          a particular telnet session is since boot
```

help Command

The `help` command is a descriptive command that explains the help that is available while navigating the command structure. Its output is as follows:

```
CES>help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

File System Commands

The `cd`, `dir`, `ls`, and `pwd` commands are used to view and verify the directory structure and files contained within the Nortel VPN Router.

The `pwd` command is used to print the working directory where the user is currently located. This will provide the user with the directory tree structure in subdirectory `ldif`. Following is an example:

```
CES>pwd
/ide0/system/slapd/ldif/
```

The `dir` and `ls` commands are similar in that they will display the contents of the directory that the user is currently located in. Following is an example of both:

```
CES>dir

Directory of /ide0/system/slapd/ldif/

  <DIR>                                        /ide0/
  <DIR>             FRI FEB 03 16:04:14 2006   .
  <DIR>             FRI FEB 03 16:04:36 2006   ..
```

```
            310349   FRI FEB 03 16:04:14 2006   527LDAP
             87354   FRI FEB 03 16:00:00 2006   TEMPLATE.LDF
            103784   FRI FEB 03 16:04:14 2006   TEST

CES>ls

Directory of /ide0/system/slapd/ldif/

  <DIR>  /ide0/
  <DIR>  .
  <DIR>  ..
         527LDAP
         TEMPLATE.LDF
         TEST
```

Notice the difference in the display characteristics of each command. The `dir` command gives greater details with file sizes and creation dates, along with the directory and filenames. The `ls` command displays only the names of the directories and files. If the presence of a file must be verified, use the `ls` command. When file detail is important, the `dir` command must be used.

The `cd` (change directory) command allows the user to navigate the directory structure. The standard directory structure starting at the root directory (`/`) is used within the Nortel VPN Router. All navigation starts from the current directory.

When a user first connects and is at the command-line prompt, the user is at the user level route directory of `ide0`.

```
CES>pwd
/ide0/
```

The files and directories located within this "root" directory are as shown here:

```
Directory of /ide0/

  <DIR>  /ide0/
  <DIR>  .
  <DIR>  ..
         BOOTROM.SYS
         LAB.CAP
  <DIR>  SYSTEM
  <DIR>  V05_05.220
  <DIR>  V05_05.245
  <DIR>  V06_00.140
```

The boot file, the `SYSTEM` directory, and any previous versions of code directories are displayed, along with any PCAP sniffer trace files that may have been created.

The SYSTEM directory is the current running server code directory. All files that are being used for control and logging of data when the Nortel VPN Router is operational are contained within the directories located under this directory.

To navigate down the directory tree, you can continually execute cd commands at each directory along the way to navigate to the directory below. Following is an example of navigating down to the ldif subdirectory:

```
CES>pwd
/ide0/
CES>cd system
CES>pwd
/ide0/system/
CES>cd slapd
CES>pwd
/ide0/system/slapd/
CES>cd ldif
CES>pwd
/ide0/system/slapd/ldif/
```

The pwd command was issued in each step to allow the user to see the progression down the directory tree.

If the directory is known, the user just needs to type the whole path while using only one cd command. Following is an example:

```
CES>pwd
/ide0/
CES>cd system/slapd/ldif
CES>pwd
/ide0/system/slapd/ldif/
CES>
```

So far, you have learned how to move down a directory tree. However, a user can move up or to a whole new directory branch altogether by typing in the full path with the cd command. A shorthand notation of dot-dot (..) may be used to move back up the tree one directory location.

Here is an example of using the shorthand notation of dot-dot (..) to move up a directory location:

```
CES>pwd
/ide0/system/slapd/ldif/
CES>cd ..
CES>pwd
/ide0/system/slapd/
```

Following is an example of typing a path with the cd command to move up the same directory branch:

```
CES>pwd
/ide0/system/slapd/ldif/
CES>cd /ide0/system
CES>pwd
/ide0/system/
```

who Command

The `who` command will display a list of user connections that are currently connected to the Nortel VPN Router. Following is an example:

```
CES>who
12589:    From    192.168.0.23
12618:    From    192.168.0.24
```

terminal Command

The `terminal` command is used to control the paging of the console or Telnet session screen. With paging on, only a screen's worth of information will be displayed. The user may move from one page to the next page by pressing the spacebar. With terminal paging off, the whole contents of what is being asked for by a command is scrolled over as many screens as are required to display the information requested. Following is an example with the use of the help question mark:

```
CES>terminal ?
Terminal screen configuration
  paging  Enables/disables paging
CES>terminal paging ?
  off
  on
CES>terminal paging on
```

verify Command

The `verify` command allows a user to verify the integrity of the server code on the Nortel VPN Router. Following is an example:

```
CES>verify ?
  system  Verify the software system integrity
CES>verify system
Software integrity check successful.
```

reset Command

The `reset` command is used to reset a WAN type port. The slot and port number of the device needs to be known in order to reset it. Following is an example of the `reset` command:

```
CES>reset ?
  bri     Resets a bri interface
  dial    Resets a dial interface
  serial  Resets a serial interface
CES>reset serial ?
  <0-7>/<1-4>  slot number / port number
```

exit Command

The `exit` command at the EXEC level exits the user from the command input prompt and presents a new login prompt. Following is an example:

```
CES>exit ?
  <cr>

CES>exit

Login:
```

IP Connectivity Commands

The commands for testing IP connectivity from the Nortel VPN Router to another device connected to or reachable from either the private or public interface are `ping` and `trace`. `ping` is used to test if a device is reachable from the Nortel VPN Router, whereas `trace` is used to aid in troubleshooting by showing all the reachable intermediate routing devices on the path between the Nortel VPN Router and the target device. This can be accomplished either using an IP address in decimal notation or a Fully Qualified Domain Name (FQDN). The use of an FQDN name assumes that the Nortel VPN Router is configured for and connected to a Domain Name Server (DNS) that it may use in the host name resolution of the FQDN name to a unique IP address.

Following are examples of the `ping` command.

This `ping` is over the public network:

```
CES>ping ?
  Hostname or A.B.C.D  Ping destination or hostname
CES>ping www.nortel.com
PING www.nortel.com (72.246.122.68): 36 data bytes
```

```
64 bytes from 72.246.122.68: icmp_seq=0. time= 62 ms
64 bytes from 72.246.122.68: icmp_seq=1. time= 61 ms
64 bytes from 72.246.122.68: icmp_seq=2. time= 61 ms
64 bytes from 72.246.122.68: icmp_seq=3. time= 62 ms
----www.nortel.com PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 61/61/62
```

This `ping` is over the private network:

```
PING 10.10.0.1: 36 data bytes
64 bytes from 10.10.0.1: icmp_seq=0. time=<1 ms
64 bytes from 10.10.0.1: icmp_seq=1. time=<1 ms
64 bytes from 10.10.0.1: icmp_seq=2. time=<1 ms
64 bytes from 10.10.0.1: icmp_seq=3. time=<1 ms
----10.10.0.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = <1/<1/<1
```

Following is an example of `trace`:

```
CES>trace ?
  ip  Enables tracing IP
CES>trace ip www.nortel.com
traceroute to www.nortel.com [ 72.246.122.68 ], 30 hops max, 60 byte
packets
.
.
.
.
* www.nortel.com [ 72.246.122.68 ] 50 ms 66 ms
```

The intermediate hops were removed to shorten these examples. These would change dependent on where the Nortel VPN router is located on the Internet. Only the target destination would be the same, and possibly a few of the intermediate hops, as you get closer to the target destination.

clear Command

The `clear` command in the User EXEC mode allows for the clearing of routes from the route table. Following is an example of how the `clear` command may be used:

```
CES>clear ?
Clears the IP routing table (user and admin mode), ARP cache, or event
log
(admin mode)
  ip          Clears the IP routing table entries
```

```
CES>clear ip ?
Clears the IP routing table entries
  route  Deletes route table entries
CES>clear ip route ?
  A.B.C.D  Destination network route to delete
CES>clear ip route 100.100.100.0
```

This example demonstrates the removal of a route to the 100.100.100.0 subnet network.

show Commands

An extensive number of options may be used with the `show` command to display the current running condition of the Nortel VPN Router. A few examples will be shown and discussed. You may investigate the remaining commands by exercising the commands, or refer to the *Nortel Reference Manual for the Command Line Interface*. A listing of the `show` commands follows:

```
CES>show ?
Displays running system information
  Admin              Displays admin information
  All                Displays information for all connection types
  Aot                Displays aot information
  async-over-tcp     Displays async-over-tcp configuration
  branch-office      Displays information for branch-office connections
  clock              Displays the system clock
  controller         Displays interface CSU/DSU information
  dhcp-relay         Displays DHCP Relay information
  dot1q              Display IEEE 802.1Q VLANs
  dsl                Displays DSL controller information
  event-log          Displays event log information
  file               Displays file system
  flash              Displays flash information
  ip                 Displays IP information
  ipsec              Displays information for IPSEC connections
  ipx                Displays ipx information
  l2f                Displays information for L2F connections
  l2tp               Displays information for L2TP connections
  map-class          Displays map classes
  multicast-relay    Displays Multicast Relay boundary list value
  ntp                Displays network time protocol commands
  pptp               Displays information for PPTP connections
  qos                Displays QOS information
  reload             Displays information about scheduled shutdown, if
                     any
  route-map          Route-map information
  serial-banner       Displays the serial banner text and status
  services            Displays services information
  sessions            Displays information about management sessions,
                      user connections and BO connections
```

```
  status              Displays Status information
  switch-settings     Displays switch settings
  system              Displays System information
  tunnel-guard        Displays tunnel guard attributes
  version             Displays information about system hardware and
                      software
```

show version Command

The `show version` command allows the user to view the version of server code that is running on the Nortel VPN Router, as well as other important data relating to the hardware configuration running on the unit. Following is an example of the `show version` command:

```
CES>show version ?
  <cr>

CES>show version

System Up Time
Up Time:                 011 02:05:25

System Configuration
Software Version:        V06_00.313
Software Build Date:     Jan 26 2006, 14:20:41
System Serial Number:    21787
MAC Address:             00-E0-7B-05-C9-40
BIOS Version:            PO5

Hardware Configuration
Processor 1:   Celeron 400 Mhz, L1D Cache:16K, L1I Cache:16K, L2
Cache:128K
Memory:        59 MB Free, 128 MB Total
Hard Disk 0:   1296 MB Free, 2134 MB Total
Diskette:      3.5 Inch
```

show flash Command

The `show flash` command allows the user to display the contents of the flash RAM where system information is stored. This information is stored on solid-state media and not on the hard drive. Following is an example of the command:

```
CES>show flash?
flash
CES>show flash ?
  contents  Displays current flash settings
```

```
CES>show flash contents ?
  <cr>

CES>show flash contents
Flash Header - copyright: Nortel Networks, Copyright 1999-2004
               tag:       NOC
               version:   1
               length:    1059
               count:     22
Flash Data -
model number: CES1510D
MAC address: 00-E0-7B-05-C9-40
serial number: 21787
feature keys:
     Maximum Ethernet ports: 2
     Maximum T-1 ports: 1
     Maximum T-3 ports: 0
     Allow PPTP tunnels: True
     Allow L2F tunnels: True
     Allow L2TP tunnels: True
     Allow IPsec tunnels: True
     Allow QoS internal: True
     Allow QoS admission: True
     Allow RSVP: True
     Allow RADIUS authentication: True
     Allow LDAP authentication: True
     Allow NT Domain authentication: True
     Allow RSA encryption: True
     Allow SSL: True
     Allow X.509 certificates: True
     Allow RADIUS accounting: True
     CPU clock rate 400 MHz
     CPU cache size 128 KB
     Number of CPUs supported: 1
     Allow IPX: True
     Allow NAT: True
     Firewall: Contivity Stateful Firewall
     Allow External LDAP authentication: True
     Maximum Hifn Accelerators: 0 (this value is not used !)
     FIPS Mode: False
     Allow Safe Mode Boot: False
     SERVER_FARM Mode: False
     Serial Driver Controlled Crash: Disabled
Flash Revision: 1
key length: 128
Boot Device: /ide0/
maximum concurrent sessions: flash: 100 runtime: 100
Last shutdown OK: Yes
system IP netmask: 255.255.255.0
system IP address: 10.10.0.10
system default gateway: 10.10.0.1
```

```
primary backup host: 10.10.0.51:
host username: anonymous
Advanced Routing Key: Installed
Contivity Stateful Firewall Key: Installed
checksum: 54223
```

show admin Command

This command shows the number of admin users currently on the unit. It is informative, but also can be used as a security check to ensure that not more than the authorized admin sessions are active on the unit at any one time. Following is an example of the command:

```
CES>show admin ?
Displays admin information
  sessions  Displays admin sessions
CES>show admin sessions

Summary:
 Current Sessions:
  Admin: 1
 Peak Sessions for Today:
  Admin: 3
 Total Sessions Since Boot:
  Admin: 54
```

show file Command

The `show file` command shows the status of the hard drive. It is an important command to indicate the health of the hard drive and whether housekeeping of the hard drive is required. Following is an example of the `show file` command:

```
CES>show file ?
  systems  Displays drive status
CES>show file systems
File System(s):
Size(b)         Free(b)         Type            Flags           Prefixes
2134802432      1296302080      disk            rw              /ide0/
```

show clock Command

Time is an essential component when analyzing and reviewing system information of the Nortel VPN Router. Checking the clock to ensure that it is set

properly will assist in troubleshooting if it is ever needed. Following is an example of the `show clock` command:

```
CES>show clock
 21:28:25 EST Sun Feb 19 2006
```

show ip Command

The `show ip` command displays all the different statistics and settings dealing with the use of IP on the Nortel VPN Router. The following is a listing of the `show ip` command options that are available:

```
CES>show ip ?
Displays IP information
  Bgp                          Displays BGP information
  car-statistics               Displays the statistics of client address
                               redistribution
  default-route-preference     Default Route Preference
  dhcp                         Displays the IP DHCP information
  forward-table                Displays the forwarding table
  interface                    Displays the interface configuration
  multicast-relay              Displays information about interfaces
                               configured for multicast relay
  name-server                  Displays DNS Server configuration
  ospf                         Displays IP OSPF routing details
  rip                          Displays IP RIP details
  route                        Displays IP routing tables
  route-policies               Displays IP route policies
  static                       Displays all configured static IP routes.
  Traffic                      Displays IP traffic statistics
  Vrrp                         Displays IP VRRP settings
```

show ip route Command

Often, it is important to review the routing table if there is an issue with IP traffic not being sent to or received from a network segment. The `show ip route` command displays the current route table. Following is an example of the `show ip route` command:

```
CES>show ip route
Protocol  IP Address  Mask             Cost   Next Hop      Interface
------------------------------------------------------------------------
STATIC    0.0.0.0     0.0.0.0          [10]   10.10.0.1     10.10.0.5
STATIC    0.0.0.0     255.255.255.255  [10]   100.100.100.1 100.100.100.100
```

This route table is abbreviated. However, it will contain all current active routes that have an effect on the routing of IP traffic.

show ip interface Command

The `show ip interface` command shows the current configured interfaces with the settings and status for each interface. Following is an example of the `show ip interface` command:

```
CES>show ip interface ?
  brief  Summary of the ip interface command
  <cr>

CES>show ip interface brief ?
  <cr>

CES>show ip interface brief
     Interface       Circuit   Status     Address        Mask
      ---------      -------   ------     -------        ----

*    Fast E[ 0/ 1]     0        Up     10.10.0.5         255.255.255.0
*    Fast E[ 1/ 1]     0        Up     100.100.100.100   255.255.255.0
```

show ip traffic Command

An important command when troubleshooting connectivity issues is the `show ip traffic` command. It allows the user to view various IP statistics that may indicate a problem. It aids the user in troubleshooting problems affecting traffic flow. Following is an example of the `show ip traffic` command:

```
CES>show ip traffic
               total 1110768
              badsum    0
            tooshort    0
            toosmall    0
             badhlen    0
              badlen    0
         infragments   62
         fragdropped    0
         fragtimeout    0
             forward 106941
        cantforward  198
       redirectsent    0
     unknownprotocol   66
           nobuffers    6
        reassembled   31
       outfragments   24
            noroute    1
          badoptions    0
          badversion    0
       zero src addr   22
        src=dst addr    0
```

```
      src addr error    0
     dest addr error    0
    mgmt filterdrops    0
    intf filterdrops    0
   route filterdrops  122
            qosdrops    0
      fw filterdrops 25680
       frag overflow    0


ICMP:
        3188 calls to icmp_error
        0 error not generated because old message was icmp
        Output histogram:
                echo reply: 12
                destination unreachable: 1
                time exceeded: 3187
        0 message with bad code fields
        0 message < minimum length
        0 bad checksum
        0 message with bad length
        Input histogram:
                echo reply: 69
                destination unreachable: 66
                echo: 12
                time exceeded: 364
        12 message responses generated
UDP:
        172691 total packets
        58269 input packets
        114422 output packets
        0 incomplete header
        0 bad data length field
        0 bad checksum
        2411 broadcasts received with no ports
        0 full socket
        47948 pcb cache lookups failed
        0 pcb hash lookup failed
TCP:
        888261 packets sent
                792960 data packets (125328738 bytes)
                1 data packet (402 bytes) retransmitted
                94665 ack-only packets (93932 delayed)
                0 URG only packet
                0 window probe packet
                53 window update packets
                582 control packets
        888359 packets received
                545114 acks (for 125324133 bytes)
                371 duplicate acks
                0 ack for unsent data
```

```
                788360 packets (119442024 bytes) received in-sequence
                13 completely duplicate packets (499 bytes)
                0 packet with some dup. data (0 byte duped)
                219 out-of-order packets (0 byte)
                0 packet (0 byte) of data after window
                0 window probe
                497 window update packets
                0 packet received after close
                0 discarded for bad checksum
                0 discarded for bad header offset field
                0 discarded because packet too short
        66 connection requests
        372 connection accepts
        379 connections established (including accepts)
        435 connections closed (including 36 drops)
        54 embryonic connections dropped
        543932 segments updated rtt (of 544000 attempts)
        150 retransmit timeouts
                0 connection dropped by rexmit timeout
        0 persist timeout
        153 keepalive timeouts
                110 keepalive probes sent
                43 connections dropped by keepalive
        0 pcb cache lookup failed
        3 bad syn packets detected


  Attack Statistics
        0 RST in window ACK sent
        0 sequence match SYN ACK sent
        0 out of window Data Injection drops
```

show services Command

The `show services` command allows the user to verify the services that are currently being provided by the Nortel VPN Router. This is used to verify that particular services are enabled. Following is an example of the `show services` command:

```
CES>show services ?
  all             Displays detailed output for all session types
  authentication  Displays information for authentication protocols
  management      Displays information for management protocols
  tunnel          Displays information for tunnels
  <cr>

CES>show services all ?
```

```
  <cr>

CES>show services all

Tunnel Type     Public    Private
---------------------------------------
IPsec           TRUE      TRUE
PPTP            TRUE      TRUE
L2TP&L2F        TRUE      TRUE
FWUA            FALSE     FALSE

VPN Tunnel
-------------------------------------------------
Maximum number of provisionable tunnels:       100

Management      Protocol    Port  Public    Private
-------------------------------------------------
HTTP            80          NONE            TRUE
HTTPS           443         FALSE           TRUE
SNMP            161         NONE            TRUE
FTP             21          NONE            TRUE
TELNET          23          NONE            TRUE
Identification              NONE            FALSE
CRL Retrieval               FALSE           TRUE
CMP                         FALSE           TRUE
Radius Accounting           FALSE           TRUE
ICMP                        TRUE            TRUE
SSL-VPN Admin GUI (SSH)     FALSE           TRUE
BGP                         FALSE           TRUE

Authentication Protocol     Public     Private
-----------------------------------------------------
RADIUS                      FALSE      FALSE

Certification Modes
------------------------------

FIPS           DISABLED
```

show switch-settings Command

The `show switch-settings` command allows the user to view global settings on the Nortel VPN Router. Following is an example of the `show switch-settings` command:

```
CES>show switch-settings
  Log File Lifetime        : 60 days
  Write System Log To File : Enabled
  FTP server passive mode  : Disabled
```

```
Data Collection Interval : Disabled
Event Log Size           : 2000 entries
File Compression         : Disabled
```

enable Command

The `enable` command allows a user to be at the Privileged EXEC mode. This mode allows the administrator user to have more Privileged rights, allowing for a greater amount of control and the ability to view a wider range of settings and logging. Following is an example of the `enable` command:

```
CES>enable ?
  <cr>

CES>enable
Password:
CES#
```

The command-line prompt changes to a pound sign (#) upon entering the Privileged EXEC mode. To return to the User EXEC mode, an `exit` command needs to be entered.

Privileged EXEC Mode

The Privileged EXEC mode has a wider range of commands for configuration and viewing. The Privileged EXEC mode is attained by entering an `enable` command at the User EXEC mode of the CLI. Following is a list of Privileged EXEC commands:

```
CES#?
Exec commands
  boot           Restarts the CES using specific loaded image
  capture        Captures network traffic
  cd             Change current directory
  clear          Clears the IP routing table (user and admin mode), ARP
                 cache, or event log (admin mode)
  clock          Sets the system clock
  configure      Enables configuration mode
  connect        Establishes a desired connection
  copy           Copy files or copy to file system related information
  create         Creates recovery diskette or updates flash
  debug          Enables debugging of some nncli commands
  delete         To delete file(s)
  dir            To display a list of files in the current directory
  disable        Disables privileged commands
  enable         Enables privileged commands
```

```
  exit            Enables settings and disables exec mode and
                  enables userlevel mode
  forced-logoff   Logs off active connections
  help            Displays information about using commands interactively
  kill            Terminates a Telnet session
  ls              To display a list of files in the current directory
  microcode       Reloads firmware. Reload may take several minutes per
                  card.
  mkdir           To create a new directory
  more            Displays the contents of a file
  no              Disables or Deletes the attributes
  ping            Sends a ping message to a destination
  pwd             To show the current directory
  reformat        Formats the floppy disk
  reload          Halt and perform a cold restart
  rename          To rename a file or a directory
  reset           Resets a port
  retrieve        Retrieves a software image for the switch
  rmdir           To remove an existing directory
  show            Displays running system information
  ssl-vpn         SSL-VPN Accelerator commands
  ssl-vpn-cli     Switch to SSL CLI
  terminal        Terminal screen configuration
  trace           Enables tracing a route to a destination
  verify          Verify the system
  who             Displays active Telnet sessions on the CES with what
                  number a particular telnet session is since boot
```

Although there are common commands with the User EXEC mode, the Privileged EXEC commands of `clear`, `reset`, and `show` have additional options. The difference in the command will be shown in the following examples.

