Version 8.00

Part No. NN46110-503 02.01
318438-D Rev 01
13 October 2008
Document status: Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Configuration — Tunneling Protocols

NORTEL

Copyright © 2008 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, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Cisco and Cisco Systems are trademarks of Cisco Systems, Inc.

Entrust and Entrust Authority are trademarks of Entrust Technologies, Incorporated.

Java is a trademark of Sun Microsystems.

Linux and Linux FreeS/WAN are trademarks of Linus Torvalds.

Macintosh is a trademark of Apple Computer, Inc.

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

Netscape, Netscape Communicator, Netscape Navigator, and Netscape Directory Server are trademarks of Netscape Communications Corporation.

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

NetWARE, NDS, and Novel intraNetWare are trademarks of Novell, Inc.

OPENView is a trademark of Hewlett-Packard Company.

SafeNet/Soft-PK Security Policy Database Editor is a trademark of Information Resource Engineering, Inc.

SecurID and Security Dynamics ACE Server are trademarks of RSA Security Inc.

SPECTRUM is a trademark of Cabletron Systems, Inc.

VeriSign is a trademark of VeriSign, Inc.

All other 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

This document describes the Nortel VPN Router tunneling protocols and provides configuration information and advanced WAN settings.

Before you begin

This document is for network managers who install and configure the Nortel VPN Router. This document assumes that you have experience with windows-based systems or graphical user interfaces (GUIs) and that you are familiar with network management.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)
: Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering 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 ({})
: Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering 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 ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering 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 (. . .)

Indicate 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, the words are connected by an underscore.

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 entering 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 — Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration.
- *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 — 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.

Printed technical manuals

To print selected technical manuals and release notes for free, directly from the Internet, go to www.nortel.com/documentation, find the product for which you need documentation, then locate the specific category and model or version for your hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web site at www.adobe.com to download a free copy of the Adobe Reader.

How to get help

This section explains how to get help for Nortel products and services.

Finding the most recent updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for updates to the most recent documentation and software for Nortel VPN Router , click one of the following links.

Link	Web site
Most recent software	Nortel page for **VPN Router** software located at support.nortel.com/go/main.jsp?cscat=SOFTWARE&poid=12325
Most recent documentation	Nortel page for **VPN Router** documentation located at support.nortel.com/go/main.jsp?cscat=DOCUMENTATION&poid=12325

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can perform the following activities:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to the following Web site:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

New in this release

The following section details what's new in *Nortel VPN Router Configuration — Tunneling Protocols* (NN46110-503) for Release 8.0.

- "Features" on page 17
- "Other changes" on page 18

Features

For information about feature-related changes, see the following sections:

- "PassGo" on page 17
- "Banner file" on page 17
- "Branch office NAT Traversal" on page 17
- "Forced logoff timer" on page 18
- "Two factor authentication" on page 18

PassGo

Release 8.0 supports PassGo tokens for authentication. For more information, see "IPsec configuration" on page 23.

Banner file

Information about the banner file, new in Release 7.0, is modified for clarity. For more information, see "Configuring group IPsec settings" on page 29.

Branch office NAT Traversal

Release 8.0 introduces Network Address Translation (NAT) Traversal support for branch office tunnels. For more information about NAT Traversal, see "IPsec settings configuration" on page 24.

Forced logoff timer

Release 8.0 increases the upper limit of the forced logoff timer to 120 hours (5 days). The default is 0, which means the option is turned off. The possible range is 00:00:00 to 119:59:59. For more information, see "Configuring IPsec client selections" on page 48.

Two factor authentication

Beginning with Release 8.0, you can select two methods of IPsec authentication for a branch office or user tunnel connection. For more information, see "Two factor authentication" on page 24.

Other changes

For information about changes that are not feature related, see the following section:

- "Document changes" on page 18

Document changes

This document is changed to comply with Nortel writing conventions.

Chapter 1
Overview of tunnel protocols

The VPN Router uses the Internet and remote connectivity to create secure Virtual Private Networks (VPN). Remote connectivity through a public data network (PDN) requires a protocol for safe transport and a connection from the remote user PC to the PDN. The VPN Router uses the most popular tunneling protocols: IP security (IPsec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Layer 2 Forwarding (L2F).

To form a tunnel, the following actions occur:

- The remote user establishes a connection with the PDN point-of-presence (POP), typically through an Internet Service Provider (ISP).
- After the IP connection starts, the remote user launches a VPN connection that specifies a connection to a VPN Router. The VPN connection specifies the IP address or fully qualified domain name (DNS name) of the public interface on the VPN Router. This VPN connection can use either the PPTP or the IPsec tunneling protocol.
- Tunnels built using L2F are slightly different. The tunnel begins at a piece of networking equipment, the network access server (NAS), located at the ISP instead of the remote user PC. The user dials into the ISP with a telephone number that causes an L2TP or L2F tunnel to connect directly to a specific corporation. This process is similar to a traditional remote dial service except that the ISP maintains the modems, not the corporation.

All tunneling protocols are enabled on the public and private networks by default. Because tunnels encrypt the data, the default setting guarantees that all interactions with the VPN Router are private. By leaving IPsec, PPTP, L2TP, and L2F enabled on the private side, you can establish tunneled connections to the VPN Router using one of the tunnel types from within your corporation. 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 your only public tunneling protocol, disable the public selection for PPTP, L2TP, and L2F.

Configuring tunnel access to the VPN Router

To configure tunnel access to the VPN Router

1. Choose **Services, Available**.

   The Services window appears.

2. Select the tunnel type.

For more information about tunnel configuration, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500). See the appropriate chapter in this document for procedures about how to change default tunnel protocol settings.

Interoperability examples

You can configure branch office tunnels between Nortel VPN Router and other products. For configuration examples, see the documents in “Interoperability example documents” on page 20. You can find these documents at www.nortel.com/documentation. Choose **Security & VPN**, and then click the VPN Router hardware platform that you use. Under **Operations**, select **Technical Tips**.

Table 1 Interoperability example documents

Document number	Document title
TT031024	Contivity Secure IP Services Gateway - Branch Office Tunnels with Contivity 221 and 251
TT040202	Contivity Secure IP Services Gateway - Contivity – Cisco PIX IPSec peer-to-peer branch office tunnel using preshared key authentication
TT040216	Contivity Secure IP Services Gateway - Contivity – Cisco PIX IPSec peer-to-peer branch office tunnel using certificates authentication
TT040430	Contivity Secure IP Services Gateway - Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication
TT-0412405a	Nortel VPN Router – Cisco VPN Concentrator branch office tunnel using pre-shared key

Table 1 Interoperability example documents (continued)

Document number	Document title
tt-0602402a	Nortel VPN Router – Cisco IOS branch office tunnel using pre-shared key authentication
tt-0603401a	Nortel VPN Router – Cisco IOS branch office tunnel using certificates authentication

Chapter 2
IPsec configuration

Nortel, and other third-party vendors, support the IP security (IPsec) tunneling protocol. IPsec is a standard that offers a strong level of encryption, integrity protection, the Internet Engineering Task Force (IETF)-recommended Internet Security Association and Key Management Protocol (ISAKMP) and Oakley Key Determination protocols, and token codes from SecurID and PassGo. IPsec offers the following features:

- Nortel, and other vendors, provide client support. You do not require special Internet service provider (ISP) services.
- Support for IP address translation by using encapsulation and packet-by-packet authentication.
- Strong encryption and token codes

  Encryption methods include the Data Encryption Standard (DES), Triple DES, and the Advanced Encryption Standard (AES). IPsec supports token codes from SecurID.

- IPsec offers integrity protection by using Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA).

Nortel provides the IPsec remote access user client software on the CD that came with your VPN Router. You can install the client software on a network server for your remote users to download. The client software is a Microsoft application available for Windows 2000 and XP releases. The software includes online Help.

At the time this document is released, Nortel provides a Microsoft Vista compatible client only by download from www.nortel.com/support. The only currently available client that supports Vista is version 6.07. A new Vista client is due to release in Q4, 2008.

The self-extracting installation files Triple DES are labeled accordingly on the CD. The installation is simple; the self-extracting installation includes everything necessary to create IPsec tunnels with the VPN Router.

- AES128-SHA1
- AES256-SHA1

- AES128 Diffie Hellman Group 2, 5, and 8
- AES256 Diffie Hellman Group 5 and 8

For more information, see the instructions included as part of the client installation.

Note: AES256 SHA1 with AES Diffie Hellman Group 8 provides better performance than AES256 SHA1 with Internet Key Encryption (IKE) AES256 Diffie Hellman Group 5.

This chapter includes the following topics:

- "Two factor authentication" on page 24
- "IPsec settings configuration" on page 24
- "AES-256 configuration for branch office tunnels" on page 42
- "IPsec client features" on page 44

Two factor authentication

Beginning with Release 8.0, you can select two methods of IPsec authentication for a branch office or user tunnel connection. The available authentication methods for tunnels remains the same: text or hexadecimal preshared key and certificates for branch office tunnels, or user name and password and certificates for user tunnels. Instead of using only one authentication type for every incoming connection, the router performs two authentication steps. For more information about authentication, see *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600).

IPsec settings configuration

To configure the VPN Router for IPsec tunneling, you first configure the parameters on a global level on the Services, IPsec window. You can individually configure IPsec parameters for groups, users, and branch offices from the Profiles menu.

An asymmetric branch office tunnel (ABOT) initiator tunnel is a Layer 3 service supported over virtual circuits. The ABOT initiator tunnel is an IP-based interface that you must configure for virtual circuit descriptors. You must configure one side as the initiator and the other as the responder. Only the initiator can bring up the tunnel. If the connection type is initiator, you do not need to define a local endpoint. Configure ABOT for an IPsec tunnel type only, and provide an initiator ID for the IPsec authentication.

- Global IPsec settings

  Globally configure IPsec from the Services, IPsec menu path.
- Group IPsec settings

  Configure group IPsec settings from the Profiles, Groups, Edit, IPsec menu path.
- Branch office connection IPsec settings

  Configure branch office IPsec settings from the Profiles, Branch Office, Edit Connection, IPsec tunnel type menu path.
- Branch Office group IPsec settings

  Configure branch office group IPsec settings from the Profiles, Branch Office, Edit Group, IPsec menu path.

