

Version 10.01

Part No. NN46110-701 01.01

325135-A Rev 01

November 2008

Document status: Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Client — Troubleshooting



Copyright © 2008 Nortel Networks. All rights reserved.

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

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

Trademarks

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

Adobe, Acrobat, and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Macintosh is a trademark of Apple Computer, Inc.

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

SafeNet is a trademark of SafeNet, Inc.

Linux is a trademark of Linus Torvalds.

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

Netscape and Netscape Communicator are trademarks of Netscape Communications Corporation.

Network General Sniffer is a trademark of Network Associates, Inc.

NetWare, IPX, NetWare, and Novell are trademarks of Novell, Inc.

RSA and SecurID are trademarks of RSA Security Inc.

Java and JavaScript are trademarks of Sun Microsystems, Inc.

Ethernet is a trademark of Xerox Corporation.

Restricted rights legend

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

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

Statement of conditions

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

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

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

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

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

Nortel Networks Inc. software license agreement

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

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

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

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

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

4. General

- a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).
- b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
- c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
- d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
- e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
- f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface	7
Before you begin	7
Text conventions	7
Related publications	10
Printed technical manuals	11
How to get help	11
Finding the most recent updates on the Nortel Web site	12
Getting help from the Nortel Web site	13
Getting help over the phone from a Nortel Solutions Center	13
Getting help from a specialist by using an Express Routing Code	13
Getting help through a Nortel distributor or reseller	14
New in this release.	15
Features	15
Client for Windows Vista	15
Other changes	15
Moved content	15
Troubleshooting fundamentals.	17
Connectivity problems	17
Performance problems	18
Client logging	18
Troubleshooting tools	19
Nortel VPN Client Status monitor	19
Microsoft PPTP Dial-Up Networking Monitor	19
Client logging configuration	21
Enabling logging on the NVC	21
Disabling logging on the NVC	22
Creating an IPSec profile using Manage Profiles	23
Creating a SSL profile using Manage Profiles	27
Testing the configuration	29

Troubleshooting	31
Diagnosing client connectivity problems	31
Common client connectivity problems	32
Troubleshooting banner message problem	35
Firewall blockage	35
NAT transversal (NAT-T) blockage	36
NAT blockage	36
Nortel VPN Client version	36
Third-party VPN client software	37
Index	39

Preface

This guide provides information about how to manage and troubleshoot the Nortel VPN Client (NVC).

Before you begin

This guide is for network managers who monitor and maintain the Nortel VPN Router. This guide assumes that you have experience with system administration 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 ({})	<p>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.</p> <p>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.</p>
brackets ([])	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is show ntp [associations], you can enter either show ntp or show ntp associations.</p> <p>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.</p>
ellipsis points (. . .)	<p>Indicate that you repeat the last element of the command as needed.</p> <p>Example: If the command syntax is more diskn:<directory>/...<file_name>, you enter more and the fully qualified name of the file.</p>
<i>italic text</i>	<p>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.</p> <p>Example: If the command syntax is ping <ip_address>, <i>ip_address</i> is one variable and you substitute one value for it.</p>
plain Courier text	<p>Indicates system output, for example, prompts and system messages.</p> <p>Example: File not found.</p>

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 Client — Configuration* (NN46110-509) 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 8.01* (NN46110-407) provides information to upgrade the server software to the most recent release.
- *Nortel VPN Client — Installation and Upgrades* (NN46110-412) provides information to install and 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 Security — Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.
- *Nortel VPN Router Troubleshooting — Server* (NN46110-602) provides information about system administrator tasks such as recovery and instructions to monitor VPN Router status and performance. This document provides troubleshooting information and event log messages.
- *Nortel VPN Router Administration* (NN46110-603) provides information about system administrator tasks such as backups, file management, serial connections, initial passwords, and general network management functions.

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. For more information about a free copy of the Adobe Reader, go to the Adobe Systems Web site at www.adobe.com.

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 to	Takes you directly to the
Latest software	Nortel page for VPN Client software located at: www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=10621
Latest documentation	Nortel page for VPN Client documentation located at: www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=10621

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 Troubleshooting — Client* (NN46110-701) for Release 10.01:

- [“Client for Windows Vista” on page 15](#)
- [“Other changes” on page 15](#)

Features

Client for Windows Vista

The Nortel VPN Client for release 10.01 is a completely new Nortel VPN Client for the Microsoft Windows Vista operating system. Release 10.01 runs only on the Windows Vista operating system.

