Version 8.00

Part No. NN46110-500 02.01
311642-M Rev 01
13 October 2008
Document status: Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Configuration — Basic Features

NORTEL

Copyright © 2007 Nortel Networks. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel, Nortel Networks, the Nortel Networks logo, and Nortel VPN Router are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Java is a trademark of Sun Microsystems.

Microsoft, Windows, Windows NT, and MS-DOS are trademarks of Microsoft Corporation.

NETVIEW is a trademark of International Business Machines Corp (IBM).

OPENView is a trademark of Hewlett-Packard Company.

SPECTRUM is a trademark of Cabletron Systems, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface 11

Before you begin 11
Text conventions 11
Related publications 14
Printed technical manuals 16
How to get Help 16
Finding the latest updates on the Nortel Web site 16
Getting help from the Nortel Web site 16
Getting help over the phone from a Nortel Solutions Center 17
Getting help from a specialist by using an Express Routing Code 17
Getting help through a Nortel distributor or reseller 17

New in this release. 19

Features 19
Custom security banner 19
Branch Office NAT traversal 19
SFTP Server 19
Enhanced management restriction 20
NTP 20

Chapter 1
Overview 21

VPN fundamentals 21
Nortel VPN Router overview 22
Licensing features 24
Command line interface 24
FIPS overview 24

Chapter 2
Basic configuration 25

Prerequisites 25
Basic configuration fundamentals 27
IP address assignments 27
IPX support 29
Management virtual address 29
Multinetting 32
Basic configuration 35
Configuring the interfaces 35
Managing through a Web browser 37
Configuring and applying access lists 39
Configuring the custom banner text 40
Restarting the Nortel VPN Router 41

Chapter 3
Basic configuration—Nortel VPN Router 1010, 1050, and 1100 43

Default configuration 43
BOQS fundamentals 45
Enterprise environment configuration 45
Service provider environment configuration 46
Deployment procedure outline 48
Configuring Nortel VPN Router 1010, 1050, and 1000 48
Prerequisites 49
Obtaining IP addresses 49
Accessing the BOQS 50
Accessing BOQS—DHCP 50
Accessing BOQS—PPPoE 50
Accessing BOQS—Static IP 51
Configuring routing 52
Creating branch office tunnels 54
Compact flash disk 55

Chapter 4
Configuring user tunnels 57

User tunnel configuration overview 57
Tunnel groups 58
Security precautions 59
Split tunneling 59
Filters 59
Authentication 60
Password management 60
Configuring group parameters 61
User tunnel configuration 64
Configuring tunnel access 65
Configuring tunneling protocols 65
Adding user groups 65
Adding a user profile in a group 66
Configuring a user account 68
Configuring inverse split tunneling 68
Configuring inverse split tunneling by using the subnet wildcard 70
Configuring the subnet wildcard 70

Chapter 5
Configuring the system. 71

Configuring the system identity 71
LAN interfaces configuration 73
Configuring the LAN interface 75
Configuring Multinetting 77
Enabling asynchronous data over TCP 80
Configuring NTP 80
Configuring system settings 82
Configuring proxy ARP 86
Configuring the SSH server 87
SSH server configuration 87
Enabling the SSH server 87
Configuring the SSH server 88
SFTP configuration 88

SFTP considerations 89
Configuring SFTP 89
Restricted product-export license requirement 90

Chapter 6
Configuring branch office tunnels 91

Branch office tunnel fundamentals 91
PPTP nested tunnels 95
Nested tunnels from within the private network 95
Nested tunnels from the public network 95
DNS for branch office tunnel endpoints 95
VPN DNS 96
Round Robin DNS 97
Configuring a branch office tunnel 99
Adding a group 100
Adding a tunnel 100
Configuring a tunnel connection 101
BOT NAT-T configuration 103
Enabling IPSec NAT-T globally 104
Modifying the NAT keepalive interval 104

Chapter 7
Configuring control tunnels 105

Control tunnel fundamentals 105
Control tunnel types 106
Branch office control tunnels 107
User control tunnel 107
Restricted mode 108
Configuring nailed-up control tunnels 108
Control tunnel configuration 109
Adding a group 109
Adding a control tunnel 110
Configuring a control tunnel connection 111

Chapter 8
Configuring IPSec mobility and persistent mode 115

IPSec mobility fundamentals 115
IPSec mobility on Nortel VPN Router 117
Performance factors of roaming 117
Status and Logging for clients and servers 118
IPSec mobility and NAT 118
Roaming from behind NAT to behind NAT 118
Roaming from behind NAT to no NAT 119
Roaming from no NAT to behind NAT 119
IPSec mobility in NAT environment 120
Routing table changes 120
ICP overview 121
Maximum roaming time 122
Persistent tunneling fundamentals 123
Session persistence time 123
Configuring IPSec mobility and persistence 124
Configuring IPSec mobility 124

Appendix A
Configuration checklist and BOQS template 127

Configuration checklist 127
BOQS template 130
Index 135

Preface

This guide introduces the Nortel VPN Router. It also provides overview and basic configuration information to help you initially set up the Nortel VPN Router.

Before you begin

This guide is for network managers who are responsible for the set up and configuration of the Nortel VPN Router. This guide is based on the assumption that you have experience with windowing systems or graphical user interfaces (GUIs) and are familiar with network management.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicates that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. Example: If the command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off** | **on**}.

braces ({ })	Indicates required elements in syntax descriptions where more than one option exists. You must choose only one option. Do not type the braces when you enter the command. Example: If the command syntax is **`ldap-server source {external | internal}`**, you must enter either **`ldap-server source external`** or **`ldap-server source internal`**, but not both.
brackets ([ ])	Indicates optional elements in syntax descriptions. Do not type the brackets when you enter the command. Example: If the command syntax is **`show ntp [associations]`**, you can enter either **`show ntp`** or **`show ntp associations`**. Example: If the command syntax is **`default rsvp`** [**`token-bucket`** {**`depth`** | **`rate`**}], you can enter **`default rsvp`**, **`default rsvp token-bucket depth`**, or **`default rsvp token-bucket rate`**.
ellipsis points (. . .)	Indicates that you repeat the last element of the command as needed. Example: If the command syntax is **`more disk`***`n`***`:`***`<directory>`***`/...`***`<file_name>`***, you enter **`more`** and the fully qualified name of the file.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, an underscore connects the words. Example: If the command syntax is **`ping`** *`<ip_address>`*, *`ip_address`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`

separator (>)	Shows menu paths. Example: Choose Status > Health Check.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. Example: If the command syntax is **`terminal paging`** {**`off`** | **`on`**}, you enter either **`terminal paging off`** or **`terminal paging on`**, but not both.

Related publications

For more information about the Nortel VPN Router, see the following publications:

- Release notes provide the most recent information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Nortel VPN Router Configuration—Client* (NN46110-306) provides information to install and configure client software for the Nortel VPN Router.
- *Nortel VPN Router Configuration—TunnelGuard* (NN46110-307) provides information to configure and use the TunnelGuard feature.
- *Nortel VPN Router Upgrades—Server Software Release 8.0* (NN46110-407) provides information to upgrade the server software to the most recent release.
- *Nortel VPN Router Installation and Upgrade—Client Software Release 8.01* (NN46110-409) provides information to upgrade the Nortel VPN Client to the most recent release.
- *Nortel VPN Router Configuration—SSL VPN Services* (NN46110-501) provides instructions to configure services on the SSL VPN Module 1000, including authentication, networks, user groups, and portal links.
- *Nortel VPN Router Configuration—Advanced Features* (NN46110-502) provides configuration information for advanced features such as the Point-to-Point Protocol (PPP), Frame Relay, and interoperability with other vendors.
- *Nortel VPN Router Configuration—Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F).
- *Nortel VPN Router Configuration—Routing* (NN46110-504) provides instructions to configure the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), Equal Cost Multipath (ECMP), routing policy services, and client address redistribution (CAR).
- *Nortel VPN Router Using the Command Line Interface* (NN46110-507) provides syntax, descriptions, and examples for the commands that you can use from the command line interface (CLI).

- *Nortel VPN Router Configuration—Firewalls, Filters, NAT, and QoS* (NN46110-508) provides instructions to configure the Stateful Firewall and Nortel VPN Router interface and tunnel filters.
- *Nortel VPN Router Security—Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.
- *Nortel VPN Router Troubleshooting—Server* (NN46110-602) provides information about system administrator tasks such as recovery and instructions to monitor VPN Router status and performance. This document provides troubleshooting information and event log messages.
- *Nortel VPN Router Administration* (NN46110-603) provides information about system administrator tasks such as backups, file management, serial connections, initial passwords, and general network management functions.
- *Nortel VPN Router Troubleshooting—Client* (NN46110-700) provides information to troubleshoot installation and connectivity problems with the Nortel VPN Client.

New in this release

The following sections details what is new in *Nortel VPN Router Configuration — Basic Features* for release 8.0.

- "Custom security banner" on page 19
- "Branch Office NAT traversal" on page 19
- "SFTP Server" on page 19
- "Enhanced management restriction" on page 20
- "NTP" on page 20

Features

See the following sections for information about feature changes:

Custom security banner

The Nortel VPN Router supports a custom banner message that appears prior to a user attempt to log on the Nortel VPN Router. For more information about the custom security banner, see "Configuring the custom banner text" on page 40.

Branch Office NAT traversal

Nortel VPN Router release 8.0 supports Branch Office NAT traversal. NAT traversal (NAT-T) solves connection problems in private TCP/IP networks that use NAT devices. For more information about NAT-T, see "Modifying the NAT keepalive interval" on page 104.

SFTP Server

Nortel VPN Router release 8.0 supports Secure Shell File Transfer Protocol (SFTP). SFTP provides secure file transfer functionality over a reliable data stream. For more information about SFTP, see "SFTP configuration" on page 88.

Enhanced management restriction

In previous Nortel VPN Router releases, you can restrict management access to specific IP addresses for HTTP, FTP, and SNMP. Nortel VPN Router release 8.00 adds support for management restriction for HTTP and SSH. For more information about enhanced management restriction, see "Configuring and applying access lists" on page 39.

NTP

Nortel VPN Router release 8.0 supports Network Time Protocol (NTP) on all public and private interfaces. For more information about NTP, see "Configuring NTP" on page 80.

Chapter 1
Overview

This chapter introduces the Nortel VPN Router and includes the following sections:

- "VPN fundamentals" on page 21
- "Nortel VPN Router overview" on page 22
- "Licensing features" on page 24
- "Command line interface" on page 24
- "FIPS overview" on page 24

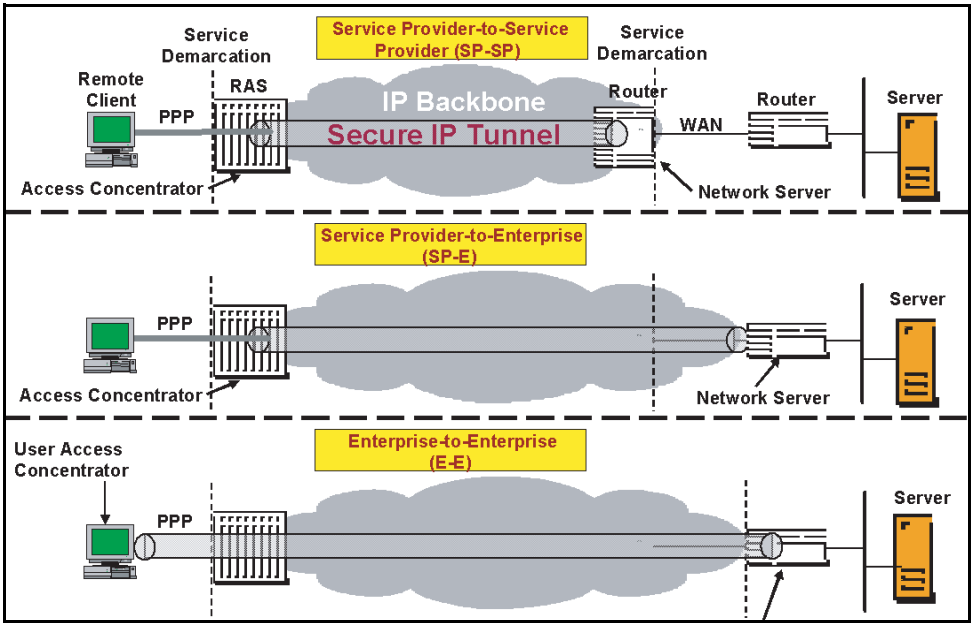
VPN fundamentals

A VPN is a private data communication channel that uses a public IP network as the basic transport for connecting corporate data centers, remote offices, mobile employees, telecommuters, customers, suppliers, and business partners. Physically discontiguous networks appear logically connected and contiguous.

A remote access VPN service requires a secure tunnel between client software on a remote device, such as a PC, and host software on a VPN router.

Figure 1 "VPN service models" on page 22 shows examples of VPN services.

Figure 1 VPN service models



The VPN router uses a combination of authorization, authentication, privacy, and access control for each user.

Nortel VPN Router overview

The Nortel VPN Router delivers security and IP services in a single integrated platform. With IP routing, Virtual Private Networking (VPN), stateful firewall, policy management, and Quality of Service (QoS) services, a single Nortel VPN Router device offers the IP services that normally require multiple purpose devices. Designed for enterprise networks, the Nortel VPN Router leverages the cost advantages of the Internet while providing secure communications across the public IP infrastructure.

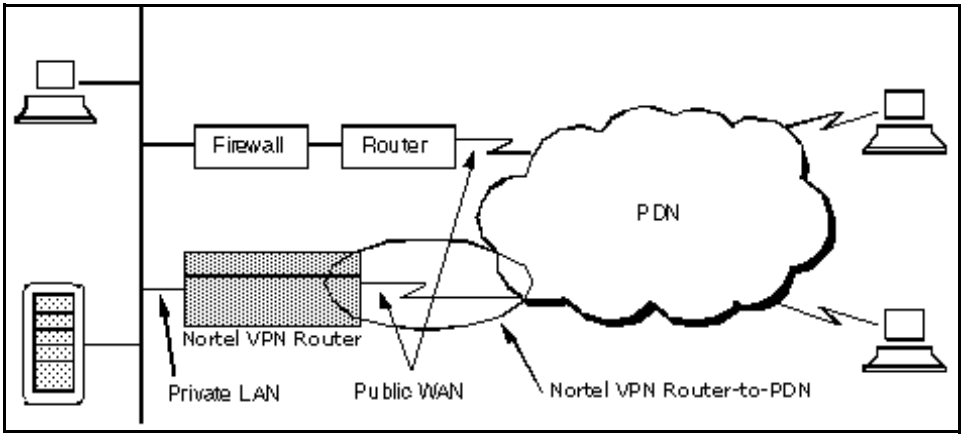
As a highly scalable device, the Nortel VPN Router addresses the security and IP services needs of the small branch site or large headquarter environment. A Nortel VPN Router acts as an IP access router or a stateful packet firewall.

The Nortel VPN Router incorporates Nortel Secure Routing Technology (SRT). SRT is a software framework that provides a security structure through all Nortel VPN Router operational components, including IP routing, VPN, firewall, and policy services. SRT ensures management consistency and scalable performance even if you run multiple IP services on the same device. SRT also provides dynamic routing over secure IP security (IPsec) tunnels, uniform security policies across VPN, routing, and firewall services and a flexible software licensing scheme.

With secure, manageable, and scalable features, you can shift information technology resources from solving the current remote user access problems to more proactive administrative and management areas.

Remote users access the Nortel VPN Router through an Internet Service Provider (ISP) to reach corporate headquarters or branch offices. The Nortel VPN Router provides remote users access to corporate databases, mail servers, and file servers. Figure 2 "Typical PDN" on page 23 shows a typical packet data network (PDN).

Figure 2 Typical PDN



The Nortel VPN Router allows ISPs to take over the role of point-of-presence (POP) providers of modem access. It improves performance while lowering overhead, which translates to significant corporate savings.

Licensing features

You can obtain licence keys from Nortel customer support. The Nortel VPN Router provides several license key options:

- Advanced Routing
- Nortel VPN Router Stateful Firewall
- VPN Tunnels
- Premium
- DSLw
- BGP only

For more information about licensing, see *Nortel VPN Router Administration* (NN46110-603).

Command line interface

Using the command line interface (CLI), you can make configuration changes to the Nortel VPN Router through a Telnet connection. You can access the command line interface by initiating a Telnet session to the Nortel VPN Router management IP address. This guide provides procedures for how to configure the Nortel VPN Router by using the GUI. For information about the CLI, see *Nortel VPN Router Using the Command Line Interface*.

FIPS overview

To be Federal Information Processing Standard (FIPS) compliant, you must order, purchase, and implement a FIPS kit. The FIPS kit contains detailed documentation for how to set up, operate, and configure the Nortel VPN Router to be FIPS compliant. The FIPS kit also includes tamper-resistant labels for you to place on the hardware as instructed in the FIPS kit documentation.

Chapter 2
Basic configuration

This chapter describes methods for configuration and management of the Nortel VPN Router.

Note: For more information about the setup of Nortel VPN Router 1010, 1050 or 1100, see "Basic configuration—Nortel VPN Router 1010, 1050, and 1100" on page 43." These VPN Router models have unique set up and configuration considerations.

This chapter includes the following topics:

- "Prerequisites" on page 25
- "Basic configuration fundamentals" on page 27
- "Basic configuration" on page 35
- "Configuring the custom banner text" on page 40
- "Restarting the Nortel VPN Router" on page 41

Prerequisites

Complete the hardware installation before you start this chapter. For more information about hardware installation, including adding local area network (LAN) or wide area network (WAN) cards, see the *Getting Started* or the installation guide that was shipped with the Nortel VPN Router.

To prepare for configuration of the Nortel VPN Router, have the following items available:

- IP address distribution plan

Prepare a plan to distribute IP addresses to remote users when they request connections. For example, you can distribute IP addresses from a Dynamic Host Control Protocol (DHCP) server or an internal client address pool.

- authentication database

  If you are not using internal authentication in the LDAP database, ensure that you have either the external Lightweight Directory Access Protocol (LDAP) or the Remote Authentication Dial In User Service (RADIUS) server IP address and password or Shared Secret (password).

- tunneling protocol client application

  Prepare the remote users for the type of tunneling protocol they need to use. The Peer-to-Peer Tunneling Protocol (PPTP) client application is available on the Nortel CD for Windows 95, and it is bundled with Windows 98 and Windows NT. Nortel also provides the IP security (IPsec) client on the Nortel CD.

- complete physical and logical network topology

  Include the following component details in this network topology:

  — physical communication links such as cable length, grade, and approximation of the physical paths of the wiring, analog, fiber and Integrated Services Digital Network (ISDN) lines

  — Nortel VPN Router details and router types

  — servers, with computer names, static IP addresses, server roles, and domain memberships

  — location of devices such as printers, hubs, Nortel VPN Routers, modems, routers, bridges, proxy servers, and firewalls (intranet and Internet) on the network

  — Wide Area Network (WAN) communication links including analog, ISDN, and Asynchronous Transfer Mode (ATM)

    Include the available bandwidth, either an approximation or the actual measured capacity, between sites.

  — number of users, including mobile users, at each site

  — manufacturer, firmware version, throughput, and special configuration requirements for devices on the network

    Record static IP addresses you assigned to devices and briefly explain why they required static addresses.

— brief explanations with the network layout
— domain architecture including the existing domain hierarchy, names, and addressing scheme
— trust relationships including representations of transitive, and one- and two-way trust relationships
— mixed environments (HP-UX, AIX, Linux, Solaris, Windows NT and 2000, and Macintosh)
— all protocols within the network

Use the "Configuration checklist" on page 127 to record the information that you need to configure basic Nortel VPN Router parameters.

Basic configuration fundamentals

This section contains fundamental information about the basic Nortel VPN Router configuration.

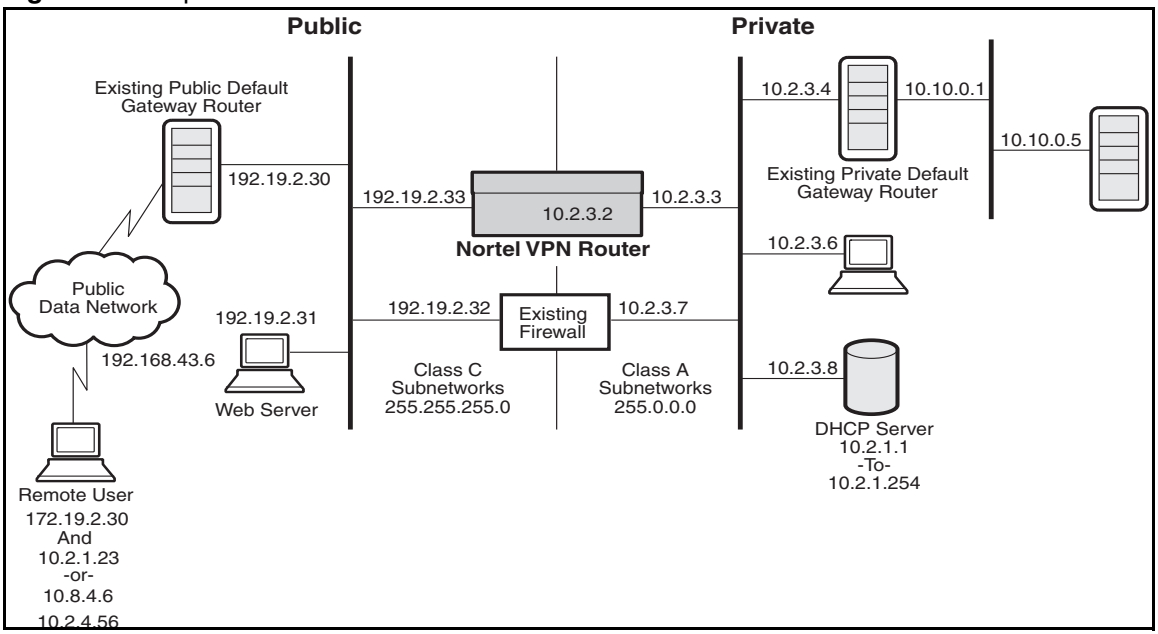
This section includes the following topics:

- "IP address assignments" on page 27
- "IPX support" on page 29
- "Management virtual address" on page 29
- "Multinetting" on page 32

IP address assignments

Figure 3 "Sample IP address associations" on page 28 shows sample IP address assignments in a network that uses a Nortel VPN Router.