Configuring global IPsec settings

To configure IPsec settings

1. Choose **Services, IPsec**.

   The IPsec Settings window appears.
2. Configure IPsec authentication. Select **User Name and Password/ Pre-Shared Key**, or **RSA Digital Signature**.

   The peer-to-peer tunnels support the following text and hexadecimal functions:

   - Text: The preshared key supports the characters: a to z, 0 to 9, and \`~!@$%^&*()_-{ }[|:;\<>./#,]+= with a length of 32 characters.

- Hexadecimal: The preshared key accepts digits from 00 through 7FFFFFFF.

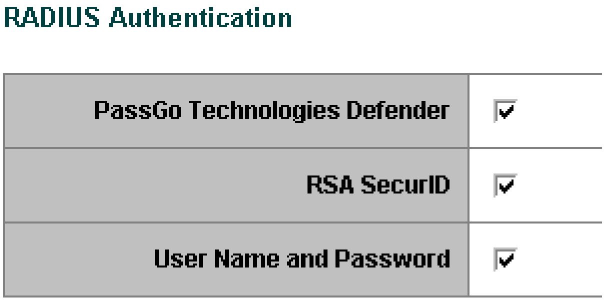
The ABOT initiator and responder support the following ID, text, and hexadecimal functions:

- The Initiator ID and password support the following characters: a - z, 0-9, and _-.:/,\!@.
- ID: The maximum length is 127.
- Text: The preshared key maximum length is 32.
- Hexadecimal: The preshared key supports digits from 00 to 7FFFFFFF.

3 Configure IPsec RADIUS authentication for the connection. Select the authentication types that your RADIUS Server supports and that you expect to use:

- PassGo Defender—PassGo Defender authentication
- RSA SecurID—RSA SecurID authentication
- User Name and Password—User name and password authentication; the user name and password are encrypted

Figure 1 Radius Authentication screen



RADIUS Authentication

PassGo Technologies Defender	☑
RSA SecurID	☑
User Name and Password	☑

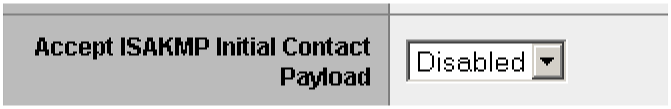
4 Configure encryption for the connection. Select the appropriate box to enable the encryption methods. The encryption methods appear in order of strength, from strongest to weakest.

> **Note:** Triple DES encryption requires more processing power than DES, which potentially reduces the performance of the switch. AES provides stronger encryption than 3DES and requires less processing power than 3DES, which provides a potential performance improvement for branch office tunnels.

5 Configure the IPsec IKE Encryption and Diffie-Hellman Group settings for the connection. If you select more than one encryption type, you can select the encryption to use on an individual group basis under **Profiles > Groups> Edit > IPsec** or **Profiles > Branch Office**.

6 Configure ISAKMP Packet Queue Management for the connection. Select the check box to enable this feature.
The following figure shows the accept ISAKMP initial contact Payload.

Figure 2 Status of ISAKMP Initial Contact Payload



Accept ISAKMP Initial Contact Payload	Disabled

7 Specify the timeout value for the ISAKMP negotiation packets in the queue. The default value is 14 seconds. Shortening the default time can result in performance degradation.

Select the **Drop Duplicate Initialization Requests** box to drop duplicate ISAKMP packets from the queue.

8 Enable Network Address Translation (NAT) Traversal for user tunnels, branch office tunnels, or both. Configure the additional IPsec NAT Traversal settings only for user tunnel connections. Devices on a private network use NAT Traversal to access the Internet simultaneously without each requiring its own external IP address. To use NAT Traversal for user tunnels, you must define a UDP port. The VPN Router uses the UDP port for all client connections. This port must be a unique and unused private network port within the range 1024 to 49 151. For more information about NAT, see *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508).

By default, NAT Traversal is disabled and no UDP port is defined.

9 Configure the authentication order. The IPsec, Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Layer 2 Forwarding (L2F) tunnel types each use an authentication order table, which lists the corresponding servers, authentication types, associated groups, and actions. The router queries the Lightweight Directory Access Protocol (LDAP) server first, and then the Remote Authentication Dial-In User Service (RADIUS), if applicable.

10 Configure load balancing. Select the **Enabled** box to enable load balancing of one VPN Router with an alternate VPN Router. Type the management IP address of the alternate host. Load balancing is a protocol between two VPN Routers that exchanges information about the number of sessions for each connection priority and the CPU utilization. During connection establishment, the first VPN Router determines which of the two VPN Routers services the session. The VPN Router and the alternate VPN Router must be in the same location (they must be in communication by using the private interface). You can load balance more than two VPN Routers if you use a Nortel Application Switch.

11 Configure the failover settings. Select the **Enabled** box to enable fail-over of the selected VPN Router. The router detects a fail-over condition in approximately two minutes. After a connection terminates or is lost, the client attempts to connect to the first-listed fail-over VPN Router. The client tries each VPN Router in succession and if no connection establishes, it stops.

Configuring group IPsec settings

To configure group IPsec settings

1. Choose **Profiles**, **Groups,** and then click **Edit** for the group you want to configure.

   The Groups > Edit window appears.

2. In the IPsec section, click **Configure**.

   The Groups > Edit > IPsec window appears.

3. Click **Configure** for a specific parameter to make changes to that parameter. Click **Configure** in the **All Fields** section to edit all parameters at the same time. Click **Inherited** to set all fields to their inherited values.
4. Configure **Split Tunneling**. All IPsec client traffic tunnels through the VPN Router by default. Use Split Tunneling to configure specific network routes to download to the client. Only these network routes go through a tunnel; other traffic goes to the local PC interface. With Split Tunneling you can print locally, for example, even if you tunnel into the VPN Router.
5. Configure Split Tunnel and inverse Split Tunnel networks. Select a network to which you want to send encrypted tunnel traffic only. You designate these networks from the Profiles, Networks menu path.
6. Use the Client Selection section to configure your VPN Router to accept tunnel connections from third-party clients, in addition to the Nortel VPN Client. For more information about supported third-party clients, see *Nortel VPN Router Release Notes — Server Software Release 8.0* (NN46110-403).

   Specify the **Allowed Clients** parameter. Use the list to select the type of clients that can create tunnels to the VPN Router.

7. Select the **Allow undefined networks for non-Nortel VPN Router clients** parameter. Enable this selection so supported third-party clients can create IPsec tunnels to internal networks. Nortel recommends that you not allow undefined networks for third-party clients, and use Split Tunneling instead. Nortel VPN Clients ignore this selection.
8. Configure **Authentication**. Choose from the following options:

- Configure **Database Authentication (LDAP)**. Enable the LDAP **User Name and Password** to authenticate user identity or use an RSA Digital Signature. The router performs authentication with a protected user ID and password through the ISAKMP.
- Use Entrust certificate authentication. From the **Default Server Certificate** list, select a server certificate.
- Configure **RADIUS and LDAP Proxy Authentication**. This method is a two step process where the VPN Router authenticates the remote user with the user name and password authentication mechanism, PassGo or SecurID hardware or software tokens, and the client uses the group ID and group password to authenticate the identity of the VPN Router.

— RADIIUS and LDAP Proxy Information

Use two-factor authentication in combination with RADIUS or LDAP Proxy (or both), where the Group ID and Group password fields must be left blank, and the RSA SecureID (and PASSGO) must be unchecked.

In cases where the two-factor authentication works with RADIUS and LDAP Proxy, the credentials received from the client that is attempting to connect are only checked against a RADIUS or LDAP Proxy server when there is no local account found with the Subject Distinguished name corresponding to the client, and when the CA certificate corresponding to the Group that the client belongs to has the "Allow all" feature enabled.

— User Name and Password

Click to enable the RADIUS or LDAP proxy user name and password to authenticate user identity. The router performs authentication with a protected user ID and password through the ISAKMP.

— PassGo Defender

Click to enable the PassGo Defender challenge response token security authentication. The PassGo Defender uses a personal identification number (PIN) and password, with a challenge response security dialog, to authenticate user identity.

— RSA SecurID

Click to enable the RSA SecurID token security authentication. The SecurID uses a PIN and the current code generated by a token assigned to the user to authenticate user identity.

Type the group ID and password, which are encrypted for transmission. The group ID provides access to the VPN Router. Subsequent LDAP and RADIUS authentication verify against the user ID

Type and confirm the group password, which provides access to the VPN Router. Subsequent LDAP and RADIUS authentication verify against the user password.

Note: The group ID and user ID must not be the same.

9 Configure **Encryption**. Select the box to enable the supported encryption methods.

The encryption methods appear in order of strength, from strongest to weakest. All of the encryption methods ensure that the packet originates from the original source at the secure end of the tunnel. Some of the encryption types do not appear on non-US models that are restricted by US Domestic export laws. Also, Message Digest (MD5) provides integrity that detects packet modifications.

Note: Triple DES encryption requires more processing power than DES, potentially reducing the performance of the switch. AES provides stronger encryption than 3DES, and requires less processing power than 3DES, providing a potential performance improvement for Branch Office tunnels.

10 Select the Diffie-Hellman Group level to apply to IKE encryptions.

Note: The choice of the IKE encryption algorithm does not affect the choice of the encryption algorithm used to encrypt data in IPsec. For example, you can use DES to encrypt the IKE exchanges, and then negotiate Triple DES for use in IPsec.

The IPsec Settings window contains an IKE Encryption and Diffie-Hellman Group section.

11 For the **Accept ISAKMP Initial Contact Payload** list**,** select **Enabled** to tear down the existing connection if an incoming connection uses the same user ID as the existing connection. This option is disabled by default.

12 For the **Perfect Forward Secrecy (PFS)** list, select **Enabled**. With PFS, keys do not derive from previous keys. PFS ensures that if one key becomes compromised, this action does not result in the compromise of subsequent keys.