clear Command

The `clear` command adds options to clear the ARP cache, flow cache, and event log. The ability to clear a route table entry remains the same as in the User EXEC mode. Following is an example of the `clear` command with the additional options:

```
CES#clear ?
Clears the IP routing table (user and admin mode), ARP cache, or event
log
(admin mode)
  arp-cache       Clears the entire ARP cache
  flow-cache      Clears Firewall/NAT flow cache
  ip              Clears the IP routing table entries
  logging         Clears the event-log
CES#clear arp-cache ?
```

```
  <cr>

CES#clear arp-cache
```

reset Command

The `reset` command has an additional option to reset the RADIUS server. The ability to reset the BRI, dial, and serial interfaces remains the same as in the User EXEC mode. Following is an example of the `reset` command with the additional option:

```
CES#reset ?
  Bri               Resets a bri interface
  Dial              Resets a dial interface
  radius-server     Reset Radius Server
  serial            Resets a serial interface
CES#reset radius-server ?
  <cr>

CES#reset radius-server
-- Operation Complete --
Ordering of Server will take effect at next radius authentication.
Date 02/20/2006  Time 20:26:15
Success
```

show Command

The `show` command in the Privileged EXEC mode has many more options than the `show` command in the User EXEC mode. Following is a listing of the commands:

```
CES#show ?
Displays running system information
  admin                     Displays admin information
  all                       Displays information for all connection
                            types
  aot                       Displays aot information
  arp                       Displays ARP table
  async-over-tcp            Displays async-over-tcp configuration
  branch-office             Displays information for branch-office
                            connections
  clip                      Displays Circuitless IP (CLIP) configuration
  clock                     Displays the system clock
  compress-files            Displays the file compression setting
  controller                Displays interface CSU/DSU information
  current-config-file       Displays the current config file
```

```
data-collection-interval  Displays data collection interval
                          information
demand                    Displays DOD configuration information
dhcp                      Displays the IP DHCP information
dhcp-relay                Displays DHCP Relay information
dot1q                     Display IEEE 802.1Q VLANs
dsl                       Displays DSL controller information
ecmp                      Displays the ECMP configuration
event-log                 Displays event log information
file                      Displays file system
flash                     Displays flash information
frame-relay               Displays Frame Relay statistics
health                    Displays the health of CES
hosts                     Displays system identity
interface                 Displays interface information
ip                        Displays IP information
ipsec                     Displays information for IPSEC connections
ipx                       Displays ipx information
l2f                       Displays information for L2F connections
l2tp                      Displays information for L2TP connections
log-file-lifetime         Displays log file lifetime information
logging                   Displays contents of various logs
map-class                 Displays map classes
microcode                 Displays microcode version
multicast-relay           Displays Multicast Relay boundary list value
ntp                       Displays network time protocol commands
pptp                      Displays information for PPTP connections
qos                       Displays QOS information
radius-server             Displays radius server information
reload                    Displays information about scheduled
                          shutdown, if any
route-map                 Route-map information
router                    Show router Options
running-config            Displays the current system running
                          information
safe-mode                 Displays the safe mode configuration
                          information
serial-banner             Displays the serial banner text and status
serial-port               Displays the serial port configuration
                          information
services                  Displays services information
sessions                  Displays information about management
                          sessions, user connections and BO
                          connections
snmp                      Displays the SNMP settings
snmp-traps                Displays SNMP Trap settings
software                  Displays available software versions
ssl-vpn                   Displays SSL-VPN accelerator information
status                    Displays Status information
switch-settings           Displays switch settings
system                    Displays System information
```

```
  tunnel-guard              Displays tunnel guard attributes
  users                     Displays users' names
  version                   Displays information about system hardware
                            and software
```

show all Command

The `show all` command displays all the tunnels that are currently established on the Nortel VPN Router. Following is an example of the `show all` command:

```
CES#show all ?
  sessions  Displays information for all sessions
CES#show all sessions ?
  detail  Displays detailed output for the specified session types
  <cr>

CES#show all sessions detail ?
  <cr>

CES#show all sessions detail

Summary:
 Current Sessions:
  Branch Office: 0
  End User: 1
  Total: 1
 Peak Sessions for Today:
  End User: 2
 Total Sessions Since Boot:
  End User: 66

Current Branch Office Sessions:

Current End User Sessions:

 User: Rich
 Account Type: IPSEC
 UID: rich
  Session ID: 13811
  IP Address Assigned: 10.10.0.211
  IP Address Public: 100.100.100.10
  Start Date: 02/20/2006
  Start Time: 16:44:32
  KBytes In: 1040
  KBytes Out: 13666
  Packets In: 18016
  Packets Out: 26713
```

show current-config-file Command

The `show current-config-file` command displays the current configuration file that the Nortel VPN Router is running on. Following is an example of the `show current-config-file` command:

```
CES#show current-config-file ?
  <cr>

CES#show current-config-file
The current config file is :
/ide0/system/config/CFG00242.DAT
```

show dhcp Command

The `show dhcp` command shows the configured DHCP servers and the parameters set for the leasing of IP addresses. Following is an example of the `show dhcp` command:

```
CES#show dhcp ?
  server  Displays known DHCP servers
  <cr>

CES#show dhcp server ?
  <cr>

CES#show dhcp server

DHCP Proxy Server Configuration
DHCP Proxy is disabled. Address Pools used.
              DHCP server:         Primary    10.10.0.1
                                   Secondary  0.0.0.0
                                   Tertiary   0.0.0.0
          DHCP Cache size:         1
Immediate Address Release:         Enabled
   DHCP Blackout Interval:         300
Override Blackout Interval
when no addresses are available:   Enabled
```

show health Command

The `show health` command is equivalent to the Health Check selection on the GUI interface screen. It gives the current status of all major components on the unit and the state of the servers providing services to the Nortel VPN Router. Following is an example of the output produced by the `show health` command:

```
CES#show health ?
  alerts     Displays alert messages
  all     Displays all conditions
  disabled     Displays disable messages
  warnings     Displays warning messages
  <cr>

CES#show health all ?
  <cr>

CES#show health all
Enabled      Audible Alarm                  Audible Alarm is enabled
Alert        NAT                            LDAP policy parse failed -
                                            Using system default policy
Alert        Auto Backup Servers            Can't backup to 10.10.0.51
Alert        RADIUS Authentication Servers  No Radius Servers Hosts are
                                            enabled.
Warning     SNMP Servers                    Server not configured
Disabled     VRRP                           Disabled
Disabled     FIPS                           FIPS Disabled.
Disabled     Anti-Spoofing                  Anti-Spoofing Disabled
Disabled     Multicast Relay                Multicast Relay is Globally
                                            Disabled
Disabled     CMP                            No Certificate Requests
                                            submitted
Disabled     Certificates Validity          No certificate defined
Disabled     DLSw                           DLSw feature disabled
Disabled     OSPF                           OSPF is not init
Disabled     Global Demand Services         Demand services globally
                                            disabled
Disabled     DHCP Server                    DHCP Server Disabled
Disabled     DhcpRelay                      Dhcp relay agent is
                                            disabled
Disabled     IPSec Failover Service         Failover service disabled
Disabled     CLIP                           CLIP is disabled
OK           Tunnelguard                    Tunnelguard Operational
OK           RIP                            Operational
OK           Routing Policy Server          Routing Policy Server is up
OK           Firewall                       Contivity Stateful Firewall
                                            Active
OK           Client Routes Marshaler        ClientRoutesMarshaler is UP
OK           LAN on Slot 1 Interface 1      Device fei1 up
OK           LAN on System Board            Device fei0 up
OK           Temporary Licenses             Operational
OK           Load Balancing Service         Server not configured
OK           Internal LDAP Server           Operational
OK           RADIUS Accounting Server       Server not enabled
OK           Network Time Protocol          Time set
OK           External LDAP Servers          Server not enabled
OK           Buffer Usage                   Utilization is below 75%
```

```
OK          Memory Usage                  Utilization is below 75%
OK          Hard Disk 0                   Utilization is below 75%
                                          on /ide0/
OK          Intrusion                     Operational
OK          Normal Temperature            Operational
OK          Voltage 12 V Minus            Operational
OK          Voltage 12 V Plus             Operational
OK          Voltage 2.5 VA                Operational
OK          Voltage 3.3 V Plus            Operational
OK          Voltage 5 V Minus             Operational
OK          Voltage 5 V Plus              Operational
OK          Chassis Fan                   Operational
OK          LDAP Proxy Servers            Server not configured
OK          IP Address Pool               Operational
OK          DNS Servers                   Operational
OK          Heart Beat
```

show interface Command

The `show interface` command will display the current configuration of an interface, along with its current status. It may be used to display the condition of every physical interface on the Nortel VPN Router. Following is an example of interfaces on the VPN Router:

```
CES#
CES#show interface ?
  Atm              Displays information on ATM interfaces
  Bri              Displays ISDN card information
  Dial             Displays dial interface information
  Fastethernet     Displays information for Fast Ethernet interfaces
  gigabitethernet  Displays information for Gigabit Ethernet interfaces
  groups           Displays interface groups information
  serial           Displays serial interface information
  <cr>
```

As an example, the Fast Ethernet interface was selected to display its configuration and current status. Following is example output of the command:

```
CES#show interface fastethernet ?
  <0-6>/<1-4>  (slot number) / (interface number)
  <cr>

CES#show interface fastethernet 0/1
FastEthernet Interface 0/1 Configuration
  Description                              :
  DHCP-relay                               : Enabled
  Duplex                                   : AutoNegotiate
  Filter                                   : deny all
```

```
IP Address                                  : 10.10.0.5
Mac pause                                   : Disabled
MTU                                         : 1500
PPPoE                                       : Disabled
Public/Private                              : Private
DHCP Service                                : Disabled
Status                                      : Enabled
Speed                                       : AutoNegotiate
TCP-Maximum Segment Size Clamping           : Disabled
TCP-Maximum Segment Size [bytes]            : 1460
802.1Q                                      : Disabled
802.1Q Interface VLAN ID                    : 1
802.1Q Interface VLAN Untagged Ingress      : TRUE
802.1Q Interface VLAN Untagged Egress       : TRUE
```

show ip Command

The `show ip` command is an important tool that will assist you in determining how the unit is configured to pass and route IP traffic. There is a vast selection of options for this command. Following is a listing of the `show ip` command options:

```
CES#show ip ?
Displays IP information
  access-list                  Displays IP access list
  as-path                      Displays AS path access list
  bgp                          Displays BGP information
  car-statistics               Displays the statistics of client address
                               redistribution
  community-list               Displays community list
  default-route-preference     Default Route Preference
  dhcp                         Displays the IP DHCP information
  forward-table                Displays the forwarding table
  interface                    Displays the interface configuration
  local                        Displays status of address acquisition
                               pool
  multicast-relay              Displays information about interfaces
                               configured for multicast relay
  name-server                  Displays DNS Server configuration
  ospf                         Displays IP OSPF routing details
  rip                          Displays IP RIP details
  route                        Displays IP routing tables
  route-policies               Displays IP route policies
  static                       Displays all configured static IP routes.
  Traffic                      Displays IP traffic statistics
  Vrrp                         Displays IP VRRP settings
```

One option of the `show ip` command is to display information on the local IP pools that are being used to assign IP addresses to VPN clients when they tunnel to the Nortel VPN router. A sample output of the `show ip local` command is as follows:

```
CES#show ip local ?
  pool  Displays local address pool
CES#show ip local pool?
pool
CES#show ip local pool

 Name     Begin          End           Mask             Total     InUse

Default   10.10.0.75     10.10.0.76    255.255.255.0    2         0
sup_grp   20.20.0.30     20.20.0.40    255.255.255.0    11        0


Address Pool Blackout Interval:    30
     if Named Pool Unavailable:    Failover
```

The `show ip route` command may be used to verify IP routes or may be used in troubleshooting a routing issue. The options with this command can allow for a granular inspection of routes by routing protocol, or to display all routes in the Nortel VPN Router. Following is a listing of the `show ip route` command options:

```
CES#show ip route ?
  A.B.C.D     Displays routes to the specified network only
  all         Displays all routes; if omitted, only the best routes are
              displayed
  bgp         Displays BGP routes only
  clip        Displays Circuitless IP (CLIP) routes
  direct      Displays direct routes only
  interface   Displays routes for specified interface only
  nat         Displays nat routes
  ospf        Displays OSPF routes only
  rip         Displays RIP routes only
  static      Displays static routes only
  summary     Displays a summary of the information in the IP routing
              table
  utunnel     Displays user tunnel routes only
  <cr>
```

The `show ip route summary` displays a quick summary of the number of routes contained within the routing table of the Nortel VPN Router and the routing protocols responsible for their placement in the table. The output of the `show ip route summary` command is as follows:

```
CES#show ip route summary ?
  <cr>

CES#show ip route summary


IP routing table summary
Maximum ECMP Paths = 1
Total routes = 11
Best routes = 11
Static routes = 6
Direct routes = 4
BGP routes = 0
RIP routes = 0
OSPF routes = 0
CLIP routes = 0
NAT routes = 0
```

The `show ip route` command allows an administrator to examine the contents of the routing table. The table can be displayed in its entirety with all routes, or just a section of the routing table by protocol. This is useful when troubleshooting a particular dynamic protocol and why routes are not being populated or removed when they should be. The options available with the `show ip route` command are as follows:

```
CES#show ip route ?
  A.B.C.D     Displays routes to the specified network only
  all         Displays all routes; if omitted, only the best routes are
              displayed
  bgp         Displays BGP routes only
  clip        Displays Circuitless IP (CLIP) routes
  direct      Displays direct routes only
  interface   Displays routes for specified interface only
  nat         Displays nat routes
  ospf        Displays OSPF routes only
  rip         Displays RIP routes only
  static      Displays static routes only
  summary     Displays a summary of the information in the IP routing
              table
  utunnel     Displays user tunnel routes only
  <cr>
```

show hosts Command

The `show hosts` command displays the information that identifies the Nortel VPN Router by its domain name if it is registered in one and the domain servers it utilizes, along with the management address of the unit. A sample output of the `show hosts` command is as follows:

```
CES#show hosts ?
  <cr>

CES#show hosts

     Management IP Address:      10.10.0.10
             DNS Host Name:      None
          DNS Domain Name:       None
        DNS Server Address
                    primary:     10.10.0.1
                  secondary:     0.0.0.0
                   tertiary:     0.0.0.0
                     fourth:     0.0.0.0
```

show ipsec Command

The `show ipsec` command is used to display the current end user tunnels that are connected to the Nortel VPN Router. It also displays other information such as IP address used and statistical information useful in determining client usage and to assist in troubleshooting client connections. A sample output of the `show ipsec` command is as follows:

```
CES#show ipsec ?
  sessions  Displays information for IPSEC End User connections
CES#show ipsec sessions ?
  detail  Displays detailed output for the specified session types
  <cr>

CES#show ipsec sessions detail ?
  <cr>

CES#show ipsec sessions detail

Summary:
 Current Sessions:
  IPSEC: 1
 Peak Sessions for Today:
  IPSEC: 1
 Total Sessions Since Boot:
  IPSEC: 2

Current End User Sessions:

 User: Rich
 Account Type: IPSEC
 UID: rich
  Session ID: 984
  IP Address Assigned: 10.10.0.211
  IP Address Public: 100.100.100.10
```

```
  Start Date: 02/24/2006
  Start Time: 19:55:46
  KBytes In: 2952
  KBytes Out: 5383
  Packets In: 37334
  Packets Out: 22632
```

show logging Command

Logging is an important feature of the Nortel VPN Router. The same information that is available through the Web-based GUI display of logs is obtainable with the use of the CLI `show logging` command. Logs aid in verifying the health of the VPN Router, as well as storing historical data for review. A list of the logs that may be displayed is as follows:

```
CES#show logging ?
  auto-save-logging      Displays auto-save-logging parameters
  capture-filter         Displays event-log capture filter parameters
  config                 Displays contents of configuration log
  display-filter         Displays event-log display filter parameters
  events                 Displays contents of event log
  history                Displays history setting used
  security               Displays contents of security log
  syslog                 Displays contents of system log
```

The `show logging` command can be used to show only particular types of notifications or all log entries. A sample output of the `show logging syslog` command is as follows:

```
CES#show logging syslog ?
  alert     Displays alert messages
  all       Display all events
  crit      Displays critical messages
  debug     Displays debug messages
  emerg     Displays emergency messages
  err       Displays error messages
  info      Displays info messages
  notice    Displays notice messages
  warning   Displays warning messages
```

The following sample output shows that there are no alerts within the syslog to display because a prompt is returned without any log information. A sample output of the `show logging syslog alert` command is as follows:

```
CES#show logging syslog alert ?
  <cr>

CES#
```

The following sample output shows that there is an event notification recorded in the syslog log file. The sample output shown here indicates that a system event is being recorded because the VPN Routers's clock has been reset via the Network Time Protocol (NTP):

```
CES#show logging syslog notice
 00:18:46 tEvtLgMgr 0 : NTP [05] time reset -0.177232 s
```

show ntp command

The `show ntp` command displays the current configuration of the NTP feature on the Nortel VPN Router. Proper time is essential for logging and the timing of events. The use of NTP allows this to be accomplished transparently once it is configured. A sample output of the `show ntp` command is as follows:

```
CES#show ntp ?
  associations  Displays associations status
  <cr>

CES#show ntp
NTP: enable
Synchronize time with Broadcast Server: enable
Synchronize time with Multicast Server: enable
Servers:
  Server IP Address    Interface       Key ID     Bursting    Version
      132.163.4.101    Private          0         Disabled      1
Authentication keys:
```

show router Command

The `show router` command displays the router options configured on the Nortel VPN Router and the current status. A sample output of the `show router` command is as follows:

```
CES#show Router ?
Show router Options
  car  Show Client Address Redistribution Config
CES#show Router car ?
  <cr>

CES#show Router car
Client Address Redistribution Configuration
  CAR: enabled
  CAR Aggregation Mode: host
  Max Number of Client Host Routes: 200
```

show snmp Command

The `show snmp` command allows for the display of the configuration of the SNMP parameters on the Nortel VPN Router. A sample output of the `show snmp` command options is as follows:

```
CES#show snmp ?
  get-host     Displays SNMP get-hosts information
  host         Displays SNMP trap hosts information
  identity     Displays SNMP identity information
  mib          Displays SNMP MIBs information
```

Depending on the SNMP option selected, a display of the settings for that option is presented. A sample output of the `show snmp mib` command is as follows:

```
CES#show snmp mib ?
  <cr>

CES#show snmp mib
  IP Tunnel:     ENABLED
  RIPv2:         ENABLED
  OSPF:          ENABLED
  BGP:           ENABLED
  VRRP:          ENABLED
  IPX:           ENABLED
  RIPSAP:        ENABLED
  DSU/CSU:       ENABLED
```

show software Command

The `show software` command displays the current version of the server code, along with all other versions of server code loaded on the Nortel VPN Router. The current running version of server code is highlighted with an asterisk. A sample output of the `show software` command is as follows:

```
CES#show software ?
  version  Displays running version (*) and list of versions loaded on
the CES
CES#show software version ?
  <cr>

CES#show software version
V06_00.313*
V05_05.220
V05_05.245
V06_00.140
```

show status Command

The `show status` command shows a wide variety of statistical information for the current status of the Nortel VPN Router. A listing of the options available for the `show status statistics` command is as follows:

```
CES#show status ?
Displays Status information
  statistics     Displays statistics
CES#show status statistics ?
  admin          Displays admin statistics
  hardware       Displays hardware statistics
  interfaces     Displays interface statistics
  network        Displays network statistics
  resources      Displays resource statistics
  routing        Displays routing statistics
  security       Displays security statistics
  system         Displays system statistics
```

There are additional options for each statistics option. A sample output of the `show status statistics system` command is as follows:

```
CES#show status statistics system ?
  config-file       Displays ASCII contents of configuration file
  event-objects     Displays the internal software objects
  file-system       Displays file system statistics
  flash-contents    Displays contents of non-volatile memory
  ntp-stats         Displays NTP statistics
  object-list       Information for Nortel Networks engineers only
  version           Displays the software version number
```

A sample of the statistics for the NTP feature of the Nortel VPN Router is as follows:

```
CES#show status statistics system ntp-stats ?
  <cr>

CES#show status statistics system ntp-stats
Date 02/26/2006  Time 02:22:45
NTP Servers: (* active server)

  remote        local     st poll   reach    delay    offset     disp
==============================================================================
*132.163.4.101  0.0.0.0   1  128    377      0.13330  -0.043510  0.01695


NTP packet:

Packet received:     808
Packet processed:    808
```

```
Packet sent:          929
Packet not sent:      0
Packet dropped:       0
Packet ignored:       0
Bad stratum:          0
Bad authentication:   0
Bad length:           0
Old version:          808
New version:          0
```

show system Command

The `show system` command has one option, `forwarding`, which displays the forwarding action enabled on the Nortel VPN Router. The information displayed shows the manner in which packets are forwarded through tunnels and physical interfaces. A sample output of the `show system forwarding` command is as follows:

```
CES#show system ?
  forwarding  Displays forwarding settings
CES#show system forwarding ?
  <cr>

CES#show system forwarding
system forwarding proxy-arp End-User tunnel enabled
system forwarding proxy-arp Branch-Office tunnel enabled
system forwarding proxy-arp Physical Interfaces disabled
system forwarding proxy-arp NAT enabled
system forwarding gratuitous-arp disabled
system forwarding tunnel-to-tunnel-traffic EU-to-EU disabled
system forwarding tunnel-to-tunnel-traffic EU-to-BO disabled
system forwarding tunnel-to-tunnel-traffic BO-to-BO disabled
system private-to-tunnel nexthop forwarding disabled
```

This command is useful in verifying the action taken on a tunneled packet while troubleshooting either branch office or user tunnel operation.

show running Configuration Command

The `show running-config` command shows the entire current running configuration on the Nortel VPN Router. It has all the settings for all the options, so the file is useful in verifying the configuration of various components and features of the VPN Router while at the CLI level. The file is extensive and it is recommended that a user perform the command to see what information is displayed when this command is executed. For the purposes of this appendix, the command will be displayed truncated with various sections highlighted and discussed.

This shows the license keys installed and active for the various features of the Nortel VPN Router that require a license key:

```
CES>show running-config
! !!! license install AR! !!! license install FW! !!! no license DW! !!!
no license BG! !!! no license PR
```

This shows the primary administrative username and its encrypted password:

```
adminname admin epassword "xlz3TY98PIw="
```

This shows the IP address of the management interface of the Nortel VPN Router:

```
ip address 10.10.0.10
```

This shows the settings on the NTP server to maintain the proper operation of the Nortel VPN Router's clock:

```
ntp server 132.163.4.101 source private key none bursting disable version 1
```

This shows all the settings of the QoS configuration for traffic shaping on the Nortel VPN router. The information contained is the complete configuration of QoS, only a small portion of which is shown here:

```
no qos bandwidth-management enable
no qos admission-control enable
qos bandwidth-rates  14400
qos bandwidth-rates  28800
qos bandwidth-rates  56000
qos bandwidth-rates  128000
qos bandwidth-rates  256000
qos bandwidth-rates  512000
```

This shows the QoS settings as they are applied to a physical interface. In this portion of the configuration file, it is the QoS information as it is applied to the Fast Ethernet interface:

```
interface Fastethernet 1/1
no qos egress-dscp-map
no qos Ingress-dscp-map
```

This shows the settings of the tunnel `deny all/in` filter. It is more extensive than the portion displayed in this appendix.

```
filter tunnel rule "deny all/in"
port "any" 0
port "dns" 53
```

```
port "dynamic port begin" 1023
port "Entrust CA" 709
port "finger" 79
port "ftp" 21
port "ftp-data" 20
```

The following shows the settings of the tunnel `deny all/out` filter. It is more extensive than the portion displayed in this appendix.

```
filter tunnel rule "deny all/out"
action deny
direction outbound
connection none
use protocol "ip"
use address "any"
use src-port eq "any"
```

The number of tunnel filters is extensive. The rules shown here are just a small percentage of the tunnel filters that are implied by the Nortel VPN Routers configuration or that have been created by users:

```
filter tunnel rule "permit all/out"
.filter tunnel rule "permit dns(tcp)/in"
.filter tunnel rule "permit dns(tcp)/out"
.filter tunnel rule "permit dns(udp)/in"
.filter tunnel rule "permit dns(udp)/out"
.
filter tunnel rule "permit Entrust CA/in"
.filter tunnel rule "permit Entrust CA/out"
.filter tunnel rule "permit finger/in"
```

The following shows a small portion of the interface `deny all/in` filter. As with tunnel filters, there are filters applied to the physical interfaces of the Nortel VPN Router.

```
filter interface rule "deny all/in"
port "any" 0
port "DNS" 53
port "Dynamic Port Begin" 1023
port "Entrust CA" 829
port "Finger" 79
port "FTP Control" 21
port "FTP Data" 20
```

The following shows a small portion of the interface filter rules that are applied to the physical interfaces of the Nortel VPN Router:

```
filter interface rule "deny all/out"
filter interface rule "permit all/in"
filter interface rule "permit all/out"
```

The following shows a portion of the configuration of the Fast Ethernet physical interface:

```
interface FastEthernet 1/1
ip address 100.100.100.100 255.255.255.0
no shutdown
filter "deny all"
publicspeed auto
no dot1q enable
dot1q interface vlan-id 1
dot1q interface untag ingress
```

The following shows the configuration of the serial console interface. It is configured to allow a modem to be attached to the Nortel VPN Router to aid in the ability to perform out-of-band management of the unit if for any reason it is no longer accessible over the Internet.

```
interface dial 7/1
auto-answer 1
baud-rate 9600
mode serial-menu
dial-prefix-string +++ATDT
filter "deny all"
no phone
modem-initialization-string +++ATZ
modem-termination-string +++ATH
no mtu
no tcp-mss enable
no tcp-mss
menu-access-level UNRESTRICTED
```

This area of the configuration file shows the public and private default routes, along with the configuration of the routing protocols the Nortel VPN Router is capable of performing. It has been abbreviated for the purposes of this appendix and the user is encouraged to view the file using the CLI command.

```
router static
ip default-network 10.10.0.1 private 10 enable
ip default-network 100.100.100.1 public 10 enable
ip route 132.163.4.101 255.255.255.255 10.10.0.1 10 enable
access-list "test" permit 10.10.0.0 255.255.255.0 exact
```

The following shows only a small portion of the overall settings that may be applied to users and groups to control the access of user client connections to the Nortel VPN Router. This section displays the settings by user group and the tunneling protocol that is being used. The size of this section is directly proportional to the amount of groups that have been created on the VPN Router.

```
group ipsec "/Base/Support"
default banner
default display-banner
default rekey timeout
default rekey data-count
default password-storage
default pfs
default mobility enable
default antireplay enable
default compress
default encryption
default encryption ike
default nortel-client action
default nortel-client version
```

The following shows a small portion of the firewall policies that have been created by the users. Each firewall policy that is created and the rules applied to it are displayed in this area.

```
policy security add "lab"
policy security "lab"
rule override add src-interface "tunnel:any" dst-interface "system" action
rule override add src-interface "trusted" dst-interface "trusted" action accept
```

