



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	185
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