13 Configure **Client Auto Connect**. The Client Auto Connect feature lets remote Nortel VPN Clients connect their IPsec tunnel sessions in a single step. With Auto Connect, client users simply click on the desired destination, for example, a Web page on the private internal network. This action first starts their ISP connection, and then makes the tunnel connection to the VPN Router, and finally makes the connection to the requested destination.

a Select **Any Network Traffic** to use the autoconnect feature for all client connection requests to authorized destinations. After the client detects network activity on the user workstation, a tunnel connection automatically launches to the VPN Router.

b Configure the **Specify Networks** and **Domains** parameters. Use this selection to limit autoconnection use to specific domains or networks. Select the authorized domains or networks.

Use the Domains selection to designate specific domains or host names that trigger the autoconnect feature. Select None if you want to limit the autoconnection feature to specific networks, which you specify in the following Networks field.

Use the Networks selection to designate specific networks that trigger the autoconnect feature. The networks configuration must exist. Select None if you do not want to designate networks.

14 Configure the Banner setting

a In the **Banner** box, type the banner text to customize an enterprise logon banner for the Nortel VPN Client.

This banner appears at the top of the client upon logon.

VPN Router supports two different banner mechanisms. The banner is an optional message that if enabled, appears on the client side of the VPN after the remote user logs on. You can use the banner to display a message.

You can create the banner message in the Banner box or in a banner file. Alternatively, you can combine both banners.

b In the **Display Banner** list, select **Enabled**.

c Optionally, you can create a banner file to provide a larger banner message to Nortel VPN Client users. In the **Banner File** box, type the name of the text file.

The banner file must conform to the 8.3 DOS naming conventions of the switch with a maximum file size of 49 Kb. More than one banner file can exist because you configure it by group. Multiple groups can share a file.

You can create the banner file as a plain text or rich text file using a word processor. Because the banner file can use rich text, you can apply special formatting, for example, bold or colors, to the banner text. Use the File Transfer Protocol (FTP) to save the file to the /ide/system/config directory of the switch (ideX is the boot device, either ide0 or ide1).

If you type information in both the Banner box and the Banner File box and the banner file is a plain text file, the Nortel VPN Router joins them together and sends the combined banner to the Nortel VPN Client. The combined banner appears in the normal security banner dialog box.

If you type information in both boxes and the banner file is a rich text file, the combined banner must be a valid rich text file. To create a valid combined file, you must type the opening {rtf tag, but not the closing } tag in the Banner box. In the banner file, do not use an opening {rtf, but do use the closing }. The combined banner appears in a rich text dialog box.

The banner file requires Nortel VPN Client v7.01 or greater. If a client earlier than v7.01 connects, the router sends only the first 1 Kb of the combined banner data, as this is the limit these clients can receive.

15 Configure the **Client Screen Saver Password Required** parameter. Configure this security feature to force the client to use a password in association with a screen saver. The default is Disabled. If you enable this

parameter and the user leaves the system and connects to a tunnel, the system becomes locked out of the tunnel after the screen saver starts. The end user enables this feature from the Start, Settings, Control Panel, Display, Screen Saver Password Protected box.

16 Configure the **Client Screen Saver Activation Time**. Use this setting together with the Client Screen Saver Password Required setting. This value defines the maximum time (in minutes) before the client screen saver activates. The default is 5 minutes.

17 Configure **Client Failover Tuning**

a Select the **Enabled** box to enable client fail-over. Client fail-over uses small packets to check and maintain, or keep alive, the connection between the client and the VPN Router.

b In the **Interval** box, type the time interval that the client waits between VPN activity checks. Nortel recommends that you use a low interval if users connect by using the client. Use a higher setting for situations such as when you use a lease line and the provider bases charges on traffic.

c Specify the maximum number of retransmissions. This value is the number of times that the client retransmits a keepalive packet to the VPN Router to check for connectivity.

18 You can optionally enable the antireplay service. While the default handling requires the sender to increment the sequence number used for antireplay, the service is effective only if the receiver checks the sequence number.

Note: You must disable antireply if you use IPsec tunnels over LANs or WANs (the typical usage). If you enable antireply, it causes incorrect DiffServ sorting. Antireply does not acknowledge DiffServ and uses it own methods to discard packets, which adversely affects the DiffServ sorting.

19 Enable mobility support for IPsec.

20 Type the number of seconds for the **Maximum Roaming** time. The default is 120 seconds.

21 Enable **Persistence** for the session.

22 Type the number of minutes for **Session Persistence Time**. The default is 60 minutes.

23 Enable the **Allow Password Storage on Client** parameter. You can allow client systems to save the logon password in its password list, or you can require that remote users enters the password each time they request authentication and access to an IPsec tunnel. Click **Enable** to allow client systems to save the logon password.

Note: If you use certificates, you cannot save the password on the client.

24 Enable **Compression**.

25 Configure the **Rekey Timeout**. Limit the lifetime of a single key used to encrypt data or else you compromise the effectiveness of a single session key. Use the Rekey Timeout setting to control how often new session keys exchange between a client and a server. Configure the Rekey Timeout setting to no less than 1 hour. The default is 08:00:00 (8 hours); a setting of 00:00:00 disables the Rekey Timeout setting. The maximum setting is 23:59:59.

26 Configure the **Rekey Data Count**. You can choose to set a Rekey Data Count depending on how much data you expect to transmit by using the tunnel with a single key. The default is 0 kbytes; a setting of 0 disables the Rekey Data Count.

27 Configure the **Domain Name**. Use this parameter to specify the name of the domain to use while an IPsec tunnel connects. Specify the domain name to ensure that domain lookup operations point to the correct domain. This option is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server maps to the correct domain.

After a tunnel connects, the remote client registry updates to use the specified domain. After the client disconnects the tunnel, it uses the original domain of the remote client.

28 Type the address of the primary Domain Name System (DNS) server on your private network. The server provides this DNS address to tunnel clients at setup and uses it through the tunnel. The DNS server translates textual host names into IP addresses for the VPN Router. For example, DNS can translate the fully qualified host www.mycompany.com to its IP address 192.19.2.33.

The primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the primary DNS server is unavailable, the user requests service of the secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers. Always use the IP address for setting a DNS server host instead of a domain name.

29 Type an address for the secondary Domain Name System (DNS) server. If the primary DNS server is unavailable, service requests go to the secondary DNS server.

30 Type an address for the primary Windows Internet Naming Service (WINS) server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Use a WINS server to access normal Windows file and print services through a tunnel connection.

Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual LMHOSTS file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

The primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the primary WINS server is unavailable, service requests go to the secondary WINS server. Always use the IP address instead of a name to configure a WINS server host.

Note: If you do not specify a WINS server, the client broadcasts for NetBIOS names.

31 Type an address for the secondary WINS server; if the primary WINS server is unavailable, service requests go to the secondary WINS server.

32 Configure the Nortel Client Requirements settings.

a In the **Minimum Version** list, select the minimum version of Nortel VPN Client required.

b In the **Action** list, select the action to take upon detection of a noncompliant client.

c In the **Message** box, type a message giving users the URL for a Web site or FTP site from which they can download the required version of the Nortel VPN Client software.

d Select a filter to apply from the list of available filters.

e Click on the **New Filter** link to create a new filter, if needed.

33 Configure the **Client Policy**. Select a client policy as appropriate. Client Policy prevents potential security violations that can occur when you use the Split Tunneling feature. With Split Tunneling client data travels either through a tunnel to the enterprise network or directly to the Internet.

34 Enable or disable the **IPsec Transport Mode Connections** parameter.

35 From the **Client Dynamic DNS Registration** list, select **Enabled** or **Disabled**. You can only use this parameter with the Nortel VPN Client. Also, your DNS server must support Dynamic DNS and allow Dynamic DNS registration. Type the domain name in the **Domain** box.

Configuring branch office connection IPsec settings

To configure branch office IPsec settings

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

The Branch Office window appears.

2 Select the associated connection, and then click **Configure**.

The Connection Configuration window appears.

3 Use the **Connection Type** list to change the tunnel type for the connection. To configure IPsec settings, select **IPsec** as the tunnel type. The default type is IPsec.

Note: 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.

4 Configure authentication attributes in the **Authentication** section of the window. Use this portion of the window to configure the authentication between the local and remote branch office VPN Routers. The options that appear in this window depend on whether you use an IPsec, PPTP, or L2TP tunnel type. You can select one of the following IPsec authentication methods:

- Text Pre-Shared Key
- Hex Pre-Shared Key
- Certificates
- DUAL: Certificates and Text Pre-Shared Key
- DUAL: Certificates and Hex Pre-Shared Key

5 Type the preshared key. This value is an alphanumeric text or hexadecimal string that is used between the local and remote branches for authentication. In order for authentication to occur, you must use the same preshared string on both the local and remote branch offices.

6 Configure the **Certificates s**ection of the window. Associate certificates with each endpoint VPN Router to provide mutual authentication between two connections. The certificate portion of the window includes information about the remote branch office system, the authority that issued the certificate, and the certificate identification.

7 Select a **Valid Issuer Certificate Authority** from the list. This CA is the issuer of the remote peer certificate or a higher level CA in the remote peer certificate hierarchy. The CA must use the trusted flag by using the certificates window. If you use a CA hierarchy, you must import all intermediary CAs below the trusted CA to the VPN Router.

8 Configure the **Remote Name**. This value is the name of the remote peer that initiates the tunnel connection. You can use either a Subject Distinguished Name (Subject DN) or a Subject Alternative Name to uniquely identify the remote branch office system. If you specify both a full subject DN and a subject alternative name on this window, the remote peer can use either identity form after it makes a connection.

9 Configure the **Subject Distinguished Name.** If you use a distinguished name to identify the remote branch office site, you can choose to type the DN as either a relative distinguished name or a full distinguished name. The DN entered here must exactly match the DN in the remote peer certificate.

a Configure the **Relative Distinguished Name**. The Relative distinguished name uses the following supported components:

Note: Do not include the attribute type as part of your entries in the Relative section. For example, for a name of CN=MyVPN Router, your entry is MyVPN Router (without the CN attribute type).