Figure 3 Sample IP address associations



See table 1 "Sample IP addressing associations" on page 28 to view the IP address associations.

Table 1 Sample IP addressing associations

IP address	Description
192.168.43.6	Dial-up networking to the Internet Service Provider (ISP)
192.19.2.30	Public default Internet Nortel VPN Router
192.19.2.33	Public LAN port IP address (remote user destination address)
192.19.2.32	Firewall public network address
10.2.3.2	Nortel VPN Router management IP address
10.2.3.3	Nortel VPN Router private LAN interface IP address
10.2.3.4	Private network default Nortel VPN Router
10.2.3.6	Sample partners FTP server for inventory and price list
10.2.3.7	Firewall private network address
10.2.3.8	DHCP server IP address
10.2.1.1 to 10.2.1.254	Private Network Addresses Assigned to Remote Tunnel Sessions: DHCP pool

Table 1 Sample IP addressing associations (continued)

172.19.2.30	ISP-assigned address
10.2.1.23	DHCP-assigned IP address for a remote user
10.8.4.6	Sample remote user static IP address
10.2.4.56	Sample client-specified address

IPX support

The Nortel VPN Router supports the Internetwork Packet Exchange (IPX) protocol. To support IPX, the Nortel VPN Router encapsulates IPX traffic within IP tunnels over PPTP. The private interfaces and public interfaces can carry IP and IPX traffic simultaneously.

Note: PPTP supports IPX traffic only for remote access connections. IPX is not supported in branch office tunnels.

Management virtual address

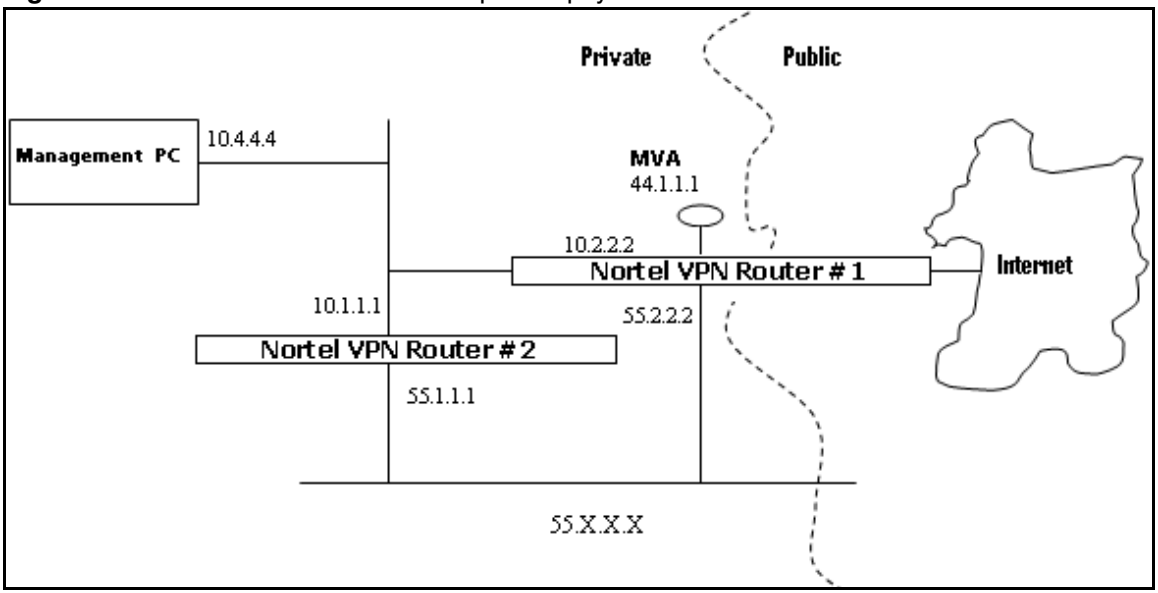
The management virtual address (MVA) is a unique circuitless IP (CLIP) address reserved for management. Use a CLIP address as an MVA to ensure that the Nortel VPN Router does not depend on a physical interface, thus preventing a single point of failure. Access to the MVA is supported on a public interface through a VPN tunnel.

The following management protocols are available for MVA from the private side:

- HTTP
- Hypertext Transfer Protocol with Secure Sockets Layer (HTTPS)
- SNM)
- FTP
- Telnet
- Identification
- CR Retrieval
- Certificate Management Protocol (CMP)

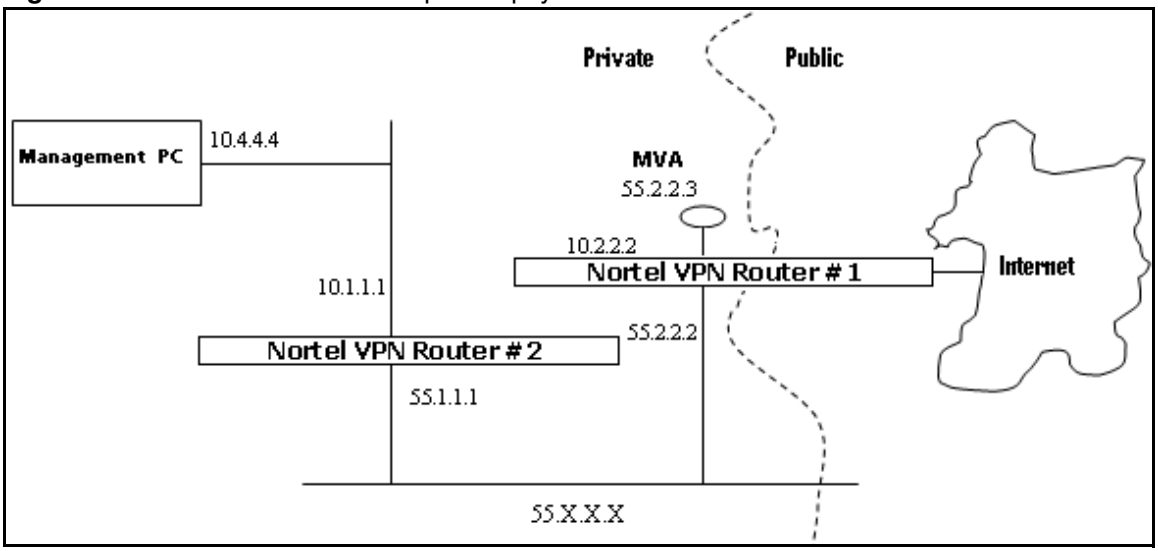
"MVA on different subnet from private physical interfaces" on page 30 shows MVA with the CLIP address on a different subnet from the private physical interfaces.

Figure 4 MVA on different subnet from private physical interfaces



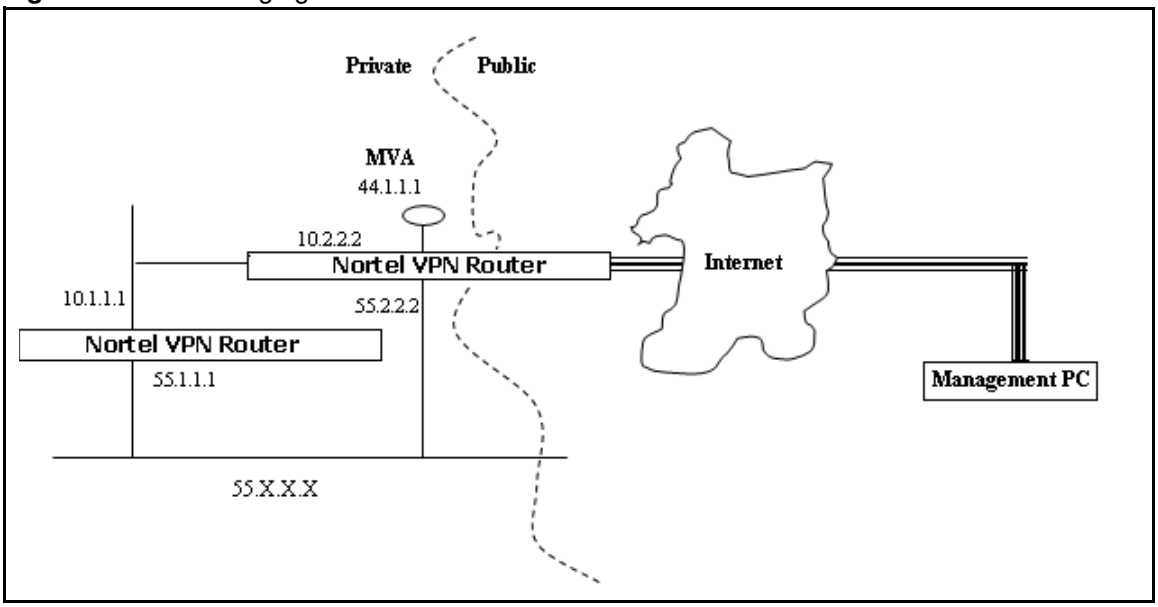
"MVA on same subnet as private physical interface" on page 31 shows MVA with the CLIP address on the same subnet as a private physical interface.

Figure 5 MVA on same subnet as private physical interface



"MVA managing the Nortel VPN Router from a remote PC" on page 32 shows how MVA uses CLIP to manage the Nortel VPN Router from a remote PC tunneled from the public side.

Figure 6 MVA managing the Nortel VPN Router from a remote PC



Multinetting

IP Multinetting is a strategy by which you can configure a maximum of eight addresses on a single Ethernet interface. The first IP address you configure on the interface is the primary address. Subsequent IP addresses are secondary addresses, which are referred to as subnets. All subnets on a physical interface share the security rules configuration of the primary subnet. You can configure only one set of interface filter rules for each physical interface.

Network administrators commonly use Multinetting in IP networks as part of a transition strategy. As networks evolve, consolidation of several physical networks is often necessary. You can consolidate the physical networks on a multinetted Nortel VPN Router interface. Multinetting migrates hosts to the new IP interface or maintains the previous IP address. You can add Multinet IP addresses to the private side or the public side of the Nortel VPN Router.

Note: Broadcast packets originated by the router must use the local subnet broadcast. After you create multiple RIP interfaces on one physical router interface, you must configure all interfaces with an explicit broadcast address of 255.255.255.255 to avoid routing loops.

You can perform statistics and log maintenance on a multinetted interface. In most cases, statistics and logs are not available separately for secondary addresses.

Overall throughput and forwarding performance has no significant degradation when you use multinetting instead of a nonmultinetting strategy.

"Services supported on a multinetted interface" on page 33 shows the services that a multinetted interface can support.

Table 2 Services supported on a multinetted interface

Service	Description
Nortel VPN Router Stateful Firewall	Supported at the interface level specified under the primary address on the interface. The same rules apply to secondary addresses on the interface.
Interface Packet Filters	Supported at the interface level specified under the primary address on the interface. The same rules apply to secondary addresses on the interface.
FW User Auth (FWUA)	Supported at the interface level specified under the primary address on the interface. The same rules apply to secondary addresses.
Network Address Translation (NAT)	Supported on multinetted addresses, with a single set of rules for all interfaces in Nortel VPN Router. NAT services are discretely available for each subnet on a multinetted interface.
Diff Serv	Supported at the interface level specified under the Primary address on the interface. The same rules apply to all other secondary addresses on the interface. The Diff Serv service includes call admission and priority, forwarding priority, and bandwidth management rate limiting on tunnel traffic.
Multinetting with Virtual LAN (VLAN) tagging	Support for multinetting on a tagged interface.
Tunneling	Support for Tunnel termination and origination separately on multinet addresses.
Authentication Protocols (RADIUS)	Supported at the interface level specified under the primary address on the interface. The same rules apply to secondary addresses on the interface.
VRRP	Supported when the primary address is the VRRP master or backup address. VRRP is not applicable on secondary addresses.
Other routing (RIP, OSPF, Static) protocols	Supported on secondary addresses. You can configure routing protocols on each secondary address.

Table 2 Services supported on a multinetted interface

Service	Description
DHCP server	Supported on secondary addresses. The internal DHCP server routes address requests to the subnet of the primary interface. The DHCP Relay function from a multinetted interface forwards the interface address as the primary address in relaying a DHCP request.
Management protocols (HTTP, HTTPS, SNMP, FTP, Telnet, Identification, CRL Retrieval, CMP)	Supported on the primary address on the interface. You cannot configure management protocols on secondary addresses.

The following Nortel VPN Routers support multinetting:

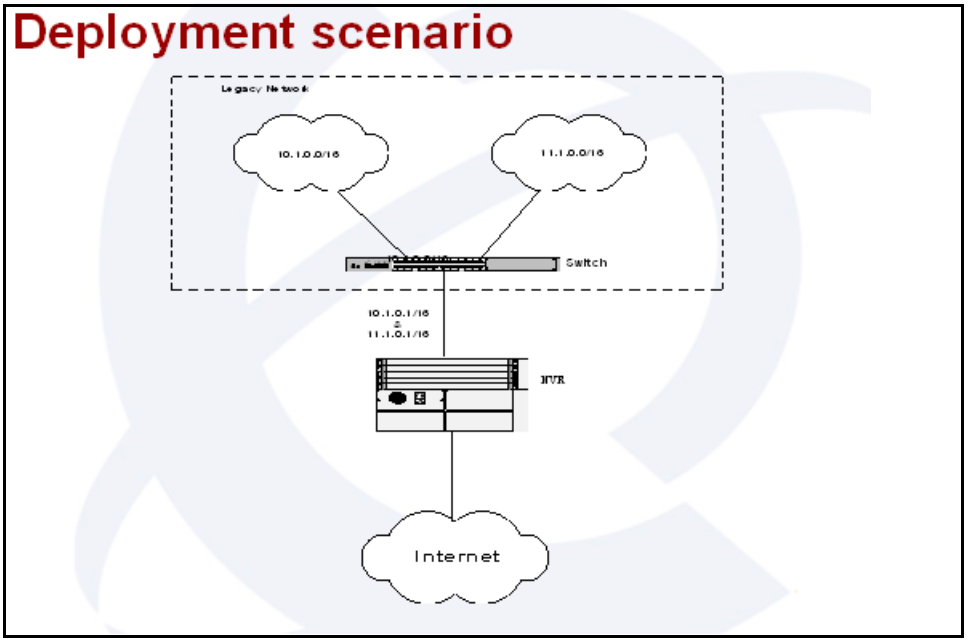
- Nortel VPN Router 1100, 1010, and 1050
- Nortel VPN Router 600
- Nortel VPN Router 1700
- Nortel VPN Router 1600 and 1500
- Nortel VPN Router 2700
- Nortel VPN Router 2600 and 2500
- Nortel VPN Router 4500 and 4600
- Nortel VPN Router 5000

The multinetting feature interoperates with the following products:

- Nortel VPN Router 100-400
- BayRS
- P8000 8100, 8600, and 1200
- Baystack LAN/Campus switches
- Cisco IOS routers.

"Deployment Scenario" on page 35 represents a legacy system that consists of two class B IP subnets: 10.1.0.0/16 and 11.1.0.0/16. Both subnets connect to one physical LAN port on Nortel VPN Router. Nortel VPN Router sends packets to and receives packets from a host on either network using the same physical port.

Figure 7 Deployment Scenario



Basic configuration

This section contains the procedures for how to initially configure the Nortel VPN Router.

To initially configure the Nortel VPN Router, perform the following procedures:

- "Configuring the interfaces" on page 35
- "Managing through a Web browser" on page 37
- "Configuring and applying access lists" on page 39

Configuring the interfaces

Configure MVA and the interfaces using a serial connection. Use the serial cable that is shipped with the Nortel VPN Router for connection from the switch to the PC.

You can then access the Serial Interface to configure the IP addresses and subnet mask so that you can then use a Web browser for Nortel VPN Router management. After the initial configuration, the Serial Interface configuration procedure is typically only necessary in a system recovery situation.

To configure the MVA and the interfaces, perform the following steps:

1. Connect the serial cable from the Nortel VPN Router serial port to a terminal or communications port of the PC.
2. Turn on the terminal or PC.
3. Open a terminal emulation program, such as HyperTerminal on the PC.

   The terminal emulator must have the following communications configuration:

   - 9600 baud
   - 8 data bits
   - 1 stop bit
   - no parity
   - no flow control
4. Press **Enter**.

   The Welcome window appears. You are prompted to supply a user name and password.

Note: The primary administrator user name and password guarantees access to the Nortel VPN Router through the serial port or a Web browser. This account has access to all windows and controls, including the serial port and recovery disk. Only one primary administrator can exist. The factory default user name is *admin* and the default password is *setup*.

---

5. Enter the default user name: **`admin`.**
6. Enter the default password: **`setup`.**

   The Main Menu appears.
7. Enter **0** to display the **Management IP Address** menu.

   The Management IP Address menu appears.

8 Enter **M** to change the Management IP address.

The current IP address appears. The Old Management IP Address field is blank on a new Nortel VPN Router.

9 Enter the Management IP address.

10 Press **Enter** to return to the **Interface** menu.

11 Enter **1** to display the configured interfaces.

12 Enter **0** to enter the Slot 0, Port 1.

13 Enter a new IP address for the interface, or press **Enter** to leave the current value.

The subnet mask menu appears.

14 Enter the desired subnet mask.

The Interface option menu appears.

15 Enter the desired option to configure the interface.

- Enter 1 for AutoNegotiation.
- Enter 2 for 100Mbs-FullDuplex.
- Enter 3 for 100Mbs-HalfDuplex.
- Enter 4 for 10Mbs-FullDuplex.
- Enter 5 for 10Mbs-HalfDuplex.

16 After you complete the configuration, press **Enter** to return to the **Interface** menu.

17 Enter **R** to return to the main menu.

18 Enter **E** to save the settings and exit.

You can now manage the Nortel VPN Router from a Web browser.

Managing through a Web browser

After you use the serial interface configuration, you can manage the Nortel VPN Router using a Web browser.

1 Launch a Web browser.

2 Enter the management IP address.

The Nortel VPN Router logon window appears. If you have not logged on before, the system prompts you to register the Nortel VPN Router to activate licenses, warranties, and services.

3 Select an option from the **Perform** list.

- Manage Router
- Guided Configuration
- Quick Start

"Web interface configuration modes" on page 38 shows the configuration modes in the Perform list. Begin with either the Quick Start or the Guided Configuration. After you are familiar with the navigational menu and capabilities, you can select Manage Switch when you log on to manage the Nortel VPN Router.

Table 3 Web interface configuration modes

Configuration type	Description
Quick Start	Configure interfaces, set up PPTP tunnels for up to three users, and establish a connection to the Nortel VPN Router. If you prepare for the configuration as recommended, the Quick Start takes approximately fifteen minutes to complete.
Guided Config	Configure and test a basic PPTP configuration. This option allows access to all configuration management facilities. The Guided Configuration guides you through the entire navigational menu from the Profiles to the Administration selections. Each functional area begins with a summary of the objectives of the area, and then guides you through the area, one subsection at a time. Context-sensitive help is available at each subsection to supplement the summary. Provided you have the information required to set up the Nortel VPN Router, the Guided Configuration takes two to three hours to complete, depending on how extensive is the configuration.
Manage Switch	Comprehensive and unguided Nortel VPN Router configuration and management.

4 Enter the system default logon and password in lowercase characters, as follows:

Login: **`admin`**
Password: **`setup`**

5 If you selected Quick Start or Guided Configuration, follow the prompts that guide you through the initial setup procedure.

Configuring and applying access lists

You can restrict the management access of source IP addresses with Access Lists (ACL). ACLs restrict connection of designated source IPs for management purposes over HTTP, HTTPS, FTP, TELNET, SSH, and SNMP.

The ACL intercepts management traffic and reads the packet to verify if the destination is System and is directed for one of the protocols. If so, the ACL verifies that the source IP address matches the ACL configured for the particular service. If no ACL is defined for HTTP, for example, HTTP traffic is permitted for IP addresses that act as a source address in the packet.

Whether the connection attempt is successful or not, the syslog logs the IP address of a source client.

To configure an ACL, perform the following steps:

1 Choose **Routing**, **Access List**.

2 Enter a unique access list name.

   Use a name or number to a maximum length of 64 characters.

3 Click **Create.**

   The Access List, Policy window appears.

4 Select an option from the **Action** list.

   - Permit
   - Deny
   - Permit all
   - Deny all

   If you select Permit or Deny, you must

   a Enter the subnet in the **Subnet** box.

   b Enter the mask in the **Mask** box.

   c Select an option from the **Mask Type** list: Exact or Range.

5 Click **Add**.

6 Click **Close**.

7 Select **Services, Available**.

The Allowed Services window appears.

8 For each management protocol, select an ACL from the **Access List** list.

9 Click **OK**.

Configuring the custom banner text

The Nortel VPN Router supports a custom banner message that appears prior to a user attempt to log on the Nortel VPN Router. The Nortel VPN Router stores the message in the banner.txt file in the /SYSTEM directory.