This section shows the users that have been configured using the local LDAP of the Nortel VPN Router:

```
user add "Rich" "/Base/Support"
user "Rich" "/Base/Support"
static-ipaddress 10.10.0.211
static-subnet-mask 255.255.255.0
ipsec uid "rich" epassword "t6eIvDy3Jj4="
default ipsec server-ca
no ipsec issuer-ca
no ipsec uid pwchange enable
administration uid "rich" epassword "t6eIvDy3Jj4="
no administration dynamic-authenticate
administration switch-manage manage
administration users-manage manage
administration group-manage "/Base/Support"
```

This section shows the configuration of groups being used for Branch Office Tunnels (BOT). This area will include all groups that were created by users for the association with and control of those tunnels. These settings correspond to the Connectivity section of the group configuration.

```
bo-group connectivity "/Base"
access-hours "Anytime"
priority call-admission highest
```

```
priority forwarding low
idle-timeout 00:01:00
forced-logoff 00:00:00
no nailed-up
no rsvp
rsvp token-bucket depth 3000
rsvp token-bucket rate 28
excess rate 5000000
! !!! Temporary set of excess rate to maximum value
committed rate 56000
excess rate 128000
excess action MARK
```

This section continues with the settings of group `Base` and the information contained and configured in the IPSec section of the group settings:

```
bo-group ipsec "/Base"
rekey timeout 08:00:00
rekey data-count 0no pfs
no antireplay enable
no compress
initial-contact enable
encryption des56-md5
encryption hmac-sha1
encryption hmac-md5
no encryption 3des-md5
no encryption des40-md5
encryption ike des56-group1
vendor-id
isakmp-retransmission interval 16
isakmp-retransmission max-attempts 4
keepalive interval 00:01:00
no keepalive ondemand-conn
df-bit CLEAR
```

This section shows the configuration of an IPSec BOT. For each such tunnel created by the user, the configuration information for that tunnel will be contained in this section of the configuration file.

```
bo-conn add "SupGrp" "/Base" conn-type peer2peer
bo-conn "SupGrp" "/Base"
state enable
filter "permit all"
local-endpoint 100.100.100.100
remote-endpoint 100.100.100.101
routing type static
routing static
local-network "localnet"
remote-network 20.20.20.0 mask 255.255.255.0 state enable cost 10
remote-network 40.40.40.0 mask 255.255.255.0 state enable cost 10
```

```
exit
tunnel-type ipsec
ipsec authentication etext-pre-shared-key "LRxLg6+rETc="
mtu enable
mtu 1788
exit
```

The following shows a small portion of the SNMP configuration on the Nortel VPN Router. The section is extensive and we recommend that the user use the CLI to review the settings enabled on the unit.

```
snmp-server get-host  10.10.0.51 "public" enabled
snmp-server mib iptunnel
snmp-server mib rip2
snmp-server mib ospf
snmp-server mib bgp
snmp-server mib vrrp
snmp-server mib ipx
snmp-server mib ripsap
snmp-server mib dsu/csu
snmp-server enable traps hardware lan-1/1 interval 00:03:00
no snmp-server enable traps hardware lan-1/1
snmp-server enable traps hardware lan-system interval 00:03:00
no snmp-server enable traps hardware lan-system
```

This section deals with the backup utility on the Nortel VPN Router. The backup has many options and can be programmed to perform scheduled backups at given time intervals set by the user. This section is more extensive than what is displayed in this appendix.

```
exception backup 1 10.10.0.51 interval 5 username "anonymous" epassword
"bd9OuemXz9A="
no exception backup advanced 1 full
exception backup advanced 1 full
no exception backup advanced 1 system
no exception backup advanced 1 configuration
no exception backup advanced 1 log
```

This section shows the firewall policies in place on the Nortel VPN Router. This is more extensive than what is shown in this appendix.

```
firewall policy
policy nat interface enable
! !!! Reboot CES for NAT interface state change to take effect.
no firewall anti-spoof
no firewall strict-tcp-rules
firewall tunnel-filter
firewall tunnel-management-filter
firewall connection-number 4000
```

The following shows the system forwarding settings on the Nortel VPN Router:

```
system forwarding proxy-arp branch-office-tunnels enable
no system forwarding proxy-arp physical-interfaces enable
system forwarding proxy-arp nat enable
no system forwarding gratuitous-arp enable
no system forwarding tunnel-to-tunnel-traffic EU-to-EU enable
no system forwarding tunnel-to-tunnel-traffic EU-to-BO enable
no system forwarding tunnel-to-tunnel-traffic BO-to-BO enable
no system forwarding nexthop-forward enable
```

This section is a partial display of the log gathering settings for the Nortel VPN Router. There are additional settings and the user is again encouraged to make use of the CLI to see its display capabilities.

```
data-collection-interval 2
log-file-lifetime 60
event-log size 2000
no compress-files enable
system-log-to-file enable
```

boot Command

This command gives the administrator the ability to boot the Nortel VPN Router using a specified boot image file. This command must be used carefully because it may change the overall operation of the device and make it incapable of being managed remotely. A sample display of the command is as follows:

```
CES#boot ?
  system  The CES
CES#boot system ?
  WORD  Software image
```

capture Command

The `capture` command is a useful troubleshooting tool that can be used to perform sniffer traces on all the interfaces (both physical and tunnel-based) of the Nortel VPN Router. This is necessary when there are communication issues as to why traffic is either not being passed or possibly being altered. The `capture` needs to be enabled by the primary administrator and the packet data is captured and stored on the local hard drive of the VPN Router. We recommend that when packet capture has been completed, it should be disabled because it requires system resources to accomplish the capture and an unnecessary overhead under normal operating conditions. A sample of the `capture` command output is as follows:

```
CES#capture ?
  add   Adds new capture
  WORD  Capture name
CES#capture add ?
  WORD  Name of the capture
CES#capture add lab.cap ?
  atm              ATM interface capture
  bri              Bri interface capture
  dial             Dial interface capture
  FastEthernet     Fast Ethernet interface capture
  GigabitEthernet  Gigabit Ethernet interface capture
  Global           Global RAW IP capture
  Serial           Serial interface capture
  Tunnel           Tunnel capture
CES#capture add lab.cap FastEthernet ?
  <0-6>/<1-4>
CES#capture add lab.cap FastEthernet 0/1 ?
  size  Capture buffer size
  <cr>

CES#capture add lab.cap FastEthernet 0/1
CES#capture ?
  add   Adds new capture
  WORD  Capture name
```

More information on the use of the `capture` capability of the Nortel VPN Router is discussed in Chapter 12.

create Command

The `create` command is used to create recovery diskettes in Nortel VPN Router units with floppy disk drives and to update the flash memory in units that do not have a floppy drive as part of their configuration. Although the command for the creation of a floppy-based recovery diskette can be exercised remotely, it requires local interaction with the unit with the insertion of the floppy disk into the drive and its removal after the recovery operation has been successfully completed. Creation of a recovery floppy diskette is highly recommended. It is good practice to create a new diskette each time a unit has its server code upgraded. The diskette should be safeguarded from damage and placed in a location that all administrative users are aware of for possible use if the need should ever occur. A sample output of the command is as follows:

```
CES#create ?
  diskette  Creates recovery diskette
  recovery  Updates flash (for recovery purposes)
CES#create diskette ?
  <cr>
```

delete Command

The `delete` command is capable of deleting files from the storage media on the Nortel VPN Router. The user should be very familiar with the file structure of the VPN Router before exercising this command because it's possible to accidentally remove files that are necessary for the operation of the VPN Router. A sample output of the command is as follows:

```
CES#delete ?
  WORD  URL of the file to be deleted
CES#delete
```

forced-logoff Command

The `forced-logoff` command is an administrative tool that is used to force one or all user and Branch Office Tunnels to be disconnected from the Nortel VPN Router. This is used by administrators when it is necessary for maintenance purposes to not have tunnels established to the unit. A sample output of the `forced-logoff` command is as follows:

```
CES#forced-logoff ?
Logs off active connections
  bo-conn  Logs off specific or all active BO connections
  user     Logs off specific or all active users
CES#forced-logoff user ?
  all-non-admin  Logs off all active non-admin users
  WORD           User name
CES#forced-logoff bo-conn ?
  all   Logs off all active BO connections
  WORD  BO connection name
```

kill Command

The `kill` command is used to kill Telnet sessions. It may be used in conjunction with the `who` command, which displays the current Telnet sessions on the Nortel VPN Router. A sample output of the `kill` and `who` commands is as follows:

```
CES#kill ?
  WORD  Telnet session ID
CES#
CES#who ?
  A.B.C.D  IP address session is from
  <cr>

CES#who
2964:    From    192.168.0.23
```

The user displayed in the `who` command can be killed using the process session ID associated with the displayed IP address. So, in this instance, to kill the Telnet session from the IP address of 192.168.0.23, the command `kill 2964` is issued to terminate that Telnet session.

mkdir Command

The `mkdir` command will create a new directory on the storage media of the Nortel VPN Router. The user should specify the whole path if the directory is to be created down the directory structure of the file system. A sample command in this case would appear as follows:

```
mkdir /<directory 1 name>/<directory 2 name>/<name of new directory>
```

Although this example shows only two directory levels deep, it may be as long as necessary to create the directory in the proper directory branch. If no path is specified, the new directory will be created in the root directory of `/ide0`.

A sample display of the `mkdir` command is as follows:

```
ES#mkdir ?
  WORD  The name of the directory to create
CES#mkdir /ide0/system/test
```

rmdir Command

The `rmdir` command will remove a directory from the storage media of the Nortel VPN Router. The user should be very familiar with the file structure of the file system in order to avoidinadvertently removing directories essential to the operation of the VPN Router. As with the `mkdir` command, the `rmdir` command requires the full path to be defined to perform the operation. A sample output of the `rmdir` command is as follows:

```
CES#rmdir /ide0/system/test
CES#
```

Upon successful removal of the directory, the user will be returned to the Privileged EXEC level command prompt.

more Command

The `more` command is used to display the contents of a file to the console or Telnet session screen. The file should be text-based. If not, the display may appear garbled and the terminal session may no longer respond correctly,

which means you'll need to terminate the session and restart a new one. A sample output of the `more` command is as follows:

```
CES# more version.dat
V06_00.313
```

reformat Command

The `reformat` command is used to reformat the floppy diskette to be used in the creation of a recovery diskette. Although the command may be executed remotely, local interaction is necessary because you need to place and remove the floppy diskette on the Nortel VPN Router. A sample output of the `reformat` command is as follows:

```
CES#reformat ?
  diskette  Reformats the diskette
CES#reformat diskette ?
  full   Formats the floppy disk in full mode.
  quick  Formats the floppy disk in quick mode.
CES#reformat diskette full ?
  <cr>
```

reload Command

The `reload` command gives a remote administrator the capability to restart the Nortel VPN Router. A variety of options are available with this command, as shown in the following sample output:

```
CES#reload ?
  At                    Reload at a specific time/date
  boot-drive            Enables reboot drive
  boot-normal           Boot in normal mode
  boot-safe             Boot in safe mode
  cancel                Cancels pending reload
  config-file           Enables boot configuration file
  disable-after-restart Prevents remote logins after shutdown
  disable-logins        Prevents new remote logins before shutdown
  in                    Reload after a time interval
  LINE                  Reason for reload
  no-sessions           Reload after all users log off
  power-off             Power down after shutdown
  restart               Restart after shutdown
  <cr>
```

Because this command will perform a cold restart of the unit, it will cause all user and Branch Office Tunnels to drop. This command must be used carefully and with proper notification to all those who would be affected when exercising this command.

rename Command

The `rename` command is used to rename a file or a directory. The assumption is that the path will be specified, or that the user will be one directory level above a directory to be named, or within a directory where a file that is to be renamed is located. A sample of the `rename` command is as follows:

```
CES#rename ?
  WORD  Source URL
CES#
CES#mkdir /ide0/system/test
CES#rename /ide0/system/test test1
CES#dir /ide0/system

Directory of /ide0/system/

  <DIR>                                                  /ide0/
   .
   .
  <DIR>          SUN FEB 26 13:56:58 2006                TEST1
  <DIR>          FRI FEB 03 16:00:12 2006                UCODE
          12     WED FEB 08 17:58:00 2006                UPGRADE.DAT
          12     FRI FEB 03 15:58:38 2006                VERSION.DAT
```

From this example, you can see that a directory `test` was created and renamed to `test1`. To verify this, a section of the `/ide0/system` directory is displayed showing that the directory `test1` currently resides within that directory structure.

retrieve Command

The `retrieve` command is used to obtain a new software image from an FTP server where it is stored. The code must be located on the server in the directory that is specified within the command. In the following sample output of the command, it is assumed that it has been placed in the root directory of the FTP server. The FTP server root directory does not necessarily have to be the root directory of the computer itself, but a directory that the FTP server interpreted to be its root. Sample output of the `retrieve` command is as follows:

```
CES#retrieve ?
  software  Enables retrieval of the latest software image
CES#retrieve software ?
  Hostname or A.B.C.D  IP addr of the host remote server
CES#retrieve software 10.10.0.51 ?
  version  Software image file version
CES#retrieve software 10.10.0.51 version ?
  WORD  Software image
CES#retrieve software 10.10.0.51 version V06_00.313 ?
  path  Path to the directory where the software is stored
  uid   User ID for the FTP server
CES#$oftware 10.10.0.51 version V06_00.313 path V06_00.313 uid anonymous ?
  password  FTP server password
CES#$51 version V06_00.313 path V06_00.313 uid anonymous password guest ?
  recurse  Do it anyway if present
  <cr>

CES#$rsion V06_00.313 path V06_00.313 uid anonymous password guest recurse ?
  <cr>
```

Notice that the path does not specify a path, but rather a filename of the optimized sever code that may be loaded directly on the Nortel VPN Router. Because no other path has been specified, it is understood that the file resides within the root directory of the FTP server. The `recurse` portion of the command represents recursion in that if the code is already resident on the unit, to overwrite it with the code that is currently being retrieved.

The optimized version of server code is indicated by the suffix extensions of `tar` and `gz` being used on the file. These files have been in use since the version V04_85 release of server code. It allows the FTP process to go much more smoothly with the extraction of a single file, and its expansion takes place directly on the unit when retrieval has been completed. Files with the `zip` extension must be unzipped into a directory named with the code version that is to be applied, and located within the root directory or specified path of the FTP server. Whenever possible, you should use the optimized version of server code because of its ease of use.

Global Configuration Mode

The Global Configuration mode allows an administrative user to configure all parameters and features of the Nortel VPN Router. However, these commands are extremely powerful, and they must be practiced so that the user is thoroughly familiar with the commands and contexts prior to executing these commands on an operational Nortel VPN Router. Also, these commands may require a particular sequence of commands to be executed in the proper order.

We highly recommend that users take the time to familiarize themselves totally with the command and its behavior on the unit prior to using it on a VPN Router that is in a production environment. Improper context, syntax, or execution of a command can cause the unit to be unmanageable remotely and, in severe conditions, can necessitate recovery actions to restore the unit to its mode of operation prior to an improper command being executed.

As with all upgrades, configuration changes, or anything that may affect the overall operation of the unit, the minimum of a backup of the configuration file and LDAP files should be done prior to exercising the command as a precaution in case recovery is made necessary.

A listing of the available configuration commands is as follows:

```
CES#configure ?
  terminal  Enable configuration from the terminal
CES#configure terminal
Enter configuration commands, one per line.  End with Ctrl/z.
CES(config)#?
Configure commands:
  aaa                       Authentication, authorization and accounting
  access-hours              Adds and configures access hours
  access-list               Adds an access list entry
  accounting                Accounting server
  adminname                 Enables administrator to enable the administrator
                            login name and password
  aot                       Async over tcp
  arp                       Adds a static ARP entry
  audible                   Enables audible alarm
  auto-save-logging         Enables auto-save-logging function for event-log
  bgp                       Enable BGP over public interfaces
  bo-conn                   Adds or configures branch office connections
  bo-group                  Enables branch office group configuration commands
  clear                     Disables the number of days the journal files will
                            be removed from internal RADIUS server
  client-policy             Adds or modifies client policy
  clip                      Configures Circuitless IP
  clock                     Sets the system clock
  cmp                       Enables certificate management protocol
  compress-files            Enables file compression
  console                   Sets or displays the restriction level of the
                            console session
  controller                configure physical I/O parameters
  create                    Creates Safe mode config
  crl                       Enables the retrieval of certificate revocation
                            list(CRLs)
  crypto                    Enables crypto certificate configuration
  data-collection-interval  Displays data collection interval information
  default                   Enables default switch settings configuration
  demand                    Configures Demand services
  dns-proxy                 Enables DNS Proxy on the CES
  domain                    Edits or adds domain set or domain
```

```
end                     Exits from configure mode
erase                   Deletes a configuration file
event-log               Specifies the size of the event log
exception               Defines backup FTP servers for the CES
exit                    Saves settings and leaves configuration mode
filter                  Enables filter configuration
fips                    Enables federal information processing standards
firewall                Enables firewall type
frame-relay             Enables Frame Relay debug mode on a specific slot
                        and port
ftp-server              Configures file transfer protocol to the system
                        management IP Address
fwua                    Enables Firewall User Authentication
group                   Configures user groups
help                    Describes the interactive help system
hostname                Enables the system hostname
http                    Configures HTTP protocol
https                   Enables HTTPS service
icmp                    Enables ICMP service
identification          Enables identification protocol to the system
                        managment IP Address
idle-timeout            Enables an automatic logout when an administrator
                        session is not in use
interface               Selects an interface to configure OR configures an
                        interface group
ip                      Enables IP settings
ipsec                   Enables IPSEC tunnel configuration
ipx                     ipx commands
l2f                     L2F tunnel configuration
l2tp                    L2TP tunnel configuration
ldap                    Control LDAP server (Mini-CLI emulation)
ldap-server             LDAP server configuration
license                 Installs license key for paid feature
load                    Bulk load configuration commands (Mini-CLI
                        emulation)
log-file-lifetime       Sets the log file's time to live (in days)
logging                 Enables the syslog server host
logout                  Disconnect this telnet session
map-class               Configures a map-class
maximum-paths           Enables the maximum equal cost paths
multicast-boundary      Enables adding interfaces to multicast boundary
                        list
multicast-relay         Enables multicast relay
network                 Adds network and allows to assign IP address and
                        subnet mask to the network
no                      Disables features
ntp                     Enables network time protocol
ospf                    Enables the maximum equal cost paths to calculate
                        within OSPF
policy                  CSF Policy Manager
pptp                    Enables PPTP tunnel configuration
prompt                  Changes session prompt
proxy                   Enables the external LDAP authentication server
```

```
qos                     Enables qos
radius                  Enables RADIUS service
radius-accounting       Enables RADIUS Accounting service
radius-client           Configures Radius Client
radius-server           Radius server configuration
restrict                Restricts management access to CES (Mini-CLI
                        emulation)
rip                     maximum equal cost paths to calculate within RIP
route-map               Add a route map
route-policy            Enables the route policy feature
router                  Specifies a routing process to configure
safe-mode               Enables Safe Mode Configuration
save                    Save current boot config (Mini-CLI emulation)
scheduler               Enables scheduler settings
serial-banner           Configure the serial banner
serial-banner-fragment  Add a new line to serial banner
serial-port             Enables serial port configuration
service                 Enables services
show                    Displays configuration information
snmp-server             SNMP Server settings
split-dns               Enables DNS Server to be split between public and
                        private domains
ssh                     Enables SSH service
ssl                     Configures SSL
ssl-vpn                 SSL-VPN Acceleration configuration mode
system                  Enables system settings
system-log-to-file      Write system log to file
telnet                  Virtual terminal protocol to the system management
                        IP address
Tunnel                  Enables the tunneling protocols, i.e., IPsec, PPTP,
                        L2TP, L2F
tunnel-guard            Enables to set tunnel guard properties
user                    User configuration mode
```

Summary

The Command Line Interpreter (CLI) command set is extensive. It provides a terminal or Telnet user great flexibility and control over the configuration and maintenance of the Nortel VPN Router. These commands allow a user to perform these functions with low-bandwidth requirements, which makes the CLI command set extremely useful in out-of-band management scenarios.

However, with the power and flexibility of these commands, the user must be careful in their use. The command line is not as intuitive as a GUI-based user interface, nor does it have complete checking on the execution of the command. Whereas the GUI interface may flag a problem, the CLI command may not. We highly recommend that users familiarize themselves totally with the commands

and the options within them prior to their use in a production environment. The best way to do this is in a lab environment where the user can exercise various commands and observe their behavior.

As you can see by the contents of this appendix, the CLI command library is extensive. This appendix is intended as a quick introduction to the use of the CLI command set and is not totally inclusive of all the options that these commands contain.

APPENDIX

C

Related Request for Comments Reference Guide

A Request for Comments (RFC) is a document that is generated to outline a standard. The RFC is published by the Internet Engineering Task Force (IETF). Most RFCs are drafts and can be changed later. All RFCs are submitted and reviewed before they are published. Once an RFC becomes a standard, no other changes are allowed to the RFC. An RFC can, however, be replaced by an updated RFC in the future.

RFCs are informational in nature and suggest processes to obtain a goal. There are even a few RFCs that are humorous and really serve no other purpose than to entertain. A few of these are listed toward the end of this appendix.

Table C-1 shows RFCs that are related to many of the standards and protocols that have been discussed in this book. This should serve as a reference where you can obtain very basic information about the RFC; you can then access the RFC for additional reading. If you need more information about a particular RFC, or about RFCs in general, you can get it from the ICTF Web site:

```
www.ietf.org/
```

Table C-1: RFC Reference

TOPIC	RFC NUMBER	TITLE	STATUS
L2F			
	2341	Cisco Layer Two Forwarding (Protocol) "L2F"	Historic
L2TP			
	2661	Layer Two Tunneling Protocol "L2TP"	Proposed Standard
	2809	Implementation of L2TP Compulsory Tunneling via RADIUS	Informational
	2888	Secure Remote Access with L2TP	Informational
	3070	Layer Two Tunneling Protocol (L2TP) over Frame Relay	Proposed Standard
	3145	L2TP Disconnect Cause Information	Proposed Standard
	3193	Securing L2TP Using IPSec	Proposed Standard
	3301	Layer Two Tunneling Protocol (L2TP): ATM access network extensions	Proposed Standard
	3308	Layer Two Tunneling Protocol (L2TP) Differentiated Services Extension	Proposed Standard
	3355	Layer Two Tunneling Protocol (L2TP) Over ATM Adaptation Layer 5 (AAL5)	Proposed Standard
	3371	Layer Two Tunneling Protocol "L2TP" Management Information Base	Proposed Standard
	3438	Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers Authority (IANA) Considerations Update	Best Current Practice
	3573	Signaling of Modem-On-Hold Status in Layer 2 Tunneling Protocol (L2TP)	Proposed Standard
	3817	Layer 2 Tunneling Protocol (L2TP) Active Discovery Relay for PPP over Ethernet (PPPoE)	Informational

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	3931	Layer Two Tunneling Protocol Version 3 (L2tpv3)	Proposed Standard
	4045	Extensions to Support Efficient Carrying of Multicast Traffic in Layer-2 Tunneling Protocol (L2TP)	Experimental
PPTP			
	2637	Point-to-Point Tunneling Protocol	Informational
IPSec			
	2207	RSVP Extensions for IPSec Data Flows	Proposed Standard
	2410	The NULL Encryption Algorithm and Its Use with IPSec	Proposed Standard
	2709	Security Model with Tunnel-mode IPSec for NAT Domains	Informational
	3104	RSIP Support for End-to-End IPSec	Experimental
	3193	Securing L2TP Using IPSec	Proposed Standard
	3456	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPSec Tunnel Mode	Proposed Standard
	3457	Requirements for IPSec Remote Access Scenarios	Informational
	3554	On the Use of Stream Control Transmission Protocol (SCTP) with IPSec	Proposed Standard
	3566	The AES-XCBC-MAC-96 Algorithm and Its Use with IPSec	Proposed Standard
	3585	IPSec Configuration Policy Information Model	Proposed Standard

(continued)

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	3602	The AES-CBC Cipher Algorithm and Its Use with IPSec	Proposed Standard
	3686	Using Advanced Encryption Standard (AES) Counter Mode with IPSec Encapsulating Security Payload (ESP)	Proposed Standard
	3715	IPSec-Network Address Translation (NAT) Compatibility Requirements	Informational
	3776	Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	Proposed Standard
	3884	Use of IPSec Transport Mode for Dynamic Routing	Informational
	3948	UDP Encapsulation of IPSec ESP Packets	Proposed Standard
	4025	A Method for Storing IPSec Keying Material in DNS	Proposed Standard
	4106	The Use of Galois/Counter Mode (GCM) in IPSec Encapsulating Security Payload (ESP)	Proposed Standard
	4196	The SEED Cipher Algorithm and Its Use with IPSec	Proposed Standard
	4304	Extended Sequence Number (ESN) Addendum to IPSec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	Proposed Standard
	4308	Cryptographic Suites for IPSec	Proposed Standard
	4309	Using Advanced Encryption Standard (AES) CCM Mode with IPSec Encapsulating Security Payload (ESP)	Proposed Standard
	4312	The Camellia Cipher Algorithm and Its Use with IPSec	Proposed Standard