- Common Name—Enter the Common Name associated with the server.
- Org Unit—Enter the Organizational Unit associated with the server.
- Organization—Enter the Organization associated with the server.
- Locality—Enter the Locality in which the server resides.
- State/Province—Enter the State or Province in which the server resides.
- Country—Enter the Country in which the user resides.

b Type the **Full Distinguished Name**. You can directly type the Full Distinguished Name (FDN) in this box rather than typing the individual components in the previously described Relative distinguished name boxes. For example:

```
CN=MyVPN Router, O=MyCompany, C=US
```

c Configure the **Subject Alternative Name**. You can optionally use a Subject Alternative Name in place of a Subject DN, and specify the format of the name. The following formats are acceptable:

- Email Name (for example, net_admin@company.com)
- DNS Name (for example, VPN Router.cleveland.company.com)
- IP Address (for example, 192.168.34.21)

10 Specify the **Local Identity**. The Local Identity is the VPN Router name that you want to use to identify itself when it initiates or responds to a connection request. You can use either a Subject Distinguished Name (Subject DN) or a Subject Alternative Name to uniquely identify your system. If you select a subject alternative name from the VPN Router certificate, that identity is used in place of your VPN Router subject DN when it communicates with peers.

Note: Your VPN Router server certificate only uses subject alternative names if your CA issued the certificate with the alternative names. For example, with the Entrust PKI the VPN connector can issue certificates with DNS names, IP addresses, or e-mail alternative names.

a Configure the **Server Certificate**. Click the list to view all certificates issued to the server.

Configuring branch office group IPsec settings

To configure branch office group IPsec settings

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

The Branch Office window appears.

2 Select the group, other than Base, and then click **Configure**.

The Branch Office > Edit Group window appears.

3 In the IPsec section, click **Configure**.

4 Click **Configure** for a specific parameter to make changes to that parameter. Click **Configure** in the **All Fields** section to edit all parameters at the same time. Click **Use Inherited** to set all fields to their inherited values.

5 In the **Encryption** section, click **Configure**, and then select the appropriate box to enable the encryption methods for this group.

Note: Triple DES encryption requires more processing power than DES, potentially reducing the performance of the switch. AES provides stronger encryption than 3DES, and requires less processing power than 3DES, providing a potential performance improvement for Branch Office tunnels.

The encryption methods appear in order of strength, from strongest to weakest. All of the following encryption methods ensure that the packet came from the original source at the secure end of the tunnel. Some of the encryption types, do not appear on non-US models that are restricted by US Domestic export laws. Also, Message Digest (MD5) provides integrity that detects packet modifications.

Note: Existing profiles do not automatically change to reflect a change in the global settings. For example, if you change the global settings for IKE Diffie-Hellman Group, you can invalidate IKE Diffie-Hellman Group selections. You must choose Profiles, Groups or Profiles, Branch Office to check IKE Diffie-Hellman Group settings in each group. You must globally select an IKE Diffie-Hellman Group that you select in user groups.

If two devices use different encryption settings, the two devices negotiate downward until each uses a compatible encryption.

6 Select the **Diffie-Hellman Group level** to apply to IKE (Internet Key Exchange) encryptions.

> **Note:** The choice of the IKE encryption algorithm does not affect the choice of the encryption algorithm used to encrypt data in IPsec. For example, one can use DES to encrypt the IKE exchanges, and then negotiate Triple DES for use in IPsec.
>
> The Services, IPsec window contains a section labeled IKE Encryption and Diffie-Hellman Group. This section provides two choices for use with IPsec.

7 Specify if the router sends the vendor ID payload during ISAKMP negotiation.

8 Specify if the router supports the aggressive mode to establish the security association (SA).

9 Enable **Perfect Forward Secrecy (PFS)**. With PFS, keys do not derive from previous keys. PFS ensures that if one key becomes compromised, this action does not result in the compromise of subsequent keys.

10 Enable **Compression** for IPsec tunneling.

11 Specify the **Rekey Timeout.** Limit the lifetime of a single key used to encrypt data or else you compromise the effectiveness of a single session key. Use the Rekey Timeout setting to control how often new session keys exchange between a client and a server. Configure the Rekey Timeout setting to no less than 1 hour. The default is 08:00:00 (8 hours); a setting of 00:00:00 disables the Rekey Timeout setting. The maximum setting is 23:59:59.

12 Configure the **Rekey Data Count.** You can choose to set a Rekey Data Count depending on how much data you expect to transmit by using the tunnel with a single key. The default is 0 kbytes; a setting of 0 disables the Rekey Data Count.

13 Configure the **ISAKMP Retransmission Interval**. This value specifies the time interval at which to make the ISAKMP retransmission.

14 Configure the **ISAKMP Retransmission Max Attempts** parameter. This value is the maximum number of attempts to make the ISAKMP retransmission.

15 Configure the **Keepalive Interval**. This value is the polling frequency that determines if a keepalive exchange is needed. The default is one minute. The allowed range is 1 second to 60 minutes. The tunnel uses this interval if the branch connection is Nailed-Up or if you enable Keepalives for on-demand connections.

16 Enable the **Keepalive** (on-demand connections) parameter. Keepalive (on-demand connections) uses a default of disabled. Enable this parameter to quickly detect lost connectivity.

17 Specify the action to take on the IPsec DF bit.

18 Configure Network Address Translation (NAT) Traversal. For more information about NAT Traversal, see *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508).

AES-256 configuration for branch office tunnels

AES-256 is available as an encryption option only if ISAKMP negotiates either Group 5 or 8. Nortel recommends that you use Group 8 as it is more efficient than Group 5. AES-256 is not available for Group 2. If you use Group 2, only AES-128 is available. This restriction prevents the use of AES-256 with relatively weak ISAKMP groups that invalidate the additional security that AES-256 provides. Although AES-256 provides more security than AES-128, it provides poor performance compared to AES-128. Consider these characteristics if you deploy AES-256.

The IPsec Key Exchange group and encryption pairs supported for Branch Office Groups are

- G8 with AES-256/SHA1
- G5 with AES-256/SHA1
- AES-256 data encryption

Configuring AES-256

To configure AES-256

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

The Branch Office window appears.

2 Select **Base** from the Group list.

3 Click **Configure**.

The Branch Office > Edit Group window appears.

4 Click **Configure** in the **IPsec** section.

5 Select **ESP - 256-bit AES with SHA1 Integrity** from the encryption options.

6 Select **256-bit AES with Group 8 (ECC 283-bit field)** from the IKE Encryption and Diffie-Hellman Group list.

Configuring AES-256 with the CLI

This section describes how to access the CLI and configure AES-256.

Accessing the CLI with Telnet

To access the CLI through a Telnet connection, you must enable Telnet on the VPN Router. To access the Nortel VPN Router CLI

1 Start a Telnet session to the VPN Router management IP address, for example:

```
Telnet 10.0.16.247
```

2 Log in to the VPN Router using an account with administrator privileges, for example:

```
Login: admin

Password: <Password>

CES>
```

After you log on, the CLI prompt (CES>) appears, indicating you are in CLI User EXEC mode. You can execute User EXEC mode command or change the command mode to execute other commands.

To configure AES-256-sha1 data encryption

```
CES(config)#bo-group ipsec "/Base"
CES(config)-bo_group/ipsec)#encryption ?
```

- — 3des-md5 Triple DES with MD5 Integrity
- — 3des-sha1 Triple DES with SHA1 Integrity
- — aes128-sha1 ESP - AES 128 with SHA1 Integrity
- — aes256-sha1 256 bit AES with SHA1 Integrity
- — des40-md5 40bit DES with MD5 Integrity
- — des56-md5 56bit DES with MD5 Integrity
- — hmac-md5 Authentication header message code message digest
- — hmac-sha1 Authentication header message code secure hash
- — ike IKE encryption and Diffie-Hellman group for the IPsec tunneling

To configure new IKE Encryption parameters

```
CES(config-bo_group/ipsec)#encryption ike ?
```

- — 128aes-group2 128 bit AES with SHA1 under MODP group 2 (1024-bit prime)
- — 128aes-group5 AES 128 with Group 5 (1536-bit prime)
- — 128aes-group8 AES 128 with Group 8 (ECC 283-bit field)
- — 256aes-group5 AES 256 with Group 5 (1536-bit prime)
- — 256aes-group8 AES 256 with Group 8 (ECC 283-bit field)
- — 3des-group2 Triple DES with group 2 (1024-bit prime)
- — 3des-group7 Triple DES with group 7 (ECC 163-bit field)

3 des56-group1 56bit DES with group 1 (768-bit prime)

IPsec client features

The VPN Router supports the following IPsec client features:

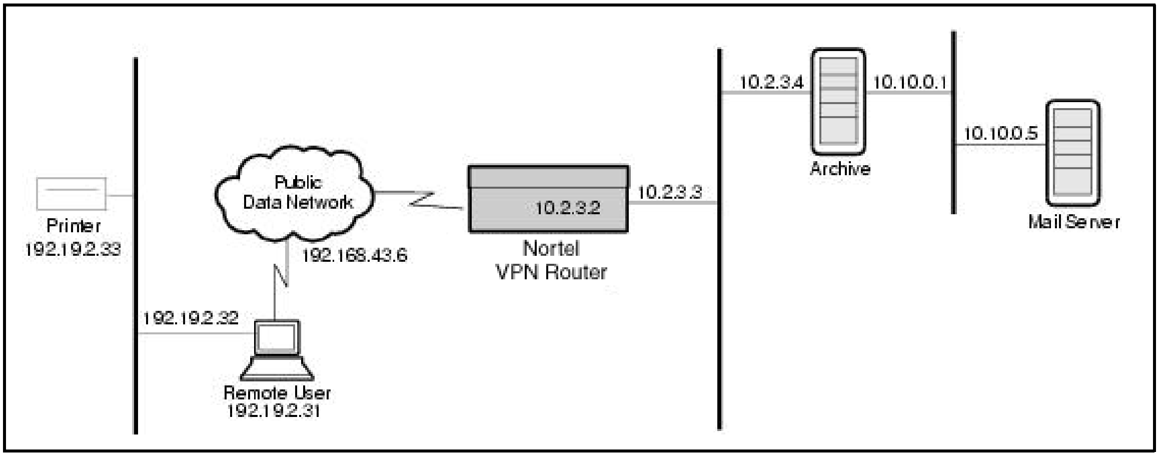
- Split Tunneling
- third-party IPsec clients
- forced logoff

- client failover
- client auto connect
- banner
- password storage
- client screen saver
- client keepalive
- domain name
- client policy

Split Tunneling

All IPsec client traffic tunnels through the VPN Router by default. Use Split Tunneling to configure specific network routes that download to the client. Only these network routes go through tunnels; other traffic goes to the local PC interface. With Split Tunneling, you can print locally, for example, even while you use a tunnel to the VPN Router. "Sample Split Tunneling environment" on page 45 shows a sample Split Tunneling environment.

