Version 8.00

Part No. NN46110-600 02.01
315897-G Rev 01
13 October 2008
Document status: Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Security — Servers, Authentication, and Certificates

NORTEL

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 guide describes how to configure the Nortel VPN Router authentication services and digital certificates.

Before you begin

This guide is for network managers who set up and configure the Nortel VPN Router. This guide assumes that you have experience with window-based systems or graphical user interfaces (GUI) 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 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 — Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F).
- *Nortel VPN Router Configuration — Routing* (NN46110-504) provides instructions to configure the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), Equal Cost Multipath (ECMP), routing policy services, and client address redistribution (CAR).

- *Nortel VPN Router Using the Command Line Interface* (NN46110-507) provides syntax, descriptions, and examples for the commands that you can use from the command line interface (CLI).
- *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508) provides instructions to configure the Stateful Firewall and VPN Router interface and tunnel filters.
- *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 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 sections detail what's new in *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600) for Release 8.0:

Features

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

4096-bit certificates

Release 8.0 increases the maximum size of a certificate to 4096 bits.

PassGo

Release 8.0 supports PassGo tokens for authentication. For more information, see "Server configuration" on page 27.

Cross certification

Release 8.0 supports two types of cross certification: hierarchical and peer-to-peer. For more information, see “Certificate configuration” on page 77.

DHCP

You can use a combination of internal DHCP, external DHCP, and address pool, but you must use at least one of those options. These options are no longer mutually exclusive. For more information, see “Server configuration” on page 27.

Online Certificate Status Protocol

Beginning with Release 8.0, the VPN Router can use the Online Certificate Status Protocol (OCSP) to retrieve the revocation status of an X.509 digital certificate. For more information, see “Authentication services” on page 19 and “Certificate configuration” on page 77.

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 about two factor authentication, see “Two factor authentication” on page 105.

Other changes

For information that is not feature related, see the following section:

- “Document changes” on page 18

Document changes

This document is changed to comply with Nortel writing conventions.

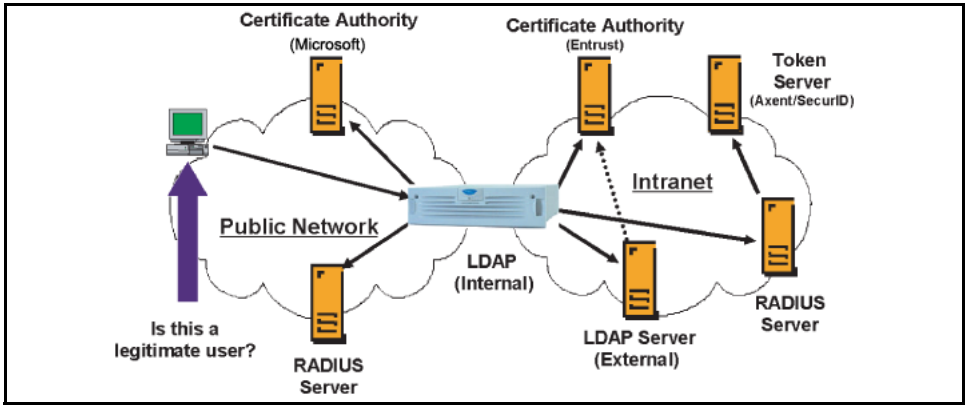
Chapter 1
Authentication services

The VPN Router must authenticate a remote user that attempts to connect through the public interface before the user gains access to the corporate network. Authentication is one of the most important functions that the VPN Router provides because it identifies users and drives many other aspects of the user-centric functionality.

For authentication and access control, the VPN Router supports an internal or external Lightweight Directory Access Protocol (LDAP) server and external Remote Authentication Dial-In User Service (RADIUS) servers. External LDAP proxy server support authenticates users against existing LDAP databases.

For more information about how users are authenticated, see "User authentication" on page 19.

Figure 1 User authentication



The VPN Router uses a group profile mechanism to augment support for several authentication services. After a remote user attempts to access the network, the VPN Router references a particular group profile to determine encryption strength, filtering profile, and Quality of Service (QoS) attributes for that user.

With user- and group-specific profiles, you can group common attributes while you preserve the flexibility to make exceptions for individual users. You control the product features and network access that apply to a user by the user identity, rather than by the source IP address or another mechanism. This method is necessary to support mobile users and users coming from other organizations.

This chapter describes the following items:

LDAP

The Lightweight Directory Access Protocol (LDAP) emerged from the X.500 directory service. Microsoft, Netscape, and Novell all support LDAP in their directory service strategies. LDAP is based on directory entries; it uses an Internet person schema that defines standard attributes, and you can extend it to include other attributes. A directory service is a central repository of user information, for example, the VPN Router supports the following elements by using LDAP:

- groups
- users
- filters
- services

RADIUS

Remote Authentication Dial-In User Services (RADIUS) is a distributed security system that uses an authentication server to verify dial-up connection attributes and authenticate connections. RADIUS is commonly used for remote access authentication.

Many security systems use a RADIUS front-end to facilitate remote access authentication. RADIUS is the most common authentication mechanism used by ISPs. Novell NDS, Microsoft Windows NT Domains, Security Dynamics ACE Server, and PassGo Defender all support RADIUS authentication. Windows NT Domain authentication controls access to NT file servers and other resources on NT networks. The RADIUS server provides a place to store user passwords, because users generally remember their file server passwords.

The X.509 digital certificates authentication mechanism works with public key encryption to provide a level of assurance that users are who they say they are.

SSL and digital certificates

The Secure Socket Layer (SSL) protocol uses digital certificates to establish secure, authenticated connections between SSL clients and servers.

The VPN Router uses a digital certificate sent from an SSL-capable LDAP server to authenticate that server. For digital certificate authentication to succeed, you must import a certificate from the authority that certifies the LDAP server into the VPN Router certificate store. This type of certificate is a certificate authority (CA) root certificate.

A single CA root certificate can certify the authenticity of multiple LDAP servers, depending on the organization of the certification hierarchy.

Tunnel certificates

The VPN Router uses X.509 certificates for authentication to IPsec-based tunnel connections. The VPN Router supports RSA digital signature authentication in the IPsec Internet Security Association and Key Management Protocol (ISAKMP). Remote users can authenticate themselves to the VPN Router using a public key pair and a certificate as credentials. In addition, the VPN Router uses its own key pair and certificate to authenticate the VPN Router to the user. The VPN Router currently supports the Entrust product suite and Microsoft certificates.

The VPN Router supports retrieval of X.509v3 certificates from Microsoft certificate storage through the Microsoft CryptoAPI (MS CAPI). Microsoft certificate storage uses standard messages (PKCS #12) to import digital certificates granted by third-party certificate authorities. The VPN Router and VPN Client can use CAs that are not tightly integrated with the client and VPN Router.

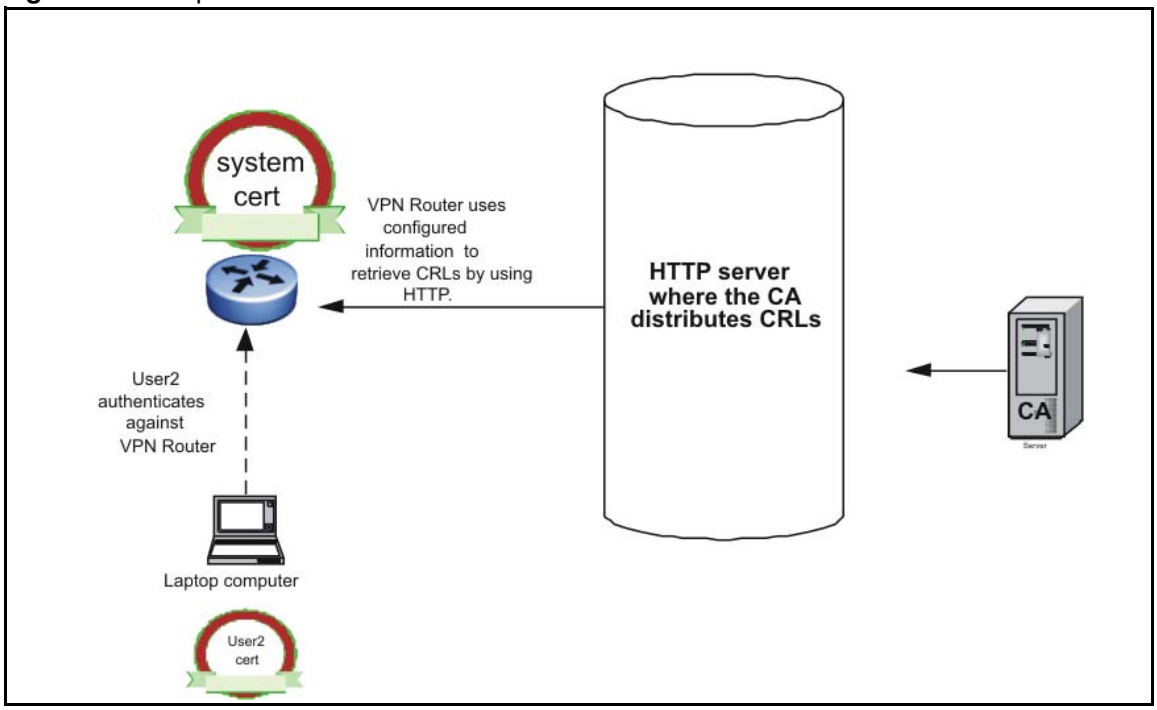
The certificate payload transports certificates or other certificate-related information through ISAKMP and can appear in an ISAKMP message. Certificate payloads are in an exchange whenever an appropriate directory service (such as Secure DNS) is not available to distribute certificates. The VPN Router supports Microsoft native client (L2TP/IPsec) PKCS #7 termination in chained environments.

To use certificates for tunnel connections requires the creation of a public key infrastructure (PKI) to issue and manage certificates for remote users and VPN Router servers.

Online Certificate Status Protocol

The VPN Router can use the Online Certificate Status Protocol (OCSP) to retrieve the revocation status of an X.509 digital certificate. Messages communicated using OCSP are encoded in ASN.1 and are usually communicated over the Hypertext Transfer Protocol (HTTP). For more information about the OCSP process, see “Example of HTTP CRL retrieval in user authentication” on page 23.

Figure 2 Example of HTTP CRL retrieval in user authentication



For more information about OCSP, see RFC 2560.

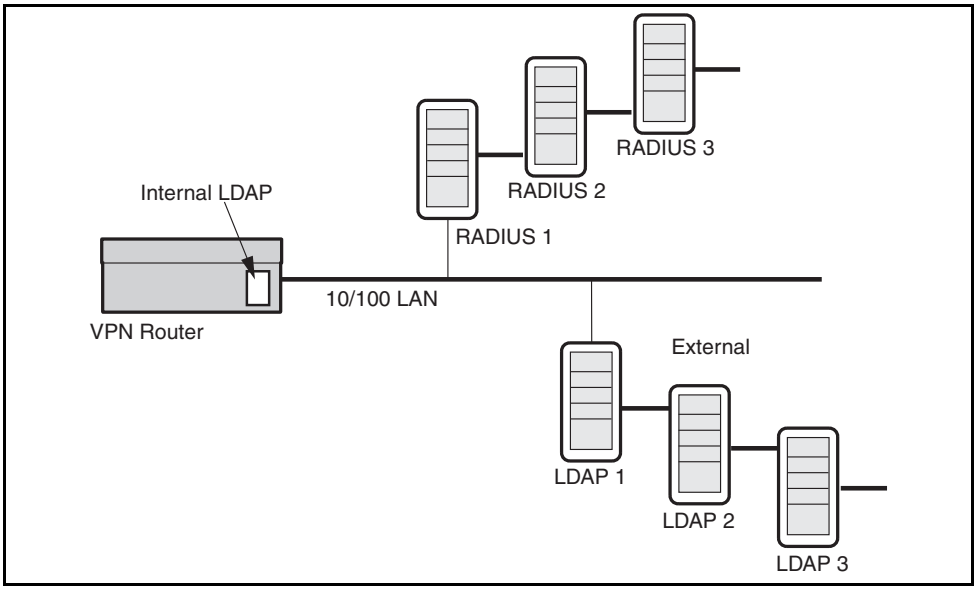
Authentication servers

The VPN Router supports LDAP and RADIUS authentication servers. The VPN Router always attempts to authenticate a remote user against the internal or external LDAP profiles.

Note: If you authenticate users by using RADIUS or LDAP authentication, you must use unique names for the group ID and user ID.

For more information about VPN Router and authentication servers, see "Authentication servers" on page 24.

Figure 3 Authentication servers



The VPN Router checks the user ID (UID) against the LDAP profile database. If the UID exists in the LDAP database, the VPN Router assigns the user to a group and the user acquires the group attributes. Next, the VPN Router checks the password, and if it is correct, the VPN Router forms a tunnel.

If the UID does not exist in the profile LDAP (internal or external) database, and if you specify RADIUS as the next server to check, the VPN Router checks the UID and password against the RADIUS database. If the UID and password are correct, the VPN Router checks to see if the RADIUS server returned a class attribute. The VPN Router treats the RADIUS class attribute as an LDAP group name. If the RADIUS server returns a class attribute, and it names an existing LDAP group, the VPN Router applies the attributes of this group to this user session and forms a tunnel. If the group name does not exist, the user acquires the RADIUS default group attributes. If the UID and password are incorrect, the VPN Router rejects the user request.

IPsec behaves the same as a Point to Point Tunneling Protocol (PPTP) session; the RADIUS server defines the group for the user after authentication using the class attribute group identifier. The difference between IPsec and PPTP is that if the RADIUS server does not return a class attribute, the user takes on the group associated with the IPsec group ID instead of the RADIUS default group. You

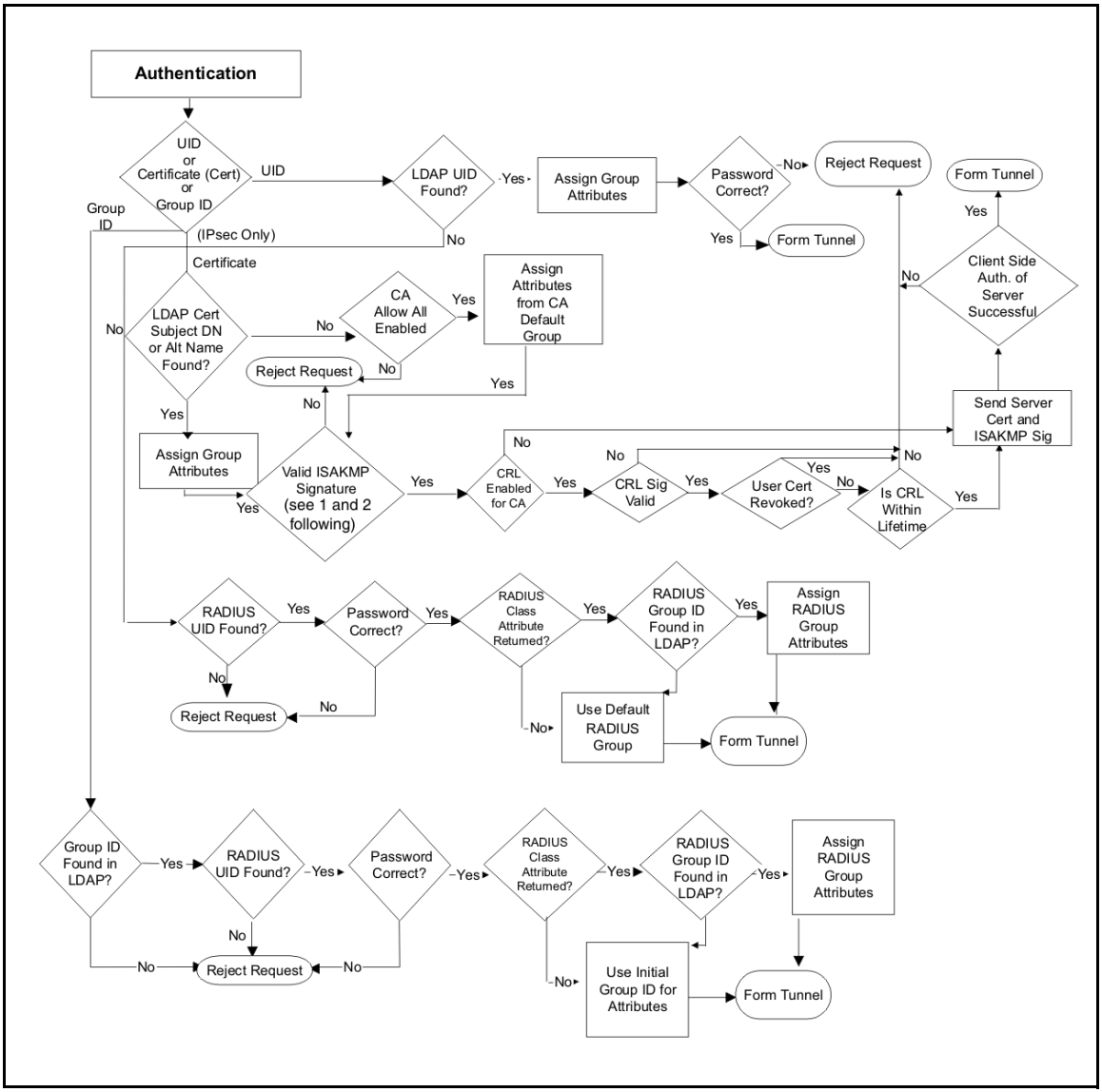
configure the IPsec group ID in the Authentication section of the Profiles, Groups, Edit, Configure IPsec window. You configure the PPTP default group on the Servers, RADIUS Auth window, RADIUS Users Obtain Default Settings from the Group option.