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
VPN			
	2547	BGP/MPLS VPNs	Informational
	2685	Virtual Private Networks Identifier	Proposed Standard
	2735	NHRP Support for Virtual Private Networks	Proposed Standard
	2764	A Framework for IP Based Virtual Private Networks	Informational
	2917	A Core MPLS IP VPN Architecture	Informational
	3809	Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)	Informational
	4026	Provider Provisioned Virtual Private Network (VPN) Terminology	Informational
	4031	Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks (PPVPNs)	Informational
	4093	Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways	Informational
	4110	A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)	Informational
	4111	Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)	Informational
	4176	Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management	Informational
	4265	Definition of Textual Conventions for Virtual Private Network (VPN) Management	Proposed Standard

(continued)

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	4364	BGP/MPLS IP Virtual Private Networks (VPNs)	Proposed Standard
	4365	Applicability Statement for BGP/MPLS IP Virtual Private Networks (VPNs)	Informational
	4381	Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)	Informational
	4382	MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base	Proposed Standard
DES/3DES			
	1969	The PPP DES Encryption Protocol (DESE)	Informational
	2419	The PPP DES Encryption Protocol, Version 2 (DESE-bis)	Proposed Standard
	2420	The PPP Triple-DES Encryption Protocol (3DESE)	Proposed Standard
	3537	Wrapping a Hashed Message Authentication Code (HMAC) Key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES) Key	Proposed Standard
IKE/ISAKMP			
	2407	The Internet IP Security Domain of Interpretation for ISAKMP	Proposed Standard
	2408	Internet Security Association and Key Management Protocol (ISAKMP)	Proposed Standard
	2409	The Internet Key Exchange (IKE)	Proposed Standard
	3526	More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE)	Proposed Standard

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	3664	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)	Proposed Standard
	3706	A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers	Informational
	3947	Negotiation of NAT-Traversal in the IKE	Proposed Standard
	4109	Algorithms for Internet Key Exchange version 1 (IKEv1)	Proposed Standard
	4306	Internet Key Exchange (IKEv2) Protocol	Proposed Standard
	4304	Extended Sequence Number (ESN) Addendum to IPSec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	Proposed Standard
	4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	Proposed Standard
	4322	Opportunistic Encryption Using the Internet Key Exchange (IKE)	Informational
AES			
	3268	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)	Proposed Standard
	3394	Advanced Encryption Standard (AES) Key Wrap Algorithm	Informational
	3537	Wrapping a Hashed Message Authentication Code (HMAC) Key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES) Key	Proposed Standard

(continued)

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	3565	Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)	Proposed Standard
	3566	The AES-XCBC-MAC-96 Algorithm and Its Use with IPSec	Proposed Standard
	3602	The AES-CBC Cipher Algorithm and Its Use with IPSec	Proposed Standard
	3664	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)	Proposed Standard
	3686	Using Advanced Encryption Standard (AES) Counter Mode with IPSec Encapsulating Security Payload (ESP)	Proposed Standard
	3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-Based Security Model	Proposed Standard
	3853	S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)	Proposed Standard
	3962	Advanced Encryption Standard (AES) Encryption for Kerberos 5	Proposed Standard
	4309	Using Advanced Encryption Standard (AES) CCM Mode with IPSec Encapsulating Security Payload (ESP)	Proposed Standard
Radius			
	2058	Remote Authentication Dial In User Service (RADIUS)	Proposed Standard
	2059	RADIUS Accounting	Informational
	2138	Remote Authentication Dial In User Service (RADIUS)	Proposed Standard

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	2139	RADIUS Accounting	Informational
	2548	Microsoft Vendor-specific RADIUS Attributes	Informational
	2618	RADIUS Authentication Client MIB	Proposed Standard
	2619	RADIUS Authentication Server MIB	Proposed Standard
	2620	RADIUS Accounting Client MIB	Informational
	2621	RADIUS Accounting Server MIB	Informational
	2809	Implementation of L2TP Compulsory Tunneling via RADIUS	Informational
	2865	Remote Authentication Dial In User Service (RADIUS)	Draft Standard
	2866	RADIUS Accounting	Informational
	2867	RADIUS Accounting Modifications for Tunnel Protocol Support	Informational
	2868	RADIUS Attributes for Tunnel Protocol Support	Informational
	2869	RADIUS Extensions	Informational
	2882	Network Access Servers Requirements: Extended RADIUS Practices	Informational
	3162	RADIUS and IPv6	Proposed Standard
	3575	IANA Considerations for RADIUS (Remote Authentication Dial In User Service)	Proposed Standard
	3576	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	Informational

(continued)

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	3579	RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)	Informational
	3580	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines	Informational
	4014	Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option	Proposed Standard
LDAP			
	1487	X.500 Lightweight Directory Access Protocol	Historic
	1558	A String Representation of LDAP Search Filters	Informational
	1777	Lightweight Directory Access Protocol (LDAP)	Historic
	1823	The LDAP Application Program Interface	Informational
	1959	An LDAP URL Format	Proposed Standard
	1960	A String Representation of LDAP Search Filters	Proposed Standard
	2164	Use of an X.500/LDAP Directory to Support MIXER Address Mapping	Proposed Standard
	2247	Using Domains in LDAP/X.500 Distinguished Names	Proposed Standard
	2251	Lightweight Directory Access Protocol (v3)	Proposed Standard
	2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions	Proposed Standard

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	2253	Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names	Proposed Standard
	2254	The String Representation of LDAP Search Filters	Proposed Standard
	2255	The LDAP URL Format	Proposed Standard
	2256	A Summary of the X.500(96) User Schema for Use with LDAPv3	Proposed Standard
	2307	An Approach for Using LDAP as a Network Information Service	Experimental
	2559	Internet X.509 Public Key Infrastructure Operational Protocols LDAPv2	Historic
	2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	Proposed Standard
	2589	Lightweight Directory Access Protocol (v3): Extensions for Dynamic Directory Services	Proposed Standard
	2596	Use of Language Codes in LDAP	Proposed Standard
	2649	An LDAP Control and Schema for Holding Operation Signatures	Experimental
	2657	LDAPv2 Client vs. the Index Mesh	Experimental
	2696	LDAP Control Extension for Simple Paged Results Manipulation	Informational
	2713	Schema for Representing Java(tm) Objects in an LDAP Directory	Informational
	2714	Schema for Representing CORBA Object References in an LDAP Directory	Informational

(continued)

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	2739	Calendar Attributes for vCard and LDAP	Proposed Standard
	2798	Definition of the inetOrgPerson LDAP Object Class	Informational
	2820	Access Control Requirements for LDAP	Informational
	2829	Authentication Methods for LDAP	Proposed Standard
	2830	Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security	Proposed Standard
	2849	The LDAP Data Interchange Format (LDIF) Technical Specification	Proposed Standard
	2891	LDAP Control Extension for Server Side Sorting of Search Results	Proposed Standard
	2926	Conversion of LDAP Schemas to and from SLP Templates	Informational
	2927	MIME Directory Profile for LDAP Schema	Informational
	3045	Storing Vendor Information in the LDAP root DSE	Informational
	3062	LDAP Password Modify Extended Operation. K. Zeilenga	Proposed Standard
	3088	OpenLDAP Root Service: An Experimental LDAP Referral Service	Experimental
	3112	LDAP Authentication Password Schema	Informational
	3296	Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories	Proposed Standard

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	3352	Connection-less Lightweight Directory Access Protocol (CLDAP) to Historic Status	Informational
	3377	Lightweight Directory Access Protocol (v3): Technical Specification	Proposed Standard
	3383	Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)	Best Current Practice
	3384	Lightweight Directory Access Protocol (version 3) Replication Requirements	Informational
	3494	Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status	Informational
	3663	Domain Administrative Data in Lightweight Directory Access Protocol (LDAP)	Experimental
	3671	Collective Attributes in the Lightweight Directory Access Protocol (LDAP)	Proposed Standard
	3672	Subentries in the Lightweight Directory Access Protocol (LDAP)	Proposed Standard
	3673	Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes	Proposed Standard
	3674	Feature Discovery in Lightweight Directory Access Protocol (LDAP)	Proposed Standard
	3687	Lightweight Directory Access Protocol (LDAP) and X.500 Component Matching Rules	Proposed Standard
	3698	Lightweight Directory Access Protocol (LDAP): Additional Matching Rules	Proposed Standard

(continued)

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	3703	Policy Core Lightweight Directory Access Protocol (LDAP) Schema	Proposed Standard
	3712	Lightweight Directory Access Protocol (LDAP): Schema for Printer Services	Informational
	3727	ASN.1 Module Definition for the LDAP and X.500 Component Matching Rules	Proposed Standard
	3771	The Lightweight Directory Access Protocol (LDAP) Intermediate Response Message	Proposed Standard
	3829	Lightweight Directory Access Protocol (LDAP) Authorization Identity Request and Response Controls	Informational
	3866	Language Tags and Ranges in the Lightweight Directory Access Protocol (LDAP)	Proposed Standard
	3876	Returning Matched Values with the Lightweight Directory Access Protocol version 3 (LDAPv3)	Proposed Standard
	3909	Lightweight Directory Access Protocol (LDAP) Cancel Operation	Proposed Standard
	3928	Lightweight Directory Access Protocol (LDAP) Client Update Protocol (LCUP)	Proposed Standard
	4104	Policy Core Extension Lightweight Directory Access Protocol Schema (PCELS)	Proposed Standard
	4370	Lightweight Directory Access Protocol (LDAP) Proxied Authorization Control	Proposed Standard
	4373	Lightweight Directory Access Protocol (LDAP) Bulk Update/ Replication Protocol (LBURP)	Informational

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
Certificates			
	2528	Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	Informational
	2538	Storing Certificates in the Domain Name System (DNS)	Proposed Standard
	3039	Internet X.509 Public Key Infrastructure Qualified Certificates Profile	Proposed Standard
	3709	Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates	Proposed Standard
	3739	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	Proposed Standard
QoS			
	2212	Specification of Guaranteed Quality of Service	Proposed Standard
	2386	A Framework for QoS-based Routing in the Internet	Informational
	2676	QoS Routing Mechanisms and OSPF Extensions	Experimental
	2990	Next Steps for the IP QoS Architecture	Informational
	3317	Differentiated Services Quality of Service Policy Information Base	Informational
	3387	Considerations from the Service Management Research Group (SMRG) on Quality of Service (QoS) in the IP Network	Informational
	3583	Requirements of a Quality of Service (QoS) Solution for Mobile IP	Informational

(continued)

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	3644	Policy Quality of Service (QoS) Information Model	Proposed Standard
	3670	Information Model for Describing Network Device QoS Datapath Mechanisms	Proposed Standard
	4323	Data Over Cable System Interface Specification Quality of Service Management Information Base (DOCSIS-QoS MIB)	Proposed Standard
VRRP			
	2338	Virtual Router Redundancy Protocol	Proposed Standard
	3768	Virtual Router Redundancy Protocol (VRRP)	Draft Standard
BGP			
	1105	Border Gateway Protocol (BGP)	Experimental
	1163	Border Gateway Protocol (BGP)	Historic
	1164	Application of the Border Gateway Protocol in the Internet	Historic
	1265	BGP Protocol Analysis	Informational
	1267	Border Gateway Protocol 3 (BGP-3)	Historic
	1268	Application of the Border Gateway Protocol in the Internet	Historic
	1269	Definitions of Managed Objects for the Border Gateway Protocol: Version 3	Proposed Standard
	1364	BGP OSPF Interaction	Proposed Standard
	1397	Default Route Advertisement In BGP2 and BGP3 Version of the Border Gateway Protocol	Proposed Standard
	1403	BGP OSPF Interaction	Historic

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	1654	A Border Gateway Protocol 4 (BGP-4)	Proposed Standard
	1655	Application of the Border Gateway Protocol in the Internet	Proposed Standard
	1656	BGP-4 Protocol Document Roadmap and Implementation Experience	Informational
	1657	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4)	Draft Standard
	1771	A Border Gateway Protocol 4 (BGP-4)	Draft Standard
	1772	Application of the Border Gateway Protocol in the Internet	Draft Standard
	1773	Experience with the BGP-4 Protocol	Informational
	1774	BGP-4 Protocol Analysis	Informational
	1966	BGP Route Reflection: An Alternative to Full Mesh IBGP	Experimental
	1997	BGP Communities Attribute	Proposed Standard
	1998	An Application of the BGP Community Attribute in Multi-home Routing	Informational
	2042	Registering New BGP Attribute Types	Informational
	2385	Protection of BGP Sessions via the TCP MD5 Signature Option	Proposed Standard
	2439	BGP Route Flap Damping	Proposed Standard
	2796	BGP Route Reflection: An Alternative to Full Mesh IBGP	Proposed Standard
	3345	Border Gateway Protocol (BGP) Persistent Route Oscillation Condition	Informational

(continued)

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	3882	Configuring BGP to Block Denial-of-Service Attacks	Informational
	4098	Terminology for Benchmarking BGP Device Convergence in the Control Plane	Informational
	4272	BGP Security Vulnerabilities Analysis	Informational
	4360	BGP Extended Communities Attribute	Proposed Standard
	4384	BGP Communities for Data Collection	Best Current Practice
OSPF			
	1131	OSPF Specification	Proposed Standard
	1245	OSPF Protocol Analysis	Informational
	1246	Experience with the OSPF Protocol	Informational
	1247	OSPF Version 2	Draft Standard
	1248	OSPF Version 2 Management Information Base	Proposed Standard
	1252	OSPF Version 2 Management Information Base	Proposed Standard
	1253	OSPF Version 2 Management Information Base	Proposed Standard
	1364	BGP OSPF Interaction	Proposed Standard
	1403	BGP OSPF Interaction	Historic
	1583	OSPF Version 2	Draft Standard
	1584	Multicast Extensions to OSPF	Proposed Standard
	1586	Guidelines for Running OSPF over Frame Relay Networks	Informational
	1587	The OSPF NSSA Option	Proposed Standard
	1745	BGP4/IDRP for IP-OSPF Interaction	Historic
	1765	OSPF Database Overflow	Experimental

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	1793	Extending OSPF to Support Demand Circuits	Proposed Standard
	1850	OSPF Version 2 Management Information Base	Draft Standard
	2154	OSPF with Digital Signatures	Experimental
	2178	OSPF Version 2	Draft Standard
	2328	OSPF Version 2	Standard
	2329	OSPF Standardization Report	Informational
	2370	The OSPF Opaque LSA Option	Proposed Standard
	2676	QoS Routing Mechanisms and OSPF Extensions	Experimental
	2740	OSPF for IPv6	Proposed Standard
	2844	OSPF over ATM and Proxy-PAR	Experimental
	3101	The OSPF Not-So-Stubby Area (NSSA) Option	Proposed Standard
	3137	OSPF Stub Router Advertisement	Informational
	3509	Alternative Implementations of OSPF Area Border Routers	Informational
	3623	Graceful OSPF Restart	Proposed Standard
	3630	Traffic Engineering (TE) Extensions to OSPF Version 2	Proposed Standard
	3883	Detecting Inactive Neighbors over OSPF Demand Circuits (DC)	Proposed Standard
	4061	Benchmarking Basic OSPF Single Router Control Plane Convergence	Informational
	4062	OSPF Benchmarking Terminology and Concepts	Informational
	4063	Considerations When Using Basic OSPF Convergence Benchmarks	Informational

(continued)

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	4136	OSPF Refresh and Flooding Reduction in Stable Topologies	Informational
	4167	Graceful OSPF Restart Implementation Report	Informational
	4203	OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)	Proposed Standard
	4222	Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance	Best Current Practice
RIP			
	1058	Routing Information Protocol	Historic
	1387	RIP Version 2 Protocol Analysis	Informational
	1388	RIP Version 2 Carrying Additional Information	Proposed Standard
	1389	RIP Version 2 MIB Extensions	Proposed Standard
	1581	Protocol Analysis for Extensions to RIP to Support Demand Circuits	Informational
	1582	Extensions to RIP to Support Demand Circuits	Proposed Standard
	1721	RIP Version 2 Protocol Analysis	Informational
	1722	RIP Version 2 Protocol Applicability Statement	Standard
	1723	RIP Version 2 Carrying Additional Information	Standard
	1724	RIP Version 2 MIB Extension	Draft Standard
	2091	Triggered Extensions to RIP to Support Demand Circuits	Proposed Standard
	2453	RIP Version 2	Standard
Just for Fun			
	0439	PARRY Encounters the DOCTOR	Unknown
	0967	All Victims Together	Unknown

Table C-1: *(continued)*

TOPIC	RFC NUMBER	TITLE	STATUS
	0968	Twas the Night Before Start-Up	Unknown
	1097	Telnet Subliminal-Message Option	Unknown
	1216	Gigabit Network Economics and Paradigm Shifts	Informational
	1217	Memo from the Consortium for Slow Commotion Research (CSCR)	Informational
	1438	Internet Engineering Task Force Statements Of Boredom (SOBs)	Informational
	1882	The 12-Days of Technology Before Christmas	Informational
	1925	The Twelve Networking Truths	Informational
	2324	Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)	Informational
	2325	Definitions of Managed Objects for Drip-Type Heated Beverage Hardware Devices Using SMIv2	Informational

APPENDIX

D

References and Resources

This appendix provides valuable references and resources.

Nortel Networks Documentation

Nortel Networks. *Installing Hardware Options for the Contivity Secure IP Services Gateway (February, 2005)*, Publication 302283-M Rev 00

Nortel Networks. *Installing Hardware Options for the Contivity Secure IP Services Gateway (May, 2005)*, Publication 302283-N Rev 00

Nortel Networks. *Contivity VPN Client Release Notes, Version 6.01 (September, 2005)*, Publication 311773-P Rev 00

Nortel Networks. *Contivity VPN Client User and Administrator Guide For: Macintosh, Mac OS X, Linux, Solaris, HP-UX, Windows CE (April, 2005)*, Publication 314455-3.1.4 Version 3.1.4

Nortel Networks. *Contivity Secure IP Services Gateway Release Notes Version 6.00 (December, 2005)*, Publication 315000-K Rev 00

Nortel Networks. *Configuring Firewalls, Filters, NAT, and QoS for the Contivity Secure IP Services Gateway Version 6.00 (August, 2005)*, Publication 315896-E Rev 00

Nortel Networks. *Configuring Servers, Authentication, and Certificates for the Contivity Secure IP Services Gateway Version 6.00 (August, 2005)*, Publication 315897-E Rev 00

Nortel Networks. *Configuring Routing for the Contivity Secure IP Services Gateway Version 6.00 (August 2005)*, Publication 315898-D Rev 00

Nortel Networks. *Configuring Advanced Features for the Contivity Secure IP Services Gateway Version 6.00 (August 2005)*, Publication 315899-E Rev 00

Nortel Networks. *Configuring Tunneling Protocols for the Contivity Secure IP Services Gateway Version 6.00 (August 2005)*, Publication 318438-B Rev 00

Nortel Networks. *(Portfolio Brief) Nortel VPN Routers (March 2005)*

RFCs

C. Hornig, RFC 0894, *Standard for the transmission of IP datagrams over Ethernet Networks, April 1984.*

G. Malkin, RFC 1723, *RIP Version 2, Carrying Additional Information, November 1994.*

G. Malkin, RFC 2453, *RIP Version 2, November 1998.*

J. Moy, RFC 1583, *OSPF Version 2, March 1994.*

J. Moy, RFC 2178, *OSPF Version 2, July 1997.*

J. Moy, RFC 2328, *OSPF Version 2, April 1998.*

K. Lougheed, Y. Rekhter, *RFC 1105, Border Gateway Protocol (BGP), June 1989.*

K. Lougheed, Y. Rekhter, *RFC 1163, Border Gateway Protocol (BGP), June 1990.*

K. Lougheed, Y. Rekhter, *RFC 1267, Border Gateway Protocol 3 (BGP-3), October 1991.*

R. Draves, *RFC 3484, Default Address Selection for Internet Protocol version 6 (IPv6), February 2003.*

R. Hinden, S. Deering, *RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture, April 2003.*

R. Hinden, S. Deering, *RFC 4291, IP Version 6 Addressing Architecture, February 2006.*

R. Hinden, RFC 3768, *Virtual Router Redundancy Protocol (VRRP), April 2004.*

R. Weltman, *RFC 4370, Lightweight Directory Access Protocol (LDAP) Proxied Authorization Control, February 2006.*

R. Weltman, M. Smith, M. Wahl, *RFC 3829, Lightweight Directory Access Protocol (LDAP) Authorization Identity Request and Response Controls, July 2004.*

P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, *RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, September 2003.*

B. Patel, B. Aboba, W. Dixon, G. Zorn, S. Booth, *RFC 3193, Securing L2TP using IPsec, November 2001.*

S. Kelly, S. Ramamoorthi, *RFC 457, Requirements for IPsec Remote Access Scenarios, January 2003.*

A. Valencia, M. Littlewood, T. Kolar, *RFC 2341, Cisco Layer Two Forwarding (Protocol) "L2F," May 1998.*

W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter, *RFC 2661, Layer Two Tunneling Protocol "L2TP," August 1999.*

K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn, *RFC 2637, Point-to-Point Tunneling Protocol, July 1999.*

H. Kummert, *RFC 2420, The PPP Triple-DES Encryption Protocol (3DESE), September 1998.*

Internet Resources

`http://www.howstuffworks.com`

`http://www.acronymfinder.com`

`http://ww.dictionary.com`

`http://www.ietf.com`

`http://www.iso.org`

`http://www.ieee.org`

Index

SYMBOLS AND NUMERICS

. (dot)
  dotted-decimal notation for octets, 9
  notation for changing directories (..), 618
3DES (Triple Data Encryption Standard)
  IPSec use of, 400, 401
  as 128-bit encryption, 134
  RFCs for, 670
  support for, 77
10Base-2 Ethernet, 342
10Base-5 Ethernet, 342
10Base-FL Ethernet, 342
10Base-T Ethernet, 342
10/100Base-T Ethernet module, 42
56-bit encryption, 134. *See also* DES
100Base-FX Ethernet, 342
128-bit encryption, 134. *See also* 3DES
1000Base-CX Ethernet, 343
1000Base-LX Ethernet, 343
1000Base-SX Ethernet, 343
1000Base-SX Ethernet module, 42–43
1000Base-T Ethernet, 343
1000Base-T Ethernet module, 42–43