Figure 3 Sample Split Tunneling environment



"Sample Split Tunneling environment" on page 45 shows Split Tunneling enabled and split tunnel network IP addresses 10.2.3.4 and 10.10.0.5. After a client establishes an IPsec tunnel, these addresses load into the client application.

The remote user, for example, downloads e-mail from the mail server at 10.10.0.5, and downloads a document from the Archive at 10.2.3.4. Next, without exiting the tunnel, the remote user can print the document through the local network interface 192.19.2.32 to the printer at 192.19.2.33. You can enable Split Tunneling through the Profiles, Groups, IPsec Configure, menu path.

You designate which network routes to tunnel through the VPN Router from the Profile, Networks menu path. Next, you associate specific network routes to specific groups through the Groups > Edit > IPsec window by configuring the Split Tunnel Networks field.

The VPN Router takes precautions against violators potentially hacking tunneled information when the VPN Router operates in Split Tunneling mode. The primary precaution drops packets that do not use the IP address assigned to the tunnel connection as its source address. For example, if you use a PPP dial-up connection to the Internet with an IP address of 192.168.21.3, and then you set up a tunneled connection to a VPN Router with an assigned tunnel IP address of 192.192.192.192, packets that attempt to pass through the tunnel connection with a source IP address of 192.168.21.3 (or an address other than 192.192.192.192) drop.

Furthermore, you can enable filters on the VPN Router to limit the protocol types that can pass through a tunneled connection.

To completely eliminate security risks, do not use the Split Tunneling feature.

Third-party IPsec clients

You use the Client Selection feature to configure your VPN Router to accept tunnel connections from third-party clients, in addition to the Nortel VPN Client.

The Client Selection feature provides more flexibility and mobility than previously available to remote users who want to connect to your VPN Router using a client other than the Nortel VPN Client. The alternate method of connecting third-party clients requires you to set up a branch office connection and configure the remote client IP address as the remote VPN Router address. This branch office method binds a client machine to a fixed IP address. This configuration limits users if they need to create tunnels from multiple systems, for example, a work desktop system and a mobile laptop.

With the client selection feature, you establish an account for a remote user, rather than for a remote machine. You configure the account within the realm of remote access users, as you do for the Nortel VPN Client users. This account gives the remote user the freedom to create tunnels to your VPN Router from different machines, and from different locations.

If you configure for the Nortel VPN Client, the VPN Router ignores the Allow undefined networks for non-VPN Router clients parameter for clients that do not use the Nortel VPN Client. The VPN Router never lets Nortel VPN Clients connect to undefined networks. You must define all reachable networks on the Profiles, Networks window.

If you configure for clients that are not Nortel VPN Clients, the router does not support the parameters preceded by an asterisk (*). You must select either the Split Tunneling or Allow undefined networks for non-VPN Router clients option for clients that are not Nortel VPN Clients. If you select both, the VPN Router uses the Split Tunneling feature and ignores the Allow undefined networks selection.

Note: Nortel recommends that you always specify Split Tunneling for groups used by clients other than Nortel VPN Clients. With Split Tunneling enabled, the third-party clients can only connect to networks listed as split tunnel networks on your VPN Router. This list ensures that your VPN Router controls which networks the third-party client can access. If you disable Split Tunneling and enable Allow undefined networks for non-VPN Router Clients, the clients can connect to all internal networks.

The VPN Router supports both preshared key and RSA digital signature authentication methods. For clients that are not Nortel VPN Clients, you must specify at least one of these authentication methods on the Services, IPsec window.

Note: You must ensure that your remote third-party client uses the same Internet Key Exchange (IKE) Phase 1 mode that your VPN Router uses. For preshared key authentication, the VPN Router uses IKE Aggressive mode. If the client only supports IKE Main mode, you must configure a branch office due to the IKE restrictions. For RSA digital signature authentication, the VPN Router uses IKE Main mode.

The VPN Router does not support RADIUS authentication. You can configure a static address for the tunnel from a client other than a Nortel VPN Client, or you can allow the client to use its own IP address as the address used within the tunnel.

Configuring IPsec client selections

To configure the client selection

1. Choose **Profiles**, **Groups**, **Edit**, **Connectivity Configure**.

   The Groups > Edit > Connectivity window appears.

2. Click **Configure** for **Forced Logoff**, and then you can specify a time after which all active users automatically log off for IPsec tunneling. The default is 0, which means the option is turned off. The possible range is 00:00:00 to 119:59:59.
3. Click **OK**.
4. Click **Configure** for IPsec.

   The Groups > Edit > IPsec window appears.

5. Use the Nortel VPN Router Client to disable keepalives between the VPN Router and the client. Client keepalive uses small packets to check and maintain, or keep alive, the connection between the client and the VPN Router. Use this option to disable keepalives when tunneling over an ISDN link, because the link is not always active. If you configure an idle timeout on the VPN Router, and disable keepalives on the client, the client cannot receive notice that the connection closes (due to the idle timeout), when the physical ISDN connection is not active.

Note: If client logs off due to the idle timeout on the VPN Router, and you configure client failover on the IPsec Settings window, that client then fails over to the defined failover server, rather than disconnects as desired.

If you disable the Keep Alive parameter on the client, it prevents the VPN Router and client from exchanging keep alive messages. Therefore, if the connection is lost, the VPN Router does not realize that the client no longer connects until the idle time is reached. If the idle timeout is Never, the resulting connection remains established for a long time, which wastes VPN Router resources.

If you configure the number of logons as 1, which is the default, the client cannot reconnect until the rekey occurs, which by default is in 8 hours. If you enable the Disable Keep Alive parameter on the client, and the connection goes down, you can prohibit the user from reconnecting for 8 hours or more, depending on the rekey value.

Also, do not set the idle timeout to 0. If you lose the connection in this situation, you must delete the session from the VPN Router to reconnect.

6 After a static branch office tunnel fails, all packets flowing through the tunnel drop. The static tunnel failover feature provides a means to detect and recover from these failures. Static tunnel failover interacts with static route API directly to remove and add static routes associated with a remote network. After a tunneling protocol detects a network failure, the static tunnel API removes static routes associated with the remote network from the route table manager.

Note: If you configure static tunnel failover, you need to configure the primary tunnel as nailed up from the Branch Office > Edit > Connectivity window. The cost must be less than that for secondary tunnels.

7 Configure the **Client Auto Connect** parameter to let remote clients connect their IPsec tunnel sessions in a single step. This method is similar to the way Microsoft Dial-Up Networking automatically connects to an ISP after you launch a Web browser. With auto connect, client users simply click on the desired destination, for example, a Web page on the private internal network. This first starts their dialup connection, and then makes the tunnel connection to the VPN Router, and finally makes the connection to the requested destination. What has, in the past, taken three distinct user operations is now accomplished by a single action.

The client auto connect settings specify those network connections that trigger the client autoconnect feature. For example, you can specify that whenever a remote client attempts to connect to a site in the xyz.com domain, the client autoconnect feature starts.

You must configure the VPN Router to allow connections to potential destinations. If you do not properly configure the VPN Router, the remote user can make the connection to the VPN Router, but cannot access the requested destination. For example, the VPN Router filters can deny access to finance.xyz.com, while the client autoconnect starts after the router receives connections to the xyz.com domain. With this configuration, after a remote client tries to access finance.xyz.com, their connection to their ISP, and then to the VPN Router automatically starts. However, because of the filters, the router denies access to finance.xyz.com.

➡ **Note:** After you enable client autoconnect, you must restart the PC on which the client runs and manually make sure the client can connect to the VPN Router.

After the client successfully connects to the VPN Router, the VPN Router downloads the list of networks and domains that trigger the autoconnect feature. This list, stored in the client registry, determines whether a tunnel connection automatically starts if one is not already active.

The following client features apply only to the Nortel VPN Client:

- Banner—You can customize an enterprise logon banner for the Nortel VPN Client by typing text in the space provided or by providing a banner file. This banner appears at the top of the IPsec client after logon.
- Password storage on client—You can allow client systems to save the logon password in this password list, or you can require that a remote user enter the password with each request for authentication and access to an IPsec tunnel. Click on Enable to allow client systems to save the logon password. If you use certificates, you cannot save the password on the client.
- Client policy—Client policy helps prevent potential security violations that can occur if you use the Split Tunneling feature. With Split Tunneling, client data travels either through a tunnel to the enterprise network or directly to the Internet.

- Client screen saver—Setting this security feature forces the client to use a password in association with the screen saver. After you enable this parameter, if the user leaves the system while connected to a tunnel, the system then gets locked out of the tunnel after the screen saver starts.
- Domain name—Use this parameter to specify the name of the domain used while an IPsec tunnel connects. Specify the domain name to ensure that domain lookup operations point to the correct domain. This action is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server maps to the correct domain. After a tunnel connects, the remote client registry updates to use the specified domain. After the client disconnects the tunnel, the client uses the original domain of the remote client.

Configuring coexistence with MS IPsec service

The Nortel VPN Client can coexist with Microsoft IPsec Policy Service. Nortel VPN Client uses NAT Traversal, User Datagram Protocol (UDP) wrapping, to avoid conflicts if you enable or start the MS IPsec policy service.

To configure coexistence with MS IPsec service

1. Choose **Services**, **IPSec**.

   The IPsec Settings window appears.