Note: The group to which the user is bound must allow the authentication method in use after the session starts.

If the UID does not exist in the profile LDAP (internal or external) database and if you specify LDAP proxy as the next server to check, the VPN Router checks the UID and password against the LDAP proxy database.

For information about the steps in user validation, see "Authentication server validation flowchart" on page 26.

Figure 4 Authentication server validation flowchart



Chapter 2
Server configuration

This chapter describes how to configure the following authentication servers for users who tunnel into the VPN Router:

- The internal Lightweight Directory Access Protocol (LDAP) server stores group and user profiles on the internal server of the VPN Router. External LDAP contains the contents of the internal LDAP server exported to a separate external LDAP server.
- The LDAP proxy server authenticates users against an existing LDAP database separate from the VPN Router database.
- External Remote Authentication Dial-In User Service (RADIUS) is a distributed security system that uses an authentication server to verify dial-up connection attributes and authenticate connections.
- RADIUS accounting logs user sessions with RADIUS-style records that contain detailed connection statistics.
- The VPN Router can function as a simple RADIUS server.

This chapter describes how to configure the VPN Router Secure Sockets Layer (SSL) administration feature. This chapter includes the following topics:

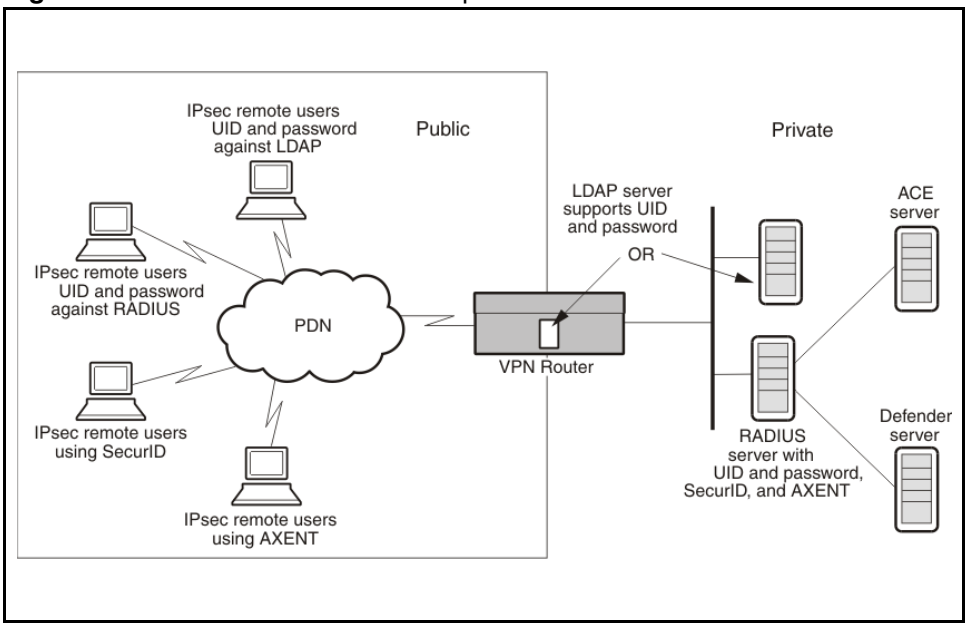
IPsec client

Authentication using the Nortel IPsec client provides the following options for remote users that connect through a VPN Router:

- user ID and password authentication against an LDAP database
- group password authentication using a RADIUS server
- token security methods (RSA SecurID and PassGo Defender)

The following figure shows IPsec client authentication options.

Figure 5 IPsec client authentication options



The following list identifies characteristics of all authentication options:

- A Diffie-Hellman key exchange, Internet Security Association and Key Management Protocol (ISAKMP)/Oakley Aggressive Mode builds the security association (SA).
- The user name and the password do not transmit in clear text; a cryptographic hash function (SHA-1) protects the user identity.

- Mutual authentication occurs between the client and the VPN Router using a keyed hash algorithm (HMAC).
- Session cookies protect against authentication replay attacks.

LDAP database servers

LDAP is a standard protocol for Internet directory services based on directory entries. A directory service is a central repository of user information, such as groups, users, filters, and services.

An entry is a collection of attributes with a distinguished name (DN), which refers to the entry unambiguously. Each entry attribute uses a type and one or more values. Types are typically mnemonic strings; for example, cn represents common name and mail represents e-mail address. The values depend on the attribute type. For example, a mail attribute value can resemble jchirac@elysee.france.gov.

LDAP directory entries are in a hierarchical tree-like structure that reflects political, geographic, and organizational boundaries. Country entries appear at the top of the tree. The next entries represent states or national organizations. The third-branch entries represent people, organizations, servers, files, or other readable database entry. You can use LDAP to read, search, add, and remove information from the centralized database.

Note: Nortel recommends that you back up your LDAP servers before you make changes so that a valid copy exists if the file becomes corrupt.

The VPN Router centrally stores remote access profiles and corporate networking details such as the addressing mechanism in an LDAP server; for example, group attributes including hours of access, filters, and authentication servers. The VPN Router queries the LDAP server for access information after a user establishes a tunnel connection. You can service the LDAP query locally by the internal LDAP server or you can redirect it to an external LDAP server, such as the Netscape Directory Server.

Note: The VPN Router does not support Novell Directory Services and Novell eDirectory.

Password encryption keys

You can use either a user-defined or a default LDAP encryption key. This key is either 8 bytes (DES) or 24 bytes (3DES) in length.

Every VPN Router contains a common default key, which encrypts user passwords stored in LDAP. By default, the VPN Router uses the Data Encryption Standard (DES), and therefore an 8-byte key for LDAP-stored passwords. To use a 24-byte key, you must first enable Triple DES (3DES) encryption.

This feature affects only passwords stored in the LDAP file. Passwords stored in the configuration file remain unchanged.

The first time that you enable 3DES and configure a 24-byte encryption key, the VPN Router updates the LDAP. This action can take some time, depending on the size of the user base.

Configuration information

The router stores internal and external LDAP keys in flash memory. The VPN Router calculates a hash from the user-defined key and stores it in the LDAP file.

To restore a VPN Router to the default internal key, you must meet the following two conditions:

- Reset the VPN Router to the factory defaults. This configuration clears the key saved in flash.
- The configuration and LDAP files to restore must be ones that you saved before you applied user defined keys.

External LDAP key information

For authentication to work between all VPN Routers using the shared LDAP, the keys must match on all VPN Routers.

To change the key, the VPN Router must use the last saved key. Keys on all routers that use a shared LDAP must match before a router can change the key. If one router changes the key, all others must use matching keys. For example, if two routers, VPN Router1 and VPN Router2, use the same external LDAP, and

VPN Router1 uses a user-defined key, VPN Router2 cannot use a key except the one that matches the key of VPN Router1. After VPN Router2 uses a key that matches, VPN Router2 can configure a new key. If VPN Router 2 uses a new key, VPN Router1 must configure a matching key before authentication succeeds.

After VPN Router1 uses a key, the LDAP passwords are encrypted using the key. If VPN Router2 uses the same key, no change occurs to the LDAP passwords.

Changing from DES to 3DES

For internal and external LDAP, 3DES uses the default internal key unless you define a user key. If you use 3DES, the VPN Router processes the entire LDAP, field by field, and configures a flag for every password that 3DES encrypts.

For both internal and external LDAP, after you enable 3DES, to return to DES, you must restore a previously saved configuration and LDAP file.

3DES external LDAP information

All VPN Routers that use a shared LDAP must run a software version that supports 3DES LDAP encryption. Even if you do not configure a VPN Router to use 3DES LDAP encryption, it can decrypt 3DES passwords from an LDAP encrypted by another VPN Router that uses 3DES.

After you enable 3DES, the LDAP passwords are encrypted using 3DES. After you enable 3DES on another VPN Router that shares the LDAP, no changes are made to the LDAP stored passwords.

3DES external LDAP proxy information

If you use an external LDAP proxy, the VPN Router, which uses its own internal LDAP file, does not use or modify the external LDAP database. However, the VPN Router modifies the bind password attached to the bind name.

Configuration scenarios

The following sections describe configuration scenarios that deal with 8- and 24-byte encryption keys and provide configuration information for these cases.

Case 1—Restoring a V7.05.300 unit upgraded from V6.05.140 with 3DES and a user encryption key enabled

Consider the following scenario:

- You configure a VPN Router that runs V6.05.140 (a version that supports only 8-byte keys) with the following configuration:
  - 3DES encryption enabled
  - an 8-byte LDAP user encryption key
- You upgrade the VPN Router to V7.05.300, and do not configure the 24-byte user encryption key.

This example is a supported configuration. You can modify the running configuration and LDAP files as required. Nortel recommends that you perform automatic backups and LDAP saves for disaster recovery.

If you must replace the VPN Router with a new VPN Router, or restore the factory defaults and reload to a full V7.05.300 version, you must perform the following procedure to restore the previously saved backup and LDAP.

Restoring a saved backup and LDAP

1. Configure the management and interface addresses.
2. Choose **Servers**, **LDAP**.
3. Configure the original 8-byte encryption key.

Note: Do not select 3DES encryption. After you enable 3DES, the system requires a 24-byte key.

4. Restore the saved V7.05.300 configuration file.
5. Restart the VPN Router.
6. Restore the saved V7.05.300 saved LDAP.

After you perform the preceding steps, the following occurs:

- The system uses 3DES.
- The system uses the original 8-byte encryption key.

- Tunnels operate.

Configure a 24-byte encryption key to avoid these steps in future.

Case 2—Upgrades and unknown key lengths

If you enable 3DES for software versions prior to 6.05.170, you can enter only an 8-byte user key. In V6.05.170 and later, you can enter only 24-byte user encryption keys after you enable 3DES LDAP encryption. The VPN Router software does not make a distinction between an 8-byte key entered in an older version of code and upgraded to 6.05.170 or later and a user key entered natively in a version later than 6.05.170.

The user encryption password box looks the same for both 8- and 24-byte keys after you enable 3DES. To avoid confusion, ensure that you re-enter a 24-byte user key after an upgrade to V6.05.170 or later.

Encrypting with 3DES password

The Nortel VPN Router administrator can secure user and application passwords with 3DES encryption, which is a more secure algorithm than the current DES.

If you use an external LDAP, you must upgrade all VPN Routers in the network to use this capability. The first VPN Router to enable 3DES encryption of user passwords first runs a script against the external LDAP to convert all user passwords from DES to 3DES.

After you enable 3DES, the LDAP automatically updates. Each VPN Router that uses this feature checks the LDAP to ensure that all passwords are in 3DES (external LDAP only).

Warning: Nortel recommends that you back up your LDAP and configuration before you enable 3DES.

You can use the GUI or the CLI to enable 3DES.

To enable 3DES

1 Choose **Servers**, **LDAP**.

The LDAP Server window appears.

2 Click **Enable TripleDES**.

After you enable TripleDES, all passwords within the box are encrypted with 3DES as well as future passwords.

3 To confirm the 3DES encryption, click **OK**.

To enable 3DES with the CLI, enter the following command:

```
ldap-server tripledes-enable
```

Configuring user password encryption keys

With the LDAP user configurable encryption key, you can configure your own user-defined encryption key instead of the default encryption key that is present on the VPN Router. If you use a user-defined encryption key with an external server, all the VPN Routers that use that external LDAP server must use the same configured encryption key.

Warning: To return to the default encryption key, after you configure a user-defined key, you must reset the VPN Router to factory defaults.

You can use the GUI or the CLI to configure the LDAP user configurable encryption key.

To change the existing encryption key

1 Choose **Servers**, **LDAP**.

The LDAP Server window appears.

2 From the encryption key options, select **Text Encryption Key** or **Hex Encryption Key**.

3 In the **Encryption Key** box, type a character string or a hexadecimal value.

Note: The following statement applies only for Nortel VPN Router Release 7.05.300 and later.
If you do not enable TripleDes LDAP Encryption, the Encryption Key value that you enter is 8 bytes—8 American Standard Code for Information Interchange (ASCII) text characters or 16 hexadecimal characters. If you enable TripleDes LDAP Encryption, the Encryption Key value that you enter is 24 bytes—24 ASCII text characters or 48 hexadecimal characters.

4 In the **Confirm Encryption Key** box, type the same value from step 3.

5 Click **OK**.

Note: The default key encrypts the passwords until you enter a user encryption key. You can use DES or 3DES to encrypt passwords stored in LDAP.

To change the existing encryption key for the 8 byte character string using the CLI, enter the following command:

```
ldap-server encryptionkey-text <password>
```

To change the existing encryption key with the hexadecimal value, enter the following command:

```
ldap-server encryptionkey-hex <password>
```

Optimizing LDAP scheduling

With the LDAP optimization scheduling option, you can configure the time and day that the VPN Router optimizes the LDAP database.

LDAP optimization is a process that frees all unused memory blocks and removes deleted LDAP data structures, making the LDAP database lookups faster and more efficient. The disadvantages of the LDAP optimization process are that it runs at the LDAP priority and is CPU intensive. In environments with heavy traffic and very large LDAP databases, the optimization can cause time-outs and data drops.

You can use the GUI or the CLI to configure optimization LDAP scheduling.

To configure LDAP optimization scheduling

1. Choose **Servers**, **LDAP**.

   The LDAP Server window appears.

2. In the Automatic Optimization row, select **Enable**.
3. In the **Time** box, type the desired time.
4. In the Automatic Optimization days of the week options, select the desired days.

To enable LDAP optimization scheduling, enter the following command:

```
ldap-server internal optimize specific-time enable
```

To disable LDAP optimization scheduling, enter the following command:

```
no ldap-server internal optimize specific-time everyday
```

To enable LDAP optimization scheduling everyday at a specific time, enter the following command:

```
ldap-server internal optimize specific-time everyday time <hh:mm>
```

where

hh:mm is the hour (00-24) and the minutes of the specific time.

To disable LDAP optimization scheduling everyday at a specific time, enter the following command:

```
no ldap-server internal optimize specific-time enable
```

To enable LDAP optimization scheduling on specific days of the week at a specific time, enter the following command:

```
ldap-server internal optimize specific-time <days of week> time
<hh:mm>
```

where

- days of week are the specific days to enable LDAP optimization scheduling
- hh:mm is the hour (00-24) and the minutes of the specific time

To disable LDAP optimization scheduling on specific days of the week, enter the following command:

```
no dap-server internal optimize specific-time <days of week>
```

where

days of week are the specific days on which to disable optimization scheduling

Configuring internal LDAP server authentication

Because the VPN Router internal LDAP server does not respond to external queries, two or more VPN Routers cannot share the same internal LDAP database. To permit sharing between VPN Routers, and to take full advantage of LDAP -based directory service replication and centralization, use a dedicated directory service.

The VPN Router synchronizes its cache every 15 minutes. For example, if you delete a user from an external LDAP database, it can take up to 15 minutes before all of the VPN Routers recognize the change. Additionally, the VPN Router records the status of the LDAP server in the event log every 15 minutes.

To configure internal LDAP

1 Choose **Servers**, **LDAP**.

The LDAP Server window appears.

The internal LDAP server is internal to the VPN Router. If you use more than one VPN Router or if you use LDAP authentication for other network services, consider using an external LDAP server.

2. To enable the internal LDAP server, click **Switch to Internal Server**. You disable the internal server if you enable an external LDAP server.
3. Under the General Configuration section, remove the fully qualified ID suffix from the UID before the system sends it to the RADIUS server by selecting the box and typing a delimiter value. An example of a user ID and suffix where Rcole is the UID and acme.com is the suffix, is rcole@acme.com. Specify the character that separates the suffix from the UID.
4. Click **Stop Server** or **Start Server**, as appropriate, when you intend to back up or restore a configuration, or after you complete the restoration of a configuration. You must stop the LDAP server before you can perform the backup and restore procedures.
5. Under **Internal Server Control**, **Directory** shows the current directory path, which begins at the root disk drive (ide0). Stop the LDAP before you perform a backup or restore procedure. To resume operation, you must restart the LDAP server.
6. To back up to a file, enter a filename (eight characters maximum) to back up the database, and then click **Backup Now** to start the backup procedure.

   This procedure backs up changes to the internal LDAP Data Interchange Format (LDIF) file only. The LDIF file is an intermediate database file that you use to move data between LDAP servers.

7. To restore from a file, select a file from the **Restore from File** list with which to restore the LDAP database, and then click **Restore Now**.

   Both the backup and restore processes can take extended periods of time, based on the size of the database.

8. The **Installed LDAP (SSL) CA Certificates** section shows whether certificates are installed. Click **Import Secure LDAP (SSL) CA Certificate** to import a CA certificate. This option provides an edit dialog box where you can paste a **PKCS#7 Base-64** certificate.
9. Click **Optimize Database** to optimize the internal LDAP database.