[“Client logging configuration” on page 21](#)

Other changes

Moved content

The following topics are moved from *Nortel VPN Router Troubleshooting — Server* (NN46110-602):

- [“Diagnosing client connectivity problems” on page 31](#)
- [“Common client connectivity problems” on page 32](#)

Troubleshooting fundamentals

As a network administrator, your primary concern is to maintain connectivity within the network. For extranet access, you must maintain secure connections between remote users and the private intranet the Nortel VPN Router services. Performance is another area of concern. You must also monitor performance to address issues before they become problems.

This chapter provides basic information to assist in troubleshooting. This chapter includes the following topics:

- [“Connectivity problems” on page 17](#)
- [“Performance problems” on page 18](#)
- [“Client logging” on page 18](#)

Connectivity problems

Connectivity problems occur when the remote user cannot establish a connection to areas of the private corporate network. There are several points of failure to consider when you diagnose connectivity problems. Problems can range from a simple modem configuration error on the client workstation to a complex High-Level Data Link Control (HDLC) protocol error on the T1 Wide Area Network (WAN) interface.

Remote access problems typically originate at the client end when the remote user cannot establish a connection, loses a connection, or has difficulty browsing the network. When connectivity problems occur and the source of the problem is unknown, Nortel recommends you follow the Open Systems Interconnect (OSI) network architecture layers. Therefore, diagnose the physical layers, such as the modem and the cables, before you move up to the network and application layers.

To diagnose the network and application layers, you can ping a host and verify that the remote user can browse the Web.

For more information about troubleshooting connectivity issues, see [“Diagnosing client connectivity problems” on page 31](#).

Performance problems

As with connectivity, there are many places in the extranet network where network performance is affected. To avoid problems and enhance the productivity of the extranet, you can regularly check network statistics, logs, and health check information, and inform users of good network practices.

Client logging

You can use both client and server logs to locate and solve connectivity problems. You can enable the logging feature specifically on the client to log all information. The logging feature generates log files for you to use when you need to recover a failed tunnel connection.

When you enable the NVC logging or if the connection establishment fails, log entries populate the log file. The parameters needed to make a connection are also logged in the log file.

The log file does not include passwords, certificates and other security-sensitive information.

Client logging does not save to files on the hard drive automatically, but you can manually export the logs.

Troubleshooting tools

This chapter contains information about the following Nortel VPN Client-specific troubleshooting tools.

Nortel VPN Client Status monitor

The Nortel VPN Client Status monitor provides network statistics on device, connection, and network errors that help monitor traffic flow and assess IPsec and SSL connection performance. Statistic counters are updated once a second. For more information on the Nortel VPN Client Status monitor, see the Nortel VPN Client online Help.

Microsoft PPTP Dial-Up Networking Monitor

Microsoft Point-to-Point Tunneling Protocol (PPTP) Dial-Up Networking Monitor provides network statistics on device, connection, and network protocols that help monitor traffic flow and assess PPTP connection performance. For more information on the PPTP Dial-Up Networking Monitor, see the PPTP help or your Microsoft PPTP client documentation.

Client logging configuration

This chapter contains procedures about Nortel VPN Client (NVC) logging. Use this information to configure logging on the NVC.

This chapter includes the following topics:

- [“Enabling logging on the NVC” on page 21](#)
- [“Disabling logging on the NVC” on page 22](#)
- [“Creating an IPSec profile using Manage Profiles” on page 23](#)
- [“Creating a SSL profile using Manage Profiles” on page 27](#)
- [“Testing the configuration” on page 29](#)

Enabling logging on the NVC

To enable logging, perform the following steps:

- 1 Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**. The Nortel VPN Client window appears.
- 2 From the left pane, click **Edit the Profile**.
The Manage Profiles window appears showing the General tab.
- 3 From the left pane, click **Manage Options**. The Manage Options window appears. Click **Logging Level**, and then choose a level to view when using the **Log Viewer**. The logging level is grayed out when the NVC is not running in administration context.

Use the information in [Table 1 “Logging levels” on page 22](#) when choosing a logging level .

Table 1 Logging levels

Logging level	Description
Debug	Shows detailed information to help you to debug a problem. Also logs positive events that mark successful milestones.
Information	Shows general type (high level) of information. Logs important and successful milestones of application execution, regardless of whether the application is working properly or not.
Warning	Shows a possible problem has occurred or can occur, but the application still functions correctly. However, it cannot continue to work properly.
Error	Shows that unexpected processing has happened. The application cannot perform a task as expected. However, the application is still up and running.
Fatal	Shows unhandled exceptions where the application has stopped working.
Disabled	The logging level is disabled. No logs are generated.