The banner message

- supports a plain text message; the Nortel VPN Router does not support special format capabilities
- appears across all management logon screens
- appears prior to or on the same screen that prompts for user name password
- supports up to 1000 characters including spaces
- appears on the serial (console) port logon
- appears after you log on to manage the system using Telnet, FTP, SFTP, HTTP, HTTPS, SSH, or SSL

To configure the custom banner message, perform the following steps:

1 Choose **Admin**, **Administrator**.

2 Enter a custom banner message in the **Authentication Banner** box.

3 Select the **Enable Authentication Banner** check box.

4 Select each check box for the protocols on which you want to enable the banner message.

5 Click **OK**.

Restarting the Nortel VPN Router

In certain circumstances, it can be necessary for you to reboot the Nortel VPN Router. You can reboot the Nortel VPN Router in two system modes: Safe mode or Normal mode. Each mode has a software image, configuration files, and an LDAP database.

Note: The Nortel VPN Router 1010, 1050, and 1100 do not implement Safe mode.

A system started in Safe mode can accept only secured management tunnel establishment. After you establish a secured management tunnel, the Nortel VPN Router allows Telnet, HTTP, and FTP traffic.

In Normal mode, the system operates with the normal software and configuration and transports both VPN traffic and management traffic.

To reboot the Nortel VPN Router, complete the following steps:

1. Connect the serial cable from the Nortel VPN Router serial port to a terminal or a communications port of the PC.
2. Power on the terminal or PC.
3. Open a terminal emulation program, such as HyperTerminal on the PC.
4. Press **Enter**.

   The Welcome window appears. You are prompted to supply a user name and password.

Note: The primary administrator user name and password guarantees access to the Nortel VPN Router through the serial port or a Web browser. This account has access to all windows and controls, including the serial port and recovery disk. Only one primary administrator can exist. The factory default user name is *admin* and the default password is *setup*.

5. Enter the default user name: **`admin`**.
6. Enter the default password: **`setup`**.

The Main Menu appears.

7 Select **B** to access the **System Boot** options.

8 Select **2** to access **System Reset** options.

9 Select an option to reset the system.

- **1** to reset the system to Normal mode
- **2** to reset the system to Safe mode

Chapter 3
Basic configuration—Nortel VPN Router 1010, 1050, and 1100

This chapter provides instructions for how to configure the Nortel VPN Router 1010, 1050, and 1100 at branch office sites.

This chapter contains the following sections:

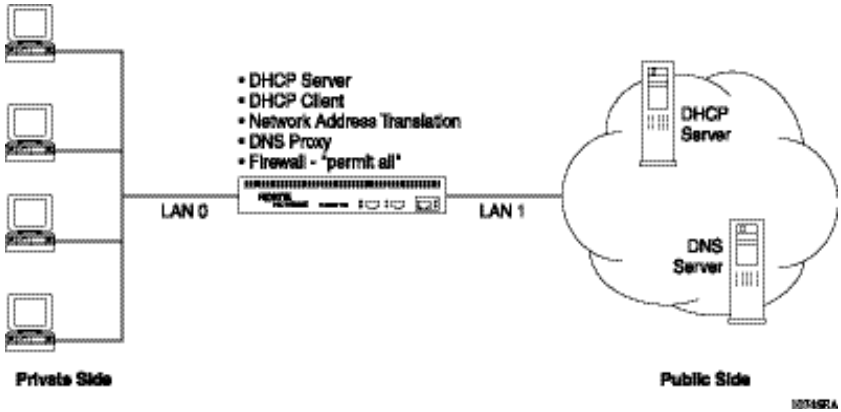
- "Default configuration" on page 43
- "BOQS fundamentals" on page 45
- "Enterprise environment configuration" on page 45
- "Service provider environment configuration" on page 46
- "Deployment procedure outline" on page 48
- "Configuring Nortel VPN Router 1010, 1050, and 1000" on page 48
- "Compact flash disk" on page 55

Default configuration

The default configuration of Nortel VPN Router 1010, 1050, and 1100 meets the requirements for small office connections. This configuration includes a public interface configured for IP and can receive an IP address from the Internet service provider (ISP) through Dynamic Host Configuration Protocol (DHCP). In the default configuration, DHCP is enabled on the private side of the Nortel VPN Router and the DHCP address pool is configured to 192.168.1.3–192.168.1.254.

"Default configuration" on page 44 show a typical default configuration.

Figure 8 Default configuration



The default configuration is as follows:

- On the private interface, the DHCP server has an address range of 192.168.1.3/24 to 192.168.1.255/24. The branch office switch uses 192.168.1.1 and 192.168.1.2 as the private and management interfaces. The DHCP server provides its address for the Domain Name System (DNS) server and default Nortel VPN Router.
- On the public interface, the DHCP client retrieves an IP address from the ISP DHCP server. The DHCP server includes parameters from the default Nortel VPN Router and the DNS server.
- The DNS proxy forwards DNS requests to an external DNS server. The DNS proxy obtains the address of the DNS server during the startup of the ISP DHCP.
- Network Address Translation (NAT) translates the private IP address into one public address that the ISP assigns to the public interface.
- Port NAT translates multiple IP addresses in the private IP address to a single public IP address. The default configuration supports only initiating IP sessions from the private side of the switch. The Port NAT reduces security risks.
- The Nortel VPN Router Interface Filter is the default firewall.
- The firewall setting PermitAll is the default setting for both the public and private interfaces.

BOQS fundamentals

Branch office quick start (BOQS) is a utility that allows you to access the Nortel VPN Router 1010, 1050, or 1100 to remotely configure the switches.

You can initiate BOQS only after you have planned the IP addressing and configured the central office switch. Then you can send provisioning parameters to the branch office locations.

The BOQS template provides a list of required values for BOQS. For more information, see "Configuration checklist and BOQS template" on page 127," for a copy of the template. You can enter the appropriate values in the right-hand column, and then fax, send, or e-mail the template to the local user along with other information that they need, such as who to contact for further information or questions.

Note: BOQS remains accessible after you configure the branch office networks. You must change the network administrator account username and password to restrict access.

After you provision the VPN services, branch office networks logically connect to a central office network or to a NOC network. You can reuse BOQS to restore the initial VPN configuration or to fix data errors.

BOQS supports two network topologies:

- Enterprise topology where the network operations center is located within the central office
- Service provider topology where the network operations center is an independent entity from the central office

Enterprise environment configuration

Before you deploy the Nortel VPN Router 1010, 1050, or 1100 switches at the local sites, you must configure routing and tunnels on the switch at the central office.

After the central office setup and the BOQS are complete, the Nortel VPN Router 1010, 1050, or 1100 is directly accessible from the central office. One hop exists between the central office and the branch office. RIP propagates routes to this subnet across the tunnel created by BOQS.

You must have two or more IP addresses than IP workstations on the Nortel VPN Router 1010, 1050, or 1100 private network. The first address from the subnet is assigned to the private interface of the branch office switch, and the second address becomes the management IP address of the switch. Each branch office must be in its own subnet.

"Subnet assignments" on page 46 shows how offices with approximately fifty workstations can each have subnets assigned.

Table 4 Subnet assignments

Private network IP address	Private network IP mask	Nortel VPN Router 1010, 1050 or 1100 private interface address	Nortel VPN Router 1010, 1050, or 1100 management interface address	Branch office workstations addresses (assigned by DHCP Server)
200.1.1.0	255.255.255.192	200.1.1.1	200.1.1.2	From 200.1.1.3 to 200.1.1.62
200.1.1.64	255.255.255.192	200.1.1.65	200.1.1.66	From 200.1.1.67 to 200.1.1.126
200.1.1.128	255.255.255.192	200.1.1.129	200.1.1.130	From 200.1.1.131 to 200.1.1.190

Service provider environment configuration

Service providers provide an isolated NOC from which they can manage all devices. The addressing scheme can be different from a central office and require a separate designated tunnel to configure the Nortel VPN Router 1010, 1050 and 1100 series of switches.

Each Nortel VPN Router 1010, 1050, and 1100 must have a distinct IP address that is visible from the NOC subnet. A NOC can assign addresses reachable from a NOC network to a Nortel VPN Router 1010, 1050, or 1100. BOQS configures NAT on the NOC tunnel to translate the addresses. If the address field is empty, the NOC must use a management address to access the Nortel VPN Router 1010, 1050, or 1100.

Because the NOC tunnel uses static routing, Nortel VPN Router 1010, 1050, and 1100 devices must have a static route to the NOC private network. BOQS enters the static route information in the NOC private address and NOC private mask fields.

You must provision the NOC switch to accept control tunnel connections from the branch office. Because static routing is used in control tunnels, you do not enable routing protocols on the NOC switch. Use the following guidelines to provision the NOC switch:

- Create all responder tunnels in one group or in subgroups for easy management.
- Configure the Connection Name of the tunnel to correspond to NOC tunnel name.
- Configure the local filter to Permit All.
- Select Text Pre-Shared Key as the IPSEC authentication method.
- Configure the Initiator ID to the value of Control Tunnel Name.
- Configure the Text Pre-Shared Key to be equal to Control Tunnel password.
- Select Static routing.
- Add accessible local networks. Include all networks from which the Nortel VPN Router 1010, 1050, or 1100 is managed.
- Do not use the NAT Local option.
- Configure Accessible Remote Networks to contain one address subnet (mask equal to 255.255.255.255) with the Nortel VPN Router 1010, 1050, or 1100 Management IP. Nortel VPN Router 1010, 1050, or 1100 Management IP is either explicitly provided in the Branch office switch manage NAT IP address or if this field is left empty, it is the second address from the subnet specified in the Branch Office Private IP Address and Mask fields.

Deployment procedure outline

The following sequence of events illustrates the deployment procedure.

1. Factory-configured Nortel VPN Router 1010, 1050, and 1100 boxes are shipped directly to the end customer.
2. The network operations center sends or faxes a provisioning worksheet separately from the device.
3. The end user unpacks and connects the Nortel VPN Router to the network using the readme file included with the Nortel VPN Router device.
4. The end user deploys the Nortel VPN Router between the Internet access device (cable or DSL modem) and the local network (Ethernet segment).
5. The end user restarts the PC to request a new IP address from the branch office DHCP server (not all operating systems require rebooting).
6. The end user opens a Web browser and types **`192.168.1.2`**, clicks **Manage Switch** and enters **`admin`** and **`setup`** as the username and password.
7. The BOQS displays a window to collect the IP and VPN configuration parameters. The end user enters the required parameters using the worksheet prepared by the NOC.
8. BOQS configures a tunnel from the branch office Nortel VPN Router to a Nortel VPN Router located at the central office and a management connection (responder control tunnel) to enable further configuration from the NOC.
9. The NOC takes over the switch configuration after the connection is Nortel VPN Router configuration—1010, 1050, and 1100.

Configuring Nortel VPN Router 1010, 1050, and 1000

This section provides information about how to configure the Nortel VPN Router 1010, 1050, and 1100 series of switches for basic Internet access through a cable or DSL modem. This set of instructions is also provided in the readme file that is shipped with the hardware.

Prerequisites

Before you connect the Nortel VPN Router 1010, 1050, or 1100, you must have the following:

- Complete the hardware installation before you start this chapter. For more information about hardware installation, see *Getting Started* or the installation guide that was shipped with the Nortel VPN Router.
- Internet connection—If the DSL or cable modem is not yet installed, contact the Internet service provider (ISP). The ISP needs the LAN 1 MAC address on the back of the Nortel VPN Router.
- Provisioning worksheet—The company or service provider that supplied the Nortel VPN Router sends this worksheet separately through e-mail or fax. The worksheet provides information that you enter into a quick-start tool to complete the configuration of the Nortel VPN Router

Note: If you did not receive the worksheet, call the ISP or the company that supplied the Nortel VPN Router 1010, 1050, or 1100. Do not connect the Nortel VPN Router until you have the worksheet.

Obtaining IP addresses

By default, the DHCP server is enabled on the private side of the Nortel VPN Router to assign IP addresses to the PCs that you connect to the LAN 0 ports.

1 Configure each PC to automatically an IP address.

Following are instructions for Windows 2000; for other operating systems, see the user documentation for the operating system.

a Choose **Start, Settings, Network and Dial-up Connections, Local Area Connections**.

b Click **Properties**.

c From the component list, select **Internet Protocol (TCP/IP)**.

d Click **Properties**.

e Select the **Obtain an IP address automatically** option.

f Click **OK**.

2 Reboot the PC to obtain a new IP address from the Nortel VPN Router.

Accessing the BOQS

Depending on the type of IP addressing the ISP uses, see the appropriate section:

- For DHCP, see "Accessing BOQS—DHCP" on page 50.
- For Point-to-Point Protocol over Ethernet (PPPoE), see "Accessing BOQS—PPPoE" on page 50.
- For static IP addressing, see "Accessing BOQS—Static IP" on page 51.

Note: If you complete the steps in the appropriate section and the Nortel VPN Router is not running, contact the service provider or company that provided the Nortel VPN Router.

Accessing BOQS—DHCP

If the ISP uses DHCP to assign an IP address to the PCs, verify that the Nortel VPN Router is connected to the Internet, and then start BOQS as follows:

1. Start the Web browser to verify connectivity to the Internet.

   By default, the LAN 1 port on the Nortel VPN Router acts as a DHCP client and receives an IP address from the public side.
2. Locate the provisioning worksheet sent by the company or provider that sent you the Nortel VPN Router.
3. Enter the following URL in the browser window: **`192.168.1.2/manage/qs.pyc`**.
4. Click **Manage Switch**.
5. Enter **`admin`** and **`setup`** as the user name and password.
6. Follow the instructions in the window that appears.

Accessing BOQS—PPPoE

If the ISP uses PPPoE to assign an IP address to the PCs, connect the Nortel VPN Router to the Internet, and then start BOQS as follows:

1. Open a Web browser.
2. Enter the following URL in the browser window: **`192.168.1.2`**.
3. Click **Manage Switch**.
4. Enter **`admin`** and **`setup`** as the user name and password.
5. Choose **System, LAN** to display the LAN Interfaces window.
6. Select **Cancel Acquisition**.
7. From the **Select Protocol** list, choose **PPPoE.**
8. Click **Apply**.

   The **Add PPPoE** Interface window appears.
9. Select **Enabled** from the **Administrative State** list.
10. Select **Permit all** from the **Interface Filter** list.
11. Click **OK**.
12. Locate the provisioning worksheet sent by the company or provider that sent you the Nortel VPN Router.
13. Enter the following URL in the browser window: **`192.168.1.2/manage/qs.pyc`**.
14. Click **Manage Switch**.
15. Enter **`admin`** and **`setup`** as the user name and password.
16. Follow the instructions in the window that appears.

Accessing BOQS—Static IP

If the ISP assigns static IP addresses to the PCs, connect the Nortel VPN Router to the Internet, and then start BOQS as follows:

1. Contact the ISP for the address to use.
2. Open a Web browser.
3. Enter the following URL in the browser window: **`192.168.1.2`**.
4. Click **Manage Switch**.
5. Enter **`admin`** and **`setup`** as the user name and password.
6. Choose **System, LAN** to display the LAN Interfaces window.

7 Select **Cancel Acquisition**.

8 From the **Select Protocol** list, select **IP.**

9 Click **Apply**.

The Add IP Address window appears.

10 Select the **Static** option.

11 Enter the IP address and subnet mask that the ISP provided.

12 From the **Interface Filter** list, select **permit all**.

13 Click **OK**.

14 Chose **Routing, Static Routes**.

15 Click **Add Public Route** under **Default Routes**.

The Add Public Default Route window appears.

16 In the **Gateway Address** field, type the default route address that the ISP provided.

17 Click **OK**.

18 Locate the provisioning worksheet sent by the company or provider that sent you the Nortel VPN Router.

19 Enter the following URL in the browser window: **`192.168.1.2/manage/qs.pyc`**.

20 Click **Manage Switch**.

21 Enter **admin** and **setup** as the user name and password.

22 Follow the instructions in the window that appears.

Configuring routing

To configure routing, complete the following steps:

1 Choose **Routing**, **RIP**.

2 Click **Enable**.

3 Enter the amount of time in seconds that you want RIP to update the routes.

The default is 30 seconds and the range of values is 5 to 65535 seconds. The hold-down timer is six times the update timer.

4. Select a metric value (1 through 4) for **Equal Cost MultiPath** for the maximum number of RIP paths.
5. Choose **Routing**, **Interfaces**.
6. Click **Configure** for the RIP protocol.

   The Routing Interfaces, Configure RIP window appears. The selected check box indicates that you globally selected RIP.
7. Select **V2, V1**, or **Off** as the transmit mode.

   Using the transmit mode, you can specify which version of RIP to use to route traffic from this Nortel VPN Router. The default is V2. Selecting OFF specifies that RIP is not used.
8. Select **V2**, **V1**, **Both**, or **Off** as the receive mode.

   Using the receive mode, you can specify which version of RIP accepts incoming traffic. The default is V2. Select OFF to specify that RIP is not used. Select Both specify that incoming transmissions using either version of RIP are accepted.
9. Select **None, Simple**, or **MD5** as the authentication type that is used as part of the RIP transmission.

   This authentication is specific to RIP and has no bearing on the authentication type as part of the connection to the Nortel VPN Router. The default is None, which specifies that no authentication is required. Simple indicates that authentication uses a simple password. MD5 specifies that authentication uses an MD5 secret. If you select either Simple or MD5, password and password confirmation boxes appear.
10. Enter a metric value for the **Cost**.

    The Cost value is the cost of sending a packet on the interface expressed in the link state metric.
11. Select **Enabled** or **Disabled** for poison reverse.

    Poison reverse updates routing loops in large networks.
12. If no default route is configured, you can select **Enabled** for **Import Default Route** to use the default route learned during RIP updates.

    Typically, you specify a default route in the route table on the Routing , Static Route**s** window. The default is disabled.

13 Select **Enabled** to specify that the default route is exported during RIP updates, or enter a metric value (1 through 15) to the default route.

14 Select **Enabled** to specify that static routes are exported during RIP updates, or enter a metric value (1 through 15) to the default route.

15 Select **Enabled** to specify that OSPF routes are exported during RIP updates, or enter a metric value (1 through 15) to the default route.

16 Select **Enabled** to specify that BGP routes are exported during RIP updates, or enter a metric value (1 through 15) to the default route.

17 Select a metric value (1 through 15) to export the static routes metric if you have a branch office connection.

   This metric informs the remote branch office connection of the routes that are used and provides the assigned metric value. The default is 1 and the maximum value is 15.

Creating branch office tunnels

Create one responder tunnel for each branch office Nortel VPN Router 1010, 1050, or 1100. To configure tunnels, complete the following steps:

1 Choose **Profiles**, **Branch Office**.

2 Click **Add**.

3 Enter a unique name in the **Group Name** box.

4 Select a parent group from the **Parent Group Name** list.

5 Click **OK**.

   The Branch Office window appears.

6 Click **Add** under **Connections**.

7 Enter a unique name in the **Connection Name** box.

   Nortel recommends that the name be the same as the initiator ID, but it can be the same as the central office tunnel name.

8 Select **Disabled** from the **Control Tunnel** list.

9 Select an option from the **Tunnel Type** list.

10 Select **Responder** from the **Connection Type** list.

11 Click **OK**.

You can configure routing on the branch office tunnels. For more information about routing protocol configuration on branch office tunnels, see *Nortel VPN Router Configuration—Routing* (NN46110-504).

Compact flash disk

Nortel VPN Routers 1010, 1050, and 1100 use a compact flash disk instead of a traditional hard disk that provides 64 MB of flash disk storage. Because of the limited storage capacity, the following functionality is not provided:

- safe mode
- java runtime plug-in
- graphs
- japanese strings
- context-sensitive help

The Help files are on the CD and on the Nortel documentation Web site.

Nortel VPN Router 1010, 1050, and 1100 uses file compression. Compressed files retain their original names and all existing directory operations that the software performs continue to work. The following functionality is compressed:

- VXworks image
- Web pages
- scripts
- text files

You can store two software images on the flash disk at the same time. Operational consideration for the compact flash disk are as follows:

- The configuration file automatically saves every minute and keeps the past three versions. The configuration file is only written when the configuration changes.
- On-disk system log (syslog) is not supported. However, you can configure an external syslog server.

- No accounting information is stored on the compact flash disk. However, an external RADIUS accounting server is supported.
- Data collection log (DCLOG) is not supported. The graphing capabilities of the GUI are also not supported.
- The compact flash disk does not store the core. The switch sends the core to an FTP server. The compact flash disk saves the configuration parameters for the FTP server. To configure the FTP coredump, go to the the Admin, Admintstrator window. Because you can configure multiple switches to coredump to the same location, the core files have a descriptive name: core_*date_24-hour-time_management_ip*.mem. For example, a core file generated by 10.0.8.186 on Oct.12th, 2001, at 4:46:06 PM is named core_20011012_164606_10.0.8.186.mem.

Chapter 4
Configuring user tunnels

Nortel VPN Router uses the Internet and tunneling protocols to create secure connections between two private networks. The following sections describe the Nortel VPN Router user tunnel configuration.