Configuring LDAP proxy server authentication

The VPN Router supports authentication against an existing LDAP server rather than creating a second user database for use with the VPN Router. The server can reside on either a private or public network that connects to the VPN Router.

Note: You must enable CSFW for the public interface to work with LDAP proxy server authentication.

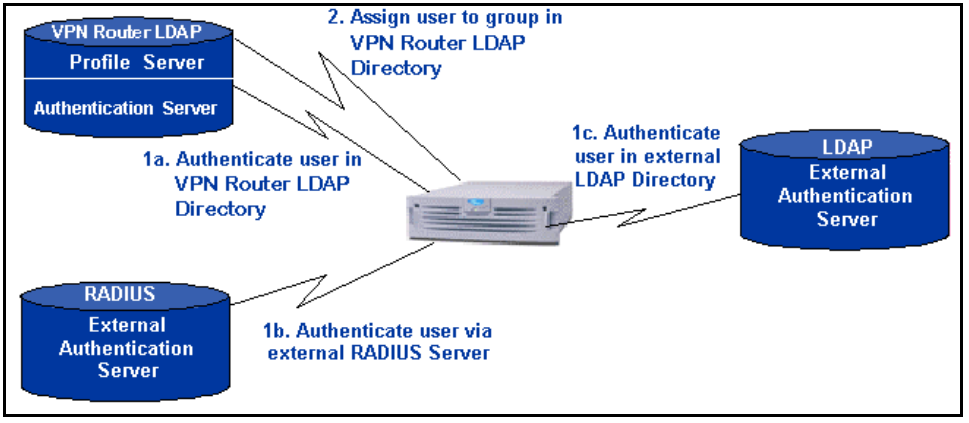
You can configure the type of authentication methods that can access the existing LDAP server. The authentication options are

- Password Authentication Protocol (PAP) (Bind authentication)
- PAP
- Challenge-Handshake Authentication Protocol (CHAP)
- Microsoft CHAP (MS-CHAP)
- MS-CHAP v2 (Bindname authentication)

The VPN Router supports LDAP v2 servers.

Figure 6 shows the authentication mechanism between the VPN Router and the external LDAP proxy configuration.

Figure 6 LDAP proxy server



The general filter specification syntax is

- If you do not specify a filter, the resultant search is (uid=username).
- If you do specify a filter string, the search is (&(uid=username)filterstring).

For example, a filter value of (|(ou=engineering)(ou=finance)) creates a search that specifies UID=username and (ou= engineering or ou=finance) (&(uid=username)(|(ou=engineering)(ou=finance)).

Certificate LDAP query syntax is (&(SubDn=<subject DN from cert>)(CAAttribute=<issuer DN from cert>)myFilter) or (&(SubAltName=<subject alt name from cert>)(CAAttribute=<issuer DN from cert>)myFilter).

To determine the SubjectDN or Altname, check to see if the UID of the session is the same as the subject DN of the certificate.

To configure LDAP proxy server authentication

1. Select **Servers**, **LDAP Proxy,** and then click **Enable Access to LDAP Proxy Server**.
2. Select the **Remove Suffix from User ID** box to remove the fully qualified ID suffix from the UID before the system sends it to the LDAP server.
3. Specify the character that separates the suffix from the UID as the delimiter value.
4. In the **LDAP Proxy Server Users Obtain Default Settings from the Group** list, select the default group to which to assign users.
5. Select a number from the **Response Timeout Interval** list.
6. Under **LDAP Proxy Servers**, in the **Base DN** box, type a base distinguished name for the server. The DN uses the form ou=organizational unit, o=organization, c=country.
7. For the remote LDAP server, type the **Master**, **Slave 1**, and **Slave 2** LDAP server host names or IP addresses. If the master server becomes unavailable, the VPN Router attempts to initiate a connection with the slave servers.
8. In the **Connection** section, type the port number (default 389) and the associated SSL port number (default 636) on which your LDAP server listens to queries.

9 Type the bind distinguished name, which is the LDAP equivalent of a user ID, that you need to access the base DN and its subentries. Leave the **Bind DN** box blank if your LDAP server uses anonymous access.

10 Enter the **Bind Password**, which can consist of up to 32 characters. The VPN Router uses this password to prove its identity (the bind DN) to the LDAP server.

11 In the **Username/Password Access** section, you can use case-insensitive character strings in LDAP search filters. The default value for each field is blank. If you do not supply a value, the authentication fails. Enter the user name and password. To enable additional policy checking, specify an LDAP search filter, which can be a case-insensitive character string (default is blank).

12 Use the **User Certificate Access** section to add digital certificates support for authentication, type the **Subject DN attribute**, such as common name, organizational unit, organization, and country.

13 Type the **Subject Alternative Name attribute**.

14 Type the **Certificate Authority (CA) attribute**.

15 Type the **LDAP filter** name.

16 In the **User Policy Attributes** section, specify attributes used to store the VPN Router group, static IP address and netmask, and customized user filter.

17 Click the **SSL Encryption** link to go to the **LDAP server SSL encryption** window. Select the encryption types the VPN Router uses during negotiation with the external LDAP server.

18 To change the order in which the VPN Router applies authentication, select **Services**, **IPsec,** and then click **Swap Server Order 2 and 3**. External LDAP proxy is disabled by default, and you must add it as an option before you can swap it.

19 Select **Profiles**, **Groups** to add or select the group that you want as the default group for LDAP users (this group is the group to which the router assigns a user if the LDAP server does not send back a class attribute).

20 Select **Profiles**, **Groups, Edit**, **Configure IPsec**. In the **Authentication** area, click **Configure**. Enter the group ID, the group password, and then confirm the group password. You cannot use the same group ID and user ID. Consider

using the LDAP group name as the default group because you must remember a default name after you enter it.

Note: The Start and Stop option disappears after you restore the LDAP database. If you need to refresh the window after the restore is complete and the restore status window is not available, you can select it from the menu.

To configure IPsec and LDAP on the client

1. In the Nortel VPN Client, select **Options**, **Authentication Options,** and then click **Group Security Authentication**.
2. Enter the group ID and group password.
3. Select one of the group authentication options.
4. Click **OK**.

LDAP proxy user authentication and password management

User authentication and password management support the LDAP v3-compliant servers, such as IBM RACF and Netscape/Novell directory server. LDAP controls within the bind response from the LDAP server combined with the error message within the bind response find the password status: expired, expiring, or valid password. You can change the Nortel VPN Client password to the proxy server if the password expires.

"LDAP proxy user authentication" on page 43 shows the proxy server access fields.

Figure 7 LDAP proxy user authentication

LDAP v3-compliant LDAP server

LDAP controls are an extension of the LDAP protocol in LDAP v3. The controls pass extended information with LDAP requests and responses. Netscape Directory Server 3.0 and later uses LDAP controls to return password information within bind responses. This information determines if the user password is expiring or already expired.

After you configure the VPN Router to use an external LDAP authentication server, it informs users that their passwords are expired or expiring and lets the client change the password. If the RACF server password expires, the VPN Router sends the password in the format old password/new password. For Netscape Directory, the VPN Router sends the LDAP modify request to modify the password and password time stamp attributes.

Note: The VPN Router currently supports Message Digest 4 (MD4), MD5, SHA, and clear text methods. The VPN Router does not support the Unix CRYPT and Salted Secure Hashing Algorithm (SSHA) encryption methods. If you encrypt passwords saved in LDAP proxy using these methods, the password change does not succeed.

LDAP controls are only passed back when the router performs a user bind. An administrative bind does not trigger password expiration controls; this means that the password must be in plain text to perform the bind, such as PAP within IPsec authentication, as used by the Nortel VPN Client.

LDAP server without LDAP control support

LDAP v2 servers typically require clients to bind before they perform operations. This enhancement uses simple authentication to bind to an LDAP server to authenticate the user. The server returns a bind response to the client that indicates the status of the session setup request.

The bind response contains the result along with the string representation of the error message. This response indicates whether the password is invalid or expired. For the IBM RACF server, the following list identifies error messages under the standard result code 0x49 (Invalid Credentials):

- R004128 = Password not Valid
- R004110 = User Revoked
- R004109 = Password Expired

The error message determines whether the password expired. If the password expires, the change password window appears on the client. The LDAP user bind to the IBM RACF server implements the password change. IBM RACF server returns the LDAP result of either success or invalid credentials.

To configure LDAP proxy user authentication and password management

1. Choose **Servers**, **LDAP Proxy**.

   The LDAP Proxy Server window appears.

2. Click **Pwd Management**.
3. Select the server type from the list. The choices are
   - Not Specified
   - IBM RACF Server
   - Netscape Directory
   - Novell eDirectory
   - Microsoft Active Directory
4. Type a value for **Password Timestamp Attribute**. This field can hold case-insensitive character strings. The default value for each field is blank. Authentication fails if no specified value exists.
5. Type the value of **Password Life Time** in days.

6 Click **OK**.

After you log on to the Nortel VPN Client, the Change VPN Password window appears with a message that your VPN password expired. To update your password

1 Type your old password in the **Old Password** box.

2 Type your new password in the **New Password** box.

3 Type your new password again in the **Verify Password** box.

4 Click **OK**.

Monitoring LDAP servers

If the VPN Router cannot reach the LDAP proxy server, it still operates and passes traffic. However, the VPN Router does not authenticate users whose information exists in a third-party directory. The VPN Router pings the LDAP proxy servers every few minutes to check their status. If the VPN Router receives an Internet Control Message Protocol (ICMP) reply, it attempts to contact the LDAP proxy server. This process is similar to the way the VPN Router monitors RADIUS servers.

External LDAP servers behave differently because the server must reply to ICMP echo requests and accept a directory bind before the VPN Router considers it available. After initialization of the external LDAP server, the VPN Router monitors the health of each external LDAP server to determine if the server is available. If the VPN Router cannot contact the directory, the VPN Router runs, but it does not terminate tunnels or pass network traffic.

Note: If you configure an external LDAP proxy server that is unavailable, you can experience delays in VPN Router provisioning times.

The VPN Router monitors the status of all configured external LDAP servers. If the VPN Router marks the server status as up, it binds and conducts a search against the directory every 15 minutes to monitor the status of the server. If the VPN Router marks the server status as down, it performs the following actions:

1. The VPN Router monitors the status of the server by issuing an ICMP echo request to the server every 15 minutes.
2. If the VPN Router receives an echo reply, it attempts to bind and search the directory.
3. If the bind and search succeeds, the VPN Router changes the status of the server to up and returns the server back into the server list for operation.

If either the bind or search fails, the server remains in the down state.

Note: If multiple systems share an external LDAP, parameters you add or remove from the external database by one system are not visible to the other system until you flush the database caches. The cache flush is a timed interval.

After the primary external LDAP server initializes, the VPN Router issues an ICMP echo request to all secondary server IP addresses and follows the previous procedure for each secondary server.

Because the VPN Router assumes only read and write access to the primary external LDAP server, it does not configure secondary server directories for VPN Router directory storage. Instead, the VPN Router relies on the LDAP replication agreements between the primary LDAP server and secondary LDAP servers to populate the secondary servers with the appropriate directory information.

During normal operations, the VPN Router utilizes the primary external LDAP server. If the primary LDAP server fails, the VPN Router fails-over to the next secondary LDAP server in succession. Only the servers marked up are attempted. After the VPN Router detects the return of the primary server, it returns to normal operations and utilizes the primary server exclusively.

RADIUS authentication service

RADIUS is a distributed security system that verifies connection attributes and authenticates connections. RADIUS is available on both public and private interfaces. You enable RADIUS on the RADIUS Service window. Packets flow from external clients to the VPN Router interface IP and port. You configure the port on the RADIUS Service window. To configure filters, choose Services, Available and in the Authentication Protocol section, select Public or Private for RADIUS.

After you enable RADIUS client authentication, the VPN Router acts as a RADIUS authentication client to external RADIUS authentication servers. You enable client authentication on the RADIUS Authentication window. External authentication servers are on either public or private networks. You determine the packet flow from the IP address or port, which you configure on the RADIUS Servers section of the RADIUS Authentication window, to external servers and back. You control the filters by choosing Servers, RADIUS Auth, Enable Access to RADIUS Authentication. After you enable RADIUS, the router uses public and private filters.

The VPN Router acts as a RADIUS accounting client to external RADIUS accounting servers. You enable accounting on the RADIUS Accounting window. External accounting servers are on either public or private networks. The packets flow from the IP address or port, which you configure on the External RADIUS Accounting Server section of the RADIUS Accounting window, to external servers and back. You configure filters with the RADIUS Accounting options on the Services window. You can use the RADIUS Authentication window to configure up to three servers for remote authentication. The RADIUS servers must contain the same user data. The VPN Router uses the alternative RADIUS servers only after it receives no response from the primary RADIUS server.

Most RADIUS servers support CHAP and PAP authentication, and some support MS-CHAP.

Note: If you require PPTP-encrypted tunnels and RADIUS authentication, you must use a RADIUS server that supports MS-CHAP. Alternatively, you can use an LDAP server for PPTP authentication.

Configuring RADIUS authentication

The VPN Router supports authentication against a RADIUS server. This server can reside on either a private or public network that connects to the VPN Router. To enable RADIUS authentication, you must configure the VPN Router with the RADIUS server host name, port number (typically 1645, but port 1812 is the RFC standard), and a shared secret. You access the VPN Router management window by choosing Servers, RADIUS Auth.

Use the RADIUS Authentication window to configure the type of authentication methods that can access the RADIUS server. Five options exist, of which only four are IPsec-related:

- CHALLENGE
- RESPONSE
- MS-CHAP-V2 is available for PPTP and L2TP tunnel users only; it is not applicable to IPsec tunneling applications
- MS-CHAP is available for PPTP and L2TP tunnel users only; it is not applicable to IPsec tunneling applications
- CHAP
- PAP

If you use token cards for authentication, you must select the appropriate technologies (SecurID, PassGo Technologies Defender, or both) from the Services, IPSec menu path, and the appropriate authentication methods (CHALLENGE, RESPONSE, or both) from the authentication methods list. For example, the SecurID passcode is the pin plus the token code.

Note: The UID and password are never passed in clear text for an IPsec client, either from the remote client or from the VPN Router that communicates with the RADIUS server. If you use PAP authentication for a PPTP session, both the user name and the password are passed in clear text to the VPN Router over the Internet.

No significant security benefit exists between using CHAP or PAP. PAP authentication consumes fewer instructions during the authentication process because the connection between the VPN Router and encryption protects the RADIUS server.

If you use RADIUS-based authentication, the IPsec client and the VPN Router require a second set of credentials for mutual authentication. These credentials are the group ID and group password.

For information about the remote access client, see the Nortel VPN Client online Help. On the IPsec client side, the remote user must

1. Choose **Options**, **Authentication Options**.
2. Click **User Group Security Authentication**.
3. Enter the group ID and group password.
4. Select one of the following options:
   - Challenge Response Token
   - Response Only Token
   - Group Password Authentication

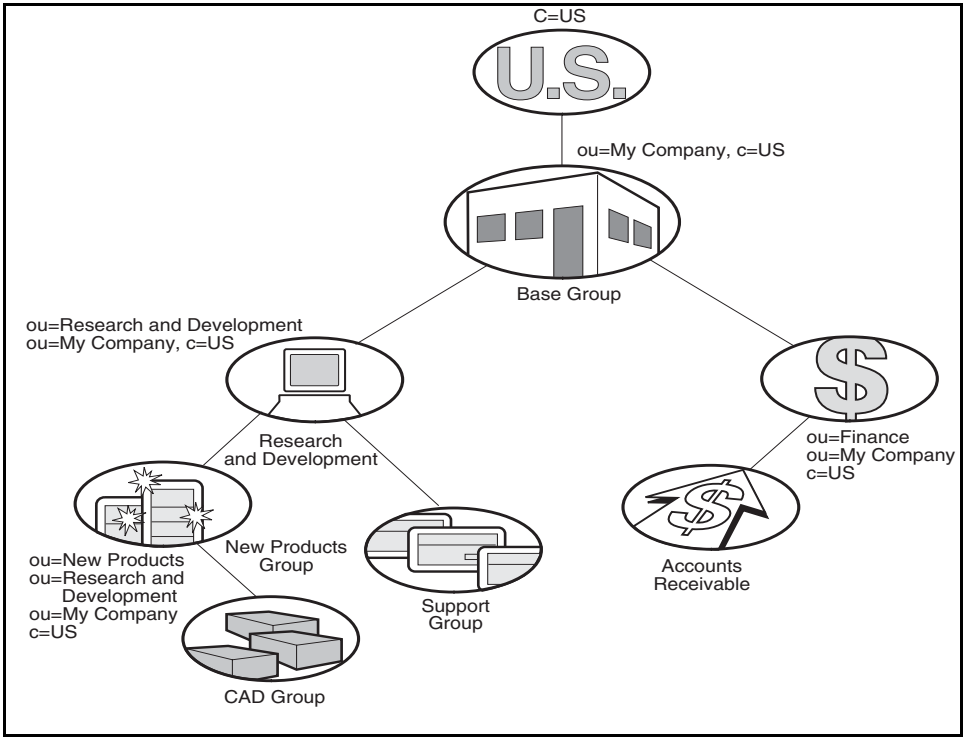
To complete the RADIUS setup, you must configure at least one group profile for RADIUS users. In this profile, you must enter the group ID, password, and the allowed group authentication options. You can configure the group profile from the Groups > Edit > IPsec window.