A

abbreviations
  alphabetical listing of, 593–612
  for CLI commands, 189
ABOTs (Aggressive mode Branch Office Tunnels)
  for cost savings, 140
  for dedicated IP address unavailability, 139–140
  disadvantage of, 140
  Initiator/Responder Tunnel configuration, 140–141, 159
  IPSec support for, 405
  keepalive signaling for tunnel, 140
  for local ISP services, 139–140
  for mobility, 140
  overview, 138–141
  reasons for using, 138–140
  SOHO installation using, 150
  VPN device in Client mode and, 146–147
ABRs (Area Border Routers), 373
accelerator module for IPSec encryption, 45, 69–70
Access Concentrators (L2TP), 274–275
access control. *See also* firewall policies
  filters, 281–282
  group versus user-specific rights, 229
  interfaces for implementing parameters, 290
accounting
  log, 218
  by RADIUS, 223, 248–250

accounting *(continued)*
reporting utility for, 571–572
software features for, 76
Acknowledgement Number field (GRE packet header), 394
acronyms, alphabetical listing of, 593–612
Address Resolution Protocol. *See* ARP
Address/Port Discovery, 327, 331
adjacencies (OSPF), 372
administration lab exercises. *See also* managing VPN Routers
about, 463
administrator user tunnel configuration, 505–511
automatic backup configuration, 477–479
BOT configuration, 479–482
CAR configuration, 521–526
CLIP configuration for management IP address, 502–505
DHCP server configuration, 488–492
groups, configuring, 469–470
IPSec Mobility configuration, 475–477
NTP configuration, 484–487
RIP configuration, 482–483
Syslog server configuration, 512–515
user IP address pool configuration, 515–521
users, configuring, 471–473
VPN Client failover configuration, 473–475
VPN Client installation, 464–465
VPN Client logging, 468–469
VPN Router initial setup, 465–468
VPN Router 100 configuration, 492–502
administrator
admin levels, 204
assigning rights via BBI, 204
changing user ID or password via serial interface, 186–187
reporting activity, 215
showing number of admin users, 625
user tunnel configuration for, 505–511
ADSL (Asymmetric Digital Subscriber Line)
benefits of, 44
option for VPN Routers, 44
overview, 16
SDSL versus, 17
support for, 79
VPN Router comparison chart, 69–70
Advanced Router License key, 80–81, 226
AES (Advanced Encryptions Standard)
Encryption Accelerator Module support for AES-128 cryptography, 45
overview, 81
RFCs for, 671–672
standards supported by VPN Router software, 77
VPN Router software version 6.00 features, 81
AF (Assured Forwarding) PHB, 409
Aggressive mode Branch Office Tunnels. *See* ABOTs
AH (Authentication Header) packet, 33, 403
AIX operating system (IBM), VPN Client support for, 106, 426
Alcatel 5620 Network Manager, 545
ALG (Application Level Gateway)
firewall SIP ALG, 332
NAT ALG for SIP, 331–332
for NAT with VoIP, 327, 331
anonymous authentication, 232
anti-spoofing
checks done with use of, 280
configuring, 288
Application layer (OSI layer 7), 3, 4, 278
Application option for Nortel VPN Client, 111, 119
application servers, 20
ARCFOUR (RC4) encryption, 77, 251
Area Border Routers (ABRs), 373
Area ID field (OSPF packet header), 15
areas (OSPF)
Area Border Routers and, 373
Autonomous System Boundary Routers and, 374

backbone area, 370
defined, 370
ARP (Address Resolution Protocol)
BBI utility for, 219–220, 581–582
clearing cache, 632–633
client access to corporate network and, 170
described, 219
overview, 351–352
Proxy ARP with NAT, 335
ASBRs (Autonomous System Boundary Routers), 374
Assured Forwarding (AF) PHB, 409
Asymmetric Digital Subscriber Line. *See* ADSL
attacks. *See also specific kinds*
DoS (Denial of Service), 29, 280, 281
dropping packets used in, 280
kinds defended by firewall, 280–281
replay, 33
Attribute Value Pair (AVP) Hiding, 36
Attributes field (RADIUS packet header), 18
authentication. *See also* certificates; LDAP; RADIUS
CHALLENGE token cards for, 245
CHAP protocol, 238, 245
group- or user-specific access rights and, 229
IPSec Tunnel authentication, 271–273
LDAP Proxy options, 237–238
L2TP/IPSec, 273–274
L2TP/IPSec tunnel authentication, 273–274
MS-CHAP protocol, 238, 245
MS-CHAP V2 protocol, 238, 245
by OSPF, 370
overview, 229–230
PAP protocol, 237, 245
PAP with Bind protocol, 238
protocols and standards supported, 78
by RADIUS, 223
RADIUS, enabling, 242–246
RADIUS options, 245–246
RESPONSE token cards for, 245
RFC-2548 support for, 245
VPN Router with authentication servers, 229, 230
Authentication Data field
in AH packet, 33, 403
in ESP packet, 34, 405
in VRRP packet header, 16
Authentication field (OSPF packet header), 15
Authentication Header (AH) packet, 33, 403
Authentication Interval field (VRRP packet header), 16
authentication servers. *See also* authentication
External LDAP, 235–237, 251–252
Internal LDAP, configuring, 232–235
LDAP model, 232
LDAP, monitoring, 240–241
LDAP Proxy, 237–240
LDAP request flowchart, 232, 233
RADIUS, enabling, 242–246
VPN Router with, 229, 230
Authentication Type field
in OSPF packet header, 15
in VRRP packet header, 16
authentication type for Nortel VPN Client
Group ID and Group password, 128–129
no Group ID and Group password, 128
Token Card, 130–132
username and password, 126–128
Authenticator field (RADIUS packet header), 18
authorization
by RADIUS, 223
reporting information, 215
automatic backups, 223, 477–479
Autonomous System Boundary Routers (ASBRs), 374
AVP (Attribute Value Pair) Hiding, 36

B

backdoors, hacker exploitation of, 28
backing up
  Internal LDAP, 235
  as proactive measure, 585
  system automatically, 223, 477–479
  system files when upgrading software, 222
Backup Interface Services. *See* BIS
bandwidth demands
  by mandatory tunneling, 150
  split tunneling for reducing, 136
bandwidth management
  bandwidth defined, 225
  configuring, 226
  DTR as measure for, 225
  license key installation for, 225–226
  overview, 225
  software features for, 76–77
banner messages (TunnelGuard), 458
Basic Rate Interface (BRI) ISDN
  overview, 17
  resetting, 620, 633
  VPN Router comparison chart, 69–70
baud rate for Console Interface, 614
BBI (browser-based interface). *See also* administration lab exercises
  Accounting screen, 218
  adding L2TP Access Concentrators via, 274–275
  Admin category, 202–203
  administrator rights assignment via, 204
  anti-spoofing configuration via, 288
  application-specific logging enabling via, 286–287
  ARP utility, 219–220, 581–582
  automatic system backups via, 223
  bandwidth management configuration via, 225–226
  certificate enabling for tunnels via, 268–269
  certificate identification with Branch Offices via, 270–271
  certificate identification with users via, 269–270
  CMP setup for VPN Router via, 255–260
  Configuration log access via, 206, 207
  connecting via management IP address, 94, 198
  connection limitation and logging via, 286
  CRL details display via, 259–260
  CRL server configuration via, 266–267
  default username and password for, 96
  directory tree model for selections, 96–97
  ease of using, 197–198
  Event log access via, 208, 209
  file management via, 205
  File System Maintenance window, 102–105
  filter adding/editing via, 311–313
  finding stateful firewall configuration information via, 283
  finding subcategory needed, 197–198
  firewall options, 284–289
  firewall policy creation via, 290–296, 305–306
  firewall policy implementation via, 307–308
  for firewall rule creation, 296–304
  Guided Config option, 96, 198
  hairpinning configuration via, 334
  Health Check utility, 216–217, 568–569, 636
  Help category, 203
  initial switch configuration tips, 198
  Interface NAT rule creation via, 329
  Internal LDAP configuration via, 233–235
  IPSec Tunnel authentication via, 271–273
  LDAP certificate installation via, 239–240, 251
  LDAP Proxy enabling via, 238–240
  login, 96
  L2TP/IPSec tunnel authentication via, 273–274
  main introduction (or interface) screen, 94–96, 198–199

main menu categories, 197
main menu window, 198–199
Malicious Scan Detection configuration via, 289
Manage from Notebook option, 96, 198
Manage Switch option, 96, 198
NAT ALG for SIP enabling via, 332
needed to upgrade VPN Router software, 83
Ping utility, 219, 220, 578–579
Profiles category, 201–202
Proxy ARP enabling via, 335
QoS category, 201
Quick Start option, 96, 198
RADIUS accounting enabling via, 248–250
RADIUS authentication enabling via, 242–246
RADIUS proxy enabling via, 246–248
recovery disk creation, 223–224, 548–549
remote logging of firewall events enabling via, 287–288
removing unused versions of VPN Router software, 102–105
reporting utilities, 562–582
Reports utility, 215, 216
Routing category, 201
Security log access via, 210, 211
server types and corresponding configuration screens, 293–294
Servers category, 202
Services category, 200
Sessions menu, 214–215
software upgrades configuration screen, 96–100
speeding performance of, 198
stateful firewall enabling via, 285–286
Statistics screen, 217–218
Status category, 203, 214–218
System category, 200
System log access via, 212, 213
System screen, 215–216
System Shutdown tool, 224
system status tools, 214–218
Trace Route tool, 218–219, 579–580
Trusted CA Certificate installation via, 260–261
Trusted CA Certificate settings via, 261–264
viewing directory details, 103–104
B-channel (Bearer-Channel) in ISDN, 17, 18
best-effort delivery, 12
BGP (Border Gateway Protocol)
advertisement process, 380
BGP version 4 (BGPv4 or BGP4), 376
as an EGP protocol, 363, 376
history of, 376
managing route information, 379–380
overview, 81–82, 376–380
path-vector routing algorithm, 380
RFCs for, 680–682
routing concepts, 378–379
Routing Information Base, 379
selection process, 380
storage process, 380
support for version 4, 77, 81–82
topologies, 377–378
update process, 380
BIS (Backup Interface Services)
day-of-week trigger for, 176, 421
example, 174, 420
interface group failure as trigger for, 175, 421
overview, 173–175, 419–421
ping failure as trigger for, 175, 421
profile, 175, 420
time-of-day trigger for, 176–177, 421
types of interfaces usable for, 174
unreachable route as trigger for, 175, 421
`boot` command, 654
booting to a recovery disk, 554
Border Gateway Protocol. *See* BGP
border routers, 363–364
BOTs (Branch Office Tunnels)
configuring, 479–482
displaying session information, 214
fixed endpoint addresses for, 136
installations commonly using, 136
with IPSec, support for, 405

BOTs (Branch Office Tunnels) *(continued)*
LAN subnet addresses permitted for, 136
for L2TP/IPSec tunnel authentication, 273
mandatory tunneling, 136, 138, 139
NAT applied to, 327–328
NAT with dynamic routing and, 330
overview, 136–138
as peer-to-peer tunnels, 136
with PPTP, support for, 396
for Regional Office, 159
SOHO installation using, 150
split tunneling, 136, 138
typical installation for mandatory tunneling, 138, 139
typical installation for split tunneling, 136–138
VPN device in Client mode and, 145–146
VPN solution, 70–71
Branch Offices
identifying with certificates, 270–271
L2TP/IPSec tunnel authentication, 273–274
office-to-branch office VPN Router solution, 47
remote branch office VPN Router solutions, 47
BRI (Basic Rate Interface) ISDN
overview, 17
resetting, 620, 633
VPN Router comparison chart, 69–70
broadcast address, 348
broadcast, defined, 348
broadcast domains
overview, 348–349
VLANs for splitting up, 353
browser-based interface. *See* BBI
bugs (known issues), 83, 107
BulletProof FTP server, 552
bus topology, 339

C

C field
in enhanced GRE packet header, 394
in GRE packet header, 38
in L2F packet header, 35, 389
CA (Certificate Authority)
CDPs (CRL Distribution Points), 261, 267–268
certificates revoked by, 264
CRL details display, 259–260
CRL overview, 264–265
CRL publication by, 265
CRL retrieval, 268
CRL server configuration, 265–267
CRL signed by private key of, 265
defined, 250
key update, 264, 268
overview, 31
as PKI service, 254
Root Authority communication by server, 255, 256
Trusted CA Certificate installation, 260–261
Trusted CA Certificate settings, 261–264
X.509 Digital Certificates and, 254
cable Internet access, ABOTs for, 139–140
cable testers, 541, 543
cables and cabling
for ADSL, 44
coaxial, 343–344
for connecting PC to VPN Router, 84
console cable, 546–547
crossover cable, 548
fiber-optic, 345
for HSSI, 45
for 1000Base-SX Ethernet, 43
for 1000Base-T Ethernet, 43
Physical layer (OSI layer 1) and, 6
repeater for connecting different types, 22
for 10/100Base-T Ethernet, 42
testing cables, 541, 543
twisted-pair, 344–345
VPN cost-effectiveness for, 30
capturing packets
`capture` command for, 654–655
packet sniffers for, 541, 542–543
PCAP utility for, 582–584
CAR (Client Address Resolution)
aggregation modes supported, 418
configuring, 521–526

dynamic route update advertisement with, 417
overview, 416–418
route types, 417
Carrier Sense Multiple Access with Collision Detection (CSMA/CD), 338, 340–341
`cd` command, 616, 617, 618–619
CDPs (CRL Distribution Points), 261, 267–268
Central Office
BOT use for, 136
client load balancing and failover, 171–172
DHCP in, 168–169
internal user redundant Internet access, 172–173
intranet using VPN technology, 165
mandatory tunneling, 136
overview, 164–166
VoIP example, 411–412
VPN for client access to corporate network, 168–171
VPN Router as intranet access point, 166–167
VPN Router placement in the network, 177–179
Certificate Authority. *See* CA
Certificate Management Protocol. *See* CMP
Certificate Revocation List. *See* CRL
certificate server for authentication, 168
certificates. *See also* CA; PKI
defined, 31
described, 250
External LDAP Proxy enhancements, 252–253
installing in External LDAP, 251
installing in Internal LDAP, 235
LDAP Proxy configuration for, 239–240
PKCS#12 Personal Information Exchange Syntax for, 253–254
as PKI service, 254
RFCs for, 679
SSL encryption with LDAP server for, 251–252
SSL use of, 31
support for X.509 Digital Certificates, 78
tunnel certificates, 253–254, 268–269
certifications, 77
`CES>` prompt, 189, 615
`CES#` prompt, 189, 631
`CES(config)#` prompt, 189
Channel Service Unit/Data Service Unit (CSU/DSU), 20, 43, 69
CHAP (Challenge Handshake Authentication Protocol), 238, 245
Checksum field
in enhanced GRE packet header, 394
in GRE packet header, 38
in IP packet header, 13
in L2F packet header, 35, 390
in OSPF packet header, 15
in VRRP packet header, 16
Circuitless IP (CLIP), 418–419, 502–505
Class A IP addresses
non-routable, standard for, 143
octets, 10
overview, 10
Class B IP addresses
non-routable, standard for, 143
notation for, 136–137
octets, 11
overview, 10, 11
Class C IP addresses
octets, 11
overview, 10, 11
Class D IP addresses
examples, 12
overview, 10, 11
Class E IP addresses, 10
Class Selector (CS) PHB, 409
`clear` command
Privileged EXEC mode (CLI), 632–633
User EXEC mode (CLI), 621–622
CLI (Command Line Interface). *See also specific modes and commands*
abbreviated commands, 189
access via serial port or Console Interface, 188, 613, 614–615
access via Telnet, 187–188, 613, 615
also known as Command Line Interpreter, 613

CLI (Command Line Interface) *(continued)*
command modes, 188–191, 613
exiting, 620
for firewall policy creation, 290
Global Configuration mode, 190–191, 660–663
Help utility, 191–196
keystroke shortcuts, 196–197
Nortel Reference Manual for the Command Line Interface, 622
overview, 187, 613, 663–664
Privileged EXEC mode, 189, 631–660
prompts, 189, 190, 615, 631
User EXEC mode, 189, 615–631
for VPN Router management, 187–197
Client Address Resolution. *See* CAR
client, defined, 423. *See also* Nortel VPN Client
Client ID field (L2F packet header), 35, 390
Client Tunnels. *See* User/Client Tunnels
client VPN software. *See* Nortel VPN Client
CLIP (Circuitless IP), 418–419, 502–505
CMP (Certificate Management Protocol)
creating a CMP-compliant certificate request, 256, 257–258
displaying certificate details, 259–260
information needed for, 255–256
Issuer Distinguished Name for, 258–259
Private Key Password for, 256
RDN (Relative Distinguished Name) for, 258–259
VPN Router setup for, 255–260
coaxial cable, 343–344
Code field (RADIUS packet header), 18
collision domains
joining to form broadcast domains, 348
overview, 347–348
Command field (RIP packet header), 14
Command Line Interface or Interpreter. *See* CLI; *specific commands*
COM1 port settings for upgrading software, 86–87
computer workstations, 20
concentrators (hubs), 6, 22
Cone NAT, 81. *See also* NAT
Configuration log
overview, 206–207
reporting utility for, 574, 575
Connection Wizard
choosing to run, 123–124
Connection Profile Complete notification window, 128, 130, 131–132
describing the connection profile, 126
filling out completely required, 125
Group ID and Group password authentication, 128–129
naming the connection profile, 125
New Connection Profile window, 125–126
no Group ID and Group password authentication, 128
overview, 436
starting from File menu, 124
Token Card Authentication, 130–132
username and password authentication, 126–128
connectionless delivery protocols, 5. *See also* UDP
console cable, 546–547
Console Interface. *See also* serial interfaces or ports
CLI access via, 613, 614–615
controlling paging of session screen, 619
login, 614
menu, 188, 614
console port
overview, 45
VPN Router comparison chart, 68
VPN Router option for, 45
Contivity Secure IP Services Gateway. *See* Nortel VPN Router software; Nortel VPN Routers
Contivity Stateful Firewall License key, 81, 283
Contivity VPN Client (CVC). *See* Nortel VPN Client
control tunnels, 181

copying
filters, 313
firewall policies, 291–292
corrupted packets, 406
cost-effectiveness
of ISPs, ABOTs for, 140
of PPPoE, 413–414
of VoIP, 412
of WANs compared to VPNs, 1
CPUs or processors
displaying types for VPN Router, 216
identifier in Configuration log, 206
identifier in Event log, 208
identifier in Security log, 210
identifier in System log, 212
VPN Router comparison chart, 68
Crannog Software Netwatch, 545
CRC (cyclic redundancy check), 6
`create` command, 655
CRL (Certificate Revocation List)
checking by VPN Router, 267–268
Checking Enabled setting, 265
Checking Mandatory setting, 266
defined, 264–265
displaying details, 259–260
Distribution Points (CDPs), 261, 267–268
enabling checking of certificates, 261, 265
Global Collection, 267–268
interface for directory on public side of VPN Router, 265
long list of, performance not affected by, 267
overview, 264–265
publication by CA, 265
retrieval, 268
Retrieval Enabled setting, 266
server configuration, 265–267
signed by CA private key, 265
System Status setting, 266
Update Frequency setting, 266
crossover cable, 548
CS (Class Selector) PHB, 409
CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 338, 340–341
CSU/DSU (Channel Service Unit/Data Service Unit), 20, 43, 69
CuteFTP client, 553
CVC (Contivity VPN Client). *See* Nortel VPN Client
cyclic redundancy check (CRC), 6

D

data bits for characters
for Console Interface, 614
when upgrading software, 87
Data Circuit Equipment (DCE)
HSSI serial interface for, 45
RS-232 serial interface for, 44
Data Encryption Standard. *See* DES
Data field
in L2F packet header, 35, 390
in L2TP packet header, 37, 400
in PPTP packet header, 36
Data Flood attack, 281
Data Link layer (OSI layer 2), 6, 8
Data Link Switching (DLSw), 77
data rate setting for upgrading software, 86
Data Terminal Equipment (DTE)
HSSI serial interface for, 45
RS-232 serial interface for, 44
Data Transfer Rate (DTR), 225
data transmission modes
full-duplex, 347
half-duplex, 346–347
simplex, 346
DB-9 interface, 46
DCE (Data Circuit Equipment)
HSSI serial interface for, 45
RS-232 serial interface for, 44
D-channel (Delta-Channel) in ISDN, 17, 18
de-encapsulation, 387
default best-effort PHB, 409
delayed packets, QoS and, 406
`delete` command, 656
Demand Services, 79, 82
Demilitarized Zone. *See* DMZ
Denial of Service (DoS) attacks, 29, 280, 281

DES (Data Encryption Standard)
as 56-bit encryption, 134
IPSec use of, 400
RFCs for, 670
SHA algorithm supported with SSL, 251
support for, 77
Destination IP Address
in IP packet header, 13
in L2F packet, 387, 388
DHCP (Dynamic Host Configuration Protocol)
for Central Office installations, 168–169
server configuration, 488–492
showing configured servers and settings, 636
user IP address assignment using, 516–518
dial access to single workstation, 25
Dial Backup service, 79, 82
Dial on Demand service, 79, 82
dialup interface
for backing up the primary interface, 174
resetting, 620, 633
dialup services
dynamic address allocation for, 139
ISDN configuration, 25
DiffServ (Differentiated Services). *See also* DSCP
Dropper function, 408
DS field in IP packet header, 408
Marker function, 408
Meter function, 408
overview, 406–408
PBH (Per Hop Behavior), 408–410
Shaper function, 408
support for, 77
VoIP use of, 412
digital certificates. *See* certificates
Digital Subscriber Line. *See* DSL
`dir` command, 616–617
direct access to VPN Routers, 181
directories
`cd` command for changing, 616, 617, 618–619
`dir` command for displaying, 616–617
dot-dot notation for changing, 618
`ls` command for displaying, 616, 617
`ls` versus `dir` command for, 617
`mkdir` command for creating, 657
`pwd` command for printing, 616, 617–619
`rename` command for, 659
`rmdir` command for removing, 657
user level root, 617
directory service, defined, 230
`disable` command, 189
disabling keepalives, 439
distance-vector routing
algorithm, 360–361, 367
protocols using, 14
DLSw (Data Link Switching), 77
DMZ (Demilitarized Zone)
defined in networking terms, 154
NAT table example, 157–158
overview, 27–28
in SOHO installation, 151–153
using private non-routable IP addresses, 155–156
using publicly routed IP addresses, 154–155
DNS (Domain Name System), 168, 169, 170
documentation
for Nortel networks, 687–688
as proactive measure, 588
release notes, 83, 107
for VPN Router software, online, 76
domains
broadcast domains, 348–349
collision domains, 347–348
defined, 347
DoS (Denial of Service) attacks, 29, 280, 281
dot (.)
dotted-decimal notation for octets, 9
notation for changing directories (..), 618
Double NAT, 320
drivers
defined, 111
with VPN Client installation, 111
with VPN Client upgrade, 120

dropped packets
as defense against attacks, 280
by DiffServ, 408
QoS and, 406
DS (Differentiated Services). *See also* DSCP
Dropper function, 408
DS field in IP packet header, 408
Marker function, 408
Meter function, 408
overview, 406–408
PBH (Per Hop Behavior), 408–410
Shaper function, 408
support for, 77
VoIP use of, 412
DS field (IP packet header), 408
DSCP (Differentiated Services Control Point)
PHB set by, 408–410
pools, 409
Precedence field and, 410
set by DiffServ Marker function, 408
DSL (Digital Subscriber Line). *See also* ADSL
dynamic address allocation for, 25
overview, 16
SOHO installation, 149
SOHO installation using, 148
symmetrical (SDSL), 17
DTE (Data Terminal Equipment)
HSSI serial interface for, 45
RS-232 serial interface for, 44
DTR (Data Transfer Rate), 225
dumb terminals, 25
Dynamic Host Configuration Protocol. *See* DHCP
dynamic IP addresses, 351
Dynamic Many-to-Many NAT, 317–318
Dynamic Many-to-One NAT, 316–317
Dynamic One-to-One NAT, 316, 317
dynamic routing. *See also specific protocols*
NAT with, 329–330
support for, 77

E

E (error message) severity code (Event log), 445
`eac[version number].exe` file, 107, 115, 116
Edit menu (Nortel VPN Client), 437, 438
EF (Expedited Forwarding) PHB, 409, 410
EGP (Exterior Gateway Protocol). *See also* BGP
defined, 363
IGP protocols versus, 376
overview, 14, 356
EIA (Electronic Industries Alliance), 45
email
hacker exploitation of, 29
servers, defined, 20
`enable` command, 189, 631
enabling
application-specific logging, 286–287
certificate use for tunnels, 268–269
connection limitation and logging, 286
CRL checking of certificates, 261, 265
CRL retrieval, 266
firewall options, 284–289
LDAP Proxy, 238–240
NAT ALG for SIP, 332
Privileged EXEC mode (CLI), 189, 631
Proxy ARP, 335
RADIUS accounting, 248–250
RADIUS authentication, 242–246
RADIUS proxy, 246–248
stateful firewall feature, 285–286
VPN Client logging, 468–469
Encapsulating Security Packet. *See* ESP
encapsulation
by Data Link layer, 6
ESP, 33–34, 134, 403, 404–405
IP-in-IP, by IPSec, 401
IP-in-IP, by PPTP, 392
by L2F, 387
encryption
accelerator module for IPSec, 45, 69–70
AES, 45, 77, 81, 671–672
ARCFOUR (RC4), 77, 251

encryption *(continued)*
DES, 77, 134, 251, 400, 670
by SSL, methods supported, 251
standards supported by VPN Router software, 77
3DES, 77, 134, 400, 401, 670
VPN Router software services, 77
for VPN tunneling, 134
for VPNs, overview, 134
Encryption Accelerator Module
overview, 45
VPN Router comparison chart, 69–70
E1 lines
overview, 44
VPN Router comparison chart, 69
Equator One network management station, 545
error detection and handling
by Data Link layer, 6
by TCP, 5
error message (E) severity code (Event log), 445
error-checking data parity bits
for Console Interface, 614
when upgrading software, 87
ESP (Encapsulating Security Packet)
bits in, 34
in IPSec, 33, 403, 404–405
packet contents, 403
packet header contents, 33–34, 404–405
in VPN tunneling, 134
Ethereal packet sniffer, 543
Ethernet
for backing up the primary interface, 174
combined with PPP in PPPoE, 413, 414
defined, 42
development of, 338
Fast Ethernet standards, 342
GbE standards, 42–43
Gigabit Ethernet standards, 343
1000Base-SX module, 42–43
1000Base-T module, 42–43
overview, 338
10/100Base-T module, 42
Traditional Ethernet standards, 342
VPN Router comparison charts, 68, 69
Ethernet LANs. *See also* LANs; *specific protocols*
broadcast domains, 348–349
cabling, 343–345
collision domains, 347–348
data transmission modes, 346–347
as flat networks, 353
overview, 7
physical topology types, 339–340
speed of, 7
traffic collisions in, 338, 340, 341
Event log
accessing via BBI, 208, 209
clearing, 632–633
CPU identifier in, 208
date and time in, 208
described, 208
event description in, 209
example, 208
number of entries retained in, 208
priority code in, 208–209
reporting utility for, 576–577
severity codes, 445
task identifier in, 208
for troubleshooting system recovery, 557, 561–562
TunnelGuard application, 457–458
VPN Client, 443–445
exchange process (OSPF), 372
`exit` command
Privileged EXEC mode (CLI), 189
User EXEC mode (CLI), 620
exiting
CLI, 189, 620
Nortel VPN Client, 437
Expedited Forwarding (EF) PHB, 409, 410
Exterior Gateway Protocol. *See* EGP
External LDAP. *See also* LDAP
cache flush required after parameter changes, 241
enabling LDAP Proxy, 238–240
installing certificates, 251
Internal LDAP versus, 232–233, 235–236
LDAP Proxy with, 236–238
monitoring servers, 241

overview, 235–237
primary versus secondary servers, 241
RADIUS with, 236–237
scenario using single server, 236
SSL communication with server, 251–252
extranet VPN deployment example, 71–72