- 4 Click **Apply** to save the option.

Disabling logging on the NVC

To disable the logging, perform the following steps:

- 1 Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**. The Nortel VPN Client window appears.
- 2 From the left pane, click **Edit the Profile**.
The Manage Profiles window appears showing the General tab.
- 3 From the left pane, click **Manage Options**. The Manage Options window appears. Deselect **Logging Level**.
- 4 Click **Apply** to save the option.

Creating an IPSec profile using Manage Profiles

Whenever you need a standard VPN tunnel, use the IPSec tunnel type. You must be in administrator mode to enable Global Profile.

Create an IPSec profile, by performing the following procedure:

- 1 Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2 From the left pane, click **Edit the Profile**.

The Manage Profiles window appears showing the General tab.

- 3 Click **New** located over the tabs. The information boxes clear to enable you to create a new profile.

- 4 From the **General** tab, choose **IPSec Tunnel** as a connection type for this profile from the **Tunnel Type** list.

- 5 Type in a profile name into the **Profile** box. You can optionally enter a description of the profile.

- 6 Click **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP.

- 7 Type a profile name into the **Profile** box. You can optionally enter a description of the profile into the **Description** box.

- 8 Type an IP address or DNS for the VPN into the **Destination** box.

- 9 Select one of the following Authentication types:

- **Username and Password**
- **Certificate Authentication**
- **Group Security Authentication**

- 10 If you choose **Username and Password** perform the following:

- a By default **Username and Password** is already selected. Type the username assigned to you by the network administrator into the **Username** box.

- b** Type the password assigned to you by the network administrator into the **Password** box.
 - c** Click **Save Password** to save the password.
- 11** If you choose **Certificate Authentication** perform the following:
 - a** Click **Certificate Authentication** to enable the certificate selection.
 - b** Click **Select**. The Select a certificate window appears. Choose either step **c** or step **d**.
 - c** If you want to allow the NVC to select a certificate, click **Automatically select a valid certificate**.
 - d** If you want to manually select a certificate, select **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list.
 - e** Click **OK** to close the window.
 - f** If you want to associate an alternate name with this certificate, select a name from the **Alt Name** list. The default is None.
 - g** Click **Save** to save the new profile.
- 12** If you choose **Group Security Authentication** perform the following:
 - a** Click **Group Security Authentication** to enable the group security authentication.
 - b** Select a group authentication type from the list.
 - **Radius Authentication**
 - **Challenge Response Token**
 - **Response Only Hardware Token**
 - **Response Only Software Token**

The fields in Authentication Information area change according to the type selected. When choosing an authentication type, see [Table 2 “IPSec authentication information requirements” on page 25](#) for the required authentication information.

Table 2 IPSec authentication information requirements

Authentication type	Authentication information
Certificate	Certificate (nonmodifiable)
Radius Authentication	<p>Username: type the username supplied by your administrator.</p> <p>Password: type the password supplied by your administrator.</p> <p>Save Password: click to save the password.</p> <p>Group ID: type the group identification supplied by your administrator.</p> <p>Group Password: type the group password supplied by your administrator.</p>
Challenge Response Token	<p>Username: type the username supplied by your administrator.</p> <p>Password: type the password supplied by your administrator.</p> <p>Save Password: click to save the password.</p> <p>Group ID: type the group identification supplied by your administrator.</p> <p>Group Password: type the group password supplied by your administrator.</p>

Table 2 IPSec authentication information requirements

Authentication type	Authentication information
Response Only Hardware Token	Username: type the username supplied by your administrator. PIN: type the PIN supplied by your administrator. Save PIN: click to save the PIN. Group ID: type the group identification supplied by your administrator. Group Password: type the group password supplied by your administrator. Use Passcode: click to enable a passcode.
Response Only Software Token	Username: type the username supplied by your administrator. PIN: type the PIN supplied by your administrator. Save PIN: click to save the PIN. Group ID: type the group identification supplied by your administrator. Group Password: type the group password supplied by your administrator.

The NVC does not share the group password between local computer accounts. If you log on to the local computer by using a different user account than the one you use to create the NVC profile, you must reenter the group password. For example, you log on to the local computer as the administrator, create the client profile, and log off. If you then log on to the local computer with a different user account, you must reenter the group password in the client profile. You must reenter the password regardless of how you install the Nortel VPN.