1. Set up and test the operation of the RADIUS server with ACE or Defender servers, depending on the type of token security you want. Do this before you attempt authentication by an IPsec client to verify that everything on this side of the network operates properly.
2. Identify and create the groups to authenticate token users, and supply the group ID and password to all users using either token card or group password authentication. PassGo and SecurID users are created and maintained in their respective servers, not in the VPN Router. Add the groups in the Groups > Edit > IPsec window.
3. Define the RADIUS server configuration settings for token security.
4. Define the tunnel settings for IPsec. Add a RADIUS server. For more information, see "Configuring IPsec authentication" on page 52.

RADIUS authentication class attribute values

For more information about the relationship between RADIUS authentication class attribute values for VPN Router users, see "RADIUS authentication class attribute values" on page 50. C is the class attribute for country, and OU is the class attribute for organizational unit.

Figure 8 RADIUS authentication class attribute values



The VPN Router supports RADIUS-supplied attributes, such as IP address and Microsoft Point-to-Point Encryption (MPPE) key and additional specific attributes. The VPN Router ignores all other returned attributes. For more information, see the Microsoft documentation and RFC 2548. This data overrides the corresponding data stored in LDAP, if it exists. "RADIUS class attributes" on page 51 shows common examples of class attributes.

Table 1 RADIUS class attributes

Name	Value format	Function
Class	ou=groupname	The router assigns the user to the group groupname, if the group exists.
Framed-IP-Address	dotted decimal	If the router uses static addresses, it uses this IP address for the tunnel session.
Framed-IP-NetMask	dotted decimal	The router uses this subnet mask with the preceding IP address.
Filter-ID	filter name	If defined, this filter name applies to the tunnel session.
DNS	domain server name	If the router uses DNS, this attribute specifies the DNS server name.
NBNS	protocol name	Specifies the NetBIOS protocol; an internet naming service. This attribute translates the NetBIOS Windows domain name to the IP address.

"RADIUS example details" on page 51 shows sample details that you enter into your RADIUS server.

Table 2 RADIUS example details

User ID	Class attribute value	Assigned group
Lee Madison	ou=New Products, ou=Research and Development	New Products
Julie Lane	None	Default
Bill Sullivan	ou=Staff	Default (ou=Staff does not exist)

The RADIUS server uses the class attribute value to associate the user ID with a group in the LDAP database.

RADIUS-Assigned Framed-IP-Address attribute

Configure a RADIUS-Assigned Framed-IP-Address attribute on the RADIUS server for the UID that the VPN Router authenticates. If you enable Static Addresses (Profiles, Groups, Edit, Connectivity window) for the assigned group, the tunnel session uses the returned IP address. Otherwise, the router assigns an IP pool address.

Note: The RADIUS server returns only a single IP address. Therefore, each UID can use only one active tunnel connection.

Configuring IPsec authentication

The following procedures describe how to configure the VPN Router to interoperate with a RADIUS server while using either IPsec or PPTP.

To configure IPsec and RADIUS

1. Choose **Servers**, **Radius Auth**.

   The RADIUS Authentication window appears.

2. Select **Enable Access to RADIUS Authentication**.
3. Select **Remove Suffix from User ID** to remove the fully-qualified ID suffix from the UID before sending it to the RADIUS server. Specify the character that separates the suffix from the UID as the delimiter value.
4. Select **Remove Prefix from User ID** to remove the fully-qualified ID prefix from the UID before sending it to the RADIUS server. Specify the character that separates the suffix from the UID as the delimiter value.
5. Select **Error Code Pass Thru Enable** to allow an error message sent to the VPN Router by the RADIUS server to pass through the VPN Router to the originating client.
6. In the **RADIUS Users Obtain Default Settings from the Group** list, select the default group to which to assign users.
7. Enable one of the following authentication methods from the Server-Supported Authentication Options section:

- **CHALLENGE**—Challenge and Response token cards

- **RESPONSE**—Response Only Token Cards
- **MS-CHAP-V2**—Microsoft encrypted CHAP Version 2
- **MSCHAP**—Microsoft encrypted CHAP Version 1; select **RFC-2548** to enable the VPN Router to interoperate with a Microsoft RADIUS Server Version 2.2 or later, or a Version 2.1 with the Microsoft Hotfix applied. Clear this check box if you use a Microsoft RADIUS Server V2.1 (without the Hotfix) or earlier
- **CHAP**—Challenge Handshake Authentication Protocol
- **PAP**—Password Authentication Protocol

8 Under the **RADIUS Servers** section, select **Enabled** for the RADIUS servers that you want to use for authentication (up to three servers). The primary server receives all RADIUS authentication inquiries unless it is out of service. A RADIUS server that fails to respond five times is temporarily taken off the server list for 30 minutes. After 30 minutes, the router tries the server again. In the event that the primary server is unreachable, the VPN Router queries the first and second alternate RADIUS servers.

9 Type either the host name or IP address of the servers. For example, finance.mycompany.com or 145.22.120.111. You can also use simple names (for example, finance) if your VPN Router uses a Domain Name System (DNS) server. For **Primary**, type the primary RADIUS server host name (required if you enable RADIUS). The primary server normally processes incoming authentication requests. For **Alternate 1**, type the first alternate RADIUS Server host name (this server processes incoming authentication requests if the primary RADIUS server is unavailable). For **Alternate 2**, type the second alternate RADIUS server host name (this server processes incoming authentication requests if the primary RADIUS Server and the first alternate server are unavailable).

10 Under **Interface**, specify whether you want to access the RADIUS server from the private or public interface. Use the address of the interface to configure the RADIUS client address information on the remote RADIUS server. You must enable RADIUS authentication as an allowed service on the **Services**, **Available** window. Select **Private** if the router reaches the RADIUS server through the private interface and uses the management address. Select **Public** if the router accesses the RADIUS server through the public interface. You must also specify the IP address for the public interface. The public IP address list builds dynamically from the information on the **System**, **LAN** window. A change, such as removing an interface card or changing an IP address, is automatically reflected in the list.

11 In the **Port** box, type the server port number that you want the RADIUS authentication requests to use. The default is port 1645.

12 In the **Secret** box, type the password to share with the VPN Router. To enhance overall security, enter a different password for each server. The shared secret encrypts the password between the VPN Router and the server if the tunnel connection uses PAP or SecurID. The secret also verifies the authenticity of each accounting request sent by the VPN Router to the RADIUS server and the authenticity of each response sent by the RADIUS server to the VPN Router.

The VPN Router can store all passwords encrypted with 3DES, but you must first enable the 3DES feature. For more information about 3DES, see "Encrypting with 3DES password" on page 33.

13 Confirm the password by reentering the **Secret** to verify that you typed the password correctly.

14 Use the **Reply Source Port** option to configure the port that the RADIUS server uses as a source in the RADIUS authentication reply. The default value is 0 (only allow a reply packet with the source port of 1645). The UDP port is the port you configure in the Port attribute of the RADIUS server configuration on the **Servers**, **RADIUS Auth** window. The default port value is 1645.

Reply Source Port is only necessary if you use a RADIUS server that sends a RADIUS authentication reply with a UDP port that differs from the originating UDP port. For example, if the VPN Router sends a RADIUS authentication packet using the UDP source port 1100 and UDP destination port 1645, the RADIUS server responds with a UDP source port of 8500 and a destination UDP port of 1100. The VPN Router expects a reply with a source UDP port of 1645 and a destination UDP port of 1100. Therefore, the router drops this packet because the UDP port 8500 is not open (by default) and filters the packet.

15 Select **Suppress Service Type** to remove the service type 8 attribute from the RADIUS access message and to return attributes to the VPN Router. This option maintains forward compatibility with newer versions of SBR.

16 In the **Response Timeout Interval** box, type the frequency in seconds that you want the VPN Router to wait before retrying to connect to the RADIUS servers. By default, the VPN Router tries once every 3 seconds. The minimum setting is 1.

17 In the **Maximum Transmit Attempts**, type the number of times that you want the VPN Router to try to connect to the RADIUS servers before failing. By default, the VPN Router tries three times.

18 Click the **RADIUS Diagnostic Report** link to verify that your RADIUS authentication configuration is correct. This report compares the settings on the RADIUS authentication window to the corresponding settings on other VPN Router configuration windows. The title of each section of the diagnostic report lists the name of the related window. For example, the IPsec RADIUS Configuration section of the report contains information related to the **Services**, **IPsec** window.

19 Enable a server and enter the server host name or IP address, the interface type, port number (1645), and secret. Click **OK**.

20 Select **Services**, **IPsec**.

The IPsec Settings window appears.

21 Click **Add RADIUS** to add a RADIUS server to the Authentication Order table.

22 Select **Profiles**, **Groups** to add or select the default group for RADIUS users (this group is the group to which the router assigns a user if the RADIUS server does not send back a class attribute).

23 Select **Profiles**, **Groups**, **Edit**, **IPsec Configure**.

The Groups > Edit > IPsec window appears.

24 The Authentication section shows the authentication method for the group selected. Enter the group ID and group password. Consider using the LDAP group name as the default group, because you must remember a default name after you enter it. If your RADIUS server returns a class attribute, ensure that the group uses the authentication method. However, you do not need a group ID and group password for a group that is returned as a class attribute.

Note: You must set the group ID and password in the Nortel VPN client as well as in the group profile to use RADIUS authentication.

To configure IPsec and RADIUS on the client

1. In the Nortel VPN Client, choose **Options**, **Authentication Options** and click **Group Security Authentication**
2. Enter the group ID and group password.
3. Select one of the group authentication options.
4. Click **OK**.

Configuring RADIUS dynamic filters

The Nortel VPN Router offers several methods to control network access for authenticated users. RADIUS distribution of filters is particularly beneficial for applications that require a large number of access filters. The alternative to RADIUS dynamic filters is to configure the filters for each user account in LDAP, which can become difficult to maintain in large networks.

Tunnel filters apply at the group level and control access to network resources as well as management access to the VPN Router. After the VPN Router authenticates a user, it assigns them to a group. Part of the group profile specifies that you apply a filter. Dynamic filters distribute filters for IPsec user tunnels by using a RADIUS return attribute. Depending on the configuration of the RADIUS server, these filters can vary by individual user, or apply to an entire class of users.

Note: These filters apply only to IPsec user tunnels; they do not apply to branch office tunnels or non-IPsec tunnels.

You must enable tunnel filters for the RADIUS dynamic filters to take effect. You can set up and manage policy filters in the RADIUS server that the VPN Router retrieves. RADIUS returns the access control list (ACL) to the VPN Router. IPsec user tunnels are dynamically filtered based on attributes returned from the authenticating RADIUS server. The returned dynamic filters are then prepended to the groups filter to which the user is bound.

Dynamic filtering minimally affects performance. Some performance degradation can occur during user tunnel creation, depending on the number of rules processed. Passing of traffic can degrade in a way similar to that which occurs if you configure a large number of tunnel filters in a user group.

You configure all dynamic filters on the remote RADIUS server. Before you configure dynamic RADIUS filters, you must first configure the RADIUS server.

Many RADIUS servers exist, each with different specifications for configuring return attributes. Regardless of how you configure return attributes, they always use the following AV-Pair to define and transmit attribute and value pairs:

- Vendor Specific Attribute (VSA)—26
- Vendor Code—9 (Cisco)
- Attribute—1 (AV Pair)

The supported syntax is

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Operator] [Port]

The following table describes the syntax of the attributes.

Table 3 Syntax of attributes

Section	Description
Prefix	ip:inacl#Num= ip:outacl#Num= Num is a number that specifies the order in the list. Inacl and outacl are the only two AV pair types supported.
Action	Deny or permit
Protocol	IP, TCP, UDP, or ICMP
Source	An IP Address, any, or host <host address>
Source wildcard mask	A source of any or host does not use this attribute. Note the mask is not a subnet mask. 0 indicates exact match for an octet. 255 indicates a don't care for all of the bits in the octet.
Destination	An IP address, any, or host <host address>
Destination wildcard mask	A source of any or host does not use this attribute. Note the mask is not a subnet mask. 0 indicates exact match for an octet. 255 indicates a don't care for all of the bits in the octet.
Operator	LT—Less than, GT—Greater than, EQ—Equal, NEQ—Not equal TCP and UDP use the Operator attribute.
Port	Port number. You must provide a port if you specify an operator.

Do not specify an outacl that denies all traffic, for example, ip:outacl#1=deny ip any any, because this prevents the IPsec client from connecting to the banner server. You must specify at least one outacl entry. You can specify a deny all filter in the group.

The following example permits all IP traffic inbound to 10.10.1.2 and all ip traffic outbound.

```
ip:inacl#1=permit ip 0.0.0.0 255.255.255.255 host 10.10.1.2
ip:outacl#1=permit ip any any
```

To configure RADIUS dynamic filters with the CLI, enter the following commands:

```
CES>enable
Password:
CES#config t
Enter configuration commands, one per line.  End with Ctrl/z.
CES(config)#group add /Base/Radius
CES(config)#group connectivity /Base/Radius
CES(config-group/con)#filters "deny all"
CES(config-group/con)#exit
CES(config)#firewall tunnel-filter
CES(config)#aaa authentication ipsec radius
CES(config)#radius-server primary host 199.74.229.28 auth-port 1645
CES(config)#radius-server primary key secret
CES(config)#radius-server primary enabled
CES(config)#radius-server authentication pap
CES(config)#radius-server default-group /Base/Radius
CES(config)#aaa authorization network radius
CES(config)#exit
CES#
```

Configuring PPTP and RADIUS

To configure PPTP and RADIUS

1. Choose **Servers**, **Radius Auth**, and then click **Enable Access to RADIUS Authentication**.
2. Enable an authentication method.
3. Click **OK**.

If the RADIUS server does not return a valid class attribute, the router places PPTP users in the default group that you configure on the Servers, RADIUS Auth window.

Note: Everything about the authentication type must match; for example, if you send an encrypted password, you must enable MS-CHAP on the RADIUS authentication window, and the RADIUS server must support MS-CHAP.

Configuring group-level RADIUS authentication

In remote access deployments, if you want to partition users across several different RADIUS servers, the VPN Router can connect to the appropriate server when it authenticates a specific user. This group-level authentication is particularly useful for large installations with many different databases, and for carriers with a business need to keep customer authentication domains separate.

To configure the group-level RADIUS authentication server for each group

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

The Groups > Edit > IPsec window appears.

2 Click the **Configure Group Level RADIUS Servers** link in the Authentication section. You can configure the following:

- a primary and two alternate RADIUS servers
- IP address, interface, port, and secret
- user ID suffix removal and delimiter value
- Response Time out and Maximum Transmission Attempts

For user name and password authentication, the PAP/CHAP settings are retrieved from the Servers, RADIUS Authentication Servers window.

Group-level RADIUS authentication works only with clients that use a group ID and password. This method excludes all non-IPsec client implementations. You must use the group ID and group password to configure each client in the group for group authentication.

Note: No separate group levels of authentication exist on a RADIUS configuration for the firewall user authentication (FWUA) users. Because FWUA users are only members of the global group configuration, if you use multiple RADIUS servers, you must add these users to the group on the VPN Router global RADIUS configuration window. This configuration also applies to PPTP and L2TP user tunnels.

Vendor-specific RADIUS attribute

You can use the vendor-specific RADIUS attribute to store VPN Router group membership information in a RADIUS vendor-specific attribute as well as to the class attribute.

Configuring RADIUS accounting

You can use the RADIUS accounting configuration window to specify how your VPN Router saves RADIUS accounting results. By default, the router stores the results locally. You can also save the RADIUS accounting information to a remote RADIUS server.

Note: If you set the date ahead, and then set it back, external RADIUS accounting no longer works.

To configure RADIUS accounting

1 Choose **Servers**, **Radius Acct**.

The RADIUS Accounting window appears.

2 Select **Enable** to enable internal RADIUS accounting. Internal RADIUS accounting is enabled by default.

3 In **Session Update Interval**, type an interval after which a snapshot of the current active tunnel sessions records to a journal file. Use the format,

hh:mm:ss, for the interval. The journal file stores the session information until the user logs off from the tunnel session, after which the session stop record saves on the local disk. If the system crashes, after reinitialization the VPN Router translates the journal file into a series of stop records on an individual session basis. This process minimizes accounting data loss. A low interval creates system overhead and requires additional processing. The default interval is 00:10:00 (10 minutes).

4. In **Remove Accounting Files**, type the number of days before the files are removed.
5. Select **Enable** to enable the Interim RADIUS Accounting Record feature. This selection is enabled by default.
6. In **Interim Update Interval**, type the interval at which time interim RADIUS records are sent to the specified external RADIUS server. Use the format hh:mm:ss for the interval. A short interval creates system overhead which requires additional processing. The default interval is 00:10:00 (10 minutes).
7. Select **Enable** to send accounting records to the external RADIUS accounting server.
8. Enter the external RADIUS server host name or IP address. If you enter a host name, use a fully qualified domain name, such as Finance.mycompany.com.
9. Click **Private** or **Public** for the Interface.
10. Enter the server port number that you want the RADIUS accounting requests to use. The default is port 1646.
11. Enter the required secret (password) of the external RADIUS server.
12. Reenter the secret (password) to verify that you typed the password correctly.
13. Click **Test Server** to verify the connectivity from your VPN Router to the external RADIUS server. A message at the top of the window shows the results of the test.