F

F (fatal message) severity code (Event log), 445
F field (L2F packet header), 34, 389
failover
overview, 172
VPN Client, 458–461, 473–475
VRRP link, 382
FDN (Full Distinguished Name), 258, 270
Federal Information Processing Standard (FIPS) 140-2 certification support, 77
fiber-optic cabling, 345
56-bit encryption, 134. *See also* DES
file maintenance for system recovery, 557, 559–561
file management, 205
File menu (Nortel VPN Client), 436–437
file server, defined, 20
file system commands, 616–619
File Transfer Protocol. *See* FTP
FileZilla FTP client, 553
FileZilla FTP server, 552
filter profile, 282
filters. *See also* packet filtering
access control, 281–282
adding rules, 312–313
copying, 313
creating new tunnel filters, 311
interface filters, defined, 311
naming, 311
Next Hop traffic filters, 314–315
profile for, 282
tunnel filters, defined, 311
FIPS (Federal Information Processing Standard) 140-2 certification support, 77
firewall policies
adding, 291
basic steps for creating, 305–306
business example, 309–310
components configurable, 290
configuration verification, 306
copying, 291–292
creating, 290–296, 305–306
Default Rules, 296, 299
defined, 290
deleting, 291
destination rules, 296
Dynamic Implied Rules, 294–295
implementing on a stateful firewall, 307–308
Implied Rules, 292–295
interface designations used when constructing, 279
Interface Specific Rules, 295–296, 299–300
interfaces for implementing, 290
IP addresses for example, 306
Override Rules, 295, 299, 309–310
overview, 290
renaming, 292
residential example, 309
rule creation, 296–304
server types and corresponding configuration screens, 293–294
source rules, 296
Static Pre-implied Rules, 293
firewalls. *See also* firewall policies; packet filtering; stateful firewalls
configuration verification, 306
Contivity Stateful Firewall License key for, 81, 283
defined, 26
DMZ with, 27–28
example implementation, 26
need for, 26
overview, 26–27
packet filtering by, 27
proxy server, 27
service properties, 290
flags
in enhanced GRE packet header, 394
in GRE packet header, 38
in IP packet header, 13

flash memory
displaying contents of, 623–625
VPN Router comparison chart, 68
flooding process (OSPF), 372
floppy diskettes
displaying type of, 216
recovery, creating, 223–224, 548–549, 655
reformatting, 658
flow cache, clearing, 632–633
flow control
defined, 36
L2TP support for, 36
setting for upgrading software, 87
footer of packets, 12
`forced-logoff` command, 656
Fraggle attack, 281
Fragment Offset field (IP packet header), 13
Frame Relay, 79
FTP (File Transfer Protocol)
as Application layer service, 3
application-specific logging for, 286–287
clients, 552–553
command overflow attack, 281
Passive, 278
`retrieve` command for obtaining software, 659–660
retrieving software upgrades via, 97–98
servers, 551–552
stateful inspection for, 278
for troubleshooting VPN Routers, 551–553
FTP Server client, 553
Full Cone NAT, 322
Full Distinguished Name (FDN), 258, 270
full-duplex data transmission mode, 347
fully meshed topology for BGP, 377–378

G

Get command (SNMP), 183, 184
Gigabit Ethernet (GbE)
standards, 42–43, 343
VPN Router comparison chart, 69
GINA login option, 111, 119
Global Configuration mode (CLI)
cautions for using, 660–661
configuration modes accessed via, 190–191
entering, 190
listing of commands, 193–198, 661–663
overview, 190, 660–661
GRE (Generic Routing Encapsulation) protocol
enhanced header for PPTP, 393–394
overview, 37
packet header contents, 37–38
for PPTP channel, 35
groups, configuring, 469–470
GUI (Graphical User Interface). *See* BBI

H

hackers
defined, 28
firewall needed as protection from, 26
methods used by, 28–29
hairpinning
configuration, 334
defined, 332
overview, 332–333
requirements, 334
with SIP, 333
with STUN server, 333
with UNIStim call server, 333
half-duplex data transmission mode, 347
hard drive
displaying information for VPN Router, 216
reformatting, 557, 559
showing status of, 625
Hard Token Support, 78
hardware. *See also* Nortel VPN Routers; *specific hardware*
importance of, 75
interface options for VPN Routers, 42–46
for LANs, 7
lower OSI layers implemented in, 2
networking, overview, 19–23
tokens in SecurID technology, 32–33

header of packets
AH packet, 33, 403
defined, 12
enhanced GRE, for PPTP, 393–394
ESP packet, 33–34, 404–405
GRE header, 37–38
IP header, 13
L2F header, 34–35, 389–390
L2TP header, 36–37, 399–400
OSPF header, 15
placed by Network layer, 6
PPTP header, 35–36
RADIUS header, 18
RIP header, 14
VRRP header, 16, 17
health check for VPN Routers, 216–217, 568–569, 636–638
Help category (BBI), 203
`help` command, 616
Help menu (Nortel VPN Client), 439–440
Help utility (CLI), 191–196
hexadecimal notation, 8
High Speed Serial Interface (HSSI), 45, 69
home offices. *See* SOHO
hop count, 359, 364
HP Openview network management station, 545
HSSI (High Speed Serial Interface), 45, 69
HTTP (HyperText Transfer Protocol), 3, 286–287
hubs, 6, 22
hubs, intelligent. *See* switches
HyperTerminal
COM1 port settings for upgrading software, 86–88
connection information entry, 85
connection type choices, 85–86
Interface configuration menu, 91–93
login prompt, 88–89
Main Startup window, 84
naming the connection, 85
path for locating, 84
session window, 88
starting, 84
troubleshooting VPN Routers using, 550–551
VPN Router information in, 88
VPN Router Main Menu, 89–94
HyperText Transfer Protocol (HTTP), 3, 286–287

I

I (informational message) severity code (Event log), 445
IBM Tivoli network management station, 545
ICMP (Internet Control Message Protocol) unreachable attack, 281
ICSA (International Computer Security Association) 1.0d certification support, 77
Identification field (IP packet header), 13
Identifier field (RADIUS packet header), 18
idle timeout, 151
IEEE (Institute of Electrical and Electronics Engineers)
Ethernet standard, 338
MAC addressing administered by, 350
VLAN standard 802.1Q Phase 2 supported, 78, 82
Web site, 689
IETF (Internet Engineering Task Force)
DiffServ developed by, 406
PHB groups and RFCs, 409
RFC publication by, 665
Web site, 689
IGP (Interior Gateway Protocol). *See also* OSPF protocol; RIP
defined, 363
EGP protocols versus, 376
overview, 13, 355
RIP used with, 14
IHL (Internet Header Length) field (IP packet header), 13
IKE (Internet Key Exchange)
IPSec use of, 401
RFCs for, 670–671

informational message (I) severity code (Event log), 445
Initiator/Responder Tunnels, 140–141, 159, 405
installing Nortel VPN Client
  administration lab exercise, 464–465
  Application option, 111, 430
  confirmation window, 111
  custom installation modes, 441–442
  directory specification, 429–430
  driver installation, 111
  extracting the files, 107–108
  final (reboot option) phase, 112
  folder and icons display, 111
  initial windows opened, 108
  install and run phase, 110–111
  licensing agreement, 108–109, 427–428
  locating the installation executable, 107, 427
  obtaining the software, 106, 426
  Quiet mode, 442
  `readme.txt` display, 112, 113, 432
  Reboot Only mode, 441
  release notes, 107
  Select Program Folder phase, 109–110
  Setup Status window, 111
  Silent mode, 441
  Skip Screens mode, 441
  Verbose mode, 442
  Welcome window, 108
  Windows GINA option, 111, 430, 431
  Windows service option, 111, 430, 431
Integrated Services Digital Network. *See* ISDN
intelligent hubs. *See* switches
Interface configuration menu (HyperTerminal)
  assigning IP address to Private LAN interface, 91, 92
  Private LAN interface IP address entry, 92
  subnet mask entry, 91, 92
interface filters
  adding rules, 312–313
  copying, 313
  defined, 311
interfaces
  displaying current configuration, 638–639
  displaying current configured interfaces, 627
  Interface Specific Rules, 295–296
  for laptops, 550
  NAT applied to, 327, 329
  physical versus virtual, 278–279
  for stateful firewalls, 278–279
  for VPN Router management, 185
Interior Gateway Protocol. *See* IGP
Internal LDAP. *See also* LDAP
  backing up, 235
  configuring, 232–235
  External LDAP versus, 232–233, 235–236
  installing certificates, 235
  monitoring servers, 240–241
  restoring, 235
internal routers, 363–364
International Computer Security Association (ICSA) 1.0d certification support, 77
International Standards Organization (ISO)
  Web site, 689
  X.500 directory service standard, 230
International Telecommunications Union (ITU), 230
Internet access
  ABOTs for using local ISP services, 139–140
  for corporate users, 172–173
Internet Control Message Protocol (ICMP) unreachable attack, 281
Internet Engineering Task Force. *See* IETF
Internet Explorer for BBI connection, 94
Internet Header Length (IHL) field (IP packet header), 13
Internet Key Exchange (IKE)
  IPSec use of, 401
  RFCs for, 670–671
Internet Protocol. *See* IP
Internet Protocol Security. *See* IPSec

Internet resources
list of, 689
Nortel site, 76, 83, 106, 426, 591
Nortel technical support, 591
Nortel Web site, 221
packet sniffers, 543
release notes for software, 83
VPN Client software, 106, 426
VPN Router software downloads and documentation, 76
VPN Router software upgrades, 221
Internet Security Association and Key Management Protocol. *See* ISAKMP
Internet server, defined, 20
Internet service providers. *See* ISPs
intranets
in Central Office, 164–165
VPN Router placement in the network, 178–179
VPN Routers as access points, 166–167
VPN technology example, 165
inverse split tunneling, 456–457
IP address count field (VRRP packet header), 16
IP addresses
all zeros addressing in inverse split mode, 455
Class A, 10, 143
Class B, 10, 11, 136–137, 143
Class C, 10, 11
Class D, 10, 11, 12
Class E, 10
classes (overview), 10
dedicated, using ABOTS when unavailable, 139–140
defined, 351
destination identified in IP packet header, 13
dynamic, 351
for IPSec tunneling, 401
for L2F tunneling, 388
management IP address, 94, 198, 283
NAT functionality and shortage of, 282
non-routable, DMZ using, 155–156
non-routable, PC-based VPN tunnel example, 142–145
non-routable, standard for, 142, 143
octets, 9, 10, 11
overview, 9–12, 351
for PPTP tunneling, 392
publicly routed, DMZ with, 154–155
RARP for, 353
setting for upgrading software, 89–91
source identified in IP packet header, 13
static, 351
user address assignment using DHCP, 516–518
user address pool configuration, 515–521
IP addresses field (VRRP packet header), 16
IP connectivity commands, 620–621
IP (Internet Protocol)
best-effort delivery by, 12
CLIP (Circuitless IP), 418–419, 502–505
displaying statistics and settings, 626, 639–640
displaying traffic statistics, 627–629
IPv4 (IP version 4), 367
IPv6 (IP version 6), 367
as Network layer protocol, 5–6
overview, 12–13
packet header contents, 13
routing services supported, 77–78
IPconfig utility, 541, 542
IP-enabled telephone handset
defined, 148
SOHO installation using, 149, 151
IP-in-IP encapsulation
IPSec use of, 401
PPTP use of, 392
IPSec Aware NAT, 321–322
IPSec (Internet Protocol Security)
AH packet, 33, 403
authentication with certificates, 271–273
cryptographic protocols used by, 400–401
dynamic routing supported, 77
Encryption Accelerator Module for, 45
ESP packet, 33, 34, 403, 404–405

IPSec (Internet Protocol Security) *(continued)*
Initiator/Responder Tunnels with, 405
IP addresses used with, 401
L2TP over, for security purposes, 398–399
L2TP/IPSec tunnel authentication, 273–274
overview, 33–34, 400–405
packet contents, 402, 403
RFCs for, 667–669
security protocols used by, 403
support for, 79
tunneling environment, 401
UDP ports with, 402–403
for User/Client Tunnels, 141
VPN Client mobility, 447–449, 475–477
IPSec VPN Client Software, 142. *See also* Nortel VPN Client
ISAKMP (Internet Security Association and Key Management Protocol)
IPSec use of, 401
RFCs for, 670–671
VPN Client keepalive, 446
ISDN (Integrated Services Digital Network)
for backing up the primary interface, 174
B-channel, 17
BRI (Basic Rate Interface), 17
D-channel, 17
dialup configuration, 25
dynamic address allocation for, 25
overview, 17
PRI (Primary Rate Interface), 18
VPN Router comparison chart for BRI, 69–70
ISO (International Standards Organization)
Web site, 689
X.500 directory service standard, 230
ISPs (Internet service providers)
ABOTs for using local services, 139–140
L2F requirements, 386–387
L2TP services with, 396–397, 398
PPTP requirements, 391
typical L2F session exchange, 387
typical PPTP session exchange, 391–392
ITU (International Telecommunications Union), 230

J

jitter, 406
Jolt2 attack, 280

K

K field
in enhanced GRE packet header, 394
in GRE packet header, 38
in L2F packet header, 34, 389
keepalives
disabling, 439
ISAKMP, 446
NAT, 446–447
signaling for tunnel, 140
silent, 439, 447
VPN Client, 439, 445–447
Kerberos authentication, 232
Key fields
in enhanced GRE packet header, 394
in GRE packet header, 38
in L2F packet header, 35, 390
keys. *See also* license keys; PKI
CA key update, 264, 268
for CMP, 256
CRL signed by CA private key, 265
defined, 32
IKE, 401, 670–671
ISAKMP, 401, 446, 670–671
PSK, 134
shared secrets, 32, 244, 250, 255
SSL use of, 32
keystroke shortcuts for CLI, 196–197
`kill` command, 656–657
knowledge sharing, 587
known issues (bugs), 83, 107

L

L field (L2TP packet header), 36, 399
Land Attack, 281
LANs (local area networks).
See also Ethernet LANs
overview, 7
subnet addresses for BOTs, 136
subnetworks, 7
VPN Routers for, 48–49
laptops
SOHO installation for, 150
for troubleshooting VPN Routers, 549–550
Layer 2 Forwarding protocol. *See* L2F protocol
Layer 2 Tunneling Protocol. *See* L2TP
layers, network. *See* OSI Reference Model
LDAP (Lightweight Directory Access Protocol)
anonymous authentication, 232
authentication methods available with LDAP Proxy, 237–238
for authentication server, 168
backing up Internal, 235
Base DN for server communication, 239
certificates with External server, 239–240, 251
certificates with Internal server, 235
CRL publication and, 265
directory service defined, 230
DNs (Distinguished Names), 231
emergence from X.500 directory service, 230
enabling LDAP Proxy, 237–240
entries, defined, 231
External LDAP Proxy enhancements, 252–253
External, overview, 235–237
External, primary versus secondary servers, 241
Internal, configuring, 232–235
internal LDAP server elements supported, 230
Internal versus External, 232–233, 235–236
Kerberos authentication, 232
model, 231–232
monitoring servers, 240–241
overview, 18, 222, 230–231
port setting for proxy, 239
principles, 231–232
removing suffixes for Fully Qualified Domain Names, 234, 238
request flowchart, 232, 233
resources stored in, 222
Response Timeout Interval for proxy, 238
restoring Internal, 235
RFCs for, 674–678
Special Characters feature, 252
stopping or starting the server, 234
support for external and internal, 78
LDAP Proxy
authentication methods available, 237–238
enabling and configuring, 238–240
enhancements for locating user records, 252–253
RADIUS support needed for, 236
User Certificate Access feature, 239–240
Length field
in AH packet, 33, 403
in ESP packet, 34, 404
in L2F packet header, 35, 390
in L2TP packet header, 37, 400
in OSPF packet header, 15
in PPTP packet header, 36
in RADIUS packet header, 18
`license install` command (CLI), 226
license keys
Additional VPN Tunnel Support, 81
Advanced Router, 80–81, 226
bandwidth management, 225
Contivity Stateful Firewall, 81, 283
licensing agreement
in release notes, 83, 107
when installing VPN Client, 108–109, 427–428
when upgrading VPN Client, 117
Lightweight Directory Access Protocol. *See* LDAP

link failover (VRRP), 382
Link-State Advertisements (LSAs), 372, 375
Link-State Databases (LSDBs), 372, 374, 375–376
link-state routing or SPF algorithm, 360, 361–362, 375–376
Linux Blind Spoof attack, 280
Linux operating system
  IPSec VPN Client support for, 142
  VPN Client support for, 106, 426
LLC (Logical Link Control) sub-layer (OSI), 6
load balancing, 172
loading new software version. *See* upgrading Nortel VPN Router software
local area networks. *See* LANs
logical topologies, 339
login
  to BBI or VPN Router GUI, 96
  to CLI Privileged EXEC mode, 189
  to Console Interface, 614
  to HyperTerminal, 88–89
  VPN Client options for, 110–111, 118–119
  to VPN Router over serial port, 186
logoff
  administrator capabilities for, 215
  forcing, 656
logs and logging. *See also specific logs*
  accessing logs via BBI, 206, 208, 210, 212
  accounting log, 218
  application-specific, enabling, 286–287
  Configuration log, 206–207, 574, 575
  connection limitation and logging, 286
  displaying logs with `show logging` command, 643–644
  Event log, 208–209, 443–445, 457–458, 557, 561–562, 576–577, 632–633
  overview, 206
  remote logging of firewall events, 287–288
  Security log, 210–211, 572–574
  Syslog server configuration, 512–515
  System log, 212–213, 574–576
  text file storage for logs, 206
  VPN Client logging, 468–469
  VPN Router, 182
`ls` command, 616, 617
LSAs (Link-State Advertisements), 372, 375
LSDBs (Link-State Databases), 372, 374, 375–376
L2F (Layer 2 Forwarding) protocol, 387
  client-based tunneling software not required for, 386
  combined with PPTP in L2TP protocol, 36
  de-encapsulated packet contents, 388–389
  IP address translation by, 387
  IP addresses used with, 388
  ISP requirements for, 386–387
  NAS with, 386
  overview, 34, 386–390
  packet contents, 387, 388–389
  packet header contents, 34–35, 389–390
  PPP link to ISP required for, 386, 388
  PPTP versus, 390, 391
  RFCs for, 666
  typical session exchange, 387
  for User/Client Tunnels, 141
L2TP (Layer 2 Tunneling Protocol)
  Access Concentrators, 274–275
  L2TP/IPSec tunnel authentication, 273–274
  over IPSec, for security purposes, 398–399
  overview, 36, 396–400
  packet contents, 397–398, 399
  packet header contents, 36–37, 399–400
  PPTP and L2TF combined in, 36
  RFCs for, 666–667
  support for, 79
  tunneling environment, 396–397
  for User/Client Tunnels, 141

M

MAC (Media Access Control) addresses
ARP for, 351–352
displaying for router, 215
illustrated, 9
OUI (Organization Unique Identifier) bits, 350
overview, 8–9, 350
RARP for, 353
VLANs based on, 354
MAC (Media Access Control) sub-layer (OSI), 6
Macintosh OS
IPSec VPN Client support for, 142
VPN Client support for, 106, 426
macros, hacker exploitation of, 29
Magic Cookie field (PPTP packet header), 36
Malicious Scan Detection configuration, 289
Manage admin level, 204
Management Information Base (MIB), 183, 645
management IP address
BBI connection using, 94, 198
CLIP configuration for, 502–505
finding, 283
required for stateful firewall configuration, 283
Management Virtual Address (MVA), 82
managing VPN Routers. *See also* administration lab exercises; BBI; CLI
administrator for, 204
bandwidth management, 76–77, 225–226
checking the current status, 205–220
CLI for, 187–197
control tunnels for, 181
direct access for, 181
file management, 205
importance of, 185
interfaces available for, 185
logging for, 182
management defined, 185
network administration for, 180–184
NTP feature for, 184
out-of-band management, 181
proactive administration, 221–224
serial interface for, 186–187
SNMP for, 182–184
system status tools for, 214–218
ways available for, 78
Web-based, 197–204
mandatory tunneling
bandwidth demands of, 150
overview, 136
packet filtering with, 153–154
requiring for SOHO installation, 149–150
typical BOT installation using, 138, 139
MD5 (Message Digest algorithm 5), 401
Media Access Control addresses. *See* MAC addresses
Media Access Control (MAC) sub-layer (OSI), 6
memory. *See* flash memory; RAM
Message Type field (PPTP packet header), 36
MIB (Management Information Base), 183, 645
Microsoft Challenge Handshake Protocol (MSCHAP), 35
Microsoft CryptoAPI (MS CAPI), 253
Microsoft FTP server, 552
Microsoft Windows operating systems
IPSec VPN Client support for, 142
Stateful Firewall Manager support for, 284
VPN Client support for, 106, 426
`mkdir` command, 657
mobility
ABOTs for, 140
IPSec, for VPN Client, 447–449, 475–477
modems
overview, 19
V.90, 45, 69–70
VPN Router comparison chart, 69–70

more command, 657–658
MRED (Multi-Level Random Early Detection), 77
MS CAPI (Microsoft CryptoAPI), 253
MSCHAP (Microsoft Challenge Handshake Protocol), 35
MS-DOS FTP client, 553
multinetting, 82
Multiplex ID field (L2F packet header), 35, 389
MVA (Management Virtual Address), 82

N

NAPT (Network Address Port Translation), 316
NAS (Network Address Server), 386, 388, 390
NAT (Network Address Translation)
address translations supported, 316
Address/Port Discovery, 327
blocked ports and, 145
Branch Office NAT, 327–328
Cone NAT supported with software version 6.00, 81
DMZ using, 157–158
Double NAT, 320
Dynamic Many-to-Many NAT, 317–318
Dynamic Many-to-One NAT, 316–317
Dynamic One-to-One NAT, 316, 317
dynamic routing protocols with, 329–330
dynamic versus static translation, 315–316
firewall SIP ALG, 332
Full Cone NAT mode, 322
hairpinning, 332–334
Interface NAT, 327, 329
IP address shortage and, 282
IPSec Aware NAT, 321–322
many-to-one, 146
modes available, 322
NAT ALG for SIP, 331–332
NAT Traversal by VPN Routers, 144–145, 325–326
for non-routable IP addresses, 144–145
overview, 282, 315
policy configuration, 330–331
policy sets, 330–331
Port Forwarding NAT, 319–320
Port Restricted Cone NAT mode, 323–324
Proxy ARP, 335
Restricted Cone NAT mode, 322–323
rule creation, 331
security policies, 330
security vulnerabilities, 282
service properties, 330
with stateful firewalls, 282
Static One-to-One NAT, 318–319
statistics, 334–335
STUN (Simple Traversal of UDP through NAT), 327, 333
summarization, 330
Symmetric NAT mode, 324–325
time-outs, 334
VoIP with, 326–327, 331
VPN Client keepalive, 446–447
VPN security and, 144
NAT Traversal
blocked ports and, 145
defined, 144
IPSec clients and, 325–326
overview, 325–326
STUN (Simple Traversal of UDP through NAT), 327, 333
UDP port for, 325, 326
VoIP and, 326–327, 331
NetBIOS (Network Basic Input/Output System), 4
Netstat utility, 539–540
Network Address Port Translation (NAPT), 316
Network Address Server (NAS), 386, 388, 390
Network Address Translation. *See* NAT
network addressing
ARP for, 351–352
IP addressing, 351
MAC addressing, 350
network address defined, 349
overview, 349
RARP for, 353

network interface cards (NICs), 21
Network layer (OSI layer 3), 5–6
network management stations, 541, 544–545
network routing. *See* routing
Network Time Protocol. *See* NTP
networking basics
  hardware, 19–23
  IP addressing, 9–12
  LAN overview, 7
  MAC addressing, 8–9
  OSI Reference Model, 2–6
  protocols and standards, 12–18
  uses for networks, 2
  WAN overview, 8
Next Header field
  in AH packet, 33, 403
  in ESP packet, 34, 404
Next Hop traffic filters, 314–315
NICs (network interface cards), 21
NOC (Network Operations Center)
  administration of VPN Routers, 180–184
  control tunnels used by, 181
  defined, 180
  direct access to VPN Routers by, 181
  logging by, 182
  out-of-band management by, 181
  SNMP used by, 182–184
  VPN Client for direct access, 181
None admin level, 204
Nortel Contivity Secure IP Services Gateway. *See* Nortel VPN Router software; Nortel VPN Routers
Nortel Contivity VPN Client (CVC). *See* Nortel VPN Client
Nortel networks documentation, 687–688
Nortel Reference Manual for the Command Line Interface, 622
Nortel technical support, 591–592
Nortel VPN Client. *See also* Nortel VPN Router software
  Authentication Options, 438
  AutoConnect, disabling or installing, 439
  CD-ROM contents, 106–107
  Central Office solution using, 168–171
  client defined, 423
  Connection Wizard process, 125–132
  custom installation modes, 441–442
  customizing, 440–442
  for direct access to VPN Routers, 181
  disabling keepalives, 439
  ease of using, 433
  Edit menu, 437, 438
  Event logging, 443–445
  exiting, 437
  failover, 458–461, 473–475
  File menu, 436–437
  Group ID and Group password authentication, 128–129
  group.ini file, 442
  Help menu, 439–440
  installing, 106–113, 426–433, 441–442, 464–465
  IPSec mobility, 447–449, 475–477
  IPSec VPN Client Software, 142
  keepalives, 439, 445–447
  logging, 468–469
  main menu items, 435–440
  Monitor window, 434–435
  Name Server Options, 439
  no Group ID and Group password authentication, 128
  operating systems supported, 106, 424–426
  Options menu, 437–439
  overview, 106, 424–426
  for PC access to corporate network, 168–171
  release notes, 107
  security banner configuration, 449–451
  SOHO installation using, 148–149
  split tunneling, 451–455
  starting, 122–132, 433, 435
  taskbar status icon, 434, 435
  Token Card Authentication, 130–132
  troubleshooting using, 550
  TunnelGuard application for, 455–458
  uninstalling existing version, 113–115
  upgrading, 113–122