13 Click **Save** to save the configuration.

Creating a SSL profile using Manage Profiles

Create a Secure Sockets Layer (SSL) VPN when you are managing the security of message transmissions. The SSL profile also includes the Predefined Login Service that automatically logs on the profile to the server. You must be in administrator mode to enable Global Profile.

Create a SSL profile, by performing the following procedure:

- 1 Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2 From the left pane, click **Edit the Profile**.

The Manage Profiles window appears showing the General tab.

- 3 Click **New** located over the tabs. The information boxes clear to enable you to create a new profile.

- 4 From the **General** tab, choose **SSL Tunnel** from the **Tunnel Type** list as a connection type for this profile.

- 5 Type a profile name into the **Profile** box. You can optionally enter a description of the profile into the **Description** box.

- 6 Click the **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP.

- 7 Type an IP address or DNS for the VPN into the **Destination** box.

- 8 Type in the port number assigned to you by your Administrator into the **Port** box.

- 9 Click **Certificate Authentication** to enable the certificate selection.

- 10 Click **Select**. The Select a certificate window appears. Choose either step [a](#) or step [b](#).

- a If you want to allow the NVC to select a certificate, click **Automatically select a valid certificate**.

- b If you want to manually select a certificate, click **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list.

- 11 Click **OK** to close the window.
- 12 If you want to associate an alternate name with this certificate, select a name from the **Alt Name** list. The default is None.
- 13 Click **Predefined Login Service** to enable Predefined Login Service configuration.
- 14 Choose a name for the service from the **Login Service Name** list. See [Table 3](#) for authentication information.
- 15 Type the username into the **Username** box.
- 16 Click **Response Only Software Token** if you want to enable this token. Type the PIN number into the **PIN** box.
- 17 Click **Save** to save the configuration.

The fields you select in the Predefined Login Service depend upon the type of Login service that you are using. When choosing an authentication type, see [Table 3 “SSL authentication information requirements” on page 28](#) for the required authentication information.

Table 3 SSL authentication information requirements

Authentication type	Authentication information
Certificate	Certificate (nonmodifiable)
Login service (second password is not required)	Username: type the username supplied by your administrator. Password: type the password supplied by your administrator. PIN: if you are using a Response Only Software token, type the PIN supplied by your administrator.
Login service (second password is required)	Username: type the username supplied by your administrator. Password: type the password supplied by your administrator. PIN: if you are using a Response Only Software token, type the PIN supplied by your administrator. Second Password: type the password supplied by your administrator.

Testing the configuration

To test the configuration, perform the following steps:

- 1 Launch the Nortel VPN Client (NVC).
- 2 Enter the password in the **Password** box.
- 3 Click **Connect**. The NVC connects to the Nortel VPN Router and checks for banner text.
- 4 Open a command prompt window.
- 5 Enter **ipconfig** to check the routing table.
- 6 Enter the ping command to ping the Nortel VPN Router to test the connection.
- 7 Choose **Start, Disconnect VPN** to disconnect the Nortel VPN Router.
- 8 Click **Yes** to confirm you want to disconnect the VPN connection.
- 9 Open the NVC log information window and view the entries.
- 10 Disconnect the Ethernet cable.
- 11 Launch the NVC.
- 12 Enter the password in the **Password** box.
- 13 Click **Connect**.
- 14 The tunnel is not established and the “Login Failure due to: Remote host not responding” error appears.
- 15 Open the NVC log information window and view the entries.
- 16 Reconnect the Ethernet cable.
- 17 Launch the NVC.
- 18 Enter the wrong password (for example, test1 instead of test) in the **Password** box.
- 19 Click **Connect**. Note the Authentication failure error message.
- 20 Check the new log entries in the **Log Viewer**.
- 21 From the left pane, click **Manage Options**. The Manage Options window appears. Deselect **Logging Level**.

- 22** Enter the wrong password (for example, test1 instead of test) in the Password box.
- 23** Click **Connect**.
- 24** Check the new log entries in the **Log Viewer**.
- 25** Enter the correct password in the **Password** box.
- 26** Click **Connect**.
- 27** Once connected, disconnect the client.
Check the log again. Note that no new entries have been added to the log file as the logging was disabled and the tunnel was established successfully.