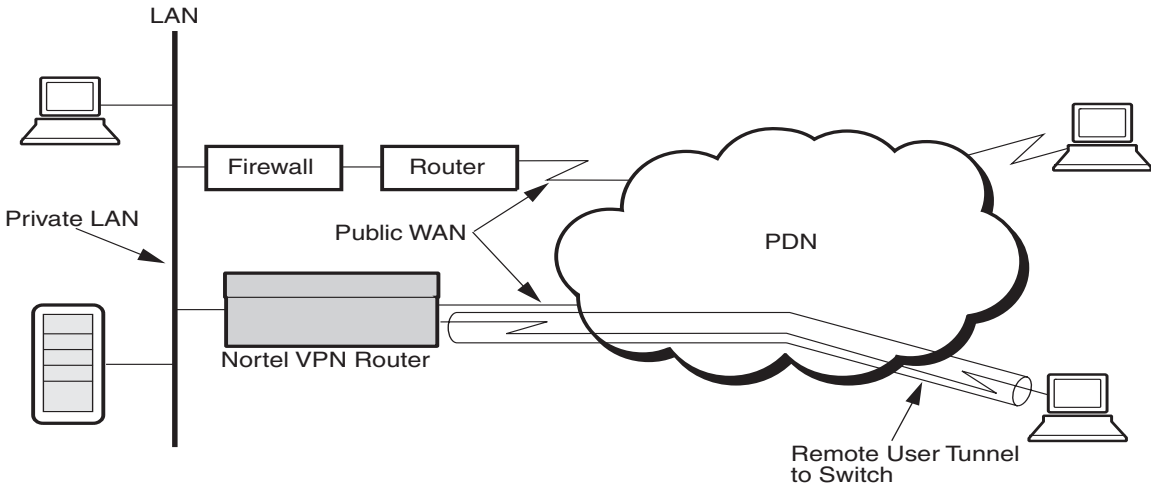
This chapter contains the following sections:

- "User tunnel configuration overview" on page 57
- "Tunnel groups" on page 58
- "Security precautions" on page 59
- "Configuring group parameters" on page 61
- "User tunnel configuration" on page 64

User tunnel configuration overview

The configuration process includes the authentication table and specific tunnel parameters, such as IPsec encryption, L2TP access concentrators, and L2F network access servers. "Tunnel connection configuration" on page 58 shows a typical network illustration with the Nortel VPN Router connected to the PDN (public data network) and to a remote user through a tunnel.

Figure 9 Tunnel connection configuration



Tunnel groups

Nortel VPN Router connection attributes allow the remote user to create a tunnel into Nortel VPN Router. However, you do not configure the connection from the remote user to the Internet Service Provider (ISP). The connection starts from a remote PC to the Internet through an ISP and ends at the Nortel VPN Router on the private, corporate network.

Nortel VPN Router associates remote users with a group, which dictates the attributes that are assigned to a remote user session. A group can consist of a single user, thereby creating a personal connection.

The Nortel VPN Router organizes groups in a hierarchical manner. At the top of the hierarchy is the base group. You add additional groups to the hierarchy as children of the base group. The base group \ contains the default characteristics that each child group inherits.

For example, \Base is the base group, Research and Development and Finance are child groups of the base group, and they are parent groups to groups below them.

A Lightweight Directory Access Protocol (LDAP) database stores users, groups, and their attributes. You can store this database internally on the Nortel VPN Router **hard disk** or externally on a network host running LDAP server software.

Security precautions

The following sections identify Nortel VPN Router security precautions for user tunnels:

- "Split tunneling" on page 59
- "Filters" on page 59
- "Authentication" on page 60
- "Password management" on page 60

Split tunneling

In split tunnel mode, Nortel VPN Router takes precautions against unauthorized user access to tunneled information. Nortel VPN Router drop packets that do not have the IP address that is assigned to the tunnel connection as its source address.

For example, you establish a PPP dial-up connection to the Internet with an IP address of 192.168.21.3. After you establish the tunneled connection to Nortel VPN Router, you assign a tunnel IP address of 192.192.192.192. Now, packets that attempt to pass through the tunnel connection with a source IP address of addresses other than 192.192.192.192 are dropped.

Filters

You can also enable Nortel VPN Router filters to limit the protocol types that can pass through a tunneled connection.

Note: User tunnels support PPP multilink, but branch office tunnels do not.

Authentication

The Nortel VPN Router checks the user ID and password against a database to authenticate each user that tries to connect to Nortel VPN Router. The Nortel VPN Router supports both LDAP and Remote Access Dial-In User Session (RADIUS) databases for authentication. If using LDAP for authentication, the LDAP server assigns the user to a group based on the user, group, and attribute information in the LDAP database.

If Nortel VPN Router authenticates a Point-to-Point Tunneling Protocol (PPTP) client against a RADIUS database, the RADIUS server can return the group for a user as a RADIUS class attribute.

If Nortel VPN Router authenticates an IPsec client, the Nortel VPN Router matches the remote user to the group ID. If the group ID and group password are correct, the Nortel VPN Router passes the user ID and password (or token card) to the RADIUS server for authentication.

For IPSec, you define a set of group attributes and give it a name. This group name is known as the Relative Distinguished Name and is added to the LDAP database.

Note: The group name Certificates (plural) is not a valid group name. If you change the name to Certificate (singular), the group is created properly.

Password management

The following are client-specific password management considerations:

- Password aging does not apply to administrator accounts.
- If you are using the IPsec client, you are warned three times about a pending password expiration. Change the password immediately. IPsec clients using versions earlier than 1.5.2 do not receive a password expiration warning.
- If you are using the PPTP client with the Connection Manager, the Connection Manager generates an impending password expiration warning.

- If you use L2TP, L2F, and PPTP without the Connection Manager, users have no warning of password expiration. In this case, the Nortel VPN Router cannot notify the client because it has no control over the client. The user must contact the
- administrator to remedy the situation. Nortel recommends you use the Connection Manager with PPTP. For L2TP or L2F, you can set the Password Maximum Age to zero (never expires).

Configuring group parameters

To configure group parameters, perform the following steps:

1. Choose **Profiles**, **Groups**.
2. Click **Edit** next to the group that you want to configure.
3. Under the **Connectivity** section, click **Configure**.
4. In the **Contact Information** field, enter the name of the administrator.
5. Select the time range from the **Access Hour** list.

   The Access Hour value specifies the time ranges during which access is allowed for users in a group. You can select New Hours Definition to customize the time ranges.
6. Select an option from the **Call Admission Priority** list.

   Options range from low to highest priority that you want to permit for the group. Each level is assigned a percentage of the total number of calls allowed access to Nortel VPN Router. If a high number of users log on, new users can be denied call access, based on their call admission priority, until existing callers disconnect.
7. Select an option from the **Forwarding Priority.**

   Option range from low to highest priority that you want to provide to user sessions in this group. Forwarding priority assures a certain level of latency and bandwidth allocation. For example, a group with the highest forwarding priority has the highest possible bandwidth service and the lowest level of latency. Conversely, if a high level of traffic traverses the line, packets for a

low-priority group can be delayed or dropped. Because a low-priority group has the least amount of bandwidth and the highest level of latency, some packets wait until the higher-priority-level packets have been forwarded to avoid dropping.

8 Enter a value in the **Number of Logins** box.

Enter the maximum number of simultaneous logons for IPsec clients. The Nortel VPN Router does not enforce the maximum number of logons across tunnel types. If you set the number of simultaneous logons to 1, a client can still access another tunnel type connection if the client is configured to use multiple tunnel types. To limit the number of connections a client can have, configure the user for a single tunnel type.

9 Select **Enabled** to enable the **Password Management** facilities.

10 Enter a value in the **Maximum Password Age** box.

The Maximum Password Age is the time after which the logon password expires. The Maximum Password Age range is from 0 (no password expiration) to 180 days (6 months). The default is 30 days.

11 Enter a value in the **Minimum Password Length** box.

The Minimum Password Length can be from 3 to 16 alphanumeric characters. If you configure the minimum length to eight characters, the remote user must use at least eight characters as the logon password. The default is 16 characters.

12 Select **Enabled** or **Disabled** from the **Alpha-Numeric Password Required** list.

Alphanumeric passwords force remote users to log on with a combination of alphabetic and numeric characters. Nortel recommends alphanumeric passwords as a security measure against hackers. The default is disabled.

13 Select **Enabled** or **Disabled** from the **Static Addresses** list.

14 Enter a value in the **Idle Timeout** box.

The Idle Timeout value specifies the amount of time before an idle connection drops. This option helps prevent resource allocation for sessions that are no longer active. The default Idle Timeout is 00:15:00 minutes; the range is 00:00:00 to 23:59:59. The maximum number of days is 29. A setting of 00:00:00 specifies no Idle Timeout. All sessions check the configuration at startup time. Therefore, the change only affects new sessions and not existing ones.

15 Enter a numeric value in the **Maximum number of failed login attempts to lock out an account** box.

16 Select an option from the **Access Network Name** list.

Users can tunnel into the Nortel VPN Router only if they tunnel from a source IP network defined by the access network. If they tunnel from a network outside the defined access network, the tunnel is refused. Use the Create New Network link to create an access network if one does not exist.

17 Select a value from the **Packets** list.

Packet filters control the type of access allowed for users in a group, based on various parameters, including Protocol ID, Direction, IP addresses, Source, Port, and TCP Connection establishment. Use the New Filter link to create tunnel filters if one does not exist.

18 Select **Enabled** or **Disabled** from the **IPX** list.

19 Select **Enabled** or **Disabled** from **IGMP** list.

20 Enter the maximum number of PPP links in **Maximum Number of Links** box.

The range is 1 to 5; the default is 1. The Multilink PPP (MP) implementation permits tunneling multilink connections from the ISP to Nortel VPN Router.

21 Select **Enabled** or **Disabled** from the **RSVP** list.

When RSVP is enabled, you can signal the network for required bandwidth. This option is disabled by default.

22 Enter a value in the **Token Bucket Depth** box.

The Token Bucket Depth influences packet flow delays within the Nortel VPN Router and participating routers in the Internet. The largest amount of data the Nortel VPN Router holds in its queue determines latency. New packets are delayed by a time that is proportional to the amount of traffic that is ahead of them in the queue, which is no greater than the Token Bucket Depth. If the queue exceeds the Token Bucket Depth, incoming packets are dropped. To guarantee reduced latency, the Bucket Depths must be small. Typically, you do not change this setting. The default is 3000 bytes.

23 Enter a value in the **Token Bucket Rate** box.

The Token Bucket Rate is the highest long-term average data rate (in Kbps) required over time for the connection. It informs the Nortel VPN Router and participating routers in the Internet how much bandwidth to reserve for the RSVP session. Typically, you do not change this setting. The default is 28 Kbps.

24 Select an address pool from the **Address Pool Name** list.

Remote users use the address pool to access Nortel VPN Router. The list shows all defined pools on the Nortel VPN Router. Select the New Address Pool link to define a new pool. The default is Default Pool.

25 In the **User Bandwidth Policy** section, you modify bandwidth parameters for this group.

a Select a **Committed Rate** from the list of available bandwidth rates. If the desired bandwidth rate is not listed, click **Define new bandwidth rate** to create a new one.

b Select an **Excess Rate** from the list.

c Select an **Excess Action** for traffic handling, either **Drop** or **Mark**.

You can optionally configure TunnelGuard settings. For more information about TunnelGuard, see *Nortel VPN Router* Configuration—TunnelGuard (NN46110-307).

User tunnel configuration

To configure user tunnels, you must first perform the following procedures:

- "Configuring tunnel access" on page 65
- "Configuring tunneling protocols" on page 65
- "Adding user groups" on page 65
- "Adding a user profile in a group" on page 66
- "Configuring a user account" on page 68
- "Configuring inverse split tunneling" on page 68
- "Configuring inverse split tunneling by using the subnet wildcard" on page 70

Configuring tunnel access

To configure tunnel access to the Nortel VPN Router, perform the following steps:

1. Choose **Services**, **Available.**
2. Select the tunnel type.
3. Select the **RADIUS** check boxes to permit RADIUS requests on the public and private interfaces of the Nortel VPN Router. If you enable RADIUS traffic, you must also enable RADIUS in the **Services**, **RADIUS** window.
4. Click **OK**.

Configuring tunneling protocols

All tunneling protocols are enabled on the public and private networks by default. Because the data in tunnels is encrypted, the default setting guarantees that all interactions with the Nortel VPN Router are private. To prevent tunnel connections of a particular type (for all users, including administrators, you can simply disable the tunnel type.

For example, if you want to use IPsec as the only public tunneling protocol, disable the Public selection for PPTP, L2TP, and L2F. By leaving IPsec, PPTP, L2TP, and L2F enabled on the private side, you can establish tunneled connections to the Nortel VPN Router using tunnel types from within the corporation.

Configuring the Nortel VPN Router tunneling protocol settings depends on the tunnel type. For more information about tunnel type configuration, see *Nortel VPN Router* Configuration—Tunneling *Protocols* (NN46110-503).

Adding user groups

To add a user group perform the following steps:

1. Choose **Profiles**, **Groups.**
2. Click **Add**.

3 In the **Group Name** box, enter a group name of up to 64 characters. Spaces are permitted.

4 Select a group from the **Parent Group** list.

For example, you can use Research and Development. The new group is a child of the selected parent group. Therefore, the new group initially inherits the parent group network access attributes, including authentication, tunnel types, filtering, and priorities. After you create a group, you can overwrite these inherited options for the new group.

5 Click **Apply.**

6 Click **OK.**

Adding a user profile in a group

To add a user profile in a group, perform the following steps:

1 Choose **Profiles**, **Users**.

2 From the **Group** list, select a group to which you want to add users.

3 Click **Display** to view the group members.

The last names and first names of the selected group users appear, sorted by last name.

4 Click **Add** to add a user to the group.

The **User Management, Add User** window appears. Only options enabled for the specified group appear on this window. Also, only options that you, as the administrator, have rights to appear.

Note: You can assign a user to two different groups, but only if the user has two different user IDs. You cannot enter the same user ID in two different groups. A user account can have up to four user IDs, depending on the group configuration, the account. If you are creating an enterprise user ID standard, try to avoid schemes that can potentially create conflicts as the company grows. For example, do not use the full first name and last initial of the user.

5 In the **Name** boxes, enter the first and last name of the user whose profile you want to add.

This user can have different IDs and passwords for each tunnel type. You can move the user to a another group by selecting a different group name.

Note: The GUI ignores leading and trailing spaces, but these must be specified if you then use CLI to edit the user name.

6 In the **Static IP Address** box beside **Remote User**, enter a remote user static IP address to use in place of a client-specified or DHCP server-assigned IP address.

This IP address is associated with the group Static IP address. If you enter an IP address instead of a DHCP server-assigned IP address, only one logon is allowed.

7 In the **Static Subnet Mask** box beside **Remote User**, enter the subnet mask.

The correct subnet mask to a remote IPsec client is important if you use split tunneling. If you enable split tunneling, packets destined to a host in the Split Tunnel Network list are directed into the tunnel by the IPsec client. All other traffic goes through a standard LAN or dial-up interface. This occurs on the client by adding the routes listed on the Split Tunnel Network list to the route table of the Microsoft TCP/IP stack and pointing those routes to the tunnel adapter interface. A route is also added to the route table based on the subnet mask assigned to the tunnel adapter. The IPsec Subnet Mask field allows you to specifically assign a subnet mask to a remote IPsec client that obtains an IP address either from the IP address pool, DHCP, RADIUS, or a static user configuration.

Note: If a host route for the destination address of the Nortel VPN Router exists in the TCP/IP route table prior to launching the Nortel VPN Client, the route is deleted if the tunnel is closed.

8 Enter a **User ID** and **password**.

The user ID has a maximum length of 256 characters. The user password has a maximum of 32 characters.

Configuring a user account

To search within a selected group, and then configure a user account perform the following steps:

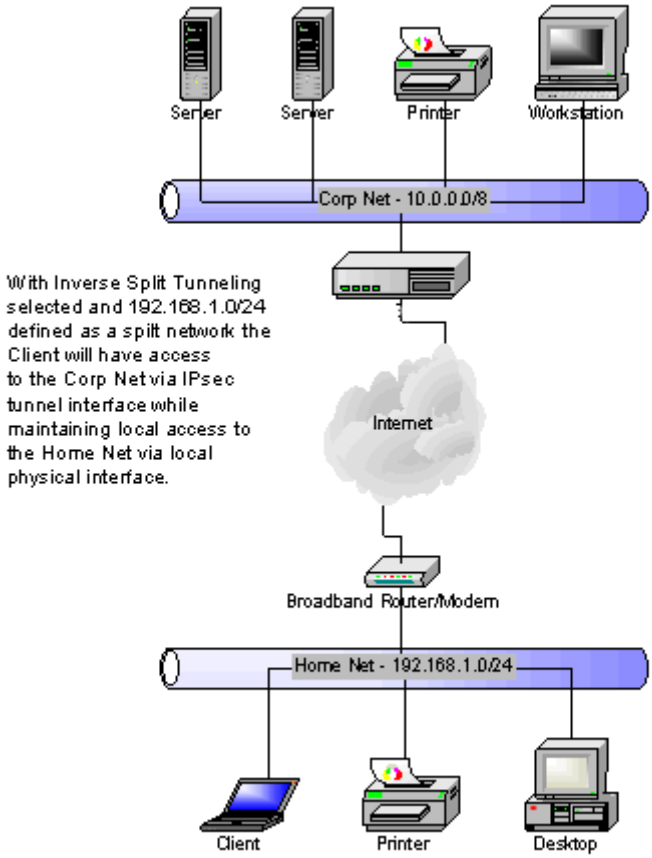
1. Choose **Profiles**, **Users**.
2. Select a group from which you want to search for a particular user from the **Group** list.
3. Click **Display**.

   The search is limited to the available groups.
4. Enter the appropriate text to search for in the **User Search** box.
   - **Last Name** searches for a last name. You must enter the entire last name.
   - **User ID** searches for a user ID.
   - **Admin Rights** searches for anyone who has View or Manage administrator privileges.
   - **LDAP** search allows you to enter an LDAP database attribute that is part of the person, organizational Person, or inetOrgPerson object database (for example, cn=common name or sn=surname) to generate the associated user profile. For more information, see the LDAP vendor documentation.
5. Select a search criteria option next to the **User Search** box.
6. Click **Search**.

Configuring inverse split tunneling

Inverse split tunneling, as show in "Inverse Split Tunneling" on page 69, allows remote users access to network resources outside of the mandatory tunnel, but maintains most of the security advantages of this tunnel type.

Figure 10 Inverse Split Tunneling



To configure inverse split tunneling, perform the following steps:

1. Choose **Profile**, **Groups**.
2. Click **Configure** under **IPSec**.
3. Select an option from the Split Tunneling list.
   - **Enabled – Inverse**
   - **Enabled – Inverse (locally connected**
   - **Disabled**
4. Click **OK**.

Configuring inverse split tunneling by using the subnet wildcard

You can configure the autodetection of directly connected local subnets by adding a subnet of 0.0.0.0 with a 0.0.0.0 mask to the inverse split tunnel networks list. If the Nortel VPN Client receives the list of inverse split networks, it expands the 0.0.0.0 to include the directly connected local subnets detected on the host. Additional subnets in a list are processed as before. The subnet 0.0.0.0/0 is simply a wildcard for expansion. After expansion, traffic destined for these subnets can flow outside the tunnel. This option is valid for both the Inverse Split and Inverse Split (Locally Connected) modes, but it most useful for the Inverse Split mode. The subnets 0.0.0.0/0 expansion generates always pass the Locally Connected test because they must be locally connected. Additional subnets listed are either duplicates of the wildcard expansion or not do pass the test.

Configuring the subnet wildcard

To configure the subnet wildcard perform the following steps:

1. Choose **Profiles, Groups.**
2. Click **Configure** under **IPSec**.
3. Select an option from the Split Tunneling list.
   - **Enabled – Inverse**
   - **Enabled – Inverse (locally connected)**
   - **Disabled**
4. Select **None** from the **Split Tunnel Networks** list.
5. Select a network from the **Inverse Split Tunnel Networks** list.
6. Click **OK.**

Persistent tunneling provides a continuous connection. After successfully establishing a tunnel session to the Nortel VPN Router, the Nortel VPN Client makes every attempt to maintain a viable VPN connection without additional user intervention.

For more information about IPSec mobility and persistence, see *Nortel VPN Router Configuration — Basic Features*.

Chapter 5
Configuring the system

This chapter contains information about how to configure system-level features and contains the following sections:

- "Configuring the system identity" on page 71
- "LAN interfaces configuration" on page 73
- "Configuring Multinetting" on page 77
- "Enabling asynchronous data over TCP" on page 80
- "Configuring NTP" on page 80
- "Configuring system settings" on page 82
- "Configuring proxy ARP" on page 86
- "Configuring the SSH server" on page 87
- "SFTP configuration" on page 88
- "Restricted product-export license requirement" on page 90

Configuring the system identity

Each Nortel VPN Router is uniquely identified by the system address and domain name system (DNS) name. You can use the DNS name instead of the IP address to identify the Nortel VPN Router and launch the management interface through a Web browser.

Use the System Identity window to change the Nortel VPN Router management IP address and provide the DNS host name and domain name. Additionally, you can assign up to three DNS addresses to resolve IP address name resolution requests. You can also reset the Nortel VPN Router Management IP address values using the serial interface.

To configure the System Identity, perform the following steps:

1 Choose **System**, **Identity**.

1 Enter an IP address in the **Management IP Address** box.

You need the management IP address to contact all system services, such as Hyptertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Network Management Protocol (SNMP). To be accessible, the management IP address must map to the same network as one of the private interfaces. For example, if you plan to assign IP address 10.2.3.3 with the subnet mask 255.255.0.0 to the private physical interface, the management IP address must reside in the 10.2.x.x network.