Nortel VPN Client *(continued)*
user profile parameters configurable for, 441
username and password authentication, 126–128
Nortel VPN Router 100
added to existing Regional Office network, 160–162
compared other models, 41, 68–70
configuring, 492–502
illustrated, 51
intended uses, 40, 46, 48
overview, 48, 50
SOHO installation using, 151–154
technical specifications, 50
tunneling to a different VPN Router model, 498–502
tunneling to another VPN Router 100, 495–498
Nortel VPN Router 200 series, 50. *See also specific models*
Nortel VPN Router 221
compared other models, 41, 68–70
illustrated, 52
intended uses, 40, 46, 50
overview, 50–51
SOHO installation using, 149, 150–151
technical specifications, 51
Nortel VPN Router 251
compared other models, 41, 68–70
illustrated, 53
intended uses, 40, 46, 52
overview, 52–53
SOHO installation using, 149, 150
technical specifications, 53
Nortel VPN Router 600
compared other models, 41, 68–70
illustrated, 54
intended uses, 40, 47, 53
overview, 53–54
software version 6.00 supported by, 79–80
technical specifications, 54
Nortel VPN Router 1000 series, 55. *See also specific models*
Nortel VPN Router 1010
compared other models, 41, 68–70
illustrated, 56
intended uses, 40, 47, 55
license upgrades available, 56
overview, 55
software version 6.00 supported by, 79
technical specifications, 55–56
Nortel VPN Router 1050
compared other models, 41, 68–70
illustrated, 58
intended uses, 40, 47, 57
license upgrades available, 57
overview, 57
software version 6.00 supported by, 79
technical specifications, 57
Nortel VPN Router 1100
compared other models, 41, 68–70
illustrated, 60
intended uses, 40, 47, 58
license upgrades available, 59
overview, 58–59
software version 6.00 supported by, 79–80
technical specifications, 59
Nortel VPN Router 1700
compared other models, 41, 68–70
intended uses, 40, 48, 60
overview, 60
software version 6.00 supported by, 79–80
Nortel VPN Router 1700 series, 59. *See also specific models*
Nortel VPN Router 1740
compared other models, 41, 68–70
illustrated, 62
intended uses, 40, 48, 61
license upgrades available, 62
overview, 61
software version 6.00 supported by, 79–80
SSL VPN Module 1000 for, 41
technical specifications, 61
Nortel VPN Router 1750
compared other models, 41, 68–70
illustrated, 64
intended uses, 40, 62
license upgrades available, 63
overview, 62–63

software version 6.00 supported by, 79–80
SSL VPN Module 1000 for, 41
technical specifications, 63
Nortel VPN Router 2700
compared other models, 41, 68–70
illustrated, 65
intended uses, 40, 49, 63
license upgrades available, 65
overview, 63–64
software version 6.00 supported by, 79–80
SSL VPN Module 1000 for, 41
technical specifications, 64–65
Nortel VPN Router 5000
compared other models, 41, 68–70
illustrated, 67
intended uses, 40, 49, 66
license upgrades available, 66
overview, 66
software version 6.00 supported by, 79–80
SSL VPN Module 1000 for, 41
technical specifications, 66
Nortel VPN Router software. *See also* Nortel VPN Client; upgrading Nortel VPN Router software
accounting services, 76
Additional VPN Tunnel Support License key, 81
Advanced Router License key, 80–81, 226
applying a new version for recovery, 557, 559
backout to previous version, 101
bandwidth management services, 76–77
certifications supported, 77
Contivity Stateful Firewall License key, 81, 283
displaying status information, 215
documentation online, 76
downloading, 76, 221
encryption services, 77
features introduced in version 6.00, 81–82
IP routing services, 77–78
loading a new version, 83–102
maintaining multiple versions, 221–222
management services, 78
memory requirements for version 6.00, 80
optional software licenses with version 6.00, 80–81
overview, 76
preloaded in VPN Routers, 76
release notes, 83
removing unused versions, 102–105
showing version of, 623, 645
SSL services, 79
stateful firewall, 78
upgrades produced for, 76, 83
user-authentication protocols and standards supported, 78
version 6.00, 79–82
version importance, 82
VPN Routers supporting version 6.00, 79–80
VPN tunneling protocols supported, 79
WAN services, 79
Nortel VPN Router troubleshooting
challenges for, 545
console cable for, 546–547
crossover cable for, 548
FTP client for, 552–553
FTP server for, 551–552
laptop computer for, 549–550
system recovery disk for, 548–549
terminal emulator for, 550–551
tools for, 546
VPN Client for, 550
Nortel VPN Routers. *See also* Nortel VPN Router software; *specific models*
address translations supported, 316
authentication servers with, 229, 230
booting with specified boot image file, 654
Branch Office Tunnel VPN solution, 70–71

Nortel VPN Routers *(continued)*
client load balancing and failover, 171–172
comparison chart, standard options, 68
comparison charts, supported optional equipment, 69–70
comparison, graphical, 41
corporate LAN solutions, 48–49
creating recovery disks, 223–224, 548–549, 655
deployment examples, 70–73
displaying all currently established tunnels, 635
displaying current configuration, 636
displaying current running configuration, 647–654
displaying forwarding action enabled, 647
displaying identifying information, 641–642
displaying options configured, 644
displaying statistical information, 646–647
displaying status information, 215–216
Extranet VPN solution, 71–72
failover, 172
groups, configuring, 469–470
hardware interface options, 42–46
health check for, 216–217, 568–569, 636–638
home office solutions, 46
initial setup, 465–468
as intranet access points, 166–167
load balancing, 172
logging, 182
management services supported, 78
NAT Traversal by, 144–145, 325–326
network administration of, 180–184
office-to-branch office solution, 47
portfolio, 40–41
as RADIUS proxy server, 246–248
for Regional Office, determining suitability, 158–160
Remote Access VPN solution, 72–73
remote branch office solutions, 47
reporting utilities, 562–582
restarting, 658–659
as secured access gateway, 277–278
shutting down, 224
software preloaded in, 76
SSL VPN Module 1000, 41
system status tools, 214–218
troubleshooting, 545–553
users, configuring, 471–473
verifying server code integrity, 619
viewing global settings, 630–631
VPN Client for direct access, 181
Nortel Web site, 76, 83, 106, 221, 426, 591
Nr field (L2TP packet header), 37, 400
Ns field (L2TP packet header), 37, 400
NTP (Network Time Protocol)
configuring, 484–487
displaying current configuration, 644
displaying statistical information, 646–647
importance for network management, 184
support for, 184

O

O field (L2TP packet header), 37, 399
octets in IP addresses, 9–11
Offset fields
in enhanced GRE packet header, 394
in GRE packet header, 38
in L2F packet header, 35, 390
in L2TP packet header, 37, 400
100Base-FX Ethernet, 342
100Base-TX Ethernet, 342
1000Base-CX Ethernet, 343
1000Base-LX Ethernet, 343
1000Base-SX Ethernet, 343
1000Base-SX Ethernet module, 42–43
1000Base-T Ethernet, 343
1000Base-T Ethernet module, 42–43
128-bit encryption, 134. *See also* 3DES
Open Shortest Path First protocol. *See* OSPF protocol
Open Systems Interconnection Reference Model. *See* OSI Reference Model

operating systems
Stateful Firewall Manager support for, 284
support documented in release notes, 83, 107
VPN Client support for, 106, 424–426
vulnerabilities to hackers, 28
Options field (IP packet header), 13
Options menu (Nortel VPN Client), 437–439
Organization Unique Identifier (OUI) bits, 350
OSI (Open Systems Interconnection) Reference Model
advantages of, 3
Application layer (Layer 7), 3, 4, 278
Data Link layer (Layer 2), 6, 8
illustrated, 3
Network layer (Layer 3), 5–6
overview, 2–3
Physical layer (Layer 1), 6
Presentation layer (Layer 6), 4
Session layer (Layer 5), 4
strict adherence not required for, 3
Transport layer (Layer 4), 4–5, 278
OSPF (Open Shortest Path First) protocol
adjacencies, 372
areas, 370, 372–374
authentication by, 370
considerations for implementing, 371–372
exchange process, 372
flooding process, 372
hello messages, 375
history of, 371
as an IGP protocol, 363, 370
link-state routing used by, 361–362, 375–376
LSAs (Link-State Advertisements), 372, 375
LSDBs (Link-State Databases), 372, 374, 375–376
NAT with, 329–330
OSPF version 2 (OSPF-2 or OSPFv2), 371
overview, 15, 374–376
packet header contents, 15
RFCs for, 682–684
routing table process, 372
SPF (Shortest Path First) algorithm, 375–376
sub-protocol processes, 372
unique router ID for, 372
version 2 supported, 77
OUI (Organization Unique Identifier) bits, 350
out-of-band management for VPN Routers, 181
out-of-order packet delivery, 406

P

P field
in L2F packet header, 34, 389
in L2TP packet header, 37, 399
Packet Capture (PCAP), 582–584
packet filtering. *See also* firewall policies
actions used by rules, 279–280
defined, 27
with mandatory tunneling, 153–154
rules, overview, 279–280
Packet Internet Grouper command. *See* `ping` command
packet sniffers, 541, 542–543. *See also* capturing packets
packets. *See also* header of packets
broadcast, 348
capturing, 582–584, 654–655
defined, 12
dropped by DiffServ, 408
dropped, QoS and, 406
dropping those used in attacks, 280
ESP, contents of, 403
IPSec, contents of, 402, 403
L2F, contents of, 387, 388–389
L2F session exchange, 387
L2TP, contents of, 397–398, 399
Network layer handling for, 6
PPPoE, 415–416
PPTP, contents of, 393
PPTP session exchange, 391–392

packets *(continued)*
QoS issues, 406
sequence numbers for, 5
System log information for, 213
tracing path of, 536–537
padding
in ESP packet, 34, 404
in IP packet header, 13
in L2TP packet header, 37
palm handheld platforms, 106
Palm OS, VPN Client support for, 426
PAP (Password Authentication Protocol)
described, 237
with LDAP Proxy, 237, 238
PAP with Bind, 238
with RADIUS, 245
parity bits
for Console Interface, 614
when upgrading software, 87
Passive FTP, stateful inspection for, 278
passwords. *See also* authentication
for administrator, changing via serial interface, 186–187
for BBI or VPN Router GUI, default, 96
for CLI Privileged EXEC mode, 189
for Console Interface, 614
expired, reporting, 215
for HyperTerminal login, 88
Private Key Password for CMP, 256
shared secrets, 32, 244, 250, 255
for VPN Client, 126, 128–129
path-vector routing algorithm, 380
Payload field (ESP packet), 34, 404
payload of packets
defined, 12
ESP packet, 33, 34, 404
PPPoE packet, 415
Payload packet with L2F, 387
PBH (Per Hop Behavior), 408–410
PCanywhere application, 25
PCAP (Packet Capture), 582–584
PC-based VPN tunnels
examples, 142–143
IPSec VPN Client support for, 142
NAT for non-routable IP addresses, 144–145
non-routable IP address standard, 142, 143
operating systems supported, 142
PCI (Peripheral Component Interconnect), 42
PCM (Pulse Code Modulation), 43
peer-to-peer tunnels. *See* BOTs
physical interfaces, 278–279.
See also interfaces; *specific interfaces*
Physical layer (OSI layer 1), 6
physical topologies of Ethernet LANs, 339–340
Ping of Death attack, 281
`ping` (Packet Internet Grouper) command
BBI Ping utility for, 219, 220, 578–579
BIS triggered by failure, 175, 421
DOS session syntax for constant ping, 100
issuing, 533–534
for LDAP server monitoring, 240–241
monitoring constant ping after upgrading software, 101
options available for, 535
over private network, 621
over public network, 620–621
overview, 219, 533
testing a node, 534–535
`trace` command versus, 620
troubleshooting using, 533–536
User EXEC mode (CLI), 620–621
using an optional parameter, 535–536
PKCS#12 Personal Information Exchange Syntax, 253–254
PKI (Public Key Infrastructure)
adding L2TP Access Concentrators, 274–275
administrative tools, 254
CA and X.509 certificates, 254
certificates, defined, 254
Certification Authority service, 254
CRL (Certificate Revocation List) overview, 264–265
CRL details display, 259–260
CRL Distribution Points (CDPs), 261, 267–268

CRL retrieval, 268
CRL server configuration, 265–267
enabling certificate use for tunnels, 268–269
identifying Branch Offices with certificates, 270–271
identifying users with certificates, 269–270
IPSec Tunnel authentication, 271–273
loading certificates, 255
L2TP/IPSec tunnel authentication, 273–274
overview, 32
requesting a server certificate, 255
server certificates using CMP, 255–260
setup, 254–264
Trusted CA Certificate installation, 260–261
Trusted CA Certificate settings, 261–264
Pocket PC operating system, 106
Point-to-Point Protocol. *See* PPP
Point-to-Point Protocol over Ethernet. *See* PPPoE
Point-to-Point Tunneling Protocol. *See* PPTP
Port Forwarding NAT, 319–320
port NAT. *See* NAT
Port Restricted Cone NAT, 323–324
port-based VLANs, 354
ports. *See also* serial interfaces or ports
LDAP Proxy setting, 239
RADIUS server setting, 244
resetting WAN type ports, 620
stateful inspection for, 278
VPN Router comparison charts, 68, 69
PPP (Point-to-Point Protocol)
combined with Ethernet in PPPoE, 413, 414
link to ISP required for L2F, 386, 388
support for, 79
PPPoE (Point-to-Point Protocol over Ethernet)
ABOTs for, 139–140
broadband connection types, 413
cost-effectiveness of, 413–414
defined, 413
overview, 413–416
packet contents, 415
PADI packets, 415
PADO packets, 415
PADT packets, 416
support for, 79
PPTP (Point-to-Point Tunneling Protocol)
advantages of, 391
client software required for tunneling, 390
combined with L2TF in L2TP protocol, 36
control messages, 395
control portion of tunnel, 392
data component of tunnel, 392
data portion of packet, 395
enhanced GRE header for, 393–394
IP addresses used with, 392
IP-in-IP encapsulation by, 392
L2F versus, 390, 391
NAS not needed with, 390
overview, 35, 390–396
packet contents, 393
packet header contents, 35–36
PPP link to ISP required for, 391
RFCs for, 667
support for, 79
two network sessions required by, 392
typical session exchange, 391–392
for User/Client Tunnels, 141
VPN Router capabilities using, 396
Pre Shared Key (PSK), 134
Presentation layer (OSI layer 6), 4
PRI (Primary Rate Interface) ISDN, 18
print server, defined, 20
printing
routing table information, 538–539
working directories, 616, 617–619
priority code
in Event log, 208–209
in Security log, 210–211
in System log, 212–213

Priority field (VRRP packet header), 16
Privileged EXEC mode (CLI)
  `boot` command, 654
  `capture` command, 654–655
  `clear` command, 632–633
  `create` command, 655
  `delete` command, 656
  `disable` command, 189
  enabling for a user, 189, 631
  `exit` command, 189
  `forced-logoff` command, 656
  installing Advanced Router License Key, 226
  `kill` command, 656–657
  `license install` command, 226
  listing of commands, 192–193, 631–632
  login, 189
  `mkdir` command, 657
  `more` command, 657–658
  overview, 189
  `reformat` command, 658
  `reload` command, 658–659
  `rename` command, 659
  `reset` command, 633
  `retrieve` command, 659–660
  `rmdir` command, 657
  `show` commands, 633–654
proactive administration
  backing up, 223, 585
  documentation, 588
  knowledge sharing, 587
  overview, 584–585
  recovery disk availability, 586
  recovery disk creation, 223–224, 548–549, 655
  remote access for support personnel, 587
  research, 585–586
  software upgrades, 220–223
  system shutdown, 224
  upgrades and configuration changes, 588–591
processors. *See* CPUs or processors
prompts for CLI
  Global Configuration mode, 190
  Privileged EXEC mode, 189, 631
  User EXEC mode, 189, 615
Protocol field
  in enhanced GRE packet header, 394
  in GRE packet header, 38
  in IP packet header, 13
  in L2F packet header, 35, 389
protocol-based VLANs, 355
protocols. *See also specific protocols*
  for Application layer, 3
  defined, 12
  for IP routing, support for, 77–78
  routing protocol types, 363
  for Session layer, 4
  for Transport layer, 5
  for tunneling, 30–38, 79, 385
  for user authentication, support for, 78
  for User/Client Tunnels, 141
  for WANs, support for, 79
proxy servers
  ARP, 335
  in the DMZ, 27
  LDAP, 236–240, 252–253
  overview, 27
  RADIUS, 236, 246–248
PSK (Pre Shared Key), 134
Public Key Infrastructure. *See* PKI
Pulse Code Modulation (PCM), 43
PuTTY terminal emulator, 551
`pwd` command, 616, 617–619

Q

QoS (Quality of Service)
  DiffServ (Differentiated Services) for, 406–410
  need for, 405–406
  problems possible, 406
  RFCs for, 679–680
  software features for, 76–77
  for VoIP, 412, 413
  VPN Router support for protocols, 410

R

R field
  in enhanced GRE packet header, 394
  in GRE packet header, 38
RADIUS (Remote Authentication Dial-In User Service)
  AAA functions, 223

adding clients to proxy, 248
authentication options, 245–246
for authentication server, 168, 242–246
client component, 242
days accounting files are stored, 249
diagnostics, 246
enabling accounting, 248–250
enabling authentication, 242–246
External LDAP with, 236–237
Interim Update Interval for accounting, 249
LDAP Proxy support, 236
Maximum Transmit Attempts setting, 245
overview, 18, 222–223
packet header contents, 18
port setting for server, 244
Private interface for, 244, 246–247, 250
proxy server, 246–248
Public interface for, 244, 246–247, 250
reporting diagnostics for, 215
resetting the server, 633
Response Timeout for accounting, 249
Response Timeout Interval for server, 244–245
resuming use of Primary server after failover, 246
RFCs for, 672–674
server component, 242
server position in relation to VPN Router, 244
Session Update Interval for accounting, 248–249
shared secret configuration, 244, 250
support for, 78, 242
RAM (Random Access Memory). *See also* flash memory
displaying information for VPN Router, 216
examples, 19
overview, 19
VPN Router comparison chart, 68
RARP (Reverse Address Resolution Protocol), 353
RAS (Remote Access Services), 24
RC4 (ARCFOUR) encryption, 77, 251
RCMD, stateful inspection for, 278
RDN (Relative Distinguished Name)
for CMP, 258–259
for identifying users with certificates, 269–270
`readme.txt` file
for VPN Client installation, 112, 113, 432
for VPN Client upgrade, 120, 121
RealAudio, stateful inspection for, 278
rebooting
`boot` command for, 654
after installing VPN Client, 112, 432
after uninstalling existing VPN Client, 115
after upgrading VPN Client, 121
Rec or Recur field
in enhanced GRE packet header, 394
in GRE packet header, 38
recovery. *See* system recovery
recovery disks. *See* system recovery disks
`reformat` command, 658
reformatting floppy diskettes, 658
Regional Office
advantages of VPNs for, 164
BOT use for, 136
determining VPN Router suitability, 158–160
requirements affecting VPN Routing needs, 164
split tunneling for, 161
tunnel types for, 159
typical configuration, 159
upgrading to VPN technology, 162–164
VPN Router 100 added to existing network, 160–162
Relative Distinguished Name (RDN)
for CMP, 258–259
for identifying users with certificates, 269–270
release notes
for VPN Client, 107
for VPN Router software, 83
`reload` command, 658–659

remote access. *See also specific methods*
applications, 25
hacker exploitation of, 28
RAS for, 24
for support personnel, 587
systems, 25
terminal servers for, 25
traditional methods for, 24
typical topology, 24
VPN deployment example, 72–73
Remote Access Services (RAS), 24
Remote Authentication Dial-In User Service. *See* RADIUS
removing or deleting
directories with `rmdir` command, 657
files with `delete` command, 656
firewall policy, 291
uninstalling existing VPN Client, 113–115
unused versions of VPN Router software, 102–105
VPN Client connection, 437
`rename` command, 659
renaming
files or directories, 659
firewall policies, 292
repeaters, 22, 23
replay attacks, 33
reporting utilities
Accounting information, 571–572
Admin directory for, 563, 564
Admin Tools for, 577–582
Config log information, 574, 575
Event log information, 576–577
Health Check information, 568–569
Reports information, 566, 567, 568
Security log information, 572–574
Sessions information, 564–565
Statistics information, 569–571
status directory for, 562–563
Status menu overview, 563
System information, 566–567
System log information, 574–576
Reports utility, 215, 216
request flowchart (LDAP), 232, 233
Requests For Comments. *See* RFCs
research before implementation, 585–586
Reserved field
in AH packet, 33
in L2F packet header, 34, 389
`reset` command
Privileged EXEC mode (CLI), 633
User EXEC mode (CLI), 620
Resource Reservation Protocol (RSVP), 77
restarting Nortel VPN Routers, 658–659
restoring
Internal LDAP, 235
system from recovery disk, 555–556, 559
Restricted Cone NAT, 322–323
`retrieve` command, 659–660
Reverse Address Resolution Protocol (RARP), 353
RFCs (Requests For Comments)
for AES, 671–672
for BGP, 680–682
for certificates, 679
defined, 665
for DES, 670
for fun, 684–685
for IKE, 670–671
for IPSec, 667–669
for ISAKMP, 670–671
for LDAP, 674–678
for L2F, 666
for L2TP, 666–667
for OSPF, 682–684
for PHB groups, 409
for PPTP, 667
publication by IETF, 665
for QoS, 679–680
for RADIUS, 672–674
resources, 688–689
for RIP, 684
for 3DES, 670
for VPN, 669–670
for VRRP, 173, 680
RIB (Routing Information Base), 379

RIP (Routing Information Protocol). *See also* routing tables
advertising routes using, 161
configuring, 482–483
as distance-vector routing protocol, 14
distance-vector routing used by, 360–361, 367
history of, 366–367
as an IGP protocol, 363, 364
NAT with, 329–330
overview, 14, 364–366
packet header contents, 14
RFCs for, 684
RIP request, 368
RIP response, 368–369
RIP-2 features, 366
RIPng (RIP next generation), 367
route determination, 367
timelines, 369
update frequency, 366
updates, 368–369
versions supported, 78
`rmdir` command, 657
`route` command, 538–539
Routed (Route-d or Route-daemon) protocol, 366
Router ID field (OSPF packet header), 15
router software. *See* Nortel VPN Router software
routers. *See also* Nortel VPN Routers; *specific models*
ABRs (Area Border Routers), 373
ASBRs (Autonomous System Boundary Routers), 374
defined, 8, 22
example of LAN-to-LAN and LAN-to-WAN networking via, 23
internal versus border, 363–364
OSPF areas and, 373–374
overview, 22
routing. *See also specific protocols*
algorithms, 359–362
basics, 356–358
EGP for, 356
IGP for, 355
protocol concepts, 363–364
protocol types, 353
unreachable route as trigger for BIS, 175, 421
routing algorithms
distance-vector routing, 360–361, 367
hop count used for, 359, 364
link-state routing, 360, 361–362, 375–376
path-vector routing, 380
Routing field (GRE packet header), 38
Routing Information Base (RIB), 379
Routing Information Protocol. *See* RIP
routing services, supported by VPN Router software, 77–78
routing tables. *See also* RIP
clearing routes from, 621–622, 632
created by router, 22
defined, 14, 356
displaying summary of routes, 640–641
displaying with `show ip route` command, 626, 641
distance-vector routing protocols and, 14
dynamic insertion of information in, 359
example, 358–359
information in, 359
OSPF process for, 372
overview, 358–359
printing information for, 538–539
process for building, 357–358
RIP Entry Table for, 14
static insertion of information in, 359
troubleshooting, 538–539
verifying routes, 640
RSA Security's SecurID technology, 32
RS-232 serial interface, 44, 614
RSVP (Resource Reservation Protocol), 77
rule creation for firewall policies
accessing menus for, 296
Action column, 303–304
Cell Option menu, 297–298
Cell Procedure menu, 297, 298, 299

rule creation for firewall policies *(continued)*
Destination column, 301–302
Dst Interface column, 299–301
Header Row menu, 297
Log column, 304
Remark column, 304
Row menu, 297
rule column headers, 298
Service column, 302–303
Source column, 301–302
Src Interface column, 299–301
Status column, 304
rule creation for NAT, 331