Troubleshooting

This chapter introduces the concepts and practices of advanced network configuration and troubleshooting for the Nortel VPN Router. Use this chapter when you diagnose client problems. This chapter includes the following topics:

- “Diagnosing client connectivity problems” on page 31
- “Common client connectivity problems” on page 32
- “Troubleshooting banner message problem” on page 35
- “Firewall blockage” on page 35
- “NAT transversal (NAT-T) blockage” on page 36
- “NAT blockage” on page 36
- “Nortel VPN Client version” on page 36
- “Third-party VPN client software” on page 37

Diagnosing client connectivity problems

A connection can fail at varying points in an extranet. If a remote user cannot access the corporate network and the source of the problem is unknown, Nortel recommends that you guide the remote user through the following steps to determine the source of the problem:

- 1 Access www.nortel.com —or another site—in the Web browser.
If you can access the Web site, the LAN connection is working properly.
- 2 Verify that the LAN connection on the local PC is active.
See “[Common client connectivity problems](#)” on page 32 to troubleshoot the connection problem.
- 3 Check that the ethernet settings are configured properly by performing the following steps:
 - a Click **Start, Settings, Network Connections** to view the properties.

- b** Verify that the settings are correct for the ethernet connection.
- 4** If you can connect but you cannot access resources or servers, check the system connection information by performing the following steps:
 - a** From the **Start** menu, choose **Run**.
 - b** In the text box, type **ipconfig**.
 - c** View the statistics for the LAN adapter.
 - d** Confirm that the entries match the statistics provided by the Internet Service Provider (ISP).
- 5** If you still cannot view resources or servers over the LAN connection, contact the ISP to verify if connection attempts were logged from the remote workstation.

The ISP can provide additional troubleshooting assistance.
- 6** If you connect to the router using two-factor authentication, ensure that the certificate exists and that you configure the preshared key.

Common client connectivity problems

This section contains information about common client connectivity problems.

If the Nortel VPN Client (NVC) is successfully connected to the ISP, but cannot access the intranet over the PPTP, SSL or IPsec NVC connection, ask the remote user to identify the error message to further troubleshoot the connection problem.

Table 4 “Common client connectivity problems” on page 33 shows the associated cause and action statements that the remote client receives at the IPsec VPN Client user at the remote workstation.

Table 4 Common client connectivity problems

Message	Cause	Action
Remote host not responding	Nortel VPN Router did not respond to the SSL or IPsec connection attempt or that User Datagram Protocol (UDP) port 500 is blocked. The VPN Router allows only a certain number of PING packets from another Internet host before requiring a tunnel connection to be established.	1. Ping the host name or IP address that you filled in the destination field To ping a host called extranet.corp.com, for example, open an MS-DOS command prompt and type ping extranet.corp.com . If you receive a reply message, the Nortel VPN Router is accessible but is not responding. If you receive a message that says Request Timed Out from the ping command, the Nortel VPN Router is inaccessible. 2. Use the MS-DOS Trace Route command (tracert.exe) on Windows systems to further diagnose the connection problem
Maximum number of sessions reached	This message indicates that the maximum number of users for the account has been reached. If you are the only user with access to your account, this error message appears when you restart an IPsec connection immediately after losing the dial-up connection to the ISP. The Nortel VPN Router takes up to one minute to determine that a connection is dropped and then logs you off your account	Wait one minute and retry the connection.
Login not allowed at this time	This message indicates that your account is limited to specific hours of access and you tried to connect outside of the allowed time.	Contact your network administrator the verify the specific hours of access.
Authentication failed	This message indicates that the SSL or IPsec user name is incorrect or the password is invalid for the user name entered.	1. Verify that the user name you entered is correct. 2. Retype the password before trying the connection again.