The VPN Router sends RADIUS accounting start and stop records to an external RADIUS server. These interim records provide information about the currently active sessions on the VPN Router. Use this information to evaluate VPN Router usage, such as connection start and stop times.

DHCP server configuration

Dynamic Host Configuration Protocol (DHCP) dynamically assigns IP addresses to clients and provides centralized network administration. After a DHCP client requests an IP address, a DHCP server grants the client exclusive use of an assigned IP address for a specified period of time.

If you configure both the DHCP server and DHCP relay on the same interface, the DHCP server takes precedence, and the DHCP server processes the DHCP packets received by the VPN Router. For the DHCP relay to function, you must disable the DHCP server for the interface on which you configure the DHCP relay.

Note: The VPN Router includes a full implementation of a DHCP server in compliance with RFC 2131 and RFC 2132.

The source of the packets the DHCP server sends is the IP address of the private interface from which these packets are sent. The server ID field in these packets uses the IP address of the interface from which these packets are sent. One exception exists for backward compatibility. After the DHCP server receives unicast DHCP discovery packets (from DHCP Relay agents, or from other Nortel VPN Routers that use this specific DHCP server as the user tunnel IP address source) that have a destination of the management IP Address of the VPN Router, the source of the response packets is the management IP. The server ID field in this case uses the management IP address.

The following restrictions apply to the DHCP server:

- You can enable the DHCP server only on private (trusted) interfaces.
- The DHCP server is enabled by default only on the private 0/1 interface of the diskless platforms.
- DHCP relay and the DHCP server are mutually exclusive on a physical port.

Note: You can enter duplicate IP addresses for the DNS servers without receiving error messages stating that duplicate addresses exist. This applies to both the GUI and CLI interfaces.

To configure the DHCP server

1. Choose **Servers**, **DHCP**.

   The DHCP Server window appears.

2. Select **DHCP Service Enabled** to enable the DHCP server.
3. In the **Default Options** section, specify the lease time in the ddd:hh:mm:ss format or select **Infinite** to indicate an unspecified period of time.
4. Click **Add** in the **Standard Options** section to access the **Add Option** window. The standard options section shows the current status of added options and lets you add new options:
   - Select the desired options from the list.
   - Select the desired type from the list.
   - Enter the appropriate value.
5. Click **OK**.
6. In the **Pool** section, click **Add** to add a pool.
7. In the **Add Pool** window, type the base IP address for the pool.
8. Type the subnet mask for the pool.
9. Type a pool name.
10. Type a description of the pool.
11. Click **OK**.
12. Select **Pool** and click **Configure** to return to the **Pool** window.
13. Use the Inclusion Range section to add blocks of IP addresses that you can then give out. Under **Inclusion Range**, click **Add**.
14. In the **Pool Inclusion** window, type the base IP address for the **Start Address**.
15. Type the end IP address.
16. Click **OK**.
17. Optionally, you can select an Exclusion Range for further control of the IP addresses that you give out. Under **Exclusion Range**, click **Add**.
18. On the **Pool Exclusion** window, type the start address for the range.
19. Type the end address for the range.
20. Click **OK**.

21 Optionally, you can force the DHCP server to assign a fixed IP address to a host every time the host logs on. Under the **Host** section, click **Add**.

22 On the **Host** window, type the host name that is registered with DNS.

23 Type the IP address that you want to reserve.

Note: The fixed IP address must be from the same subnet as the pool you configure on the VPN Router.

24 Type the Ethernet (MAC) address.

25 Click **OK**.

26 The server does not implement configuration changes until it restarts. Return to **Server**, **DHCP**, and then click **Restart Service** to restart the DHCP server.

27 To verify the configuration changes, choose **Status**, **Health Check** or **Status, Statistics**, **DHCP Stats**.

Remote user IP address pool configuration

Remote access users who use tunneling protocols require two IP addresses to form packets. The addresses are normally referred to as outer and inner addresses. The outer address, or public address, is visible when packets travel through the public data networks (PDN). The client negotiates this address with the ISP to which it connects. The VPN Router does not control this address.

The inner IP address is the address that appears on the private network after the router removes the outer layers of the packet. Therefore, this address must be within the private network address space. The VPN Router provides the remote user with the inner IP address during tunnel setup. This address can come from the internal DHCP, a local address pool, an external DHCP server,, a RADIUS server, or from an external LDAP proxy server.

The VPN Router assigns the inner IP address from one of several sources, using the following order:

1 user-specified (excluding IPsec)

2 static address, either the LDAP database, the RADIUS server, or the external LDAP proxy servers

3 local address pools, internal DHCP pools, or external DHCP pools

Use the Remote User IP Address Pool window to select a method for users to obtain IP addresses to access the private network. The VPN Router services these addresses, and they are available to remote users on demand. You can choose IP addresses assigned from one of the following:

- internal DHCP pool
- external DHCP pool
- internal address pool

If you use external DHCP pools, a DHCP server on the private LAN segment dynamically assigns IP addresses on behalf of remote users. You must use an existing DHCP server to choose this option. A broadcast or unicast (depending on the option you select) DHCP request contacts the DHCP server. The DHCP server associates the accepted IP addresses with the management IP address.If you use internal DHCP pools, an internal DHCP server assigns the IP addresses. A unicast DHCP request (sent to 127.0.0.1) contacts the DHCP server.

You can enable a combination of Internal DHCP, External DHCP and Address Pool but you must enable at least one of those options. When you specify an external DHCP server, you must enter the primary server address, and you can configure two backup server addresses.

If you use an IP address pool using external DHCP servers, the pool name on the external server must match the pool name you configure for the group on the VPN Router. One exception exists: if the pool name you configure for the group on the VPN Router is Default, you do not need to match the name of the pool defined on the DHCP server.

In previous software releases, you can specify a pool name on the VPN Router that does not exist on the DHCP server. Beginning with Release 8.0, if the pool names do not match, users in the group cannot form Nortel VPN Client connections with the router.

The external DHCP server option provides the following:

- A cache of prenegotiated DHCP addresses so that the client does not wait to acquire an address at logon.
- All DHCP controls, for example, cache size, immediate release, blackout time, and blackout override, can fine tune the behavior of the DHCP client.

The internal DHCP server option also provides the following:

- A cache of prenegotiated DHCP addresses so that the client does not wait to acquire an address at logon.
- All DHCP controls, for example, cache size, immediate release, blackout time, and blackout override, can fine tune the behavior of the DHCP client.
- Named pools are supported. The pool name from the user or group profile selects which of the internal DHCP server pools a local address comes from.

If you use local address pools, a default pool can provide addresses after the preferred pool is exhausted or unavailable. The default fail over control enables or disables the default pool.

To configure a DHCP address pool

1 Choose **Servers**, **User IP Addr**.

The Remote User IP Address Pool window appears.

2 Select either **Internal DHCP Server**, **External DHCP Server**, or **Address Pool**.

3 Select **Internal DHCP Server** to allow a block of addresses.

To use this pool. on the **Profiles**, **Groups**, **Edit**, **Connectivity Configure** window, you must select **Internal DHCP** as the user IP address source and select the internal pool in the **Address Pool Name** list.

4 Select **Any External DHCP Server** to allow an available external DHCP server to provide the requested IP addresses. Any External DHCP Server is the default selection.

To use this pool, on the **Profiles**, **Groups**, **Edit**, **Connectivity Configure** window, you must select **External DHCP** as the user IP address source and specify the external pool in the **Address Pool Name** box.

5 Select **Specified DHCP Server** to allow only a specified DHCP server to provide IP addresses. Indicate the IP addresses of the servers that provide DHCP service, including primary, secondary, and tertiary. A status field provides information about the associated servers. Secondary or tertiary server configuration is optional.

6 Type the **DHCP Cache Size**. This value is the number of IP addresses held in the VPN Router cache. The minimum number of IP addresses held is 1, and the maximum is derived from the maximum number of tunnel sessions that the VPN Router supports.

7 Select **Immediate Address Release** if a limited number of available IP addresses exist and you want the VPN Router to release the IP address back to the DHCP server immediately. IP addresses from disconnected tunnel sessions remain unavailable for the time you specify (300 to 7200 seconds). This delay prohibits immediate reuse by another user that can represent a security risk.

8 For **DHCP Blackout Interval**, type the amount of time in seconds that a DHCP address is held in a blackout state before it returns to the DHCP server or the DHCP cache.

9 Select **Override Blackout Interval when no addresses are available** to enable this option.

To add a user IP address pool

1 Choose **Servers**, **User IP Addr**.

The Remote User IP Address Pool window appears.

2 Click **Add** to add a new address pool.

3 Type the starting IP address and ending IP address for this pool. Make sure that none of the pool addresses are the same as those used for the LAN interfaces or the management interface IP address. The VPN Router does not check the IP address supplied by a PPTP client to see if it is assigned to a LAN interface, management interface, or address pool.

To avoid potential conflicts, you can verify the current state of the **Use Client-Specified Address** option from the **Profiles**, **Groups**, **Edit**, **Configure PPTP** window.

4 Type the **Subnet Mask** for the pool. You can later edit the subnet mask as necessary.

5 Beside Pool, click **Default** and type the name of the pool. The name must match the group profile for either DHCP or for a local address pool.

   Select **Profiles**, **Groups**, **Edit**, **Connectivity Configure,** and then click the **Address Pool Name** list to select the address pool used by remote users to access the VPN Router. The list shows all pools on the VPN Router.

   Optionally, select **New** to define a new pool and type the name of the pool. The default for this option is Default.

6 Click **OK** to save the entries for the IP address pool, and return to the **Remote User IP Address Pool** window.

7 In the **Address Pool Exhausted Amount** box, type a value for the percentage of the pool address to use before the system triggers an SNMP trap.

8 In the **Address Pool Blackout Interval** box, type the number of seconds to wait before the system makes an address available again.

9 Select the action to take if the named address pool is not available.

10 Click **OK**.

You can use internal address pools to select the block of addresses a particular users local address comes from. You can name internal pools, but you must also specify the pool name in the group profile. For example, a profile for software engineering and hardware engineering groups can select addresses from the engineering address pool. You can also define a default internal address pool to supply an address if the preferred pool is exhausted or otherwise unavailable.

To remove a user IP address source from the VPN Router configuration, you must first remove it from the group profile.

DHCP relay configuration

The DHCP relay agent on a VPN Router forwards DHCP and Bootstrap Protocol (BOOTP) messages between a server and a client on different subnets. After a locally attached host issues a DHCP or BOOTP request as a broadcast message, the VPN Router relays the message to a specified DHCP or BOOTP server. The DHCP relay agent also forwards DHCP replies from server to client.

Note: The DHCP relay agent can run only on the private physical interfaces and tunnels.

You can enable or disable DHCP relay for each interface and specify the DHCP servers for each interface. After you enable DHCP relay on an interface, the VPN Router forwards DHCP requests from the interface to the DHCP server configured for the same interface.

The DHCP relay agent unicasts DHCP packets only to the specified Helper servers (up to three). You must specify the Server 1 address. Server 2 and Server 3 addresses are optional. Additionally, you can enable and disable each DHCP server by checking or unchecking Enable.

To add a DHCP relay interface

1. Choose **Servers**, **DHCP Relay,** and then click **Add**.
2. Select a physical interface from the list.
3. For the state, select either **Enabled** or **Disabled**.
4. For the DHCP Server, enter the IP address, and then click **Enabled** for Helper 1, Helper 2, or Helper 3.
5. Click **OK**.

To view DHCP relay statistics

1. Choose **Servers**, **DHCP Relay**.

   The DHCP Relay window appears.

2. Click **Statistics**.

The DHCP Relay Statistics window provides the following details:

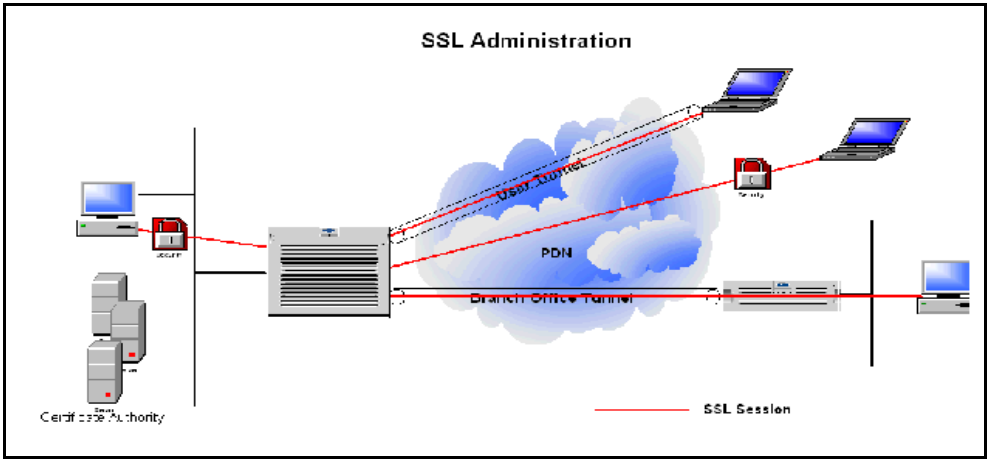
- In—total number of all the incoming DHCP packets
- Out—total number of forwarded DHCP packets
- Discarded—total number of incoming packets that were ignored because of bad content
- Relayed To Server—total number of packets forwarded to a DHCP server
- Relayed To Client—total number of packets forwarded to DHCP client

SSL administration

The SSL administration feature provides secure management of the VPN Router over SSL-enabled HTTP (HTTPS) over all tunnel and interface types. Remote management of a VPN Router requires only an SSL-enabled Web browser, which most operating systems include.

"SSL administration" on page 70 shows an example of SSL administration.

Figure 9 SSL administration



SSL/TLS uses TCP port 443 for secure HTTP communication. Interface and tunnel filters govern HTTPS packets destined for the management IP address. If you enable tunnel filters, you must permit HTTPS for SSL management through a VPN tunnel.

The Stateful Firewall applies only to HTTPS traffic routed through the device, not to the management IP address.

The VPN Router uses HTTPS services for FWUA and SSL-enabled administration.

The following cipher combinations exist:

- (DHE_RSA_WITH_3DES_EDE_CBC_SHA, 0x16)
- (RSA_WITH_3DES_EDE_CBC_SHA, 0x0a)
- (RSA_WITH_RC4_128_SHA, 0x05)
- (RSA_WITH_RC4_128_MD5, 0x04)
- (RSA_EXPORT1024_WITH_RC4_56_SHA, 0x64)
- (RSA_EXPORT1024_WITH_DES_CBC_SHA, 0x62)
- (RSA_EXPORT1024_WITH_RC4_56_MD5, 0x60)
- (DHE_RSA_WITH_DES_CBC_SHA, 0x15)
- (RSA_WITH_DES_CBC_SHA, 0x09)
- (DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, 0x14)
- (RSA_EXPORT_WITH_DES40_CBC_SHA, 0x08)

To use SSL administration, you must

- Enable HTTPS services for the public or private interface on the Services, Available window.
- Explicitly allow HTTPS if you enable tunnel filters on the Profiles, Filters window for management through a VPN tunnel.
- Install a valid server certificate on the VPN Router and apply it to the SSL/TLS services to authenticate and validate SSL connections.
- Select ciphers and apply the server certificate on the Services, SSL/TLS window.
- Use an SSL-enabled Web browser.
- Use a valid administrator user name and password.

Browser security checks

If you use certificates, Netscape Communicator and Internet Explorer perform different security checks. Nortel recommends that you perform the following configuration to obtain the best performance when you administer the VPN Router using SSL administration.

1. Make an entry in the hosts file that corresponds to your VPN Router management IP address, such as 11.0.0.12 VPNRouter1.
2. Import the root certificate that issued your VPN Router server certificate into the browser store as follows:
3. For Netscape Communicator to accept the mime type application/ x-x509-ca-cert, choose **Edit**, **Preferences**.
4. Click **Applications**.
5. Click **New Type**.

   A new window appears.
6. Fill in the following information in the new window:
   - Description of type—CAcert
   - File extension—cacert
   - MIME Type—application/x-x509-ca-cert
   - Application to use—netscape.exe
7. Click **OK** to complete the Netscape configuration.
8. Save the base64 format root CA certificate onto a file with extension .cacert.
9. Select **File**, **Open Page** and open the file. Netscape Communicator guides you to install the CA certificate.
10. In Internet Explorer, select **Tools**, **Internet options**, **content**, **certificates**, **trusted root certification authority** tab, and select **import**.
11. Import the **root certificate** that issued your VPN Router server certificate into the JRE certificate store.

Note: To satisfy a further name check by Netscape browsers, make the VPN Router server certificate common name either a DNS name that resolves to the management IP address or the management IP address.