If you configure the Nortel VPN Router on one network but plan to move it to another network, change the management IP address and private LAN interface addresses before moving the Nortel VPN Router. Then, communicate with the Nortel VPN Router through the new management IP address.

2 Select the **MIB view as "software loopback"** box.

3 Enter a unique name in the the **DNS Host Name** box to identify the system.

Use the same name used by the DNS server to identify the management IP address of the Nortel VPN Router that is on the private network. You can enter up to 64 characters maximum.

4 Enter the name in the **DNS Domain Name** box.

Enter the name of the Internet domain into which you place the Nortel VPN Router. The DNS domain name must be the same Internet domain as the system name in the DNS server. A domain is a part of the Internet name hierarchy that refers to general groups of networks. The groups are distinguished by organization type or geography. For example, mycompany.com is the domain name for a commercial (.com) enterprise.

5 Select the **DNS Proxy** check box to enable the DNS Proxy to act as a DNS server to the private side. It it enabled by default.

6 Select the **Split DNS** check box if you have a split name space.

7 In the **Primary** box, enter the address of the DNS server that the DNS proxy tries to contact first.

8 In the **Second** box, enter an address for the second DNS server. If the primary DNS server do not respond in a few seconds, service is requested of the second DNS server.

9 In the **Third** box, enter an address for the third DNS server. If the Primary and Secondary DNS servers does not respond, service is requested of the third DNS server.

10 For **Fourth**, enter an address for the fourth DNS server. If the preceding servers do not respond, service is requested of the fourth DNS server.

11 Click **OK**.

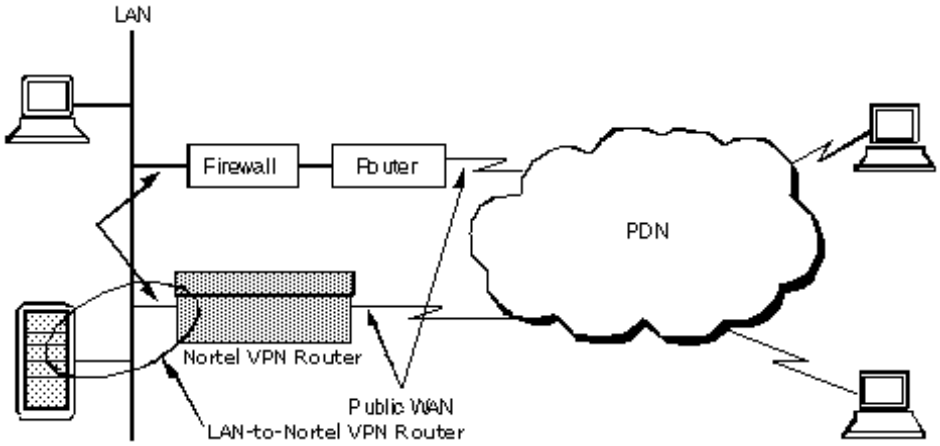
The Nortel VPN Router validates the DNS addresses and provides operational or error status reports.

LAN interfaces configuration

The Local Area Network (LAN) interface on the system board is configured as private by default. When you insert additional interfaces into the expansion slots, the interfaces are public by default. A public interface is an interface that is attached to a public data network such as the Internet.

"LAN-to-Nortel VPN Router connection" on page 73 shows a connection from a LAN to a Nortel VPN Router.

Figure 11 LAN-to-Nortel VPN Router connection



The Nortel VPN Router rejects nontunneled protocols and accepts tunneled protocols such as IP Security (IPSec), Peer-to-Peer Tunnelling Protocol (PPTP), Layer 2 Tunnelling Protocol (L2TP), Layer 2 Forwarding (L2F).

The Nortel VPN Router also accepts diagnostic ping on a public interface. A host can send only enough packets to a public interface to establish a tunnel connection. If the tunnel is not established before a preset maximum number-of-packets-allowed counter is reached, the packets from that host are discarded.

If the public interface is configured to act as a Dynamic Host Configuration Protocol (DHCP) client, the DHCP client needs to correspond to an external DHCP server to acquire the IP address, subnet mask, and default route parameters. You can set a cost value to give preferential routing if two or more public DHCP clients exist. In this situation, Digital Subscriber Line (DSL) and cable modem are the preferred choice for connections to the internet.

Private interfaces are attached to the private network and can accept nontunneled networking protocols such as Transfer Control Protocol/Internet Protocol (TCP/IP,) FTP, and HTTP. The Private interface also accepts tunneled protocols such as IPsec, PPTP, L2TP, and L2F, that you can use for secure management access to the Nortel VPN Router.

Note: The private LAN interface and the management IP address must be on the same network, and the public LAN interface must be on a different network, both physically and logically.

If you have one network only and want to position the Nortel VPN Router behind the firewall and router, use a private LAN interface. Do not use a public LAN interface.

From the System, LAN window, you can do the following:

- Add IP addresses.
- Modify the interface characteristics.
- View the link statistics.
- Select the tunneling protocol to use.

IP is the standard Internet Protocol, and Point to Point Protocol over Ethernet (PPPoE) allows PPP to run over Ethernet.

Note: You cannot use dynamic routing on PPPoE interfaces. DHCP is configured by default on the Nortel VPN Router 1010, 1050, and 1100. Therefore, you must first select Cancel Acquisition and then select PPPoE from the Select Protocol menu. You can use, PPPoE on only one interface at a time. IPX is not supported.

This window also provides the following information about the LAN interfaces:

- the current IP address that is assigned to the interface
- which bits of the IP address represent the network the device is on and which bits represent the host ID on the network

  The device uses the subnet mask to determine which IP addresses are directly reachable on the network and which IP addresses must be routed through a Nortel VPN Router. A sample IP address is 10.2.3.3 with a subnet mask of 255.255.0.0. This indicates that all hosts with addresses 10.2.*n.n* are directly reachable.
- state of the Nortel VPN Router Stateful Firewall on the LAN interface

  If no interface filter is configured, the default of Deny All applies. The Deny All and the Deny All (default filter) have the same effect. Deny All (default filter) means that no filter is configured so the default behavior applies, which is to deny all packets.
- whether the IP address is a primary or secondary address

Note: When the link is not active on the Ethernet port, the management window can take up to three minutes to return Ethernet parameters changes.

Configuring the LAN interface

To configure the LAN interface, perform the following steps:

1. Choose **System**, **LAN**.
2. Click **Configure** for the interface.

3 Under the **Configuration** section, select an option from the **Speed/Duplex** list.

Note: You can also use the Interface selection on the Nortel VPN Router Serial Port menu to set autonegotiation.

Select Auto-Negotiate to specify that the Nortel VPN Router automatically set the port speed and mode to match the best service provided by the connected station, up to 100 Mbps in full-duplex mode. Auto-Negotiate is the default selection, and complies with the IEEE 802.3u autonegotiating standard.

Select one of the following selections to manually set the LAN interface port speed and mode to match the speed and mode used by the connected station.

- 100Mbs/Full duplex
- 100Mbs/Half duplex
- 10Mbs/Full duplex
- 10Mbs/Half duplex

Note: You cannot connect to the remote system if the system is not using autonegotiation or if it uses an incompatible form of autonegotiation. If this occurs, manually set the Nortel VPN Router speed and mode settings to match those used by the remote system.

4 Select an option from the **SNMP If Speed** check boxes.

- **Display Ethernet Speed**
- **Display Specified Speed**

If you chose **Display Specified Speed**, enter the speed in the **bps** box.

5 You can provide an optional **Description** for the LAN interface. The description appears on the LAN Interfaces window.

6 Enter the **MTU** value.

The MTU sets the maximum size of a data packet transmitted from the interface. It does not affect the size of a packet accepted by the interface. Packets larger than the MTU are either fragmented or dropped. The Don’t Fragment (DF) bit in the IP header determines what action is taken.

7 Select the **MAC Pause (Frame-based flow control)** check box on the selected interface port.

MAC Pause enables the Nortel VPN Router to automatically adjust and control the flow of incoming and or outgoing packets from standard speed LAN devices.

8 Specify a value for **MAC Pause Ticks**.

9 Select a value from the **Free Receive FIFO Threshold** list. The default is 0.

10 Select **Enabled** or **Disabled** for the **802.1Q VLAN** setting.

Enabling 802.1Q VLAN requires that you set this option to Enabled, and then click OK. This takes you back to the System, LAN window.

11 Enter an identification number in the **VLAN ID** box in the range 1 to 4094, inclusive. The default value is 1.

12 Select **Accept Untagged** to accept Ingress inbound frames untagged or **Discard Untagged** to drop them.

13 Select **Tagged** to tag Egress frames. Untagged is default.

14 Click **Configure Subinterfaces** to configure and to view existing VLAN subinterfaces on the selected interface.

15 Click **Subinterface Statistics** to view current statistical information about the selected VLAN subinterface.

Configuring Multinetting

Multinetting requires a primary interface that must be present before you add secondary addresses. However, in a configuration in which both primary and secondary addresses are defined, you cannot change the primary address.

You must delete all secondary addresses before you change the primary address.

To add an IP address, perform the following steps:

1 Choose **System**, **LAN**.

2 Click **Add Multinet**.

The LAN Interfaces, Add IP Address window appears.

3 Enter an IP address in the **IP Address** box.

4 Enter a subnet mask in the **Subnet Mask** box.

5 Click **OK**.

To delete an IP address, perform the following steps:

1 Choose **System**, **LAN**.

2 Select the secondary IP address to delete.

3 Click **Delete**.

Note: You can delete a secondary subnet without effecting the remaining secondary subnets. To delete the primary subnet, remove all the secondary subnets.

To obtain an IP address, perform the following steps:

1 Choose **System**, **LAN**.

2 Click **Edit**.

3 Enter an IP address.

The IP address consists of 32 bits, which are written as four octets (8-bit bytes) in dotted-decimal format; for example 192.168.34.21.

The subnet mask defines how many bits of the IP address represent the network the device is on and how many bits represent the host ID on the network.

The device uses the subnet mask to determine which IP addresses are directly reachable on the network and which must be routed through a Nortel VPN Router. A sample IP address is 10.2.3.3 with a subnet mask of 255.255.0.0. This indicates that all hosts with addresses 10.2.*n.n* are directly reachable.

4 Click **Enabled** to enable **TCP MSS** (Maximum Segment Size) clamping.

5 Set the **TCP MSS** value in this field.

The MSS must be 40 bytes less than the largest packet the implementation can reassemble.

6 Select an option from the **Interface Filter** list.

The interface filter shows whether or not the Nortel VPN Router Firewall is in use.

Note: If you change the interface filter setting, a message informs you that you must restart the Nortel VPN Router before the new interface filter is used. If the Nortel VPN Router Firewall is not enabled, the new selection has no effect.

---

7 Use the **New Interface Filter** link to go to the **Profiles**, **Filters** window and create a new filter. The default Interface Filter setting is Deny All.

You can copy a tunnel filter for use as an interface filter. However, if you copy a filter, the operation does not copy components such as rules, ports, protocols, or addresses that have the same name as an existing component in the destination filter set. Use unique names for the device in all filter rules.

Enabling asynchronous data over TCP

Asynchronous data over TCP (AOT) is a protocol that enables transport of asynchronous data packets over a TCP/IP network. A TCP packet is decapsulated and the data is then forward to the synchronous driver to the asynchronous device or host.

The asynchronous protocol is used for communication of an alarm device with an alarm host on a slow speed serial line. Unlike synchronous transmission, asynchronous transmission does not use clocking signals to time the data transmission. Instead, asynchronous transmission uses start and stop bits to control the transmission. AOT is either a connection initiator or a listener, but it cannot be both. The selection of service is through AOT configuration. Only a single TCP connection is supported.

To enable asynchronous data over TCP/IP, perform the following steps:

1. Choose **Services, AoT**.
2. Check to enable asynchronous over TCP/IP communications. The default is disabled.
3. Select **Public** or **Private** for Service.
4. Click **Connection Originator**.
5. Specify the **Peer IP** address.
6. Specify the **Local IP** address.
7. Specify the **Port Number**, a value in the range 1000 to 9999.
8. Enter the maximum **Number of Ticks** for character idle time out, up to 60. The minimum idle time is a tick of the system clock and is 16.6milliseconds. The configuration allows selection of 1 to 60 ticks.

Configuring NTP

You can configure Network Time Protocol (NTP) on the Nortel VPN Router.

NTP synchronizes the clocks of various devices across networks. It automatically synchronizes the time (within milliseconds) of network devices. The Nortel VPN Router receives NTP updates from an NTP time server and continuously synchronizes its clock to universal standard time. The Nortel VPN Router supports up to eight NTP (unicast) servers and broadcast, multicast servers.

Note: If the Management IP address is higher than the LAN IP and the private network can access the NTP server, NTP operates properly, but the local address shows up as 0.0.0.0 on the Status, Statistics, NTP Stats window.

To configure NTP, perform the following steps:

1. Choose **System**, **Date** and **Time**.
2. Select the **Configure Network Protocol Time** link.
1. Select the **Enable** check box.
2. Perform one of the following steps:
   - If you want the Nortel VPN Router to respond to broadcast messages, select the **Synchronize time with NTP Broadcast Server** check box.
   - If you want the Nortel VPN Router to respond to multicast messages, select the **Synchronize time with NTP Multicast Server** check box. The IP multicast address is 224.0.1.1 for NTP.

     NTP listens for both broadcast and multicast messages at the group address of the global network. To avoid disruption in multicast mode, both the client and servers use authentication and the same trusted key and key identifier.
3. In the same window under **Servers**, click **Add** to add a server.
4. In the **Server IP Address** box, enter the IP address of the NTP unicast server.
5. Under **Interface**, select either **Private** or **Public**.
6. For the selection, select an IP address or **Dynamic** from the list.

   If you are using the Nortel VPN Router Firewall, you need to configure an interface filter to add NTP.
7. From the **Key ID** list, select a key ID option.

This specifies the Key ID for Message Digest (MD5) authentication. In authentication mode, each packet uses MD5 algorithms to transmits a 32-bit Key ID and a 64- or 128-bit cryptographic checksum. The peer receives and recomputes the checksum, and then compares the checksum with the one in the packet. The sender and receiver must share at least one MD5 key and must associate the MD5 key with the same Key ID.

8 From the **Bursting** list, select **Enable** to configure NTP to send a burst of eight packets at each poll interval.

9 From the **Version** list, select the NTP version number used on the NTP server. The default is 3.

10 Click **OK**.

11 Under **Trusted Keys**, click **Add** to add an area key ID.

The Add/Edit Trusted Key window appears.

12 Enter the key ID, the password and the password confirmation.

13 Click **OK**.

Configuring system settings

You can reboot the Nortel VPN Router in one of the two system modes: safe mode or normal mode. Each mode has its own software image, configuration files, and LDAP database.

A system booted in safe mode can only accept secured management tunnel establishment. After the secured management tunnel is established, Telnet, HTTP, and FTP traffic can transmit through the Nortel VPN Router; no other VPN traffic can transmit through the secured management tunnel or the Nortel VPN Router. In normal mode, the system operates with the normal software and configuration and transports both VPN traffic and management traffic.

To configure the system settings perform the following steps:

1 Choose **System, Settings**.

2 Select the **Enable** check box to enable **Safe Mode**.

3 Type in the number of minutes to determine how the long the system operates in Safe Mode before a reboot attempt in Normal Mode.

The parameters that you must set to allow the Nortel VPN Router to communicate through the serial port. After you change the Serial Port Configuration mode, you must restart the Nortel VPN Router for the change to take effect.

4 Select an option from the **Menu Access Leve**l list.

- **Unrestricted**-All commands are available to the user (default).
- **Restricted 1**-System Reset commands plus the commands to change interface IP address and mask.
- **Restricted 2**-Only Reset commands are available.

5 Select one of the following Modes of operation:

- **Serial Menu** (default)

  In this mode, a standard menu interface is presented. You can use an application such as Hyper Terminal, if you are directly connected to the Nortel VPN Router, to access the menu interface. The Nortel VPN Router uses the COM port for a serial menu terminal session. The Nortel VPN Router serial port baud rate is 9600 by default. If you change the serial interface baud rate, you must click Reset.

- **PPP**

  In this mode, you can configure the Nortel VPN Router to use the Point-to-Point Protocol (PPP) over the serial port. This feature allows you to manage the Nortel VPN Router from a remote location using PPP and the serial interface. If the Nortel VPN Router were to become unreachable over the Internet, you can still dial up and manage it through the serial interface menu.

- **Auto Detect**

  In this mode, you can access all management services (HTTP, Telnet, FTP, SNMP) through the Web interface. After a session is established through PPP, the serial interface acts as a private WAN interface with an internal IP address.

  Auto Detect automatically detects whether the Nortel VPN Router is using PPP or serial menu mode at startup. It cannot determine the Nortel VPN Router baud rate, nor can it determine a change from PPP to serial menu mode, except upon startup. Auto Detect checks the mode each time the Nortel VPN Router is restarted. To perform an Auto Detect check, the Nortel VPN Router sends out AT command set characters to configure a

modem if one is attached. If the Nortel VPN Router is in Auto Detect mode, and if a terminal session is connected and the terminal baud rate is the same as the Nortel VPN Router, the terminal displays the AT command sets on the window. Press Enter more than five times before a serial menu session is started.

- **AoT**

  In this mode, you can transport asynchronous data packets over a TCP/IP network.

6 Select one of the following baud rates to match the **Baud Rate** of the terminal:

- 57600
- 38400
- 19200
- 9600 (default)
- 4800 (4800 and lower applies only if AoT is selected)
- 2400
- 1200
- 600
- 300
- 150

Data, Parity, and Stop applies only if AoT is selected.

7 Enter the **Modem Initialization** string.

For more information about the vendor-specific character initialization string, see the manufacturer documentation. For the best results, preconfigure the modem, and use the Nortel VPN Router default initialization string (ATZ).

8 If you select the baud rate, you must click **Reset** to change the port to the new baud rate.

9 Select the **Log File Life Time** or **Log File Disk Limit** options.

The default log file life time is 60 days and the default log disk limit is 100 megabytes. Select a value for the log file life time from the list.

10 Select the **Write System Log To File** check box to enable saving log data to a file.

11 Select the **FTP server passive mode** check box.

If you do not select this check box, you can still use passive FTP connections to connect to the unit, but you cannot perform directory listings or upload and download files.

12 Enter the **data collection interval**.

The data collection interval specifies how the long the system waits before collecting new system data for logging. Enter the time in minutes.

Configuring proxy ARP

You can configure the Nortel VPN Router to respond to ARP requests on a physical interfaces. The Nortel VPN Router responds to the following types of routes:

- User tunnels are routes created for user tunnels. This entry is enabled by default and cannot be changed.
- Branch office tunnels are routes available through branch office connections. This option is disabled by default.
- Physical interfaces are routes available through physical interfaces. This option is disabled by default.

To configure proxy ARP, perform the following steps:

1. Choose **System**, **Forwarding**.
2. Click the appropriate check boxes under **Proxy ARP** to enable the different types of route types. All of these options are disabled by default for security reasons.
3. Click **Enable Gratuitous ARP** to send out a gratuitous ARP request on the private interface with the best matching subnet if a user tunnel is established.
4. Under **Tunnel to Tunnel Traffic**, select one of the following options:
   - **Allow End User to End User** to allow a remote user who is tunneled into the corporate Nortel VPN Router to access other remote users that are also tunneled into the Nortel VPN Router.
   - **Allow End User to Branch Office** to allow a remote user who is tunneled into the corporate Nortel VPN Router to access the resources of branch offices connected to the Nortel VPN Router.
   - **Allow Branch Office to Branch Office** to allow users who are on one branch office connected to the Nortel VPN Router to access resources on other branch offices that are connected to the Nortel VPN Router.
5. Click to enable **Apply Packet Filter on Private to Tunnel Traffic**.

Configuring the SSH server

You can enable an SSH server to allow secure CLI sessions, such as Telnet, to the Nortel VPN Router. You can also enable the private and public interface filters, set the port for the SSH server, and restart the server. SSHv1 clients are not supported on the SSH server.

SSH server configuration

Before using the SSH server, you must first enable it, and then set the parameters.

Enabling the SSH server

To enable the SSH server, perform the following steps:

1. Choose **Servers**, **SSH**.
2. To enable the SSH Server, select the **SSH Service Enabled** check box.

   From this window, you can also enable SFTP. For more information about SFPT, see "SFTP configuration" on page 88
3. Click **OK**.

Note: If an error occurs after you enable the SSH server, and then click OK, restart the server.

Configuring the SSH server

To set the parameters for the SSH server, perform the following steps:

1. Choose **Services, Available**.
2. In the **Port** box, enter the SSH server port number.

Note: If an SSL VPN card exists in the Nortel VPN Router, the port for the SSH server cannot be 22.

3. To enable filters, select either the **Public** or the **Private** check box.
4. Click **OK**.

SFTP configuration

The SSH File Transfer Protocol (SFTP) provides secure file transfer functionality over a reliable data stream. SFTP is the standard file transfer protocol for use with the SSH2 protocol. SFTP uses SSH to provide authentication and security; therefore, you interact with SFTP the same way as you interact with FTP.

The difference between SFTP and FTP is that SFTP is secure, whereas FTP is not. During a FTP session, the username and password are transmitted in clear text. If someone is eavesdropping, it is not difficult for them to log the FTP user name and password.

If you access the Nortel VPN Router using an SFTP client, you can perform the same tasks as you do with an FTP client such as

- change a directory
- delete a directory
- list directory contents
- get files
- put files
- delete files

SFTP considerations

Before you enable SFTP, consider the following:

- When enabled, SFTP runs on all available interfaces.
- SFTP server does not allow SCP clients to connect.
- The Nortel VPN Router supports s a maximum of eight concurrent SSH and SFTP sessions combined.
- SFTP is disabled by default and does not require a license key.
- If you enable or disable SFTP, you must restart the Nortel VPN Router.
- After a software upgrade, you must reenable the SFTP service even if the SSH Server was enabled in the previous release.