2. Enable NAT Traversal for user tunnels.
3. Configure the UDP port to an unused port.
4. Click **OK**.

Custom API

The VPN Router supports a third-party encryption Application Programing Interface (API) that adds support to the platform for other encryption types, such as GOST. Because of legal restrictions regarding the source of the encryption code and the existence of certain encryption types, this API provides a means for third party entities to add country-specific encryption types to the platform.

For example, a GOST encryption module developed in one country does not work in another country. Each module must be country-specific.

The API communicates with an encryption module that a third-party vendor provides and installs. Nortel verifies and adds a digital signature on the module. The VPN Router recognizes only modules with the Nortel digital signature. As of Version 7.0 VPN Router software, a module is available through CAN LLC in Moscow, Russia, that enables the encryption over branch-to-branch tunnels. Only CAN provides and installs the modules.

Note: The API exists in the standard shipping software starting with Version 7.0. Encryption modules do not ship with the software.

The custom API directory is under /ide0/plugins.

Enabling the custom API

To enable the custom API:

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

The Branch Office window appears.

2 Select the group you want to edit, and then click **Configure**.

The Branch Office > Edit Group window appears.

3 Click **Configure** for IPsec.

4 In the **IKE Encryption and Diffie-Hellman** section, click **Configure**.

5 Select **Custom group provided by a plugin**.

6 Enable the **Vendor ID** parameter.

Chapter 3 PPTP configuration

Nortel supports the Point-to-Point Tunneling Protocol (PPTP). The Microsoft PPTP client is available with Windows 2000 and XP. Network TeleSystems (www.nts.com) provides tunneling product support for Windows 3.1 and Macintosh operating systems.

You can obtain the PPTP client upgrade for Windows directly from Microsoft (www.microsoft.com). This site also provides installation instructions.

The PPTP client software is on the Nortel VPN Router CD and built into the Windows XP operating system. PPTP offers the following features:

- A range of clients can make connections without special ISP service requirements.
- The PPTP client is available for the most common client operating systems.
- PPTP supports IP address translation using encapsulation, support for IPX tunneling, and RC4 encryption (either 56- or 128-bit, within the limits of United States export law).

Use nested tunnels to create a PPTP end user tunnel inside an IPsec branch office tunnel or an asynchronous branch office tunnel. You can use a nested tunnel from within the private network or from the public side. You can individually log off nested tunnel sessions from the Status, Sessions, Active Session window.

This chapter includes the following topics:

- "Configuring PPTP settings" on page 54
- "Configuring group PPTP settings" on page 55
- "Configuring branch office connection PPTP settings" on page 57

Configuring PPTP settings

You can change the default values for PPTP settings at one of these locations:

- Services, PPTP
- Profiles, Groups, Edit, PPTP
- Profiles, Branch Office, Edit Connection, PPTP Tunnel Type

To change global PPTP settings

1 Choose **Services, PPTP**.

The PPTP Settings window appears.

2 Configure the authentication settings. Use PPTP settings to select a specific authentication server type, for example, Remote Authentication Dial In User Service (RADIUS). You can specify a combination of the following authentication schemes for each server type: Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), Password Authentication Protocol (PAP), or None.

➡ **Note:** Not all RADIUS servers support all forms of authentication. Failure to match PPP authentication methods with RADIUS server capabilities results in user-authentication failures. Check the RADIUS documentation from your vendor for additional information.

3 Configure the PPP Multilink section. Use the list to enable or disable the PPP Multilink. Clients use a PPP Multilink to open multiple PPP connections to a host. (For more information about PPP Multilink, see RFC 2701.)

4 Configure the authentication order. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The router queries the Lightweight Directory Access Protocol (LDAP) server first, and then RADIUS, if applicable.

Configuring group PPTP settings

To change group PPTP settings

1 Choose **Profiles**, **Groups**, and then click **Edit** for the associated group that you want to configure.

The Groups > Edit window appears.

2 Click **Configure** in the **PPTP** section of the window.

The Groups > Edit > PPTP window appears.

3 Click **Configure** for a specific parameter to make changes to that parameter. Click **Configure** in the **All Fields** section to edit all parameters at the same time. Click **Use Inherited** to set all fields to their inherited values.

4 Select one or more of the **PPTP Authentication** methods.

5 Enable the PPTP Microsoft Point-to-Point Compression (MPPC) packet compression. Use compression if you select encryption on analog modems because encryption renders the compression of a modem ineffective, and it can severely affect the performance of compressible applications. Also, compressing data before transmission makes more efficient use of lower speed network links.

Use data compression in most typical situations. Users with cable modems or *x*DSL connections to the ISP, or local on the LAN, do not compress packets. The speed of the link, relative to the rate of compression and the benefit of compression before encryption, is negligible or does not increase performance.

Also, the router cannot compress some data, for example, a previously compressed file does not lend itself well to additional compression.

6 Configure the **Use Client-Specified Address** parameter. If you enable this parameter, the VPN Router accepts the IP address from a remote user system during tunnel setup. This option is disabled by default.

If you enable this option and the client provides an IP address, this address is the IP address that is used by the client for the duration of the tunneled session (it becomes the first or default choice).

7 Type the address of the primary Domain Name System (DNS) server on your private network. The server provides this DNS address to tunnel clients at setup and uses it through the tunnel. The DNS server translates textual host names into IP addresses for the VPN Router. For example, DNS can translate the fully qualified host www.mycompany.com to its IP address 192.19.2.33.

   The primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the primary DNS server is unavailable, service requests go to the secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers.

   Always use the IP address instead of a domain name to configure a DNS server host.

8 Type an address for the secondary Domain Name System (DNS) server. If the primary DNS server is unavailable, service requests go to the secondary DNS server.

9 Type an address for the primary Windows Internet Naming Service (WINS) server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Use a WINS server to access normal Windows file and print services through a tunnel connection.

   Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual LMHOSTS file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

   The primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the primary WINS server is unavailable, service requests go to the secondary WINS server. Always use the IP address instead of a name to configure a WINS server host.

Note: If you do not specify a WINS server, the client broadcasts for NetBIOS names.

10 Type an address for the secondary WINS server; if the Primary WINS server is unavailable, service requests go to the secondary WINS server.

Configuring branch office connection PPTP settings

To change PPTP settings for a branch office connection

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

   The Branch Office window appears.

2. Select the associated connection, and then click **Configure**.

   The Connection Configuration window appears.

3. To configure PPTP settings, select **PPTP** as the tunnel type.
4. Type the local user ID for the local VPN Router.
5. Type the user ID of the remote VPN Router.
6. Type the password for the peer user ID, and then confirm the password to verify that you typed it correctly.
7. From the **Compression** list, select **Enabled** or **Disabled**. Select **Enabled** to enable the IPsec Hi/fn Lempel Ziv Stac (LZS) compression or the PPTP, Layer 2 Tunneling Protocol (L2TP), or Layer 2 Forwarding (L2F) MPPC packet compression. Use compression if you select encryption on analog modems because encryption renders the compression of a modem ineffective, and it can severely affect the performance of compressible applications. Also, compressing data before transmission makes more efficient use of lower speed network links.
8. Configure encryption.
9. From the **Compression/Encryption Stateless Mode** list, select **Enabled** or **Disabled**. You must enable both encryption and compression to use this parameter.
10. Click **OK**.

Chapter 4
L2TP configuration

Nortel supports the Layer 2 Tunneling Protocol (L2TP). L2TP combines the best features of Layer 2 Forwarding (L2F) and Point-to-Point Tunneling Protocol (PPTP). L2TP tunneling provides secure remote access to corporate networks across the public Internet. L2TP tunnels generally establish between a network access server (NAS) at the Internet service provider (ISP) and the VPN Router.

Use L2TP to specify Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), or Password Authentication Protocol (PAP) authentication, enable compression, and assign Domain Name System (DNS) and Windows Internet Naming Service (WINS) servers to the tunnel.

You can use IPsec transport-protected L2TP tunneling for both remote access traffic and branch office tunnel traffic. Windows 2000 can act as a peer in a branch office connection using L2TP and IPsec or IPsec tunnel mode. Also, Windows 2000 can act as a client using L2TP and IPsec. Authentication for L2TP and IPsec tunnels can use either shared secret or digital certificate. It also provides configuration support for both voluntary and compulsory L2TP and IPsec remote access connections. (Windows 2000 authentication must be digital certificate.)

The VPN Router supports IPsec transport mode to support the termination of Microsoft Windows 2000 L2TP and IPsec connections and to provide security for L2TP traffic for client-to-VPN Router connections and VPN Router-to-VPN Router connections.

➡ **Note:** You must use stateless mode for L2TP tunnels if you have an environment where packets can be lost. Stateful mode forces the tunnel to drop more packets after it detects a packet loss. Multicast does not work over a Nortel VPN Router Open Shortest Path First (OSPF) L2TP tunnel through a Cisco router.

This chapter includes the following topics:

- "Configuring branch office for L2TP over IPsec" on page 69
- "Configuring Windows 2000" on page 71

L2TP settings configuration

Configure L2TP parameters on a global level on the Services, L2TP window and individually for groups and branch office connections from the Profiles menu.

- Global IPsec

  Globally configure L2TP from the Services, L2TP menu path.

- Group L2TP

  Configure group L2TP settings from the Profiles, Groups, Edit, L2TP menu path.

- Branch Office Connection L2TP

  Configure branch office connection L2TP settings from the Profiles, Branch Office, Edit Connection menu path.

Configuring global L2TP settings

To change global L2TP settings

1 Choose **Services**, **L2TP**.

The L2TP Settings window appears.

2 Configure L2TP authentication. L2TP settings allow you to select a specific authentication server type; for example, Remote Authentication Dial In User Service (RADIUS). You can specify a combination of the following authentication schemes for each server type: Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), Password Authentication Protocol (PAP), or None.

Note: Not all RADIUS servers support all forms of authentication. Failure to match Point-to-Point Protocol (PPP) authentication methods with RADIUS server capabilities results in user-authentication failures. Check the RADIUS documentation from your vendor for additional information.