Configuring SSL/TLS and configuring HTTP services

To configure SSL/TLS and enable HTTP services

1 Choose **Services**, **Available,** and then select HTTPS services on the public or private interfaces to permit TCP port 443 through the system filter. If you enable HTTPS on both the public and private interfaces, you permit port 443 through either interface. For more information about the Services window with port 443 selected for HTTPS, see "HTTPS services" on page 73.

Note: You must change the port from port 443 to run HTTPS to configure an SSL VPN server at the default 443 port while still allowing HTTPS management.

Figure 10 HTTPS services

Management Protocol	Port	Public	Private	Access List
HTTP	80		☑	(None)
HTTPS	440	☑	☑	(None)
SSH Server	402	☑	☑	(None)
SNMP	161		☑	(None)
FTP	21		☑	(None)
TELNET	23		☑	(None)
SSL-VPN Admin GUI (SSH)		☑	☑	
Identification			☐	
CRL Retrieval		☐	☑	
CMP		☐	☑	

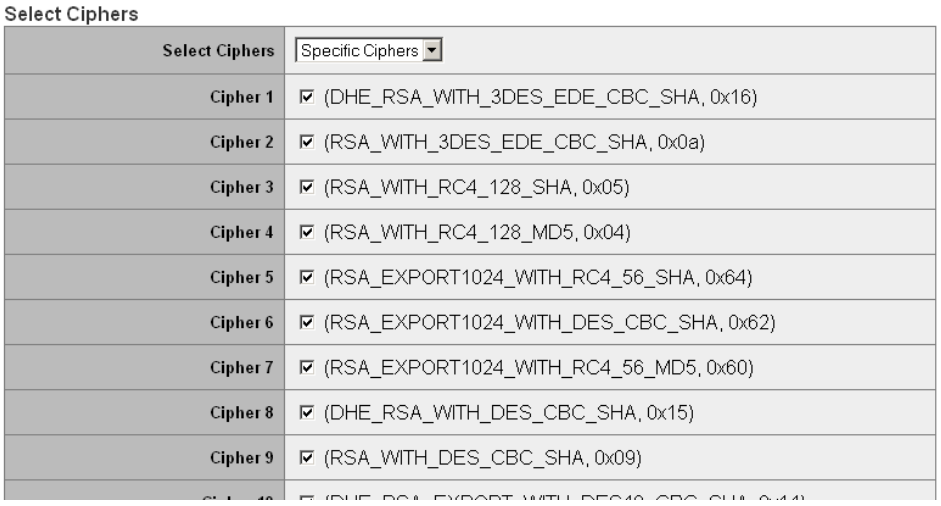
2 Select **Services**, **SSL TLS**, select the necessary ciphers, and then select a digital server certificate (for example, CN=ces1, O=MyOrg, C=US).

For more information about the SSL TLS window with select ciphers, see "Select ciphers" on page 74.

3 Click **Advanced Options**, and then select the check box if you do not want empty fragments for CBC ciphers inserted.

4 Click **Apply**.

Figure 11 Select ciphers



5 Verify **SSL** is enabled on the Web browser of the management PC.

To test the SSL administration feature, direct an SSL-enabled Web browser to the private interface of the VPN Router. To use this service from the public side of the VPN Router, you must direct your browser to the public IP address.

DNS server configuration

The DNS maps host names to IP addresses. Use DNS to provide an updated set of mappings for all Internet devices.

A DNS server holds the segment of the DNS database for which it is the authority. DNS clients are TCP/IP applications that refer to hosts by host name. If an application needs to convert a host name to an IP address, it uses the client portion. This action creates a DNS query that specifies the host name and sends the query to a server. The server looks for the host IP address by looking in its database or by making queries to other servers. The server returns a DNS response to the application that contains either the IP address or an error indicating that the host name is unknown.

Companies often set up their own DNS internally, and leave it to the ISP to handle all external DNS. These companies use their own DNS servers, but use the external DNS servers for noncompany names. This method splits the DNS names into two separate systems: the private, company-controlled DNS names and the Internet DNS names.

The VPN Router provides the following DNS services:

- DNS Proxy where the VPN Router caches information from corporate DNS for faster address resolution. This method eliminates the need for a separate branch office server. For more information, see "DHCP server configuration" on page 62 and "DNS server configuration" on page 74.
- Split Proxy DNS occurs after a negative response from a DNS server (private) prompts the VPN Router to try a second DNS server (Internet). Split DNS supports private and Internet names without mixing the two and eliminates the need to publish private names on public DNS. For more information, see "DHCP server configuration" on page 62 and "DNS server configuration" on page 74.

You can configure the VPN Router 1010, 1050, or 1100 as a DNS proxy, which means that it can act like a DNS server for a PC on the private network. The PCs send their DNS queries to the DNS proxy, which in turn passes the query to its set of true DNS servers. Whether you configure a DHCP client or Point-to-Point Protocol Over Ethernet (PPPoE) determines which DNS servers respond. After the DNS proxy receives a DNS query from a PC, it passes the query on to the DNS servers until it receives a response, which it subsequently returns to the PC.

You can configure up to four DNS servers. The ISP can assign more than one DNS server, which display on the window. Enable split DNS if your DNS name space splits into private names and public names; a DNS server knows the private names while another server knows the public Internet DNS names.

To configure a DNS server

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

The System Identity window appears.

2 Enable **DNS Proxy** if you want the DNS Proxy to act as a DNS server to the private side. It resolves names for locally connected hosts and those from other DNS zones. It it enabled by default.

3. Enable **Split DNS** if you use a split name space.
4. For Primary Server, type the DNS server IP address that the DNS proxy tries to contact first.
5. For Second Server, type an IP address for the second DNS server. If the primary DNS server does not respond in a few seconds, the proxy requests service from the second DNS server.
6. For Third Server, type an IP address for the third DNS server. If the primary and secondary DNS servers do not respond, the proxy requests service from the third DNS server.
7. For Fourth Server, type an IP address for the fourth DNS server. If the preceding servers do not respond, the proxy requests service from the fourth DNS server.
8. Click **OK**. The VPN Router checks all of the DNS addresses to see if they respond, and then provides an operational or error status.

Chapter 3
Certificate configuration

Digital certificates bind the public encryption or signing key of an entity to its identity, and verify that identity with a trusted third party (the certification authority). Use digital certificates to authenticate both Lightweight Directory Access Protocol (LDAP) and VPN connections. This chapter includes the following topics:

LDAP server SSL encryption

The Secure Socket Layer (SSL) provides Internet security and privacy and ensures privacy between the VPN Router and the external LDAP server. The SSL protocol negotiates encryption keys and authenticates the server before data is exchanged. SSL maintains the transmission channels security and integrity through encryption, authentication, and message authentication codes. The SSL implementation supports the following encryption methods:

- RC4 128-bit Message Digest 5 (MD5) encryption—most secure method. The longer the encryption key, the more secure the encryption. US export law controls the export of 128-bit encryption keys.
- DES 56-bit SHA encryption—mid-level encryption method, less secure than RC4-128, but more secure than RC4-40.
- RC4 40-bit MD5 encryption—least secure method of encryption.

You can configure SSL parameters after you switch from internal to external LDAP servers.

Installing LDAP certificates

The LDAP connection between the VPN Router and the directory server is authenticated asymmetrically. Initially a one-way authenticated SSL connection establishes after the directory server passes its certificate to the VPN Router. After SSL authentication establishes, the VPN Router authenticates itself to the directory server by presenting its LDAP bind DN and password.

For the SSL connection to succeed, the VPN Router must trust the issuer of the certificate presented by the directory server during the initial SSL authentication.

To import an LDAP proxy SSL proxy certificate

1. Choose **System**, **Certificates**, and then click **Import Tunnel or Transport Certificate**.
2. Paste the PKCS #7 formatted Certificate Authority (CA) certificate into the box.
3. Click **OK**.

To import an LDAP SSL certificate

1 Choose **Servers**, **LDAP**.

The LDAP Server window appears.

2 Click **Import Secure LDAP (SSL) CA certificate**.

3 Paste the PKCS #7 formatted CA certificate into the box.

4 Click **OK**.

LDAP special characters

You use the LDAP special character enhancement to create certificate subject distinguished names (DN) that contain previously unsupported special characters, such as the comma. This enhancement is compliant with RFC 2253.

You do not need to enable the special character support if the certificate subject DN does not contain special characters such as comma (,), quotes (") or backslash (\) as valid characters.

Note: You need to update the LDAP to use this feature if you upgrade from an older version, and the certificate subject DN already contains special characters. Contact Nortel technical support for details to update the LDAP.

To configure LDAP special characters

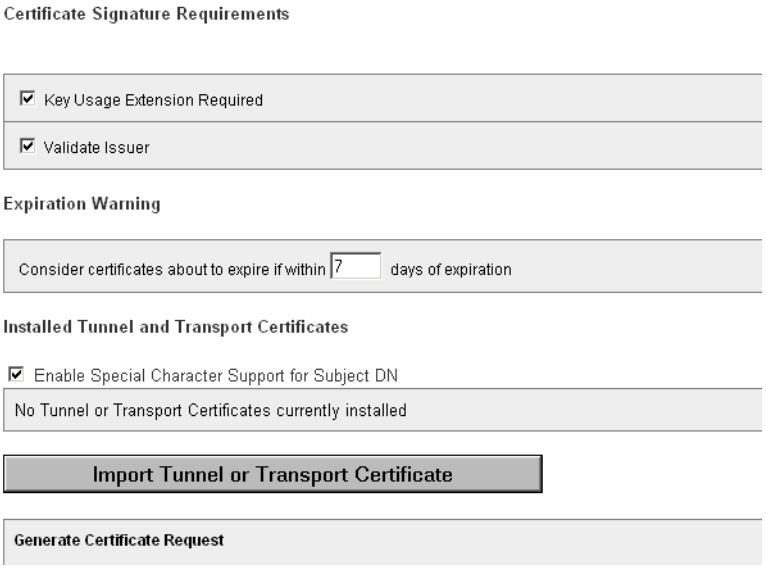
1 Choose **System**, **Certificates**.

The Certificate Configuration window appears.

2 Select **Enable Special Character Support for Subject DN**. The default is disabled.

"LDAP special characters" on page 80 shows the System, Certificates window with LDAP special characters enabled.

Figure 12 LDAP special characters



External LDAP proxy

External LDAP proxy supports the mapping of the following certificate subject DN attributes to defined LDAP attributes:

- User cert Common Name attribute
- User cert e-mail address attribute
- User cert serial number attribute
- User cert uid attribute
- Subject Alternative Name attribute

The advanced setup includes flexible mapping. The basic setup is the default on upgrade.

Configurable warning time for certificate expiration

You can configure the VPN Router so that Health Check Certificates Validity sends a warning that a certificate is due to expire. You must enable SNMP traps, and Server Trap Configuration must include Certificates Validity, with the Send One parameter cleared.

To configure certificate expiration warning

1 Choose **System**, **Certificates**.

The Certificate Configuration window appears.

2 In the Expiration Warning section, type the number of days. The default is 7 days; the maximum is 365. Figure 12 shows the default of 7.

3 Click **OK**.

VPN security using digital certificates

You can use X.509 certificates to authenticate IPsec tunnels and Layer 2 Tunneling Protocol (L2TP)/IPsec tunnels. The VPN Router supports RSA digital signature authentication for the IPsec Internet Key Exchange (IKE) key management protocol. Remote users can authenticate themselves to the VPN Router using a public key pair and a certificate as credentials. The VPN Router uses its own key pair and certificate to authenticate the VPN Router to the user. The VPN Router must explicitly import and trust the CA certificate that issued the certificate to the tunnel initiator.

Public key infrastructure

A public key infrastructure (PKI) issues and manages certificates for both network hosts and end users. An important decision about the design of a PKI is how to implement CA services. You can use commercially available products from a vendor such as Entrust, where the CA resides in your facility and you operate.

CA and X.509 certificates

The CA issues and revokes certificates within a PKI. The CA ensures certificates are valid by signing each certificate with its own digital signature. The CA stores a copy of all signed certificates in a publicly accessible certificate repository. Certificate users use this repository to verify that other user certificates are valid.

Loading certificates

You must install two types of certificates in the VPN Router: server certificates and trusted CA certificates. Server certificates are certificates that the VPN Router requests for itself, and uses to prove its identity to connecting tunnels. Trusted CA certificates are certificates that issue end user or branch office tunnel certificates, and that the VPN Router imports to establish a common trust.

You can request server certificates either manually (using cut and paste #7 and #10) or automatically with Certificate Management Protocol (CMP) support.

Generating a server certificate request

Consult the CA user documentation for instructions about how to generate reference numbers and authorization codes, as well as general CA administration information. If you use Entrust CA generated certificates with your VPN Router

- Both Entrust Web certificates and Entrust Enterprise certificates work properly when you use Hypertext Transfer Protocol (HTTP)-based cut and paste operations.
- Entrust does not support CMP renewal for Web certificates if you use CMP automated lifecycle management to request and renew certificates.

Installing server certificates using cut and paste #7 and #10

To install server certificates using PKCS #7 and #10

1. Choose **System**, **Certificates**.

   The Certificate Configuration window appears.

2. Click **PKCS #10 (or PKCS #7) Certificate Request**.
3. If prompted, initialize the private key password to secure the certificate on the VPN Router.
4. Click **OK**.
5. Fill out the required information for the certificate request.
6. Click **OK**.

7 Copy and paste or save your encoded certificate request (including certificate request begin and certificate request end lines) to a file.

8 Click **Return**.

9 Follow the instructions from your CA provider about how to obtain a certificate.

10 Submit the request to the applicable CA by pasting the encoding into the CA request window, following the instructions provided by the CA to sign the certificate request.

11 Click **Import Tunnel or Transport Certificate**.

12 Select **Server Certificate** to indicate that you are importing a server certificate. Import the signed certificate request and click **OK**.

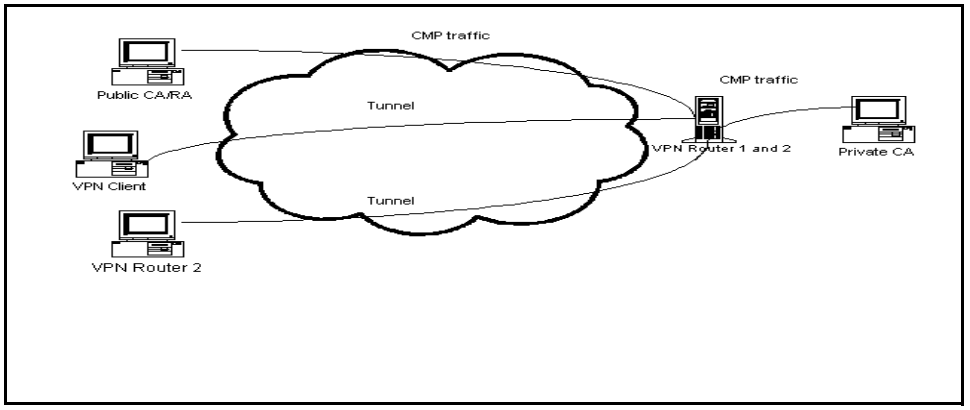
Note: If you use Entrust CA, this request must use a subject distinguished name with a common name that is equal to the Entrust reference number that preauthorizes the certificate issuance.

Installing server certificates using CMP

Use the CMP to create a CMP compliant certificate request. CMP targets management functions for the entire certificate or key life for enrollment, renewal, recovery, and revocation. CMP defines message formats and includes its own message protection. The CA is on the private network if it uses a publicly accessible IP address.

"Sample CMP environment" on page 84 shows a CMP environment.

Figure 13 Sample CMP environment



To initialize the VPN Router for initial certificate enrollment with CMP, you need the following:

- issuer name—CA distinguished name
- subject name—EE distinguished name (common name, organization, organizational unit)
- reference number—identifies the secret value
- transaction ID or authorization code—initial secret value
- enrollment URL or destination (host name or IP address) and optional port number
- imported root CA certificate

To enter this information

1. Choose **System, Certificates.**

   The Certificate Configuration window appears.

2. Click **Certificate Management Protocol (CMP)**. The Certificate Request—CMP window shows the status of outstanding requests and the fields to fill in for a new request.
3. For a new request, type the reference number the CA provides.
4. Type the authorization code supplied by the CA.
5. Select one of the following keys (generally, larger keys are more secure):

- 512
- 768
- 1024
- 2048 (US only)
- 4096

6 Type the port number.

7 Type the registration address or URL.

8 Select **Import Issuer CA Certificate** if you want to automatically import the CA Root certificate with this request.

9 Under **Subject Distinguished Name** (optional), select **Relative** if you are providing a relative name or **Full** if you are providing a full name. If you select **Relative**, type the relative name details:

10 Type the common name associated with the VPN Router.

11 Type the organizational unit associated with the VPN Router.

12 Type the organization associated with the VPN Router.

13 Type the locality where the VPN Router resides.

14 Type the state or province where the VPN Router resides.

15 Type the country where the VPN Router resides.

16 Under **Issuer Distinguished Name** (optional), select **Relative** if you are providing a relative name or **Full** if you are providing a full name. If you select **Relative**, type the relative name details:

17 Type the common name associated with the VPN Router.

18 Type the organizational unit associated with the VPN Router.

19 Type the organization associated with the VPN Router.

20 Type the locality where the VPN Router resides.

21 Type the state or province where the VPN Router resides.

22 Type the country where the VPN Router resides.

23 Click **Apply**.

24 On the **System, Certificates, Certificate Generation** window, select **Details**. Details shows information from the certificate enrollment process. It provides the address for the key update, key recovery, and revocation purposes.