Configuring SFTP

To configure SFTP, perform the following steps:

1. Choose **Servers**, **SSH**.
2. Select the **SSH Service enabled** check box.
3. Select **SFTP Service enabled** check box.
4. Click **Restart Service**.

   A window appears and asks you to confirm that you want to restart the SSH server.
5. Click **OK**.
6. Click **Refresh** to see that the operational state.
7. When the operational state is **SSH Server is running**, click **Close**.

   The SSH Server window appears.

Restricted product-export license requirement

This product incorporates encryption technology that is highly restricted and can require an export license from the *U.S.* Department of Commerce, Bureau of Export Administration, prior to international shipment.

A product that incorporates encryption with a key length up to 56 bits can be eligible for international shipment pursuant to a license exception. However, products that incorporate encryption technology exceeding 56 bits requires an export license from the *U.S.* Department of Commerce.

Pursuant to such license, the product can be marketed and sold only to a limited class of international users. Entities, other than Nortel, that want to export this product must first obtain license approval from the *U.S.* Department of Commerce.

Further, the user of this product cannot reexport, transfer, or divert the product to country to which such reexports are restricted or embargoed under United States export control laws and regulations, or to national or resident of such restricted or embargoed countries, or provide the product to military end user or for military end use, including the design, development, or production of chemical, nuclear, or biological weapons.

Chapter 6
Configuring branch office tunnels

This chapter includes information about the following topics:

- "Branch office tunnel fundamentals" on page 91
- "Configuring a branch office tunnel" on page 99
- "BOT NAT-T configuration" on page 103

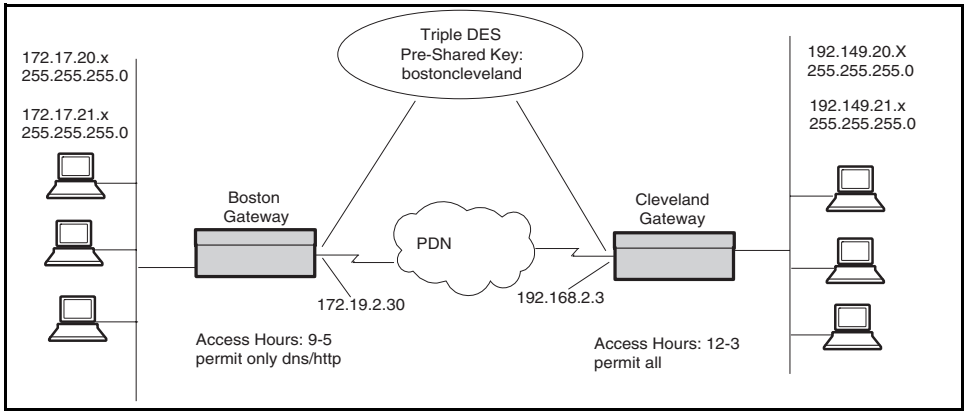
Branch office tunnel fundamentals

You can configure a secure tunnel connection between two private networks. The secure tunnel connection is called a branch office tunnel. Typically, one private network is behind a locally configured Nortel VPN Router while the other private network is behind a remote Nortel VPN Router. You can configure the accessible subnetworks behind each remote Nortel VPN Router.

The Nortel VPN Router supports symmetric, peer-to-peer, and asymmetric branch. An asymmetric branch office tunnel is a branch office tunnel where one of the endpoints does not have a fixed IP address. Such situations exist in the small branch office or Small Office Home Office (SOHO) environments where the Nortel VPN Router public interface is behind a Digital Subscriber Line (DSL) or cable modem. The DSL or cable modem services typically do not guarantee a static IP address. Branch office tunnels in these situations are asymmetric because only one side of the tunnel can initiate a connection.

"Typical branch office environment" on page 92 shows a typical branch office environment.

Figure 12 Typical branch office environment

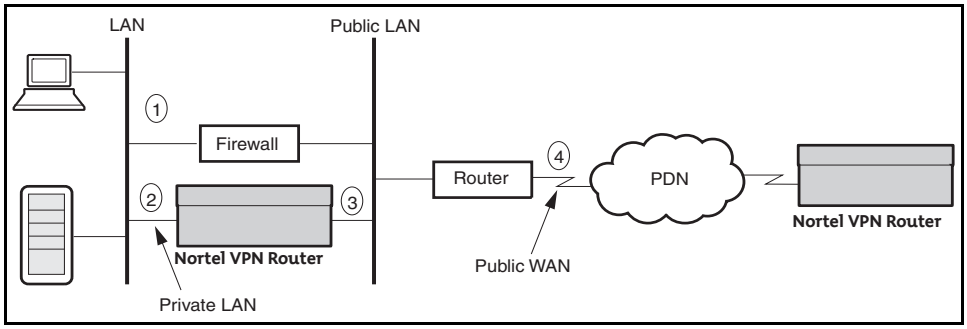


In a mixed environment, you can create tunnel connections to certain networks, and have all other traffic go to the Internet. You must configure the default Nortel VPN Router with a static route to the branch office Nortel VPN Routers for accessible networks. The default private LAN router (the firewall) redirects packets intended for remote branch office subnets.

In branch-to-branch configurations, configure each branch Nortel VPN Router with the same encryption settings and pre-shared key. Each Nortel VPN Router configuration inverts the accessible local and remote subnetwork addresses and subnet masks.

"Branch-to-branch with a firewall and a router" on page 92 shows a branch-to-branch configuration with a firewall and a router.

Figure 13 Branch-to-branch with a firewall and a router



In the branch-to-branch illustration, the following interactions occur:

1. The PC sends packets to the default route (the firewall).
2. The firewall redirects the packets to the local Nortel VPN Router branch office connection.
3. The encapsulated data goes onto the public WAN.
4. The public WAN routes directs the encapsulated data to the remote Nortel VPN Router branch office connection.

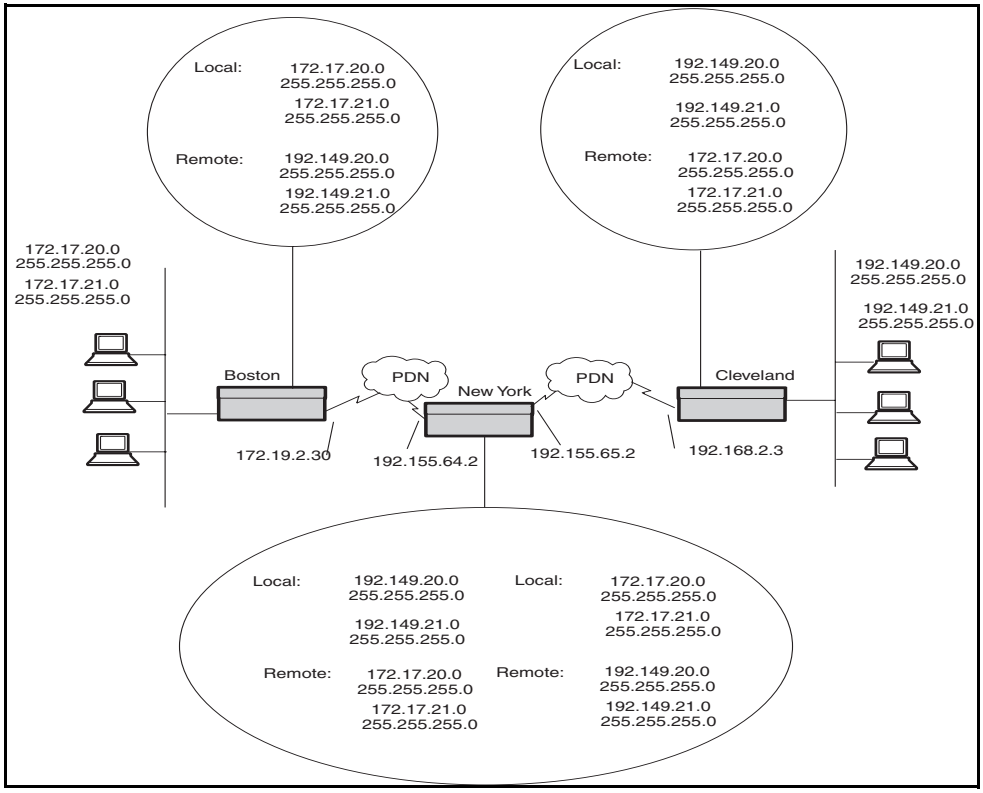
For a Nortel VPN Router that has a WAN link, actions 3 and 4 collapse together, and the encapsulated data is directed to the remote server.

In a topology with three Nortel VPN Routers, the two indirectly connected Nortel VPN Routers can create tunnels as long as each Nortel VPN Router includes all local and remote subnetworks and subnetwork masks as accessible networks.

"Indirectly connected branch offices" on page 94 shows the relationship between three Nortel VPN Routers and the local and remote networks configured for each link to allow indirectly connected branch offices to bring up tunnels. The New York Nortel VPN Router in the middle has two branch office connections configured.

All connections must have identical encryption settings. However, only adjacent connections must share keys. In the following figure, the Boston–New York connection shares keys and the New York–Cleveland connection shares keys. Boston and Cleveland are not required to share keys.

Figure 14 Indirectly connected branch offices



In a branch office configuration, two or more branches can use the same LAN addressing scheme. Users communicate across the branches.

Note: End user tunnels support PPP multilink, but branch office tunnels do not.

Using Network Address Translation (NAT), branch office connections can eliminate problems with overlapping addresses on both sides of the connection, and you can hide the LAN addresses. For more information about setting branch offices with NAT, see *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508).

PPTP nested tunnels

With nested tunnels, you can create a Peer-to-Peer Tunnelling Protocol (PPTP) user tunnel inside an IP Security (IPSec) branch office tunnel or an asynchronous branch office tunnel. You can have a nested tunnel from within the private network or from the public side.

Nested tunnels from within the private network

A nested tunnel from within the private network allows an end user to originate a PPTP connection from a client PC on the private network. After the client connects, PPTP control packets arrive at the Nortel VPN Router where it enters the IPsec branch office tunnel. The Nortel VPN Router at the entry point routes the control packets to the other end of the branch office connection. The PPTP connection ends at the Nortel VPN Router at the exit node of the branch office connection on the private interface. The control packets for the PPTP tunnel are processed and the Nortel VPN Router at the exit node of the branch office creates a new PPTP tunnel inside the branch office tunnel.

The nested PPTP tunnel status is based on the assumption that the branch office connection is a virtual link. When the branch office session is deleted or logged off, the nested PPTP sessions also deletes or logs off.

Nested tunnels from the public network

Nested tunnels from the public network allow remote users to connect from the Internet to a private network through the IPSec client. After connecting the IPSec client, the user can start a nested PPTP tunnel to the other end of the established branch office.

DNS for branch office tunnel endpoints

After you configure branch office tunnels, you can enter a Domain Name System (DNS) name for the tunnel endpoint. The Nortel VPN Router uses domain name address resolution to resolve the actual IP address of the endpoint.

The Nortel VPN Router provides the following DNS services:

- VPN DNS

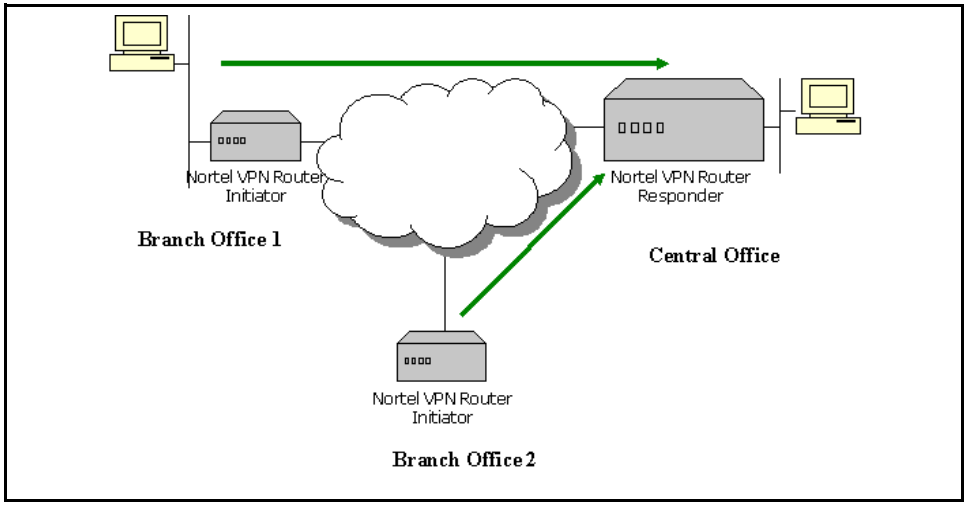
- Round Robin DNS

VPN DNS

You can configure IPSec asynchronous branch office tunnels to use the DNS name of a remote peer rather than IP address. In "VPN DNS" on page 96 the initiator from the branch office brings up a tunnel to a responder in the central office. If the IP address changes, no reconfiguration on initiator sites is required. This reduces the configuration time and simplifies the management. The Nortel VPN Router client supports this feature and the client can use the Nortel VPN Router domain name to bring up an IPSec user tunnel.

Without the VNP DNS, the initiator needs to know the IP address of the responder and reconfigure the address each time the address changes.

Figure 15 VPN DNS



After you configure an initiator for an asynchronous branch office tunnel, you can use a domain name of a remote peer instead of the IP address.

To configure VPN DNS on a branch office tunnel, perform the following steps:

1. Choose **Profiles, Branch Office**.
2. In the **Connections** section, click the **Select** option next to the connection that you want to configure.

3 Click **Configure.**

The Connection Configuration window appears.

4 In the **Endpoints** section, select a local IP address from the **Local IP Address** list.

5 Enter a DNS name of a responder endpoint in the **Remote IP Address** box.

6 Click **OK**.

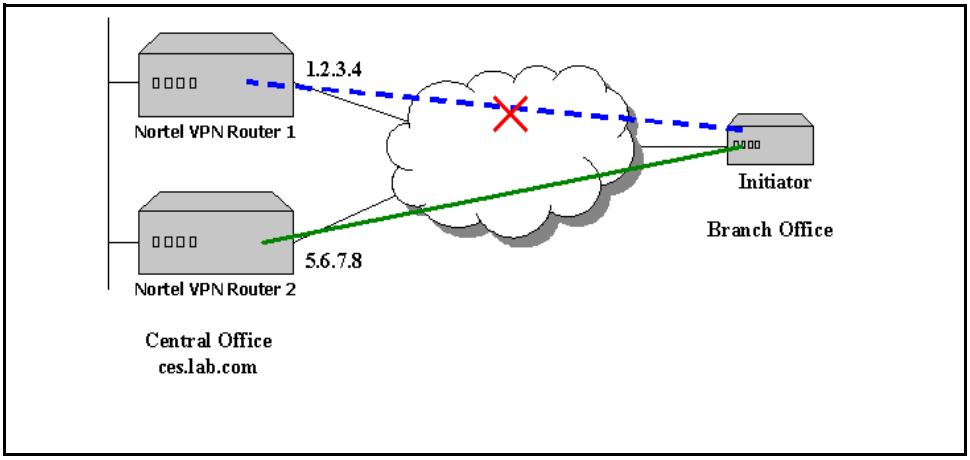
Round Robin DNS

Round Robin DNS provides a form of load balancing. Services on the Internet typically have more than one server facing the public network to share the load. Each of these servers has a unique IP address, but share a common DNS name.

A DNS server tracks all IP addresses that correspond to a particular domain name. When a user requests a lookup for that domain, the DNS provides the known addresses in random order. The user can pick one of the addresses to communicate with the service. The Nortel VPN Router uses the first address provided. If the first address is unresponsive, the Nortel VPN Router performs a new query.

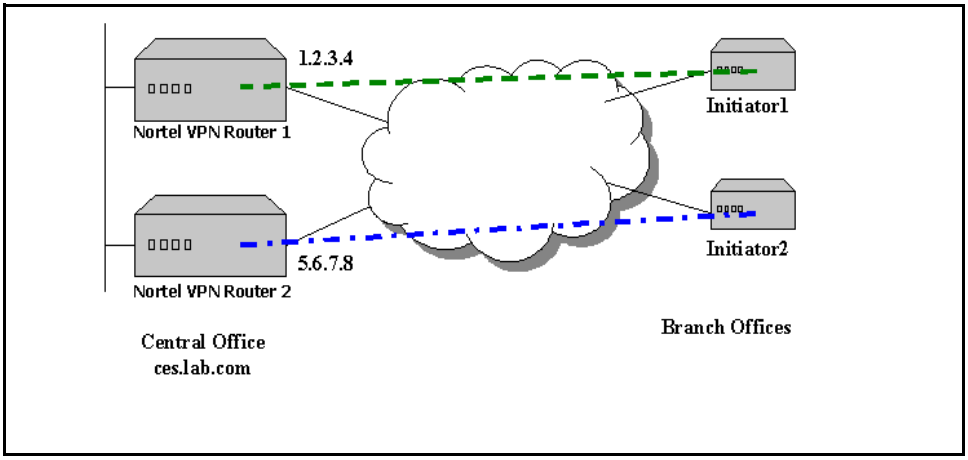
Round Robin DNS achieves failover. "Failover example" on page 98 shows a central office that has two Nortel VPN Routers. The first Nortel VPN Router has a public IP address 1.2.3.4, and the second has a public IP address 5.6.7.8. Both addresses are mapped to the same DNS name ces.lab.com. The initiator has the domain name of the responder ces.lab.com. When the initiator performs a DNS query, the DNS server returns IP addresses 1.2.3.4, and 5.6.7.8. The initiator selects 1.2.3.4 because it is first in the list of addresses and establishes a tunnel. If 1.2.3.4 goes down, the initiator must reestablish the tunnel and send a new DNS query. The DNS server returns addresses 5.6.7.8 and 1.2.3.4 because of the Round Robin operation. The initiator selects address 5.6.7.8 because it is the first in the list and establishes a tunnel with the second Nortel VPN Router, achieving a failover.

Figure 16 Failover example



You can use Round Robin DNS to achieve a simple load balancing between Nortel VPN Routers. "Load balancing example" on page 99 shows a central office that has two Nortel VPN Routers. The first Nortel VPN Router has the public IP address 1.2.3.4 and the second has the public IP address 5.6.7.8. Both addresses map to the same DNS name, such as ces.lab.com. Multiple branch offices exist. The initiators at the branch offices use a domain name as a remote endpoint of the asynchronous branch office tunnel. When two initiators at the remote sites attempt to establish a tunnel, a DNS query resolves the configured domain name ces.lab.com to the IP address. DNS uses Round Robin DNS to return 1.2.3.4 and 5.6.7.8 for branch one and 5.6.7.8 and 1.2.3.4 for branch two. The initiator at branch office one uses 1.2.3.4 as a remote point because it was the first response in the list. The initiator at branch office two uses 5.6.7.8 as a remote point because it was the first DNS response in the list.

Figure 17 Load balancing example



Configuring a branch office tunnel

To create a new branch office tunnel, give it a name and associate it with a group. You can choose an existing group or create a new one. The branch office connection then uses the group attributes, such as password management and encryption. You set the group attributes on the Profiles, Groups window.

The branch office connection then inherits the attributes of that group. You can associate multiple branch offices with the same group to save setup time and increase management efficiency. For example, you can create several VPN connections from remote sales offices into the enterprise headquarters. In this case, you create the connections in the same group so they have the same attributes, such as hours of access, encryption method, and password management. Certain configuration changes are not reflected in the active branch office tunnel until you disable, and then reenable it. Configuration changes that require you to disable and reendable the branch office tunnel are as follows:

- changes to the tunnel filter used by the branch office (changing which filter is applied is reflected in the active branch office tunnel)
- changes to the NAT policy used by the branch office
- routing changes, such as adding or deleting a default route

Adding a group

To create a new group, perform the following steps:

1. Choose **Profiles, Branch Office**.
2. In **Groups** section, click **Add.**

   The Add Group window appears.
3. Enter a name, and then select the parent group whose attributes the new group inherits; for example, /Base.

   The group name can be a maximum of 64 characters and spaces are permitted. The new group inherits the attributes of its parent group, which are then used by the branch office connection.
4. Click **OK**.

   The Branch Office window returns.
5. Click **Search All Groups** to use a connection name or partial connection name to locate and display all matching groups. You can then configure the specific group or groups that you want.
6. Enter the name you want to search for in the **Search Criteria** box.
7. Click **Search**.

   The Search All Groups Results window appears, listing groups that match all or part of the specified connection name.
8. Select a group.
9. Click **Configure** to review or modify the group attributes.

Adding a tunnel

To add a tunnel connection, perform the following steps:

1. Choose **Profiles, Branch Office**.
2. Click **Add**.

   The Add Connection window appears.
3. Enter the **Connection name** (up to 128 characters).

4 If this is a **Control Tunnel**, select **Enabled**.

5 From the **Tunnel Type** list, select **PPTP**, **IPSec**, or **LT2P**.

6 From the **Connection Type** list, select **Peer to Peer**, **Responder**, or **Initiator**.

7 Click **OK**.

Configuring a tunnel connection

To configure a connection, perform the following steps:

1 Choose **Profiles, Branch Office**.

2 Select the button next to the connection name.

3 Click **Configure**.

The Connection Configuration window appears.