3 In the **PPP Multilink** list, select **Enabled**.

4 Configure the authentication order. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The router queries the LDAP server first, and then RADIUS, if applicable.

5 Configure L2TP access concentrators.

- Delete—Click to remove the concentrator. You must confirm your deletion request.
- Add—Click to go to the Add L2TP Access Concentrator window. Use the L2TP Add Access Concentrators window to configure the authentication between the VPN Router and the NAS.
- Edit—Click to go to the Edit L2TP Access Concentrator window and modify the settings of a concentrator.

Configuring group L2TP settings

To change group level L2TP settings

1 Choose **Profiles**, **Groups**, and then click Edit for the associated group that you want to configure.

The Groups > Edit window appears.

2 Click **Configure** in the L2TP section of the window.

The Groups > Edit > L2TP window appears.

3 Click **Configure** for a specific parameter to make changes to that parameter. Click **Configure** in the **All Fields** section to edit all parameters at the same time. Click **Use Inherited** to set all fields to their inherited values.

4 Select one or more of the L2TP authentication methods.

5 Configure **Compression**. Select **Enabled** from the list to enable the L2TP Microsoft Point-to-Point Compression (MPPC) packet compression. Use compression if you select encryption on analog modems because encryption renders the compression of a modem ineffective, and it can severely affect the performance of compressible applications. Also, compressing data before transmission makes more efficient use of lower speed network links.

Use data compression in most situations. Users with cable modems or *x*DSL connections to the ISP, or locally on the LAN, find it unnecessary to compress packets. The speed of the link, relative to the rate of compression and the benefit of compressing before encrypting, is negligible or does not increase performance.

Also, the router cannot compress some data; for example, a previously compressed file does not lend itself well to additional compression.

6 Configure the **Use Client-Specified Address** parameter. If you enable the parameter, the VPN Router accepts the IP address from a remote user system during tunnel setup. This option is disabled by default.

If you enable this parameter and the client provides an IP address, this address is the IP address that is used by the client for the duration of the tunneled session (it becomes the first or default choice).

7 Type the address of the primary DNS server on your private network. The server provides this DNS address to tunnel clients at setup and uses it through the tunnel. The DNS server translates textual host names into IP addresses for the VPN Router. For example, DNS can translate the fully qualified host www.mycompany.com to its IP address 192.19.2.33.

The primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the primary DNS server is unavailable, service requests go to the secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers.

Always use the IP address for setting a DNS server host instead of a domain name.

8 Type an address for the secondary DNS server. If the primary DNS server is unavailable, service requests go to the secondary DNS server.

9 Type an address for the primary WINS server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Use a WINS server to access normal Windows file and print services through a tunnel connection.

Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual Lmhosts file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

The primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the primary WINS server is unavailable, service requests go to the secondary WINS server. Always use the IP address instead of a name to configure a WINS server host.

Note: If you do not specify a WINS server, the client broadcasts for NetBIOS names.

10 Type an address for the secondary WINS server; if the primary WINS server is unavailable, service requests go to the secondary WINS server.

11 Select the minimum level of data protection.

12 Specify the group from which this tunnel obtains its IPsec transport mode credentials.

Configuring branch office connection L2TP settings

To change L2TP settings for a branch office connection

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

The Branch Office window appears.

2 Select the associated connection, and then click **Configure**.

The Connection Configuration window appears.

3 To configure L2TP settings, select **L2TP** as the tunnel type.

4 Type the local user ID for the local VPN Router.

5 Type the user ID of the remote VPN Router (the peer).

6 Type the password for the peer user ID, and then confirm the password to verify that you typed it correctly.

7 From the **Compression** list, select **Enabled** to enable the L2TP Microsoft Point-to-Point Compression (MPPC) packet compression. Use compression if you select encryption on analog modems because encryption renders the compression of a modem ineffective, and it can severely affect the performance of compressible applications. Also, compressing data before transmission makes more efficient use of lower speed network links.

8 Configure encryption.

9 From the **Compression/Encryption Stateless Mode list**, select **Enabled** or **Disabled**. You must enable both encryption and compression to use this selection.

10 From the **L2TP Access Concentrator** list, select a host. Use this entry to specify the L2TP Access Concentrator that you want to perform authentication between the VPN Router and the NAS. You can click **Create Access Concentrator** to jump to the window where you can create a new access concentrator.

11 Select an IPsec data protection level. You must disable both compression and encryption to use data protection.

12 Click **OK**.

Configuring L2TP over IPsec

Windows 2000 supports only L2TP with IPsec transport mode for remote access or branch office. Windows 2000 cannot use L2TP without IPsec. Windows 2000 supports only RSA digital certificates for IPsec transport authentication with the VPN Router. Windows 2000 Professional Server or Advanced Server can act as a Windows 2000 L2TP and IPsec client to a VPN Router server.

To configure L2TP over IPsec on the VPN Router

1 Choose **Profiles**, **Users** to configure an L2TP user account on the VPN Router.

The User Management window appears.

2 Select the group name to which you want the user to belong, and then click **Display**.

3 Click **Add User**.

The User Management > Add User window appears.

4 Type an L2TP user ID and password.

5 Before you complete user configuration, you must install an issued certificate on the VPN Router.

a. Generate a certificate request from the **System**, **Certificates** window. Transfer this request to a certificate authority (CA) server that issues the certificate. You can then install the certificate from the same window.

b. You must also install the CA server certificate on the VPN Router through the **Certificate Configuration** window. If a different CA issues the Windows 2000 certificate, you must also install its certificate.

6. Configure an IPsec transport account on the VPN Router in one of three ways:

- Configure the **Subject DN** or **Alternate Subject Name** of the Windows 2000 certificate on the same window as the L2TP user account. From the **Valid Issuer Certificate Authority** list, select the CA who issued the Windows 2000 certificate. From the **Server Certificate** list, select the VPN Router certificate return to Windows 2000. Windows 2000 checks the issuer certificate also, so choose a certificate issued by a CA known by the Windows 2000 server. You can select **Require Own IPsec Credentials** now if you want to ensure that this L2TP user always uses this IPsec transport account.
- Choose **System**, **Certificates**, and then select the **Enable 'Allow All' Feature** box. For the CA that issued the Windows 2000 certificate, select the **Enabled** box under the **Allow All** section. Select a user group from the **Default Group** list. Be sure you enable and configure (not inherit) Allow IPsec Transport for the user group selected in its IPsec group properties. This configuration is very useful if L2TP user accounts are in RADIUS, because the LDAP server does not need to store L2TP or IPsec transport information for each user.
- Create a separate user that contains the IPsec transport account. Do not check the Require Own IPsec Credentials for either this user or the L2TP user. This router supports this configuration for L2TP user accounts in RADIUS or compulsory tunneling (when many L2TP users share an IPsec transport connection). Alternatively (for testing), you can install a single certificate on multiple Windows 2000 PCs, in which case they share a single IPsec transport account. Windows 2000 does not support compulsory tunneling.

7. Configure the L2TP profile for the user:

a. At a minimum, you must configure the desired minimum data protection level for the user. The router discards L2TP traffic that arrives through an IPsec transport that does not meet this requirement. Configure this protection in the L2TP properties of the group, which applies to all L2TP users under this group. The router does not perform a semantic check on your selections. For example, if you select 3DES as the minimum protection level, that implies that the router must negotiate 3DES with the Windows 2000 PC. To do this, you must enable DES in the **Services**, **IPsec** window, in the IPsec properties of the group that contains the IPsec transport account, and on the Windows 2000 machine as an acceptable encryption type. "Mapping minimum data protection levels to encryption levels" on page 67 describes the mapping of minimum data protection levels.

Table 1 Mapping minimum data protection levels to encryption levels

Minimum data protection level	**Encryption levels**
128-bit AES	ESP-AES with SHA1 Integrity
Triple DES	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity
56-bit DES	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity ESP-56-bit DES with SHA1 Integrity ESP-56-bit DES with MD5 Integrity
40-bit DES	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity ESP-56-bit DES with SHA1 Integrity ESP-56-bit DES with MD5 Integrity ESP-40-bit DES with SHA1 Integrity ESP-40-bit DES with MD5 Integrity
Authentication only	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity ESP-56-bit DES with SHA1 Integrity ESP-56-bit DES with MD5 Integrity ESP-40-bit DES with MD5 Integrity ESP-40-bit DES with SHA1 Integrity ESP-NULL (Authentication Only) with SHA1 Integrity ESP-NULL (Authentication Only) with MD5 Integrity AH-Authentication Only (HMAC-SHA1) AH-Authentication Only (HMAC-MD5)

Table 1 Mapping minimum data protection levels to encryption levels (continued)

Minimum data protection level	Encryption levels
Not required	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity ESP-56-bit DES with SHA1 Integrity ESP-56-bit DES with MD5 Integrity ESP-40-bit DES with SHA1 Integrity ESP-40-bit DES with MD5 Integrity ESP-NULL (Authentication Only) with SHA1 Integrity ESP-NULL (Authentication Only) with MD5 Integrity AH-Authentication Only (HMAC-SHA1) AH-Authentication Only (HMAC-MD5) Data passes through even if it does not come through an IPsec transport with this data protection level.

b If you do not select the **Require Own IPsec Credentials** box on the L2TP user window, the **Require IPsec Transport Mode Connections from** list on the Groups > Edit > L2TP window must use a user group that contains a set of allowed IPsec transport accounts. These IPsec transport accounts can exist at a level below this group. The router discards L2TP traffic that arrives through an IPsec transport not in this group.

c Optionally, enable compression in the L2TP group properties. You must enable compress on both the VPN Router and the Windows 2000 computer to compress PPP traffic. Windows 2000 does not support compression at the IPsec transport level.

d Authentication can be MSCHAPV1, MSCHAPV2, CHAP, or PAP. Windows 2000 uses these authentication methods in the following preferential order: MSCHAPV2, MSCHAPV1, CHAP, and finally PAP. Windows 2000 does verify that you select the **Not Encrypted** box.