Table 4 Common client connectivity problems

Message	Cause	Action
No proposal chosen	This message indicates that the Nortel VPN Router is not configured to handle the authentication method configured under the current connection profile.	Use the correct IPsec parameters, such as a choice of ESP-3DES with SHA1. Make sure the parameters match the parameters of the client (for example, an International client).
Other IPsec errors	This message indicates that an error in configuration on the Nortel VPN Router that only the network administrator can correct.	Contact the Network Administrator with the specific error message.
The physical connection has been lost	This message indicates that the PPP connection to your ISP is disconnected.	<ol style="list-style-type: none"> 1. Reestablish the PPP dial-up connection to the ISP. 2. Reestablish the extranet connection to the remote network.
The secure extranet connection has been lost	<p>This message indicates that the Nortel VPN Router you are connected to has either logged your connection off or is no longer responding. This message applies to IPsec only.</p> <p>The connection was probably lost due to the Idle Timeout configured on the Nortel VPN Router. If no data is transferred through the extranet connection for a long period of time, normally 15 minutes or more, the Nortel VPN Router automatically disconnects the connection.</p>	<ol style="list-style-type: none"> 1. Click Connect to reestablish the extranet connection. If you are unable to reestablish the extranet connection, the dial-up connection prevents data from traveling between the Nortel VPN Client and the Nortel VPN Router. 2. Hang up the dial-up connection and reconnect before you try to reestablish a connection. <p>If you are still unable to connect to the Nortel VPN Router, perform the following steps:</p> <ol style="list-style-type: none"> 1. Open an MS-DOS Command Prompt. 2. Ping the Nortel VPN Router using the host name or address that you specified in the Destination field. <p>If you receive a Destination Unreachable error message, there is a routing problem at the ISP. If you receive a Request Timed Out error message, the Nortel VPN Router is probably not available and you can contact your network administrator.</p>
Auto disconnect closes the dial-up connection during data transfer activity	This message indicates that the Microsoft Auto Disconnect feature does not recognize data activity because it did not pass through Internet Explorer. Microsoft has documented this as a known problem in Windows 95. This error occurs in Windows 95 only,	<p>Auto Disconnect if you do not use Internet Explorer to access data on the remote network. To do this:</p> <ol style="list-style-type: none"> 1. Open the Control Panel. 2. Choose the Internet icon. 3. Select the Connection property tab. 4. Clear the Disconnect if idle for check box.

Troubleshooting banner message problem

This contains troubleshooting information about the hang at banner text message that might appear when launching the NVC.

In some situations, when you attempt to bring up a user tunnel from the NVC to Nortel VPN Routers, the tunnel establishment might hang at the Checking for banner text message.

Firewall blockage

A common reason for the banner message to hang is a firewall or router, placed somewhere along the path from the remote computer to the gateway, blocks ESP or AH traffic. The firewall can be a personal firewall installed on the remote computer, a firewall or router at the Internet Service Provider (ISP), or a corporate firewall. In this situation, IPSec ISAKMP traffic that negotiates the tunnel establishment, the tunnel establishes, but the ESP- or AH-encapsulated traffic inside the tunnel does not get through. When the banner text is retrieved through the established tunnel, the banner message or any other traffic secured by the ESP or AH never reaches the client and the NVC continues to wait for response from the gateway until a timeout period is reached.

To resolve this issue, ensure the following traffic is allowed to pass through the firewalls along the path:

- UDP protocol (17) port 500, both inbound and outbound
- ESP protocol (50), both inbound and outbound
- AH protocol (51), both inbound and outbound

It is not necessary to specify source and destination ports for ESP or AH protocols, but if a particular firewall implementation requires it, use zero or N/A as ports dependent on firewall or router requirements.

NAT transversal (NAT-T) blockage

The same scenario occurs as in the previous step if NAT-T is configured and the firewall blocks UDP port selected for NAT-T along the path. To resolve this, ensure the port specified in the NAT-T section of the Services IPsec window (shown below) is allowed to pass through the firewalls on a personal, corporate, or ISP level).

- 1 Access the Nortel VPN Router.
- 2 Choose **Services, IPsec**.
- 3 Scroll down the page to the **NAT Transversal** section.
- 4 Verify that the port specified in the **UDP Port** box can pass through the personal, corporate, or ISP firewalls.

NAT blockage

Verify the NAT configurations at the remote Nortel VPN Client implementation to see if it prevents IPsec traffic to go through. Verify that NAT is configured appropriately and IPsec (ISAKMP, ESP, AH) or UDP (if NAT Traversal is used) traffic can pass through the particular NAT implementation.

Nortel VPN Client version

Ensure you use the most recent version of the NVC. If you have a support contract, you can download the upgrade from the Nortel Technical Support Web site: www.nortel.com/support.

Third-party VPN client software

Ensure no third-party VPN client software is running at the same time as the NVC. If third-party VPN client software runs at the same time as the NVC, it could interfere with NVC operation. In this case, disable or even uninstall third-party VPN clients because they might run in the background preventing successful NVC connections. Open the network interface properties window and uncheck any third-party adapters or drivers.

Index

D

dial-up
 problems 31

E

Extranet Access
 client monitor 19

L

Logging 21

P

Profiles
 IPSec profile 23
 SSL profile 27
publications
 hard copy 11

T

technical publications 11
Testing configuration 29
Third-party client software 37
troubleshooting
 modem and dial-up problems 31