4 From the **Tunnel Type** list, select **IPsec**, **PPTP**, or **L2TP** for the connection. The default type is IPsec.

If you change the tunnel type, the fields in the Authentication portion of this window change to reflect the different configuration requirements for the selected tunnel type.

5 Select an option from the **Connection Type** list.

- **Peer to peer** connection type is the traditional branch office tunnel, where either side can initiate traffic.
- **Initiator**, where with asynchronous branch office tunnels, one side must be configured as the initiator and the other as the responder. Only the initiator can bring up the tunnel. If the connection type is set to initiator, you do not define a local endpoint. Configure only an IPsec tunnel type. IPsec authentication requires an initiator ID. Asynchronous branch office tunnels work only on public interfaces.
- **Responder**, where neither local or remote endpoints are required. You must configure IPsec authentication to specify the same initiator ID as in the associated initiator branch office tunnel.

6 Click **Enable** to enable the branch office connection.

For security, the branch office connection automatically disabled if you attempt to save an incorrect configuration.

7 Select the **Endpoints** for the initiator and responder connection types.

- For the local endpoint address, click the list and select the address of the local Nortel VPN Router (for example, 132.168.2.3).
- In the remote endpoint address field, enter the address of the remote Nortel VPN Router (for example, 132.19.2.30) that you want to form the opposite end of the branch office connection. For initiator connection types, you can enter the DNS host name.

8 Select a filter from the **Filters** list.

The default is **permit all**. You can specify one filter. Packet filtering controls the types of access allowed for users of this branch connection. Filters are based on various parameters, including protocol ID, direction, IP addresses, source, port, and TCP connection establishment. Filters are defined on the Profiles, Filters window.

9 For **Authentication**, configure the authentication that is used between the local and remote branch office. The fields that appear in this window depend on whether you are using an IPsec, PPTP, or L2TP tunnel type.

Set up the authentication method for the connection, for example, text pre-shared key. Enter the key, and then retype it in the **Confirm Text String** field.

If you create a branch office connection using an IPsec certificate and you choose IP address as the alternate name, you must use the IP address of the public interface that is on the branch office end of the connection.

10 Select to reset the **Tunnel MTU**.

After you change the MTU value, you must reboot the Nortel VPN for the new value to take effect.

11 Enter an **MTU Value**.

Enter a value from 576 through 1788 bytes. The default value is 1788.

12 Under **NAT**, select either **PortNAT** or **none**.

NAT enables you to build the VPN without the need to reconfigure or rename the existing network. NAT sets are defined on the Profiles, NAT window. For more information about NAT, see *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508).

13 For **IP Configuration**, select either **Static** or **Dynamic** routing for this branch office connection:

- If you choose Static routing, you must manually specify the Accessible Networks, with are the private internal networks behind a Nortel VPN Router that are accessed through the branch office connection.
- If you select Dynamic, the routing protocol automatically determines the accessible networks based on information that is entered on the System, LAN Interfaces, Edit IP Address window. If you select Dynamic, additional settings for OSPF and RIP appears.

14 Click **Create Local Network** to define a local network.

The Local networks are the subnetworks on the private internal network of the local Nortel VPN Router. If you want to edit an existing local network, select it from the list. The Connection Configuration window appears. These networks have been previously set up on the Profiles, Networks window.

15 To add **Remote Networks**, click **Add** to add the remote networks for the branch office configuration.

Remote networks are the subnetworks on the private network of the remote Nortel VPN Router.

16 Verify the branch office connection by sending ping packets to the management IP address of the local Nortel VPN Router. You can also establish a Web connection to the local Nortel VPN Router and attempt to configure it.

BOT NAT-T configuration

NAT traversal (NAT-T) solves connection problems in private TCP/IP networks that use NAT devices. IPsec VPN clients can use NAT-T to allow ESP packets to transmit through the NAT device. If you install the Nortel VPN Router behind a NAT device that does not support IPSec, the VPN switches on both ends of the tunnel must encapsulate the IPsec packets to prevent the NAT device from dropping the packets. Without NAT-T, client-to-client networking applications can experience connection problems especially in peer-to-peer and VoIP networks.

For more information about BOT NAT-T, see Nortel VPN Router Configuration - Firewalls, Filters, NAT, and QoS (NN46110-508).

To enable NAT-T on branch office tunnels, perform the following procedures:

- "Enabling IPSec NAT-T globally" on page 104
- "Modifying the NAT keepalive interval" on page 104

Enabling IPSec NAT-T globally

To enable IPSec NAT-T globally, perform the following steps:

1. Choose **Services**, **IPSEC**.
2. Under **NAT traversal**, select **Enabled for Branch Office Tunnel**.

If you do not see the NAT-T section, scroll down the window until it appears.

3. Click **OK**.

Modifying the NAT keepalive interval

To modify the NAT keepalive interval, perform the following steps:

1. Ensure that IPSec NAT-T is enabled globally.
2. Choose **Profiles**, **Branch Office**.
3. Select a group from the **Group** list.
4. Click **Configure**.

   The Branch Office, Edit Group window appears.
5. Click **Configure** for IPSEC.

   The Branch Office window appears.
6. Enter a value in the **NAT Traversal Keepalive** box.

   The NAT traversal keepalive value configures the interval at which the Keepalive messages transmit to the NAT device. The format is: HH:MM:SS.
7. Click **OK**.

Chapter 7
Configuring control tunnels

This chapter includes information about the following topics:

- "Control tunnel fundamentals" on page 105
- "Configuring nailed-up control tunnels" on page 108
- "Control tunnel configuration" on page 109

Control tunnel fundamentals

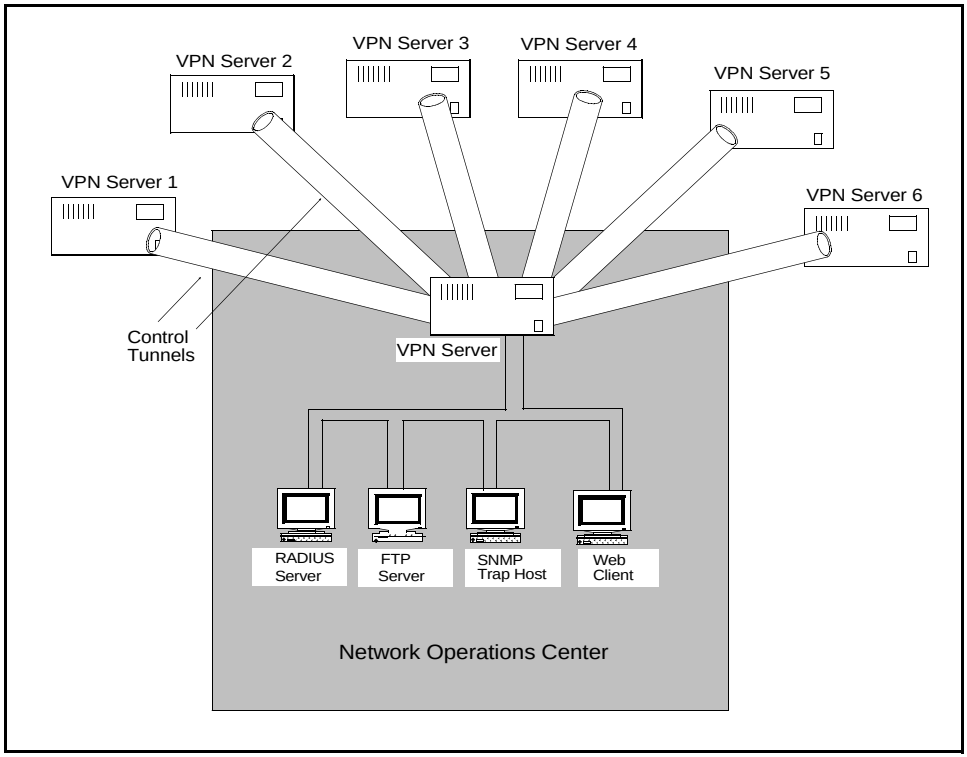
Control tunnels allow you to securely manage a Nortel VPN Router over the Internet. Control tunnels provide secure management and network data integrity.

Through a control tunnel, you can allow access to File Transfer Protocol (FTP), Dynamic Host Configuration Protocol (DHCP), RADIUS, and Domain Name System (DNS) servers from the Nortel VPN Router. You can configure an encrypted tunnel to a remote Nortel VPN Router. Through that tunnel, you can configure the necessary management tools, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Network Management Protocol (SNMP), and Telnet.

Note: To establish a control tunnel over a Network Address Translation (NAT) connection, use IP Security (IPSec)-capable NAT. Control tunnels cannot establish a connection while the Nortel VPN Router Stateful Firewall is enabled if you use the Autodetect IPSec-capable NAT feature.

"Branch office control tunnel" on page 106 shows a sample branch office control tunnel environment where a central VPN server can control several VPN devices and configure services, such as RADIUS, FTP backup, SNMP traps through Web client management, or Telnet.

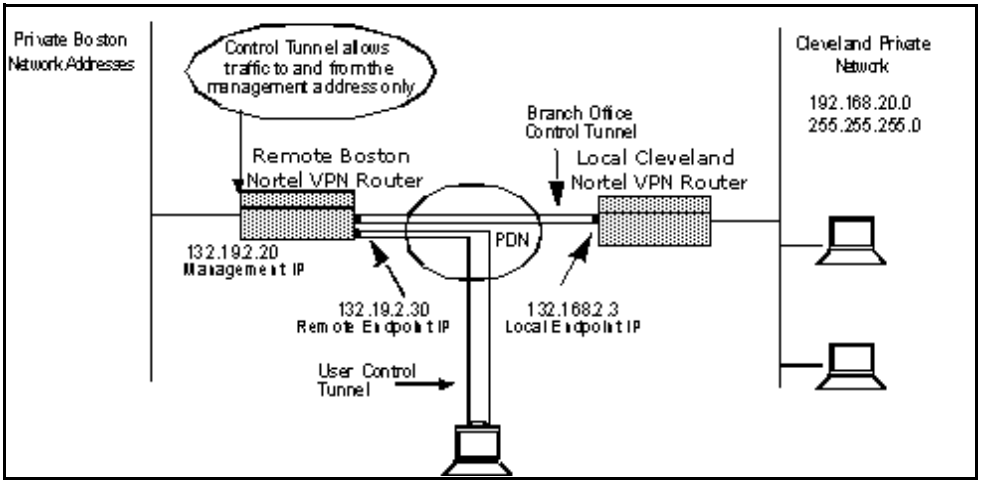
Figure 18 Branch office control tunnel



Control tunnel types

Two types of control tunnels exist: branch office control tunnels and user control tunnels. With both tunnel types, you can establish a secure IPsec tunnel to a system that you want to manage. The traffic inside the tunnels is limited to the Nortel VPN Router management IP address only, which is unique to control tunnels. "Sample control tunnel environment" on page 107 shows a branch office control tunnel from a network operations center and a user control tunnel.

Figure 19 Sample control tunnel environment



Branch office control tunnels

Branch office control tunnels allow anyone on the configured network to communicate with the Nortel VPN Router. Nortel VPN Router can communicate with various systems within a network operations center or corporate headquarters.

User control tunnel

A Nortel VPN Client communicates through a user control tunnel with a Nortel VPN Router. Network management personnel can remotely access the Nortel VPN Router to perform management tasks.

Additionally, you can configure a user control tunnel so that a remote user can establish a control tunnel by using the IPsec client. You create this user account with password authentication in the Control Tunnels group through the serial port.

Restricted mode

The Restricted mode feature prevents management of the Nortel VPN Router unless the management occurs through a control tunnel. This limits the scope of management to someone who has the proper credentials both to set up the tunnel and has administrative access privileges. Having the proper access privileges acts as a level of security.

You enable Restricted mode through the Serial Interface menu or the command line interface available through Telnet. In Restricted mode, you can perform the key management functions through the control tunnel, including HTTP, FTP, SNMP, and Telnet. All other attempts to perform these actions outside of the control tunnel fails. You cannot enter restricted mode unless there an active control tunnel exists.

Configuring nailed-up control tunnels

You can maintain control tunnels even if no traffic traverses the control tunnel.

Note: If you change settings to the branch office connection that uses nailed up tunnels, you must disable the tunnel for the changes to take effect.

To create a nailed-up control tunnel using the nailed-up parameter, perform the following steps:

1. Choose **Profiles**, **Branch Office.**
2. Click **Edit** next to the group that you want to have nailed up.

   The Edit Group window appears.
3. In the Connectivity section, click **Configure**.

   The **Connectivity** window appears.
4. Click **Configure** next to the **Nailed Up** field.
5. Select **Enabled** or **Disabled** from the list.

Enable this parameter only on the initiating side of the tunnel.

Note: Another way to nail up control tunnels, is to create a script that continuously sends ping packets to the management IP address of the Nortel VPN Router on the customer premise through the control tunnel from a host at the network operations center. The pings must occur at an interval that is less than the Idle Timeout value. These pings act as a liveliness detection and perform keepalive signals for the end connection, and report to the sender that the packet was received or that there was no response.

6 Click **Enabled**. The default is Disabled.

7 Click **OK**.

Control tunnel configuration

To create a special branch office connection, you must create a control tunnel definition on the remote customer Nortel VPN Router.

After you configure the local Nortel VPN Router, you must configure the Nortel VPN Router located at the remote site. Complete the following steps to define the branch office connection for the remote Nortel VPN Router.

Adding a group

To create a new group perform the following steps:

1 Choose **Profiles, Branch Office**.

2 In **Groups** section, click **Add.**

The Add Group window appears.

3 Enter a name.

4 Select the parent group whose attributes the new group inherits; for example, / Base.

The group name can be a maximum of 64 characters (spaces are permitted). The new group inherits the attributes (for example, Access Hours) of its parent group, which are then used by the branch office connection.

5 Click **OK**.

The Branch Office window appears

You can also click Search All Groups to use a connection name or partial connection name to locate and display all matching groups. You can then configure the specific group or groups that you want.

Enter the name you want to search for in the Search Criteria window, and then click Search. The Search All Groups Results window appears, listing groups that match all or part of the specified connection name.

You can select a Group, and then click Configure to review or modify the group attributes.

Adding a control tunnel

To add a control tunnel connection, perform the following steps:

1 Choose **Profiles, Branch Office.**

2 In the **Connections** section, click **Add**.

The Add Connection window appears.

3 Enter the **Connection name** (up to 128 characters).

4 From the **Control Tunnel** list, select **Enabled**.

5 From the **Tunnel Type** list, select **PPTP**, **IPSec**, or **LT2P**.

6 From the **Connection Type** list, select **Peer to Peer**, **Responder** or **Initiator**.

7 Click **OK**.

The page refreshes.

8 Click **OK**.

Configuring a control tunnel connection

To configure a Control Tunnel connection, perform the following steps:

1. Chose **Profiles, Branch Office**.
2. Select the connection.
3. Click **Configure**.

   The Connection Configuration window appears.

4. From the **Tunnel Typ**e list, select **IPsec**, **PPTP**, or **L2TP**. The default type is IPsec.

   If you change the tunnel type, the fields in the Authentication portion of this window change to reflect the different configuration requirements for the selected tunnel type.

5. Select the **Connection Type** that you want this branch office to use.
   - **Peer to peer**, which is the traditional branch office tunnel, where either side can initiate traffic.
   - **Initiator**, where, with asynchronous branch office tunnels, one side must be configured as the initiator and the other as the responder. Only the initiator can bring up the tunnel. If the connection type is set to initiator, you do not need to define a local endpoint. Configure only an IPsec tunnel type. IPsec authentication requires an initiator ID. Asynchronous branch office tunnels work only on public interfaces.
   - **Responder**, where neither local or remote endpoints are required. You must configure IPsec authentication to specify the same initiator ID as in the associated initiator branch office tunnel.
6. Click **Enable** to enable the branch office connection.

   For security reasons, the branch office connection is automatically disabled if you attempt to save an incorrect configuration.

7. Select the **Endpoints** for the initiator and responder connection types.
   - For the local endpoint address, click the list and select the address of the local Nortel VPN Router (for example, 132.168.2.3).

- In the remote endpoint address field, enter the address of the remote Nortel VPN Router (for example, 132.19.2.30) that you want to form the opposite end of the branch office connection. For initiator connection types, you can enter the DNS host name.

8 Select the filter from the **Filters** list. The default is **permit all**.

You can specify one filter. Packet filtering controls the types of access allowed for users of this branch connection. Filters are based on various parameters, including protocol ID, direction, IP addresses, source, port, and TCP connection establishment. Filters are defined on the Profiles, Filters window.

9 For **Authentication**, configure the authentication that is used between the local and remote branch office.

The fields that appear in this window depend on whether you are using an IPsec, PPTP, or L2TP tunnel type.

Set up the authentication method for the connection. Enter the key, and then retype it in the Confirm Text String field.

If you create a branch office connection using an IPsec certificate and you choose IP address as the alternate name, you must use the IP address of the public interface that is on the branch office end of the connection.

10 Select to reset the **Tunnel MTU**.

After you change the MTU value, you must reboot the Nortel VPN for the new value to take effect.

11 Enter an **MTU Value**.

Enter a value from 576 through 1788 bytes. The default value is 1788.

12 Under **NAT**, select either **PortNAT** or **none**.

NAT enables you to build the VPN without requiring that you reconfigure or rename the existing network. NAT sets are defined on the **Profiles, NAT** window. For more information about NAT, see *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508).

13 For **IP Configuration**, select either **Static** or **Dynamic** routing for this branch office connection:

- If you choose Static routing, you must manually specify the Accessible Networks, which are the private internal networks behind a Nortel VPN Router that you can access through the branch office connection.

- If you choose Dynamic, the routing protocol automatically determines the accessible networks based on information that is entered on the System, LAN Interfaces, Edit IP Address window.

14 To define a local network, click **Create Local Network** to go the Profiles, Networks window.

The Local networks are the subnetworks on the private internal network of the local Nortel VPN Router. If you want to edit an existing local network, select it from the list. The Connection Configuration window appears. These networks have been previously set up on the Profiles, Networks window.

15 To add **Remote Networks**, click **Add** to go to the **Add Networks** window.

Remote networks are the subnetworks on the private network of the remote Nortel VPN Router.

16 Verify the branch office connection by sending ping packets to the management IP address of the local Nortel VPN Router. You can also establish a Web connection to the local Nortel VPN Router and attempt to configure it.

Chapter 8
Configuring IPSec mobility and persistent mode

This chapter includes information about the following topics:

- "IPSec mobility fundamentals" on page 115
- "IPSec mobility on Nortel VPN Router" on page 117
- "Persistent tunneling fundamentals" on page 123
- "Configuring IPSec mobility and persistence" on page 124

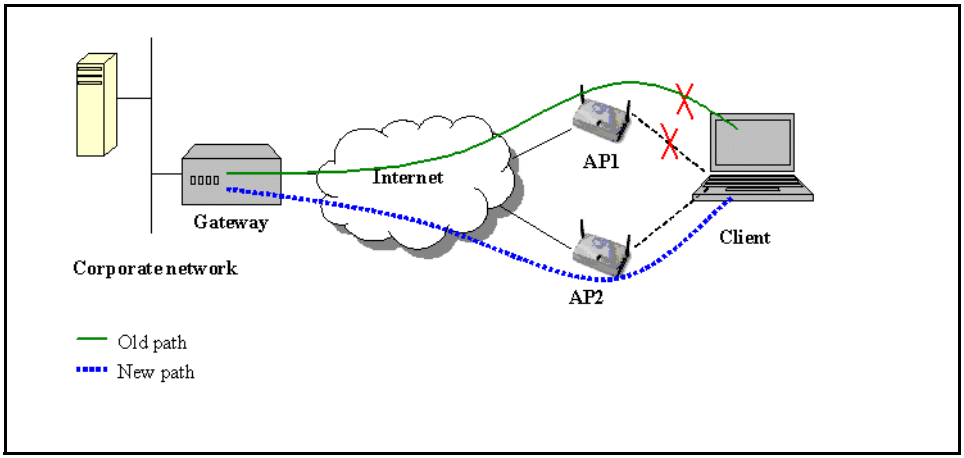
IPSec mobility fundamentals

You can secure access to their corporate networks through VPN using the IP Security (IPSec) protocol. IPSec allows users, located outside the local network to establish a secure tunnel to a private network through the Internet. With the popularity of wireless access, it is important to move freely among multiple networks without losing a secure connection.

Currently, IPSec does not support this movement without tearing down and reestablishing the VPN connection. Breaking and reestablishing a secure connection can cause disruptions to applications running across the tunnel. For example in "Example configuration" on page 116, if a client has a wireless connection to the Internet and has established a secure tunnel to the corporate private network through access point 1 (AP1) and the client's connection to AP1 goes down for some reason, the client roams to the access point 2 (AP2) and obtains a new IP address.

The Nortel VPN Router on the corporate network brings the secure IPSec connection down because of a lack of response from original client IP address and the absence of security associations (SA) for the new IP address. Thus, the client must reestablish a tunnel through AP2. If the client has an open File Transfer Protocol (FTP) session to the server on the private side of the corporate network, this session closes.

Figure 20 Example configuration



To solve this problem, use mobile IP technology to maintain IPSec connections. For more information, see RFC 3344. In this configuration, the IP address of the mobile machine does not change after it moves from a home network to a foreign network. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. When away from home, mobile IP uses protocol tunneling to hide a mobile node home address from intervening routers between its home network and its current location. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

IP mobility technology for IPSec can be inefficient due to double tunneling, which can be an issue for resource-limited wireless networks. In addition, mobile IP requires deployment of extra equipment and administration that can increase the cost of the solution and can be a potential cause of interoperability problems between different vendors and providers.