S

S field
in enhanced GRE packet header, 394
in GRE packet header, 38
in L2F packet header, 34, 389
in L2TP packet header, 36, 399
s field
in enhanced GRE packet header, 394
in GRE packet header, 38
S (success message) severity code (Event log), 445
SDSL (Symmetrical Digital Subscriber Line), 17
Secure Hash Algorithm (SHA), 251
Secure Socket Layer. *See* SSL
SecureCRT terminal emulator, 551
SecurID technology, 32–33
security. *See also* authentication; firewalls; NAT
certifications supported by VPN Router software, 77
definitions of, 277
filters, 311–315
IPSec standard for, 33–34
L2F protocol for, 34–35
L2TP over IPSec for, 398–399
L2TP protocol for, 36–37
PKI for, 32
PPTP protocol for, 35–36
SecurID technology for, 32–33
Security log, 210–211, 572–574
SNMP, 183
SSL for, 30–32
tearing down tunnels for, 151
T1 line issues, 162–163
security banner configuration (VPN Client), 449–451
Security log
overview, 210–211
reporting utility for, 572–574
Security Parameters Index (SPI) field
in AH packet, 33, 403
in ESP packet, 34, 404
security policies. *See* firewall policies
Sequence field (L2F packet header), 35, 389
sequence numbers
in AH packet, 33, 403
in enhanced GRE packet header, 394
in ESP packet, 34, 404
in GRE packet header, 38
in L2F packet header, 35, 389
in TCP, 5
sequential topology for BGP, 377–378
serial interfaces or ports
changing administrator user ID or password via, 186–187
CLI access via, 188, 613, 614–615
COM1 settings for upgrading software, 86–87
defined, 44
HSSI, 45
login to VPN Router, 186
menu, 186–187, 188
options for VPN Routers, 44, 45
resetting, 620, 633
RS-232, 44, 614
speed of, 44, 45
for VPN Router management, 186–187
V.35, 44
X.21, 44
serial number, displaying for system, 215
servers. *See also specific types*
configuration screens for, 293–294
defined, 20
types of, 20

services, verifying current, 629–630
Serv-U FTP server, 552
Session ID field (L2TP packet header), 37, 400
Session layer (OSI layer 5), 4
sessions
  accounting log for, 218
  information about active, 214–215
  L2F session exchange, 387
  PPTP session exchange, 391–392
  reporting information, 215
Set command (SNMP), 183, 184
SHA (Secure Hash Algorithm), 251
SHA-1 authentication
  Encryption Accelerator Module support for, 45
  IPSec use of, 401
shared secrets
  for CMP, 255
  defined, 32
  RADIUS accounting setting, 250
  RADIUS server setting, 244
sharing knowledge, 587
Shortest Path First (SPF) or link-state routing algorithm, 360, 361–362, 375–376
`show` commands
  further information, 622
  listing (Privileged EXEC mode), 633–635
  listing (User EXEC mode), 622–623
  Privileged EXEC mode (CLI), 633–654
  `show admin`, 625
  `show all`, 635
  `show clock`, 625–626
  `show current-config-file`, 636
  `show dhcp`, 636
  `show file`, 625
  `show flash`, 623–625
  `show health`, 636–638
  `show hosts`, 641–642
  `show interface`, 638–639
  `show ip`, 626, 639–640
  `show ip interface`, 627
  `show ip local`, 640
  `show ip route`, 626, 640, 641
  `show ip route summary`, 640–641
  `show ip traffic`, 627–629
  `show ipsec`, 642–643
  `show logging`, 643–644
  `show ntp`, 644
  `show router`, 644
  `show running-config`, 647–654
  `show services`, 629–630
  `show snmp`, 645
  `show snmp mib`, 645
  `show software`, 645
  `show status`, 646
  `show status statistics`, 646
  `show status statistics system`, 646–647
  `show switch-settings`, 630–631
  `show system`, 647
  `show version`, 623
  User EXEC mode (CLI), 622–631
shutting down the system, 224
Simple Mail Transfer Protocol (SMTP), 3
Simple Traversal of UDP through NAT (STUN), 327, 333
simplex data transmission mode, 347
SIP signaling protocol
  firewall SIP ALG, 332
  hairpinning with, 333
  NAT ALG for SIP, 331–332
slots, VPN Router comparison chart for, 68
small offices. *See* SOHO
SMTP (Simple Mail Transfer Protocol), 3
Smurf attack, 281
sniffer trace file, 542
sniffing
  `capture` command for, 654–655
  packet sniffers for, 541, 542–543
  PCAP for, 582–584
SNMP (Simple Network Management Protocol)
  advantages of, 182
  agents, 182, 183
  ALG support, 331–332
  commands, 183, 184
  components, 182

SNMP (Simple Network Management Protocol) *(continued)*
displaying configuration on VPN Router, 645
management workstation, 183
MIB (Management Information Base), 183, 645
in the network, 183
security, 183
SNMP network management station, 182
for VPN Router management, 182–184
soft telephone, 148
Soft Token Support, 78
software. *See also* Nortel VPN Client; Nortel VPN Router software; *specific software*
defined, 75
importance of, 75
for laptops, 550
for soft telephone, 148
TCP/IP utilities, 533–541
third-party troubleshooting tools, 529, 543, 545, 551
upper OSI layers implemented in, 2
Software Requirement Set (SRS) Builder, 456
SOHO (Small Office/Home Office)
BOT versus ABOT for, 150
DMZ with, 151–153
firewall policy example, 309
home office scenarios, 148–150
installation using VPN Router 100, 151–154
installation using VPN Router 221, 149, 150–151
installation using VPN Router 251, 149, 150
mandatory tunneling with, 149–150
small office scenarios, 149, 150–154
small offices versus home offices, 148
typical installations, 148–151
VoIP for, 148, 151
VPN Router home office solutions, 46
VPN tunneling for, 148–154
Solaris operating system (Sun)
Stateful Firewall Manager support for, 284
VPN Client support for, 106
Source IP Address
in IP packet header, 13
in L2F packet, 387
spam, hacker exploitation of, 29
Special Characters feature (LDAP), 252
speed
of E1 lines, 44
of Ethernet LANs, 7
Ethernet standards, 42–43, 342–343
of serial interfaces, 44, 45
of T1 lines, 43
SPF (Shortest Path First) or link-state routing algorithm, 360, 361–362, 375–376
SPI (Security Parameters Index) field
in AH packet, 33, 403
in ESP packet, 34, 404
split tunneling
considerations for enabling, 455–456
defined, 42
inverse, 456–457
overview, 136, 451–453
Regional Office example, 161
typical BOT installation using, 136–138
with VPN Client, 451–455
spoofing
anti-spoofing, 280, 288
defined, 280
SQLNET, stateful inspection for, 278
SRS (Software Requirement Set) Builder, 456
SSL (Secure Socket Layer)
Certificate Authority for, 31
certificates, 31
components, 31
defined, 30
encryption methods supported, 251
External LDAP server with, 251–252
keys, 32
Nortel SSL VPN Module 1000 for, 41
overview, 30–32

shared secrets, 32
support for, 79
VPN Router comparison chart, 69–70
standards. *See also specific standards*
defined, 12
encryption, support for, 77
Ethernet, 42
Fast Ethernet, 342
Gigabit Ethernet, 343
for non-routable IP addresses, 142, 143
for serial interfaces, 44, 45
Traditional Ethernet, 342
user authentication, support for, 78
V.90 modem, 45
for VPN tunneling, 30–38
for WANs, support for, 79
X.500 directory service, 230
star topology, 339–340
starting
Connection Wizard from File menu, 124
HyperTerminal, 84
Internet Explorer, 94
LDAP server, 234
restarting VPN Routers, 658–659
VPN Client, 122–124, 433, 435
starting Nortel VPN Client. *See also* Connection Wizard
choosing to run the Connection Wizard, 123–124
Connection Wizard process, 125–132
from a directory, 122, 123
first time, 122–132
after the first time, 123
menu choices after, 435–440
from Windows Start menu, 122, 123, 433
Stateful Firewall Manager, 284
stateful firewalls. *See also* firewall policies; firewalls; packet filtering
access control filters, 281–282
anti-spoofing, 280
anti-spoofing configuration, 288
application stateful inspection, 278
attack detection, 280–281
basics, 277–282
configuration verification, 306
configuring, 283–289
Contivity Stateful Firewall License key for, 81, 283
defined, 78
enabling application-specific logging, 286–287
enabling connection limitation and logging, 286
enabling the feature, 285–286
filter rules, 279–280
firewall policy implementation, 307–308
interfaces, 278–279
Malicious Scan Detection configuration, 289
NAT with, 282
options available for, 284
prerequisites for configuring, 283
remote logging of firewall events, 287–288
for secured access gateway functionality, 277–278
service properties, 290
stateful inspection, 27, 278
support for, 78
system requirements for Stateful Firewall Manager, 284
stateful inspection
at Application layer, 278
application stateful inspection, 278
defined, 27
overview, 278
at Transport layer, 278
static IP addresses, 351
Static One-to-One NAT, 318–319
statistics
for IP, displaying, 626, 639–640
for IP traffic, displaying, 627–629
for NAT, 334–335
for NTP, displaying, 646–647
for VPN Router, displaying via BBI, 217–218, 569–571
for VPN Router, displaying via CLI, 646–647

stop bits
for Console Interface, 614
when upgrading software, 87
stopping LDAP server, 234
STUN (Simple Traversal of UDP through NAT), 327, 333
subnet mask
with L2F, 388
for Private LAN interface, 91, 92
subnetworks
defined, 7
LAN addresses for BOTs, 136
routing not required between subnets, 356
subnet-based VLANs, 355
success message (S) severity code (Event log), 445
summarization, 330
Sun Solaris operating system
Stateful Firewall Manager support for, 284
VPN Client support for, 106
support personnel, remote access for, 587
switches
BBI access and, 198
example forwarding data in a LAN, 21
hubs versus, 22
overview, 21
Symmetric NAT, 324–325
Symmetrical Digital Subscriber Line (SDSL), 17
SYN flood attack, 280
Syslog server configuration, 512–515
System log
overview, 212–213
reporting utility for, 574–576
Syslog server configuration, 512–515
system recovery. *See also* system recovery disks
Apply new version option, 557, 559
for disk-based VPN Routers, 554–558
for diskless VPN Routers, 558–562
Perform File Maintenance option, 557, 559–561
pushbutton for, 553
Reformat hard disk option, 557, 559
restarting the system, 558
System Restore option, 555–556, 559
View Event log option, 557, 561–562
system recovery disks. *See also* system recovery
booting to, 554
creating, 223–224, 548–549, 655
defined, 548, 553
keeping available, 586
system recovery using, 554–558
for troubleshooting VPN Routers, 548–549
System Shutdown tool, 224

T

T field (L2TP packet header), 36, 399
TCP (Transmission Control Protocol), 5
Tcpdump packet sniffer, 543
TCP/IP (Transmission Control Protocol/Internet Protocol)
as Session layer protocol, 4
troubleshooting utilities for, 533–541
TDM (Time Division Multiplexing), 43
Teardrop/Teardrop-2 attacks, 280
technical standards. *See* standards
technical support (Nortel), 591–592
Telecommunications Industry Association (TIA), 45
telephone number for support, 591
telephone services. *See* VoIP
telephones
hairpinning for, 332–334
IP-enabled handset, 148
soft, 148
Telnet
CLI access via, 187–188, 613, 615
CLI User EXEC mode established via, 615
controlling paging of session screen, 619
killing sessions, 656–657
10Base-2 Ethernet, 342
10Base-5 Ethernet, 342

10Base-FL Ethernet, 342
10Base-T Ethernet, 342
10/100Base-T Ethernet module, 42
`terminal` command, 619
terminal emulators, 550–551
terminal servers, 25
terminology (acronyms and abbreviations), 593–612
testing. *See also* troubleshooting
  nodes with `ping` command, 534–535
  to prove or replicate a problem, 531–532
TFTP (Trivial FTP), stateful inspection for, 278
Thinnet, defined, 342
third-party troubleshooting tools
  caveat regarding, 529
  FTP clients, 553
  FTP servers, 552
  network management stations, 545
  packet sniffers, 543
  terminal emulators, 551
3DES (Triple Data Encryption Standard)
  IPSec use of, 400, 401
  as 128-bit encryption, 134
  RFCs for, 670
  support for, 77
TIA (Telecommunications Industry Association), 45
time. *See also* NTP
  NAT time-outs, 334
  `show clock` command for, 625–626
  time-of-day trigger for BIS, 176–177, 421
Time Division Multiplexing (TDM), 43
time stamp
  in Configuration log, 206
  in Security log, 210
  in System log, 212
Time to Live (TTL)
  IP packet header field for, 13
  Trace Route tool use of, 219
Token Card Authentication (Nortel VPN Client), 130–132
tokens in SecurID technology, 32–33
T1 lines
  overview, 43
  security issues, 162–163
  VPN Router comparison chart, 69
  VPN Router option for, 43
topologies
  BGP, 377–378
  Ethernet LANs, 339–340
  physical versus logical, 339
TOS (Type of Service) field
  in IP packet header, 13
  replaced by DS field, 408
`trace` command
  overview, 620, 621
  `ping` command versus, 620
  User EXEC mode (CLI), 620, 621
Trace Route tool (BBI), 218–219, 579–580
traceroute (`tracert`) tool, 536–537
Transmission Control Protocol (TCP), 5
Transmission Control Protocol/Internet Protocol (TCP/IP)
  as Session layer protocol, 4
  troubleshooting utilities for, 533–541
transmission modes for data
  full-duplex, 347
  half-duplex, 346–347
  simplex, 346
Transport layer (OSI layer 4), 4–5, 278
Trap operations (SNMP), 183, 184
Triple Data Encryption Standard. *See* 3DES
Trivial FTP (TFTP), stateful inspection for, 278
troubleshooting. *See also* Nortel VPN Router troubleshooting
  cable testers for, 541, 543
  `capture` command for, 654–655
  common solutions, 532
  diagnosing the problem, 531
  file-retrieval problems, 205
  IPconfig utility for, 541, 542
  logical steps for, 530–532
  need for, 529
  Netstat utility for, 539–540
  network management stations for, 541, 544–545

troubleshooting *(continued)*
Nortel technical support for, 591–592
packet capture for, 582–584
packet sniffers for, 541, 542–543
`ping` command for, 533–536
proactive measures, 584–591
questions to consider, 530
RADIUS Diagnostic Report for, 246
`route` command for, 538–539
routing tables, 538–539
`show clock` command for, 625–626
`show ip route` command for, 640, 641
`show ip traffic` command for, 627–629
`show ipsec` command for, 642–643
`show system` command for, 647
system recovery, 553–562
TCP/IP utilities for, 533–541
testing to prove or replicate the problem, 531–532
third-party tools for, 529, 543, 545, 551
`trace` command for, 620, 621
traceroute tool for, 536–537
understanding the problem, 530–531
VPN Router reporting utilities for, 562–582
VPN Routers, 545–553
Trusted CA Certificate
access control by subject DN, 262–263
Allow All Policy, 262
CA key update, 264, 268
group and certificate association configuration, 263
group association required for, 261
installation, 260–261
user identification group assignment, 262
T3 lines, HSSI serial interface for, 45
TTL (Time to Live)
IP packet header field for, 13
Trace Route tool use of, 219
tunnel filters
adding rules, 312–313
Allow Management Traffic options, Local Services, 312–313
Allow Management Traffic options, Remote Server, 313
copying, 313
creating, 311
defined, 311
Tunnel ID field (L2TP packet header), 37, 400
tunnel rekey, 151
TunnelGuard application
banner messages, 458
considerations for installing, 457
Event logs, 457–458
features overview, 457–458
icon colors, 457
overview, 455
Software Requirement Set Builder, 456
TunnelGuard Agent, 456
TunnelGuard Daemon, 455–456
tunneling. *See also* ABOTs; BOTs; *specific protocols and standards*
Additional VPN Tunnel Support License key for, 81
control tunnels, 181
displaying all established tunnels on VPN Router, 635
displaying current end user tunnels, 642–643
displaying session information, 214
DMZ creation and usages, 154–158
encryption for, 134
idle timeout, 151
Initiator/Responder Tunnel, 140–141
interface designations in security policies, 279
inverse split, 456–457
IPSec Tunnel authentication, 271–273
keepalive signaling for, 140
L2TP/IPSec tunnel authentication, 273–274
mandatory, 136, 138, 139, 149–150, 153–154
overview, 134, 385
PC-based VPN tunnels, 142–145
protocols and standards, 30–38, 385
protocols supported, 79

Regional Office configuration, 159
rules for traffic required for, 290
security purposes for tearing down, 151
for small office or home office, 148–154
split, 136, 138, 161, 451–455
tunnel certificates, 253–254, 268–269
tunnel rekey, 151
User/Client Tunnels, 141–147
visualization of, 134, 135
VoIP carried over, 148
VPN Router comparison chart, 68
VPN Router 100 configuration, 492–502
VPN-enabled device acting in Client mode and, 145–147
twisted-pair cabling, 344–345
Type field
in OSPF packet header, 15
in VRRP packet header, 16
Type of Service (TOS) field
in IP packet header, 13
replaced by DS field, 408

U

UDP Bomb attack, 280
UDP (User Datagram Protocol)
attacks using, 280, 281
as connectionless delivery protocol, 5
IPSec use of ports, 402–403
overview, 5
port for NAT Traversal, 325, 326
as Transport layer protocol, 5
uninstalling existing Nortel VPN Client
locating the executable file, 113
Setup Status window, 115
uninstall phase, 115
using Windows Start menu, 114
UNIStim call server, hairpinning with, 333
UNIX operating system, VPN Client support for, 106
upgrading Nortel VPN Client
Application option, 119
confirmation window, 120
driver installation, 120
final phase, 121–122
initial windows opened, 116
install and run phase, 118–120
licensing agreement, 117
locating the executable file, 115, 116
need for, 113
proactive measures for, 588–591
`readme.txt` display, 120, 121
by running the installation program, 113
Select Program Folder phase, 118, 119
Setup Status window, 120
uninstalling existing version, 113–115
Windows GINA option, 119
Windows service option, 119
upgrading Nortel VPN Router software
assigning IP address to Private LAN interface, 91, 92
backout to previous version, 101
booting the VPN Router, 88
connecting Internet Explorer to management IP address, 94
connecting your PC to the VPN Router, 84
Connection Description phase, 84–86
connection type choices, 85–86
constant ping to Private LAN interface IP address, 100–101
FTP information entry, 97–98
GUI setup needed for, 83
loading the new version, 99–100
locating HyperTerminal, 84
login to HyperTerminal, 88–89
maintaining multiple versions, 221–222
management IP address entry, 89–90
naming the connection, 85
Port Settings phase, 86–88
Private LAN interface IP address entry, 90–91
proactive measures for, 588–591
reasons for new versions, 76, 83
retrieving software, 96–99
saving HyperTerminal settings, 93
software upgrades configuration screen, 96–100

upgrading Nortel VPN Router software *(continued)*
starting HyperTerminal, 84
starting Internet Explorer, 94
subnet mask for Private LAN interface, 91, 92
verifying the version installed, 101–102
VPN Router HyperTerminal Main Menu settings, 89–94
upgrading Regional Office to VPN technology, 162–164
user authentication. *See* authentication
User Datagram Protocol. *See* UDP
User EXEC mode (CLI)
`clear` command, 621–622
`enable` command, 631
established via Telnet, 615
`exit` command, 620
file system commands, 616–619
`help` command, 616
IP connectivity commands, 620–621
listing commands available, 91–92, 615–616
listing subcommands available, 192
overview, 189, 615
`reset` command, 620
`show` commands, 622–631
`terminal` command, 619
`verify` command, 619
`who` command, 619
user ID. *See* username or user ID
User/Client Tunnels
configuring for administrator, 505–511
connection types for, 141
with IPSec, support for, 405
overview, 141
PC-based, 142–145
with PPTP, support for, 396
for VPN-enabled device acting in Client mode, 145–147
username or user ID. *See also* authentication
administrator, changing via serial interface, 186–187
for BBI or VPN Router GUI, default, 96
for Console Interface, 614
for HyperTerminal login, 88
for VPN Client authentication, 126
users, configuring, 471–473

V

VDOLive, stateful inspection for, 278
`verify` command, 619
verifying
current services, 629–630
firewall configuration, 306
routing table routes, 640
server code integrity, 619
VPN Router version installed, 101–102
Version field
in enhanced GRE packet header, 394
in GRE packet header, 38
in IP packet header, 13
in L2F packet header, 35, 389
in L2TP packet header, 37, 400
in OSPF packet header, 15
in RIP packet header, 14
in VRRP packet header, 16
View admin level, 204
virtual interfaces, 279
Virtual Private Network Consortium (VPNC) certification support, 77
Virtual Private Networks. *See* VPNs
Virtual Router ID (VRID) field (VRRP packet header), 16
Virtual Router Redundancy Protocol. *See* VRRP
viruses, defined, 29
VLANs (Virtual Local Area Networks)
broadcast domain split up by, 353
MAC address-based, 354
packet switching between, 353–354
port-based, 354
protocol-based, 355
routing the first packet between, 353–354
subnet-based, 355
support for 802.1Q, 78, 82
types supported, 354–355

V.90 (V.Last) modems
VPN Router comparison chart, 69–70
VPN Router option for, 45
VoIP (Voice over IP)
Central Office example, 411–412
for corporate telephone services, 148
cost-effectiveness of, 412
DiffServ used by, 412
hairpinning, 332–334
implementation challenges, 413
IP-enabled telephone handset for, 148
NAT with, 326–327, 331
overview, 410–413
QoS for, 412, 413
soft telephone for, 148
with SOHO installations, 148, 151
VPN client software. *See* Nortel VPN Client
VPN Router GUI. *See* BBI
VPN Router HyperTerminal Main Menu
option 0 (Management Address), 89–91
option 1 (Interfaces), 91–93
option E (Exit, Save and Invoke Changes), 93
saving settings, 93
VPN Router software. *See* Nortel VPN Router software
VPN Routers. *See* Nortel VPN Routers; *specific models*
VPN tunneling. *See* tunneling
VPNC (Virtual Private Network Consortium) certification support, 77
VPN-enabled router in Client mode
ABOTs and, 146–147
BOTs and, 145–146
VPNs (Virtual Private Networks). *See also* tunneling
benefits of, 1, 29–30, 164
BIS (Backup Interface Services), 173–177
Central Office configuration, 164–173
IP address with L2F, 388
network administration of VPN Routers, 180–184
overview, 133–135
placement in the network, 177–179
Regional Office configuration, 158–164
RFCs for, 669–670
rigorous encryption for, 134
secure, defined, 29
for small office or home office, 148–154
tunneling protocols and standards, 30–38
upgrading Regional Office to, 162–164
VRID (Virtual Router ID) field (VRRP packet header), 16
VRRP (Virtual Router Redundancy Protocol)
for internal user redundant Internet access, 173
link failover, 382
overview, 16, 381–382
packet header contents, 16, 17
RFCs for, 680
support for, 78
V.35 serial interface, 44

W

W (warning message) severity code (Event log), 445
WANs (wide area networks)
for backing up the primary interface, 174
cards built-in to VPN Routers, 162–163
cost-effectiveness compared to VPNs, 1
illustrated, 8
overview, 8
protocols and standards supported, 79
resetting ports, 620
Web resources. *See* Internet resources
Web-based management. *See* BBI
`who` command
`kill` command with, 656–657
User EXEC mode (CLI), 619
wide area networks. *See* WANs
Windows operating systems (Microsoft)
IPSec VPN Client support for, 142
Stateful Firewall Manager support for, 284
VPN Client support for, 106, 426

Windows service login option, 111, 119
Windump packet sniffer, 543
WINS (Windows Internet Naming Service), 168, 169, 170
WS_FTP FTP client, 553

X

X.500 directory service standard, 230
X.509 Digital Certificates
  CA and, 254
  MS CAPI for retrieval, 253
  support for, 78
X.21 serial interface, 44