8 Configure the IPsec transport profile by enabling the **Require IPsec Transport Mode Connections from** parameter in the group that contains the IPsec transport account.

9 By default, Windows 2000 does not enable Perfect Forward Secrecy (PFS). The router enables PFS by default. These two settings are not compatible and generate an appropriate error in the event log after a connection attempt. To disable PFS on the VPN Router, go to the IPsec properties of the IPsec transport group and disable PFS.

Configuring branch office for L2TP over IPsec

Windows 2000 Server or Advanced Server can act as a Windows 2000 L2TP and IPsec VPN Router to a VPN Router. Both static routing and dynamic routing, for example, Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), are possible through this branch connection.

To configure the VPN Router

1. Configure an L2TP branch connection on the VPN Router. Choose **Profiles**, **Branch Office** and either add a new connection or configure an existing connection.
2. Type the IP address of the Windows 2000 server as the remote endpoint. Select **L2TP** as the tunnel type.
3. Choose **unencrypted**.
4. Type a local UID for the VPN Router.
5. Type a peer UID for Windows 2000.
6. Type a shared password.
7. Specify if you want compression. As with remote access, Windows 2000 does not support compression for the IPsec transport connection.
8. If you want to support L2TP tunnel authentication, you must provide an L2TP access concentrator definition. Windows 2000 does not support L2TP tunnel authentication.
9. Select the minimum data protection level. If you select anything other than **Not Required**, you must configure an IPsec account. “Mapping minimum data protection levels to encryption levels” on page 67 shows mappings of data protection levels to encryption levels.
10. As with remote access, you must configure the IPsec transport account. By default, Windows 2000 supports only certificate authentication. The CA Allow All authentication option is not available for branch office connections. The L2TP branch office must use the IPsec transport account specified in the connection if you need data protection.
11. You can configure routing as either static or dynamic.

To configure Windows 2000

1. You must install a certificate for Windows 2000 and the CA certificates.
2. Start the **Routing and Remote Access** administrative tool.
3. Right-click on **Routing Interfaces,** and then choose **New Demand-dial Interface**.
4. Type the name of the branch connection. This name becomes the L2TP user ID of the VPN Router. MSCHAPV2 is case sensitive for user IDs. To ensure interoperability with the VPN Router, use lowercase user IDs.
5. Select **Connect** using VPN.
6. Select **L2TP** as the VPN type.
7. Type the interface address of the VPN Router.
8. Select **Route IP packets** on this interface, and then select **Add a user account** so a remote router can dial in.
9. Type a password for the VPN Router L2TP user ID. If the VPN Router initiates branch office connections to Windows 2000, this password must match the one you enter on the VPN Router Branch Office Connection window. Otherwise, this password does not matter.
10. Choose the Windows 2000 L2TP user ID and the shared password. If the Windows 2000 initiates branch office connections to the VPN Router, this password must match the one you enter on the VPN Router Branch Office Connection window. You can leave the **Domain** box blank.
11. The VPN Router supports only MSCHAPV2 as a branch office L2TP authentication method, so be sure you enable this method in the properties (it is by default).
12. If you want static routes to demand dial on this connection, expand **IP Routing**, **Static Routes** and right-click on **New Static Route**. Select the interface just created and type the subnet information. Be sure you enable **Use this route to initiate demand-dial connections**. Alternatively, you can dial the connection by right-clicking on it and selecting **Connect**.

Configuring Windows 2000

Windows 2000 Professional, Server, or Advanced Server can act as a Windows 2000 L2TP and IPsec client to a VPN Router server. To install a certificate on the Windows 2000 PC using a Windows 2000 Microsoft CA, connect to a CA server and obtain a certificate. This process involves pointing a browser at the CA server with the URL <IP address>/certsrv.

1. Choose **Request a Certificate**, and then click **Next**.
2. Choose **Advanced request**, and then click **Next**.
3. Click **Submit a certificate request to this CA using a form**, and then click **Next**.
4. On the form provide the identifying information. This information becomes the subject DN in the certificate, which you type on the VPN Router IPsec transport account.
5. Under **Intended Purpose**, select **IPsec Certificate**.
6. Under **Key Options**, select **Use local machine store**.
7. Click **Submit**.
8. Click **Check on a pending certificate**.
9. Select the certificate, and then click **Next**.
10. Click **Install this certificate**. This option installs the certificate in the local computer certificate store. To view this store, run the `mmc` command from the **Start**, **Run** prompt. Select **Console**, **Add/Remove Snap-in**. From the list of snap-ins, choose **Certificates** and select **Computer account**. At the console, expand **Personal**, **Certificates** under **Certificates (Local Computer)**. The installed certificate appears. Click on the certificate to open an information window that indicates its validity and that a private key exists for this certificate.

To install the CA server certificate for the Windows 2000

1. If a different CA issues the VPN Router certificate, install that server certificate. For the Microsoft CA, go to the home page and select **Retrieve the CA certificate or certificate revocation list**.

2 Click on **Install this CA certification path**. This installs the CA certificate as a trusted CA, which you can see in mmc under **Trusted Root Certificates**, **Certificates**.

To configure the dial-up networking entry to use L2TP over IPsec

1 Click on **My Computer**, and then click on **Network and Dial-up Connections.** Click on **Make New Connection**.

2 Choose **Connect** to connect to a private network through the Internet for the network connection type.

3 Type the interface address of the VPN Router server.

4 Edit the properties of this new connection, and then click the **Networking** tab.

5 Change the type of VPN server to **L2TP**.

6 Connect to the VPN Router using the L2TP user ID and password you create on the VPN Router. The certificate installed previously establishes the IPsec transport connection.

Chapter 5 L2F configuration

Nortel supports the Layer 2 Forwarding (L2F) tunneling protocol. L2F tunneling provides remote access to corporate networks across the public Internet. L2F tunnels generally establish between the network access server at the Internet service provider (ISP) and the Nortel VPN Router.

You do not require direct client software for L2F beyond the Point-to-Point Protocol (PPP) dialer software, such as the dial-up networking utility provided with Windows 95 and Windows 98. The ISP creates the L2F tunnels to the corporate VPN Router on behalf of the user. These connections depend on the domain associated with the dial-in user name. Therefore, ISPs must offer services that are based on L2F; currently, L2F is available on a limited basis. L2F provides IP address translation using encapsulation and support for IPX tunneling, but it does not perform encryption. L2F offers the following features:

- requires special ISP services
- no requirement for special software on the client
- no data encryption

This chapter includes the following topic:

- “L2F settings configuration” on page 73

L2F settings configuration

Configure L2F parameters on a global level on the Services, L2F window and individually for groups, users, and branch offices from the Profiles menu.

- Global L2F

  Globally configure L2F from the Services, L2F menu path.
- Group L2F

  Configure group L2F settings from the Profiles, Groups, Edit, L2F menu path.

Configuring global L2F settings

To change global L2F settings

1 Choose **Services**, **L2F**.

The L2F Settings window appears.

2 Configure L2F authentication. You can add a Remote Authentication Dail In User Service (RADIUS) server for authentication. In the **Authentication** section of this window, specify an authentication scheme of either **CHAP** or **PAP**.

3 Configure the L2F authentication order. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The router queries the Lightweight Directory Access Protocol (LDAP) server first, and then RADIUS, if applicable.

4 Configure the **Network Access Servers** section. This table provides the user IDs for the network access servers (NAS) and VPN Router, and the possible actions you can take. The NAS acts like a middle point between the remote user and the VPN Router. The NAS authenticates each side, and after validation is complete, a tunnel forms. The user uses a standard connection (for example, PPP) to the NAS, but an L2F tunnel forms between the NAS and the VPN Router.

Configuring group L2F settings

To change group L2F settings

1 Choose **Profiles**, **Groups**, and then click **Edit** for the associated group that you want to configure.

The Groups > Edit window appears.

2 In the L2F section, click **Configure**.

The Groups > Edit > L2F window appears.

3 Click **Configure** for a specific parameter to make changes to that parameter. Click **Configure** in the **All Fields** section to edit all parameters at the same time. Click **Use Inherited** to set all fields to their inherited values.

4 Select one or more of the L2F authentication methods.

5 Configure the compression setting. Select **Enabled** to enable the L2F Microsoft Point-to-Point Compression (MPPC) packet compression. Use compression if you select encryption on analog modems because encryption renders the compression of a modem ineffective, and it can severely affect the performance of compressible applications. Also, compressing data before transmission makes more efficient use of lower speed network links.

Use data compression in most typical situations. Users with cable modems or *x*DSL connections to the ISP, or locally on the LAN, find it unnecessary to compress packets. The speed of the link, relative to the rate of compression and the benefit of compressing before encrypting, is negligible or does not increase performance.

Also, the router cannot compress some data; for example, a previously compressed file does not lend itself well to additional compression.

6 Set the **Use Client-Specified Address** parameter. If you enable the client-specified address, the VPN Router accepts the IP address from a remote user system during tunnel setup. This option is disabled by default.

If you enable this option and the client provides an IP address, this address is the IP address that is used by the client for the duration of the tunneled session (it becomes the first or default choice).

7 Type the address of the primary Domain Name System (DNS) server on your private network. The server provides this DNS address to tunnel clients at setup and uses it through the tunnel. The DNS server translates textual host names into IP addresses for the VPN Router. For example, DNS can translate the fully qualified host www.mycompany.com to its IP address 192.19.2.33.

The primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the primary DNS server is unavailable, service requests go to the secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers.

Always use the IP address for setting a DNS server host instead of a domain name.

8 Type an address for the secondary Domain Name System (DNS) server. If the primary DNS server is unavailable, service requests go to the secondary DNS

server.

9 Type an address for the primary Windows Internet Naming Service (WINS) server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Use a WINS server to access normal Windows file and print services through a tunnel connection.

Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual LMHOSTS file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

The primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the primary WINS server is unavailable, service requests go to the secondary WINS server. Always use the IP address instead of a name to configure a WINS server host.

Note: If you do not specify a WINS server, the client broadcasts for NetBIOS names.

10 Type an address for the secondary WINS server; if the primary WINS server is unavailable, service requests go to the secondary WINS server.

Index