Nortel solves the IPSec mobility problem by enhancing its IPSec implementation.

IPSec mobility on Nortel VPN Router

Nortel VPN Router provides a new concept of IPsec mobility. The Nortel VPN Router IPSec implementation allows support for mobile clients to maintain tunnel connectivity when the roam from one access point to another. It maintains Transmission Control Protocol (TCP)-based applications and provides minimum disruptions to User Datagram Protocol (UDP)-based applications.

With IPSec mobility, configuration parameters pass to the Nortel VPN Router client after a successful IPSec tunnel establishment. The configuration parameters instruct the client to operate in IPSec mobility mode. These parameters force the client to monitor and communicate roaming address changes to the server. If a mobile node changes IP address, the operating system notifies the client of the change. The client communicates the IP address change to the Nortel VPN Router so that the Internet Key Exchange (IKE) and IPSec server associate (SA) databases add the new address. Internet Security and Key Management Protocol (ISAKMP) informational exchange messages send the change to the Nortel VPN Router. After the Nortel VPN Router receives a notify message with a new client IP address, it updates the databases, uses the received IP as the outer IP address, and responds to the client with an acknowledgment.

Performance factors of roaming

Factors that impact the performance of roaming on the Nortel VPN Router include.

- how quickly the adaptor or operating system detects changes in interface state
- Dynamic Host Configuration Protocol (DHCP) settings of the PC or the DHCP server
- how quickly the operating system acquires the new IP address from the network
- network delays or congestion

Status and Logging for clients and servers

The Nortel VPN Client logs events to the log file. This includes events such as Nortel VPN Client sending messages that the IP address changed, and receiving acknowledgement that these messages were received by the Nortel VPN Router.

The Nortel VPN Client status monitor reports if roaming is enabled for the session. The event log on the Nortel VPN Router reports on IPSec mobility actions.

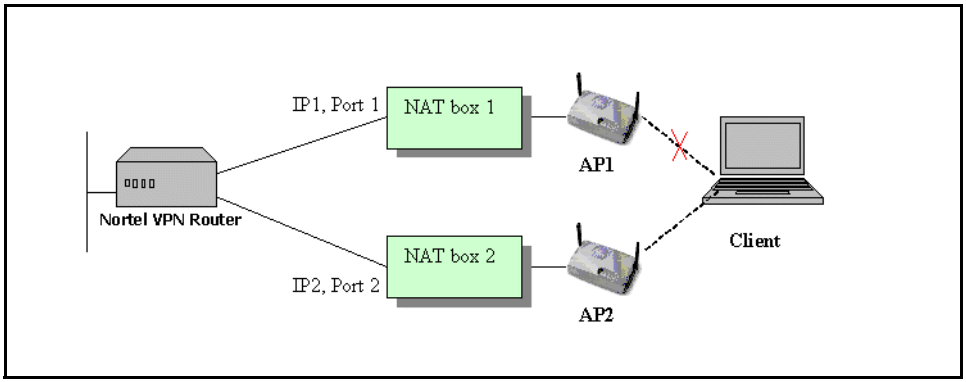
IPSec mobility and NAT

If Nortel VPN Client is behind a NAT switch with NAT traversal enabled and encapsulation for ESP protocol is used, UDP encapsulation is preserved after roaming.

Roaming from behind NAT to behind NAT

In "Roaming from behind NAT to behind NAT" on page 118, before roaming the client was connects through access point 1 (AP1) and NAT box 1 and had an IP1 IP address. After roaming, the client is connected through access point 2 (AP2) and NAT box 2 and gets an IP address IP2. In this case, the client IP address and UDP port have been changed after roaming. If a new IP address has been received by the client, it sends a NAT keep-alive so that the server can find the Encapsulating Security Payload (ESP) UDP port mapping and send the data to the client using port mapping.

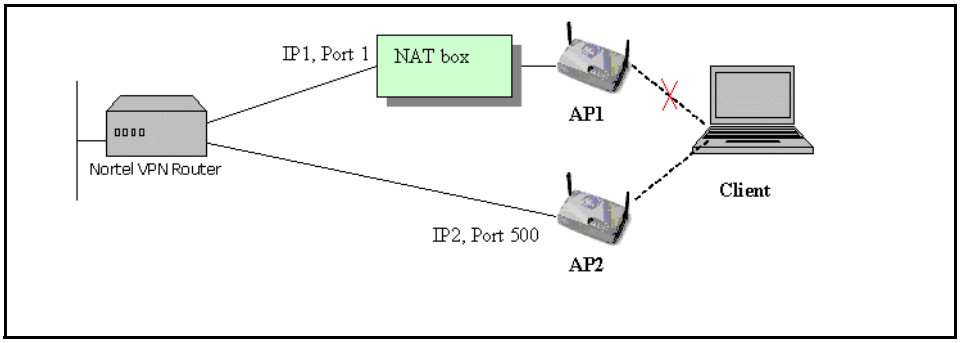
Figure 21 Roaming from behind NAT to behind NAT



Roaming from behind NAT to no NAT

"Roaming from behind NAT to no NAT" on page 119 shows how, without roaming, a client connected to the Nortel VPN Router through AP1 and the NAT switch. The client has the IP1 IP address. With roaming, the client connects through AP2 without NAT and uses UDP encapsulation.

Figure 22 Roaming from behind NAT to no NAT



Roaming from no NAT to behind NAT

Before roaming, the client had access through AP2 and after roaming through AP1 and NAT box, a situation that is the reverse of the one in the previous figure. In this case, the IPSec connection is dropped as NAT detection is made in IKE phase 1, and NAT traversal is negotiated in quick mode. Therefore, with the tunnel already negotiated and established, the change cannot take place unless renegotiation occurs.

Similar problems can arise when the client roams from behind IPSec-aware NAT devices to behind other NAT devices. To avoid NAT-related problems, the Always UDP Encap option under the IPSec group configuration forces UDP wrapping on IPSec user tunnels even if NAT was not detected during connection establishment.

IPSec mobility in NAT environment

In some situations, roaming in the environment of NAT devices can prevent users from taking full advantage of IPSec mobility feature. "Configuration considerations" on page 120 illustrates some configuration considerations that increase roaming effectiveness in NAT environment.

Table 5 Configuration considerations

Initial Nortel VPN Client connection was behind	After roaming Nortel VPN Client connection is behind	Nortel VPN Router configuration consideration to make mobility work successfully
No NAT	No NAT	None
	IPSec unaware NAT	Always NAT Traversal
	IPSec aware NAT	Always NAT Traversal
IPSec aware NAT	No NAT	None*
	IPSec unaware NAT	Always NAT Traversal or Auto-Detect NAT
	IPSec aware NAT	None*
Non-IPSec aware NAT	No NAT	None*
	IPSec unaware NAT	None*
	IPSec aware NAT	None*

*The appropriate IPSec group settings, such as Auto-Detect NAT, Always UDP Encap, or Auto-Detect IPSec-capable NAT, makes the initial connection successful. No changes are required for roaming to work.

Routing table changes

Routing table changes apply to the Nortel VPN Client. If operating in split tunneling mode, the Nortel VPN Client periodically checks the routing table on the client PC to determine if the table is altered. This checking detects intrusions and unauthorized access to the private network. If a routing table change is detected, the tunnel is brought down.

When operating in IPSec mobility mode with split tunneling enabled, the Nortel VPN Client does not consider the routing table to be maliciously altered and does not bring down the tunnel in the following cases:

- IP address change for an adapter
- adapter has been removed
- adapter is plugged in and connects

ICP overview

If the Nortel VPN Client fails to notify the Nortel VPN Router of the logoff or tunnel termination due to network problems, the client session can still be in the session table for the period of time specified by the Idle Timeout. If the client tries to reconnect and the previous session is not yet expired, the client cannot log on because only one active session is allowed for each user by default.

Use the Initial Contact Payload (ICP) feature to clear old sessions. The server terminates an old session if a new session has the same user ID as the old one.

Note: With IPC, the server cannot identify the session to terminate if a user is logged on multiple times. Nortel recommends using IPC if the maximum logon is set to 1.

Beginning with Nortel VPN Client release 5.01, the Nortel VPN Client sends the ICP message, which the Nortel VPN Router can accept or reject based on the Nortel VPN Router configuration. The Accept ISAKMP Initial Contact Payload parameter configured for each group specifies Nortel VPN Router action towards received ICP message.

Maximum roaming time

Maximum roaming time is the time used by the Nortel VPN Client to keep the tunnel from going down after the IP address on the physical interface is lost.

For example, if you move from area 1 (AP1) to area 2 (AP2) and the IP address on the interface is lost, it can take time to establish contact with AP2 in area 2. You can configure this maximum roam time to allow the client to keep the connection open for two hours, and then if necessary, the same session can be revitalized at another location.

Use caution when you configure the idle timeout and the client failover timers. For example, idle timeout can start during roaming time and as a result the Nortel VPN Router logs off the session. If the client obtains a new IP address and sends an Address Change Notification, the Nortel VPN Router does not recognize the new IP address and logs off the session. A similar situation can arise with the client failover tuning timers.

If the Nortel VPN Router initiates a rekey during the roaming time and cannot reach the client, the rekey can fail. If the rekey fails, the Nortel VPN Router brings down the session and roaming does not succeed even after the client obtains a new IP address. This occurs because the Nortel VPN Router has no knowledge about the client going through roaming time at rekey.

The forced logoff timer is independent of roaming time. The Nortel VPN Router is expected to logoff the session whether or not roaming is in progress.

NAT keepalive timers have no impact on roaming timeout because the Nortel VPN Router updates the UDP port numbers based on an encrypted Address Change Notification message.

After the Nortel VPN Client obtains a new IP address, it retransmits the Address Change Notification message four times at eight second intervals until an acknowledgement is received from the Nortel VPN Router. If no acknowledgement is received, the client disconnects.

Session persistence time has no direct impact on roaming time.

Persistent tunneling fundamentals

Using a persistent VPN connection, you can maintain a VPN connection without user intervention for a designated period of time. After successfully establishing a tunnel session to the Nortel VPN Router, the Nortel VPN Client makes every attempt to maintain a viable VPN connection.

Persistence uses the automatic failover feature and extends the feature to allow you to establish a new tunnel without needing to reenter user credentials. A configuration option on the Nortel VPN Router allows you to specify that VPN clients cache their VPN credentials for a specified period of time. If failover is initiated during this time (persistent time), the client automatically sends the credentials the user submitted to set up the first tunnel session.

Note: If an authentication method with a challenge, one-time password (such as secure ID), or Nortel VPN Router one-time password is enabled, it does not work for persistence. However, user name password-based and certificate-based authentication works.

The Nortel VPN Client accepts a list of failover hosts configured on the Nortel VPN Router and tries to connect to those servers if the connection with the primary server is lost. As each failover server destination is attempted, you are prompted, allowing you the option to cancel the operation. If the user does not intervene, the connection attempt continues. With persistence enabled, after going through the list of failover servers, the client tries the primary, and then the initially supplied failover servers again in the loop until the client connects or until the persistency timer expires, whichever comes first.

Session persistence time

The purpose of the session persistence timer is to allow the persistent tunnel only for the specified amount of time after the initial logon. This prevents security threats, such as a stolen laptop, from accessing the network due to persistence for longer durations. If you configure this timer to 24 hours, users can use the VPN connectivity for work without requiring to logon more than once.

Nortel recommends that you configure session persistence time to be longer than the roaming time as persistence starts only after roaming fails. No direct relationship between persistence and other timers on the Nortel VPN Router exists.

However, the Nortel VPN Client does not enter persistence mode if the previous log off occurred due to a log off message received from the Nortel VPN Router. This allows you to force a rogue user to log off even if persistence is enabled. The client continues to attempt connections to a list of servers cyclically after the existing tunnel goes down for a period equal to persistence time after the initial log on.

Persistent mode works without a failover list to retry the connection to the same Nortel VPN Router. The original Nortel VPN Router is included in the list that the client tries to connect to. If no servers are configured in the failover list, the original Nortel VPN Router is tried persistently.

Configuring IPSec mobility and persistence

IPSec mobility is a Advanced licensed feature. Contact a Nortel representative to obtain a license key. For more information about license keys, see *Nortel VPN Router Administration* (NN46110-603).

Configuring IPSec mobility

Configure the IPSec mobility and persistence features at the user or group level. For more information about configuring NAT traversal, see *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508).

You do not have to enable IPSec mobility and persistence together. You can use either or both as is suitable for the environment.

To configure IPSec mobility and persistence, perform the following steps:

1. Choose **Profiles, Groups**.
2. In the **IPSec** section, click **Configure**.

   The Edit IPSec window appears.

3. Scroll down to **Mobility Support.**
4. Select **Enabled**. The default is Disabled.
5. For **Max Roaming Time (seconds),** enter the number of seconds.

   The default is 120 seconds. The maximum roaming time (1 to 7200 seconds) specifies how long the tunnel stays in the suspended state, or time allowed for the roaming to take effect.

   When you configure Max Roaming Time, consider the IPSec Idle Timeout and rekey timeout settings. Configure Max Roaming Time to be less than the Idle Timeout interval to prevent the session timeout prior to roaming completion.
6. For **Persistence,** select **Enabled** or **Disabled**. The default is Disabled.
7. For **Session Persistence Time (minutes)**, enter the number of minutes (1 to 1440). The default is 60 minutes.
8. Click **OK**.

IPSec mobility performs at higher level than physical adapters. As a result, the PC on which the Nortel VPN Client runs can change between physical adapters (wireless or wireline), and roaming continues to work as long as IP connectivity between the Nortel VPN Router and the client with the newly acquired address or interface exists. If you have problems with roaming to specific interfaces, ensure that you can establish an initial connection with that adapter to confirm IP connectivity.

Appendix A
Configuration checklist and BOQS template

Configuration checklist

Use the following checklist to record the information that you need to configure basic Nortel VPN Router parameters.

Table 6 Configuration checklist

GUI window	Values required	Values
System, Identity	Management IP address	
System, Identity	Host name Domain name	
System, Identity	Primary IP address Secondary IP address Tertiary IP address	
System, LAN	Private IP address Public IP address	
System, WAN (if using T1, V.35, or T3)	ISP provided information	
System, Date and Time	Manual entry of date and time or NTP configuration server broadcast or multicast IP address	
Services, Available Tunnel Type	IPsec private address IPsec public address PPTP private address PPTP public address Layer 2 Transport Protocol (L2TP) and Layer 2 Forwarding (L2F) public address L2TP and L2F private address	

Table 6 Configuration checklist (continued)

GUI window	Values required	Values
Services, Available Management Protocol	Hypertext Transfer Protocol (HTTP) private address HTTP public address Simple Network Management Protocol (SNMP) private address SNMP public address File Transfer Protocol (FTP) private address FTP public address Telnet private address Telnet public address Certificate Revocation list (CRL) retrieval private address CRL retrieval public address	
Routing, Static Routes Enabled/Disabled	Public Nortel VPN Router IP address Private Nortel VPN Router IP address	
Routing, OSPF Enabled/ Disabled	Router ID AS boundary router (true or false)	
Routing, Rip Enabled/Disabled	True or false	
Routing, Interfaces LAN IP Address	Open Shortest Path First (OSPF) (enabled or disabled) Routing Information Protocol (RIP) (enabled or disabled) Virtual Router Redundancy Protocol (VRRP) (enabled or disabled)	

Table 6 Configuration checklist (continued)

GUI window	Values required	Values
Servers, Radius Auth	Access (enabled or disabled Server-Supported Option (enabled or disabled) Radius Servers (enabled or disabled) Primary host name or IP addresses, public or private, Port, Shared secret/confirmed Alternate 1 host name or IP addresses, public or private, Port, Shared secret/confirmed Alternate 2 host name or IP addresses, public or private, Port, Shared secret/confirmed	
Servers, LDAP	Internal or external Base Directory Number (DN) Master IP address, port or Secure Sockets Layer (SSL) Bind DN, Bind password, Confirmed Slave 1 IP address, port or SSL Bind DN, Bind password, Confirmed Slave 2 IP address, port or SSL Bind DN, Bind password, Confirmed	
Servers, User IP Addr	Broadcast Any DHCP or DHCP servers: Primary IP address Secondary IP address Tertiary IP address Address pool: Pool name Start End Subnet mask	

Table 6 Configuration checklist (continued)

GUI window	Values required	Values
Admin, License Keys Install License Keys	Advanced routing install key Nortel VPN Router Stateful Firewall install key	
Admin, Auto Backup	Automatic Backup file servers IP address of FTP servers for backup: Host Path User ID Password	

BOQS template

The branch office quick start template provides a list of values that the local Nortel VPN Router 1010, 1050, and 1100 user needs to enter on the BOQS window. You can enter the appropriate values in the right-hand column, and then fax, send, or e-mail the template to the local user along with other required information, such as who to contact for further information or questions.

Central office tunnel configuration	**Your value**
Central office tunnel name	
Central office tunnel password	
Central office public IP address	
Central office DNS server IP address	
Central office WINS sever IP address	
Private network IP address	
Private network mask	
Network operation center tunnel configuration	**Your value**
Network operation center tunnel name	
Network operation center tunnel password	
Network operations center public IP address	
Network operations center private network IP address	

Central office tunnel configuration	Your value
Network operations center private net mask	
Branch office switch management IP address	

"BOQS parameters" on page 132 contains the BOQS parameters.

Table 7 BOQS parameters

Parameter	Description
Central office tunnel name	Name of the branch office tunnel on the central office switch.
Central office tunnel password	Password for the branch office tunnel.
Central office public IP address	Public address of the central office switch (same for all branch offices).
Central office DNS server IP address	IP address of the DNS server in the central office. The DHCP server configured on private interface distributes this address to the branch office. You can configure multiple addresses, but you must separate them with commas. This field is optional and can be left empty.
Central office WINS sever IP address	IP address of the WINS server in the central office. The DHCP server configured on private interface distributes this address to the branch office workstations. You can configure multiple addresses, but you must separate them with commas. This field is optional and can be left empty.
Private network IP address	Subnet address of the branch office network.
Private network mask	Subnet mask of the branch office network.
Network Operation Center tunnel configuration	
Network operation center tunnel name	Name of the branch office tunnel configured on NOC switch (same as initiator ID on the NOC switch).
Network operation center tunnel password	Text pre-shared key used in branch office tunnel.
Network operations center public IP address	Public address of the NOC switch (same for all branch offices).
Network operations center private network IP address	IP Address part of subnet address in which NOC is located (private subnet of NOC switch).

Table 7 BOQS parameters

Parameter	Description
Network operations center private net mask	IP mask of subnet address in which NOC is located (private subnet of NOC switch).
Branch office switch management IP address	Address used by the NOC to manage switch. Must be unique for each Nortel VPN Router 1010, 1050, and 1100 and reachable from the NOC. If left empty, can be managed with the second address of the subnet configured in branch office private network IP address and IP mask field

Index

A

access hours 61

accessible networks 92, 93

asymmetric branch office tunnel (ABOT) 91

asynchronous data over TCP (AOT) 80

authentication
- branch office 102, 112

B

base group 58

branch office
- authentication 102, 112
- configuring 91
- encryption settings 93
- indirectly connected switches 93
- routing 103, 112

branch office quick start
- parameters 132
- template 45

branch office quick start template
- template 130

branch office tunnel types
- asymmetric 91
- peer to peer 91

C

call admission
- priority 61

children of base group 58

Command Line Interface (CLI) 24

compact flash disk 55

configuration
- choices 38
- preparing for 25
- Web interface options 38

configuring
- branch offices 91

connection types
- initiator 101, 111
- responder 101, 111

control tunnels 105
- branch office 107
- creating 109
- nailed-up 108
- restricted mode 108
- user 107

D

data collection
- interval 85

default
- login 38
- password 38

DHCP
- client 74

DNS
- branch office tunnel endpoints 95
- host name 72
- round robin DNS 97

E

encryption
- settings for branch office 93

F

FIPS
overview 24
firewall
branch office 92
interaction with branch office 93
flash disk system
compressed files 55
forwarding priority 61

G

getting started 71
group
associations 59

I

idle timeout 62
indirectly connected switches 93
interface
filter 75
Internet domain 72
inverse split tunneling 68
IP address
assigning 27
currently assigned 75
IPSec mobility
configuring 124
logging 118
IPX 29
ISP
tunnels 58

L

LAN interfaces 73
last name search 68
LDAP
attribute search 68
license keys
advanced routing 24
firewall 24
tunnel 24
licenses 38
log file
configuration 84
life time 84
login 38

M

MAC Pause 77
management IP address 72
Multinetting 77

N

nested tunnels 95
Network Address Translation (NAT) 94
Network Time Protocol (NTP) 80
Nortel VPN Router 1010/1050/1100
compact flash disk 55
ISP environment 46
setting up 48

P

password 38
Peer to peer 101, 111
persistent tunneling 70, 123
port speed 76
prerequisites 25
private LAN 73
proxy ARP 86
public data network (PDN) 73
publications
hard copy 16

R

register 38
relative distinguished name 60
remote access 23
round robin DNS
  failover 97
  load balancing 98

S

Safe mode 41, 82
serial interface 29, 36
services 38
split tunnel 67
split tunnel mode 59
subnet mask 75
subnetworks 91
Switch concepts 21
Symmetric Branch Office tunnel 91
system identity 71

T

technical publications 16
template 45
terminal emulator 36
tunnel types 65

U

user
  ID search 68
user groups
  adding 65
  searching 68
user profile
  adding 66
user tunnels 64

V

VPN DNS 96
VPN Router Access 23

W

Web browser interface 37
Web interface options 38