25 In the **port** box, type the port number of the CA.

26 In the **Enrollment Address** box, type the IP address of the CA.

27 Click **Renew Certificate Now** to renew the certificate now.

28 In the **Renew Days before expiration** section, select and type the number of days before the certificate expires.

29 In the **Recover Certificate** box, type the certificate reference number and authentication code.

30 Click **Revoke Certificate Now** to revoke the certificate.

Installing trusted CA certificates

The trusted CA certificate issues the certificate that the remote user or branch office tunnel uses to authenticate, and you must load and mark the certificate as trusted in the VPN Router.

To import trusted CA certificates in PKCS #10 format

1 Choose **System**, **Certificates**.

The Certificate Configuration window appears.

2 Select **Import Tunnel or Transport Certificate**.

3 Select **Trusted CA Certificate** (default).

4 Paste the certificate into the box.

5 Click **OK**. The Installed Tunnel Certificates table shows the certificate entry.

6 Select **Enable 'Allow All' Feature**, if desired.

7 Click **OK**. You now use the CA certificate with which remote users can authenticate. Repeat this operation if multiple CAs issues user certificates.

Optionally, you can configure a certificate revocation list (CRL) distribution point to enable revocation checking of client certificates. Choose **System, Certificates: Installed Tunnel and Transport Certificates: CA Details**, configure the appropriate CRL information, and then click **OK**.

The Enabled check box enables CRL checking of certificates for a particular CA. You must configure the proper values for access to the CRL LDAP or HTTP directory store. For more information, see "Certificate revocation list configuration" on page 93.

Configuring certificate parameters

You can set the following parameters from the Certificate Configuration window:

1. Under **Certificate Signature Requirements**, select **Key Usage Extension Required** if you want the Key Usage V3 extension present in all certificates presented as part of a tunnel initiation (user and branch office).
2. Under **Certificate Signature Requirements**, select **Validate Issuer** if you do not accept a subordinate CA without a parent CA. If you do not select this option, a subordinate CA is accepted even if it is not validated.
3. Under **Installed Tunnel and Transport Certificates**, enable **Allow All** to allow in all tunnel requests authenticated by a particular CA. This option provides a significant configuration savings because you do not provision individual users into the VPN Router.
4. Select **Trusted** if the certificate is trusted. For CA certificates, this indicates that tunnel requests that present this issuer as the signer of their certificate are trusted. For server certificates, this method turns off the certificate without deleting it.

The System, Certificate Details window provides the following certificate details:

- This Certificate Belongs To shows the X.500 distinguished name of the certificate owner.
- This Certificate Was Issued By shows the issuer of the certificate (the CA). In addition to the main attributes, this field also shows the serial number of the issuer certificate.
- Validity Dates shows the starting and ending dates during which the certificate is valid (for example, 01/29/02 through 01/29/03).
- Certificate Fingerprint shows the unique identifier that is derived from MD5 hashing the certificates. Compare the identifier with the fingerprint supplied directly by the certificate issuer (for example, a CA). If the fingerprints do not match exactly, the certificate is forged or modified.

- Version provides information about the version.
- Signature Algorithm provides information about the signature algorithm.
- Public Key provides information about the public key.
- Extensions provides information about the extensions used.

You must configure a group that uses certificate-based authentication to present a server certificate to remote parties that are initiating tunnel requests. The Default Server Certificate is the Subject DN of the certificate that you want to use as the identity of the VPN Router when it initiates or responds to a connection request associated with that group. Tunnel requests are bound to a particular group by the CA certificate that the remote party presents as the signer of its certificate. You can configure the local identity for the group on the Profiles, Groups, Edit window.

Trusted CA certificate settings

To authenticate incoming tunnel requests, you must associate every CA certificate with a group. The group assignment of incoming tunnel requests is accomplished by either finding the user provisioned in the VPN Router directory (internal or external), or by allowing all users issued by a particular CA to gain access. If you allow all users issued by a particular CA, two ways exist to determine the group to which an initiator is assigned:

- direct assignment into the group assigned to that CA
- access control by subject DN

Group assignment by user identification

If the subject DN of the certificate presented by the remote initiator of the tunnel is a user on that VPN Router, the group that the user is bound to is the one indicated in the user configuration.

Allow All policy

If you use Allow All, the VPN Router trusts the CA to establish the true identity of a user. If the user certificate is within the certificate validity period, the certificate signature is verified using the CA certificate, and if the user certificate is not on the CRL from the CA, the tunnel connection is permitted. After the CA certifies users, they can create a tunnel connection as long as their certificate is in good standing.

You can allow all users with certificates issued by this CA to authenticate with the VPN Router, regardless of whether a user entry exists in the LDAP database. By default, the CA certificate does not allow all users authentication. Only users with their subject distinguished names (DNs) entered into the User Management window can authenticate using certificates issued by this CA. If you enable Allow All, you must also select a group for these users from the Default Group list. If you want only specific instances of users to authenticate with the CA authority, you must configure each of these users from the User Management > Edit User window, and disable Allow All authentication for this CA. Only these users can then perform IPsec RSA Digital Signature Authentication using a certificate issued by this particular CA.

You must enable the Allow All feature for each CA certificate against which you want to permit authentication without an explicit user entry. This action allows anyone with a valid certificate from the particular CA to establish a tunnel connection. Also, you must associate a default group with that certificate. The client that authenticates with the Allow All feature then uses the attributes associated with that group. You can also assign Allow All users to specific groups by matching the relative DN of a connecting certificate user. You are not limited to a single default group.

Note: Branch office connections do not support the CA certificate Allow All feature. Therefore, you must configure an explicit branch office connection.

Access control by Subject DN

This form of mapping incoming requests to groups parses the subject DN of incoming certificates to a configured depth and associates it with a corresponding group. During the client authentication process, the VPN Router tries to match the client certificate subject DN with all the associations of the CA. The match can be a partial match or an exact match. In the case of a partial match, the VPN Router uses the longest match from the root of the DN. After a match is found, the router assigns the client to the corresponding group. If no match is found, the router assigns the client to the default group of the CA.

A DN uses multiple components, the relative distinguished name (RDN). The most common components are common name (CN), country name (C), locality name (L), state or province name (S), organization (O), and organizational unit (OU). The order of the RDN does not matter unless multiple OUs are present, but ordering the DN in the following sequence avoids ambiguity: C, S, L, O, OU, and CN.

The following examples show group mappings:

```
ou=VPNRouter, o=Nortel, c=US/base/vpnrouter
ou=Engineering, ou=VPNRouter, o=Nortel, c=US/base/vpnrouter/
Engineering
ou=Marketing, ou=VPNRouter, o=Nortel, c=US/base/vpnrouter/
Marketing
ou=Engineering, o=Bay Networks, L=Boston, S=MA, c=us/base/bay
```

Group and certificate association configuration

This feature provides finer control for you to associate a certificate with a group for IPsec tunnel connections. Each CA user can configure a lookup table between the certificate subject DN and a VPN Router group. After a new tunnel that uses the certificate is authenticated, the VPN Router uses the certificate subject DN to look up the group in the table. If a match (or partial match) exists, the new tunnel binds to the group specified in the table.

If no match is found in the lookup table, the new tunnel binds to the default group if it is configured and if you enable the Allow All feature. Otherwise, the tunnel is denied.

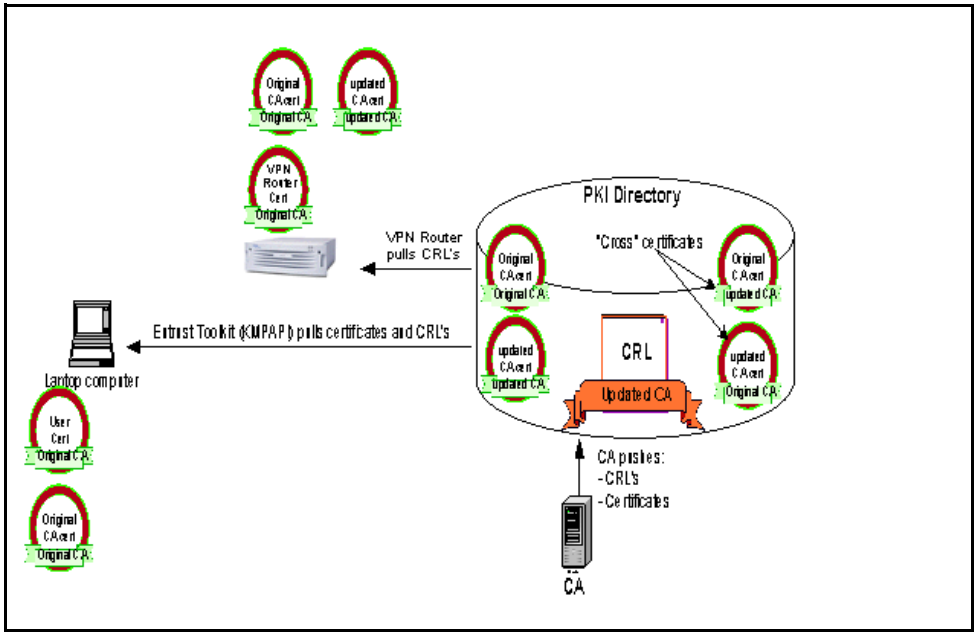
All the attributes (Lookup Table, Allow All, and default group) are CA-specific. To configure the group and certificate lookup table

1. Select the **CA**.
2. Click **Details**.
3. Click **Add** under **Group Access Control**. Use a partial Subject DN (omit one or more left most fields) to simplify the configuration. You can select **Relative** or **Full** to specify the partial Subject DN. Relative automatically generates the DN string. Do not omit a field in the middle of the certificate subject DN, such as o=Nortel or st=MA.
4. Select a group from the list.
5. Click **OK**.

CA key update

The CA key update provides uninterrupted certificate authenticated user and branch office tunnel connections before, during, and after the CA performs the Entrust Key Update function in a PKI environment. You can perform a key update for security or other reasons. "CA Key Update ready for authentication" on page 92 shows a CA Key Update ready for authentication.

Figure 14 CA Key Update ready for authentication



Prior to a key update, the CA pushes the original CA certificate (which is a self-signed root certificate in the preceding diagram) out to the directory, along with the CRL it produced (a list of revoked certificates, digitally signed by the CA certificate). Both the VPN Router and the user PC use certificates signed by that CA, as well as the self-signed CA certificate itself. The user authenticates the VPN Router certificate because it uses the original CA certificate that created the VPN Router certificate stored locally. Likewise, the VPN Router authenticates the user because it uses the CA certificate that issued the user certificate. The VPN Router can also verify that the user certificate is not revoked, because it periodically retrieves the latest CRL from the directory. The VPN Router can authenticate that CRL because it uses the CA certificate that signed it.

After a CA Key Update occurs, the directory contains four certificates:

- the original self-signed
- the new self-signed
- two cross certificates

From this point forward, the updated CA signs all CRLs issued by the CA.

No user tunnel or VPN Router server authentication issues exist at this point, because the original CA signs the certificates presented by the VPN Router and the user, and both parties use the CA certificate stored locally for authentication.

Authenticating the CRL presents a problem for the VPN Router because it is signed by the updated CA certificate, and the VPN Router does not use that updated CA certificate locally to authenticate the CRL signature. The solution is to import the updated CA certificate into the VPN Router.

Import the updated CA certificate into the VPN Router immediately following the CA key update. All post key update CRL processing and therefore tunnel authentication, fail until you complete this action.

Certificate revocation list configuration

A CA can revoke user and server certificates whenever the associated key pair is no longer valid, the key pair is compromised, the user leaves the organization, or a server is retired. After a CA revokes a certificate, the CA updates an associated revocation list with the revoked certificate serial number. This list is the CRL. A CA can use one or more associated CRLs.

Note: When you try to delete a referenced certificate, an error message appears. The certificate is not removed until you remove all references to that certificate.

The CA publishes CRLs in an associated LDAP-accessible directory service. The CA administrator configures the publication frequency. In an Entrust environment, a new CRL automatically publishes at a set time, at a time manually set by an administrator, or whenever a certificate is revoked.

Note: If a CRL directory is on the public side of the VPN Router, the VPN Router retrieves the CRLs through the public interface. The router drops reply packets if the size of the CRL is large enough that the LDAP response includes 40 IP packets or more. To correct this problem, enable the Stateful Firewall.

The VPN Router can optionally use CRLs to verify the revocation status of user certificates. If you enable it on the VPN Router, the router periodically retrieves CRLs from the CA LDAP directory store and caches them in the VPN Router associated LDAP database. This process provides rapid verification of user certificates during IPsec tunnel establishment. You can configure the frequency with which the VPN Router checks for a new CRL.

The VPN Router can use the Online Certificate Status Protocol (OCSP) to retrieve the revocation status of an X.509 digital certificate. You can use either OCSP or the LDAP CRL distribution retrieval method for certificate authentication. Use OCSP for the following reasons:

- OCSP can provide more timely information regarding the revocation status of a certificate.
- OCSP removes the need for clients to retrieve the CRLs themselves, which leads to less network traffic and better bandwidth management.
- The VPN Router does not need to fetch or parse the CRLs, which saves valuable server resources for other tasks.

The VPN Router supports up to three OCSP servers. Two servers are alternative servers. If the master OCSP server is down, the VPN Router chooses the second OCSP server and the third OCSP server if the master and second are both down, for certificate status check.

If you use multiple LDAP and HTTP servers, you can arrange the order of the servers. The VPN Router uses the highest order CRL server first to retrieve the CRL. If CRL retrieval fails from the current CRL server, the VPN Router shifts to the next configured CRL server to try the retrieval.

The CA signs the CRL using a private key, which protects it against tampering. The VPN Router verifies the CRL signature each time it uses the CRL. You must configure a CRL server for each trusted CA certificate that you import into the VPN Router.

Note: The LDAP or HTTP server that contains CRLs for the CA certificates on the VPN Router must be reachable from the public or private interface.

Configuring CRL servers

In the CRL Validation Type section, select either CRL or OCSP to perform the CRL validation. The following list provides explanations for CRL settings:

- OCSP
  - OCSP Servers configures the details for the primary and optional alternate OCSP servers. Select Enable for a particular server. Specify a host name or IP address, the port number, and the path.
  - Add Nonce to Request includes nonce support in the OCSP request and response.
  - OCSP Query Timeout configures the timeout for the OCSP server status check.
  - Check CA Certificate status configures the time interval after which to check the CA certificate status.
  - Send OCSP Request In Server Status Check sends the OCSP request in the server status check.
  - OCSP Server Status Check Interval configures the time interval after which to check the OCSP server status.
- LDAP (CRL option)
  - CRL Retrieval Enabled determines whether the VPN Router tries to retrieve a CRL from the configured directory. If the CRL retrieval is successful, the VPN Router verifies the revocation status of the presented certificates. The VPN Router sends a trap to the Simple Network Management Protocol (SNMP) management server on every instance of CRL retrieval (success or failure). If you do not select this option, the VPN Router does not attempt to retrieve a CRL, and does not verify revocation status of presented certificates. Clear this option to turn off CRL checking. To enable CRL Retrieval, click Enable for CRL Retrieval on the Admin, SNMP Traps, Trap Groups Server, Configure window. If the VPN Router reboots or fails to retrieve a CRL, the CRL retrieval option on the VPN Router is cleared.
  - CRL Checking Mandatory determines if a CRL must exist when an IPsec tunnel establishes to a particular CA. If you select this option, the VPN Router must use a CRL for tunnel connections to succeed. If you do not select this option, the VPN Router establishes certificate authenticated tunnels when no CRL is present.

— CRL Update Frequency represents the frequency, a value in minutes, at which the VPN Router queries the CA LDAP server for a newly published CRL. The default value of 0 indicates that this VPN Router does not update CRLs. This option is useful if more than one VPN Router shares an LDAP database, but you want only one VPN Router to actually perform the update operation. To minimize the load on an external LDAP server, make sure that only one or two VPN Routers update a shared CRL entry in a multiple-VPN Router, shared external LDAP environment.

— CRL Update Specific Time configures the time and day that a CRL request is sent to the CRL Server.

— CRL System Status is read-only and automatically updates to reflect the CRL update activity.

— CRL query optimization configures CRL performance improvement (LDAP import only). Clear this option to disable CRL performance improvements.

Configuring CRL Retrieval Scheduling

To configure CRL Retrieval Scheduling

1 Choose **System**, **Certificates**.

The Certificate Configuration window appears.

2 In the desired certificate row, click **details**.

3 To apply the **CRL Update Specific Time**, select the check box.

4 To select the days to apply the CRL Update Specific Time, select the desired day options.

5 In the **Time** box, type the desired time, in 24-hour format.

6 To enable the CRL Update Specific Time, click **Update CRL Now**.

7 Click **OK**.

To configure the CRL Update Specific Time on specific days and a specific time with the CLI, use the following command:

```
crl update specific-time time <hh:mm>
```

where
hh:mm is the hour (0 to 24) and minutes of the time to apply the CRL update.

This command uses the following options:

Table 4 CRL update specific time command options

crl update specific-time time <hh:mm> followed by:	
`none | every | [monday] [tuesday] [wednesday] [thursday] [friday] [saturday] [sunday]`	Specifies the choices for the application of CRL update as none, everyday, or on specific days.

To configure the CRL update so that it does not occur on specific days, use the following command:

```
no crl update specific-time
```

This command uses the following options:

Table 5 CRL update specific time no command options

no crl update specific-time followed by:	
`[monday] [tuesday] [wednesday] [thursday] [friday] [saturday] [sunday]`	Specifies the days on which the CRL update does not apply.

To spontaneously apply a CRL update, use the following command:

```
crl update now
```

To configure CRL servers

1 Choose **System**, **Certificates, CA Certificate: Details**, and then click **Manage CRL Servers**. The Manage CRL Servers window provides a list of

currently configured CRL servers for the CA that you can edit or delete. You can configure and add a new CRL server in the New CRL Server section.

2 Select a retrieval method: either **LDAP** or **HTTP**.

3 For LDAP only, in the **Search Base** box, type the portion of the X.500 directory where the CA stores certificate revocation lists. The following is a sample search base entry:

```
ou=Engineering, o=Nortel, c=US
```

4 For HTTP only, in the **Path** box, specify the path to the HTTP server.

5 In the **Host** box, type the host name or IP address of the HTTP or LDAP-accessible directory server that stores the published CRLs. If you use a host name instead of an IP address, you must configure one or more DNS servers on the System, Identity window.

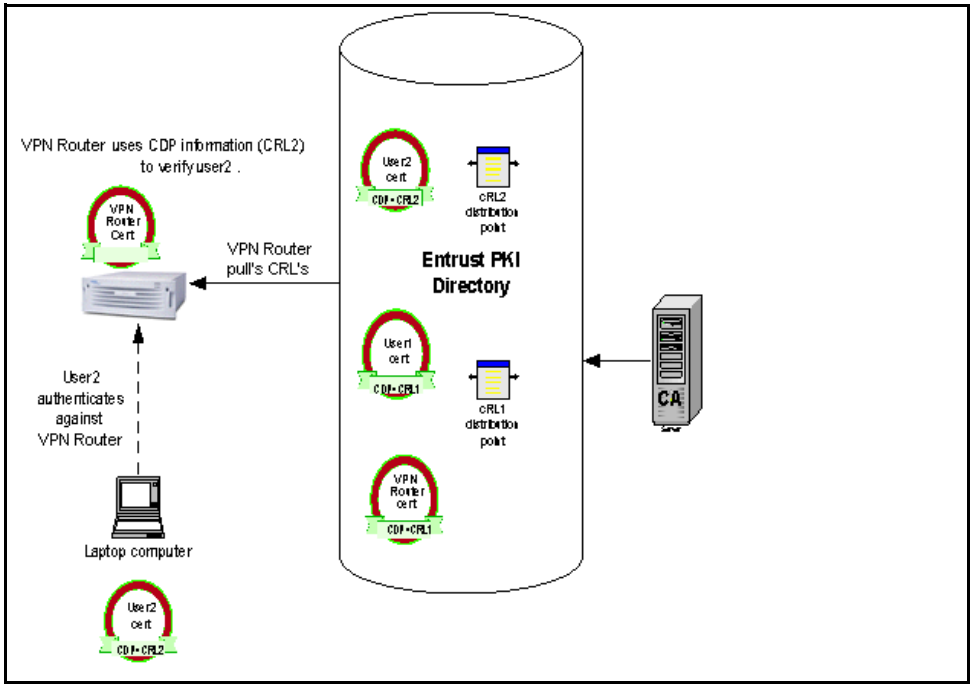
6 In the **Connection** box, type the port number associated with the HTTP or LDAP server. Optionally, select **Enable SSL** to secure the connection with the LDAP server. SSL is not required to handle CRLs because a CRL is signed and is therefore protected against modification and spoofing.

7 Select **Enabled** or **Disabled** to enable or disable the CRL server.

CRL distribution points

CRL distribution points (CDP) identify how CRL vendor-specific information is obtained. The VPN Router supports CDPs for Entrust CAs. After you implement a CDP, users authenticate only against the CRL that is specified in the certificate CDP. This method provides fast tunnel establishment. "CRL distribution points" on page 99 shows an example of CRL distribution points.

Figure 15 CRL distribution points



A tunnel establishes quickly if you authenticate only against the specified CRL in certificates CDP. If you present a certificate for verification, a CDP from your certificate is obtained. The VPN Router uses that CDP information to build a filter for LDAP query and obtain only CRL records that match your CDP. That way you authenticate against one CRL instead of all available CRLs.

Even if the list of CRLs is long, it does not affect performance of the VPN Router because you use only one CRL. If you configure CRL checking to mandatory and CRLs are not present on the VPN Router, the router sends a request to the CA LDAP to obtain only the CRL specified in the user certificate CDP. The VPN Router LDAP loads only that CRL.

After you enable CRL optimization, Global CRL collection, which is stored in VPN Router memory, performs the CRL checking. After you implement CDP support, a user certificate obtained from the Entrust CA is verified against one CRL from Global CRL collection.

CRL retrieval

All CRL records are retrieved periodically. You can configure the interval at which CRL records update. Each CRL record uses a next update time to determine if the CRL record is stale. If the CRL record is stale, it is refreshed from CA LDAP.

Enabling certificate use for tunnels

For IPsec, you must enable RSA digital signature support for default groups associated with CAs, and the groups that contain specific instances of users who are using certificate-based authentication.

To enable RSA digital signature support

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

   The Groups > Edit > IPsec window appears.

2. In the **Authentication** area, select **RSA Digital Signature**.
3. Select the appropriate Default Server Certificate from the list. This certificate is sent to clients to authenticate the VPN Router identity. Issue this server certificate from the same CA PKI that issued the remote access client certificates.
4. Click **OK**.

For L2TP/IPsec authentication

1. Choose **Profiles**, **Branch Office**, **Configure** for an L2TP branch office connection.

   The Connection Configuration window appears.

2 From the list, select the authentication method that you want to use for the branch office connection.

Note: After you change the authentication type, the window immediately changes to reflect the requirements of the new authentication method. Changes that you make on the Authentication portion of the previous window are lost.

3 Type the local UID. This ID is the user ID of the local VPN Router.

4 Type the peer UID. This ID is the user ID of the remote VPN Router.

5 Type the password for the UID, and then confirm the password to verify that you typed it correctly. If you select a variation of MS-CHAP V2 authentication, no password is required for the local UID.

Identifying individual users with certificates

An alternative to allowing all users issued by a particular CA to gain access to the VPN Router is to identify users explicitly by certificate attributes.

To create IPsec certificate credentials

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

The User Management > Edit User window appears.

2 In the **IPsec Certificate Credentials** section, select a valid issuer CA from the list. You configure these CAs from the **System**, **Certificates: Generate Certificate Request** window.

3 Configure either the relative distinguished name or the full distinguished name.

The relative distinguished name is a collection of components that uniquely identify the remote peer in an IPsec certificate environment.

4 You can optionally enter a subject alternative name in place of a subject DN, and specify the type of the name. The following formats are acceptable:

- Email name (for example, net_admin@company.com)
- DNS name (for example, gateway.cleveland.company.com)

- IP address (for example, 192.168.34.21)

5 Click **OK**.

Identifying branch offices with certificates

You use the Authentication section of the Profiles, Branch Office, Connection Configuration window to configure the authentication between the local and remote branch office VPN Routers. The boxes that appear in this window depend on whether you are using an IPsec, PPTP, or L2TP tunnel type. This section describes IPsec and L2TP authentication.

Select the authentication method that you want to use for the branch office connection from the list.

Note: After you change the authentication type, the window immediately changes to reflect the requirements of the new authentication method. Changes that you make on the Authentication part of the previous window are lost.

IPsec authentication

In the Authentication section, complete the following information

1 Type the preshared key as a text or hexadecimal string. This string is an alphanumeric text or hexadecimal string for authentication between the local and remote branches. For authentication to occur, you must use the same string on both the local and remote branch offices.

2 Associate certificates with each endpoint VPN Router to allow for mutual authentication between two connections. The Certificate section includes information about the remote branch office system, the authority that issued the certificate, and the certificate identification.

3 Remote Identity 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 when it makes a connection.

4 Select a valid issuer CA from the **Valid Issuer Certificate Authority** list. This CA is the issuer of the remote peer certificate or a higher-level CA in the certificate hierarchy of the remote peer. You must configure the trusted flag for the CA on the Certificates window. If you use a CA hierarchy, you must import all intermediary CAs below the trusted CA to the VPN Router. These certificate authorities are configured on the System, Certificates: Generate Certificate Request window.

5 If you use a distinguished name to identify the remote branch office site, you can enter the DN as either a relative distinguished name or a full distinguished name. The DN you enter must exactly match the DN in the remote peer certificate.

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

6 The relative distinguished name uses the following supported components:

- Common Name—type the common name with which the server is associated
- Org Unit—type the organizational unit with which the server is associated
- Organization—type the organization with which the server is associated
- Locality—type the locality in which the server resides
- State/Province—type the state or province in which the server resides
- Country—type the country in which the user resides

7 The local identity is the name of the VPN Router 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 this system. If you select a subject alternative name from the VPN Router certificate, that identity is used instead of the VPN Router subject DN when the router communicates with peers.

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

8 Click the list to view all certificates that are issued to the server. Configure server certificates on the **System**, **Certificates**: **Generate Certificate Request** window.

L2TP/IPsec authentication

In the Authentication section, complete the following information

1 Under **Local UID**, type the user ID of the local VPN Router.

2 Under **Peer UID**, type the user ID of the remote VPN Router.

3 Type the password for the local UID, and then confirm the password to verify that you typed it correctly. If you select a variation of MS-CHAP V2 authentication, no password is required for the Local UID.

4 Select **Enable** or **Disable** to enable or disable compression.

5 Select to enable or disable the **Compression/Encryption Stateless Mode** option. This option is not used if encryption and compression are both disabled.

6 The **L2TP Access Concentrator** (for L2TP authentication only) list appears if you selected L2TP as the preferred tunnel type for the branch office connection. Use this entry to specify the L2TP access concentrator that you want to perform authentication between the VPN Router and the NAS.

7 Select an **IPsec data protection minimum level** (Triple DES, 56-bit DES, or Authentication Only). To configure this option, you must disable L2TP encryption and compression.

8 Select a valid issuer CA from the list.

9 Enter the DN to identify the remote branch office site.

10 Select the server certificate issued by the same CA as the remote branch certificate from Local Identity list.

11 Click **OK**.

Two factor authentication

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, but instead of using only one authentication type for every incoming connection, the router performs two authentication steps. Single authentication is the default mode for tunnel authentication.

Two factor authentication is based on the Extended Authentication within ISAKMP/Oakley (XAUTH) draft. The feature uses ISAKMP messages on User Datagram Protocol (UDP) port 500.

Two factor authentication improves security because users must supply two credentials to gain network access. One credential is something the user knows, for example, a user name and password, or preshared key, while the other credential is something stored on the user workstation or on a card (a certificate). You must enable two factor authentication for both ends of the branch office connection. To use two factor authentication you must store user names and passwords on an internal or external LDAP or RADIUS server.

If you enable two factor authentication for a branch office tunnel, you must supply both a certificate and a preshared key, either hexadecimal or text. For a user tunnel, you must supply both a certificate and a user name and password. To implement two factor authentication for user tunnels, you must use Nortel VPN Client 8.01 or later.

If you enable two factor authentication for an established branch office tunnel, the tunnel shuts down, and then reestablishes to use the new authentication mechanism. If you enable two factor authentication for an established user connection, the existing tunnel is not affected. The tunnel uses the new authentication mechanism after the next logon.

To enable two factor authentication

1. Choose **Profiles**, **Groups**, and then click **Edit** for the group.

   The Groups > Edit window appears.

2. For **IPsec**, click **Configure**.

   The Groups > Edit > IPsec window appears.

3. For **Authentication**, click **Configure**.
4. Select **Enable** for Two Factor Authentication.

   You cannot use two factor authentication at the same time as group ID authentication.

5. Select an authentication type.

   Two factor authentication ignores the RSA SecurID option. The router checks the local LDAP before it tries external servers. If you select both RADIUS and LDAP proxy, the router uses the authentication order you configure on the IPSec Settings window.

6. Click **OK**.

To configure two factor authentication for a branch office tunnel

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

   The Branch Office window appears.

2. Select the connection to configure, and then click **Configure**.

   The Connection Configuration window appears.

3. In the **Authentication** list, select either **Dual: Certificates and Text Pre-Shared Key** or **Dual: Certificates and Hex Pre-Shared Key**.
4. Complete the shared key information.
5. Complete the certificate information.
6. Click **OK**.

To configure two factor authentication for a user tunnel

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

   The User Management window appears.

2. Select the group to which the user belongs, and then click **Display**.
3. For the specific user, click **Edit**.

   The User Management > Edit User window appears.

4. For **IPsec Authentication**, select **Two Factor Authentication**.
5. In the **User Accounts** area, configure the IPsec information.
6. In the **IPsec Certificate Credentials** area, configure the necessary information.
7. Click **OK**.

Cross certificate configuration

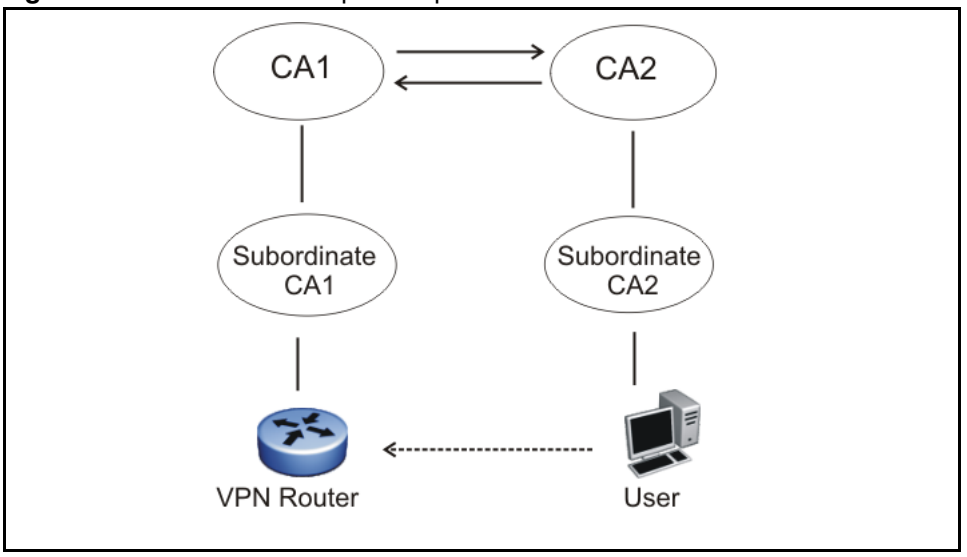
Cross certification is useful if you update your certification infrastructure and need to maintain business operations during the transition from one CA to another. The VPN Router supports two types of cross certification: hierarchical and peer-to-peer.

In a hierarchical configuration, the root CA is self-signed and serves as the trust anchor for all the PKI entities. If you introduce subordinate CAs, the root CA signs the subordinate CA public key and users from the root and subordinate trust one another.

In a peer-to-peer configuration, two self-signed CAs exist and each CA serves as a trust anchor for the PKI entities directly beneath it. After you establish the cross certification, each CA signs the other CA public key and users from each CA trust one another.

With Entrust software, you can use both cross certificate configurations at the same time. For more information about how you can use the VPN Router with both configurations at the same time, see “Hierarchical and peer-to-peer cross certification” on page 108.

Figure 16 Hierarchical and peer-to-peer cross certification



To use both methods simultaneously, you must configure each Entrust CA to maintain its own LDAP. You must also chain the LDAP of each CA to the LDAP of the other CAs, including subordinate CAs. For more information about how to configure chaining as part of the CA server configuration, see the Entrust documentation.

To use cross certification with VPN users, you must use Nortel VPN Client 8.01. The client includes the following Entrust dynamic link libraries (DLL):

- kmpapi32.dll version 6.0.555.1258
- enterr.dll version 6.0.520.1295

The VPN Router provides cross certification support with the following conditions:

- Cross certification supports only IPsec-based user and branch office tunnels.
- Cross certification supports only the Entrust PKI, the IPsec toolkit, and the online cross-certification method.

  Nortel supports online cross-certification of Entrust hosts, however, you must contact Entrust support for assistance with LDAP communication.

Cross certification supports the MS-CAPI store by using the Entrust Security Provider (ESP) product. For assistance with this product, contact Entrust support.

- Cross certification does not change the CRL process.
- If the VPN Router uses a certificate that you imported before cross certification, you must remove the original certificate and replace it with the cross certificate.

Import all CA certificates to the VPN Router. Fore more information, see "Installing trusted CA certificates" on page 86. The VPN Router must use a server certificate issued by a CA.

Configure the Nortel VPN Client to use Entrust for digital certificate authentication. For more information, see *Nortel VPN Router Configuration — Client* (NN46110-306).

Index

G

H

I

L

M

O

P

R

S

T

V

X