Version 8.00

NN46110-403 03.01
315000-U Rev 01
12 November 2008
Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Release Notes — Server Software Release 8.00

Nortel Networks 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

New in this release

The following sections detail what's new in *Nortel VPN Router Release Notes — Server Software Release* (NN46110-403) for Release 8.00.

Features

See the following sections for information about feature changes.

New features

Release 8.0 introduces the following new features:

Feature changes

Release 8.0 introduces the following functionality changes to existing features:

Other changes

See the following section for information about changes that are not feature-related:

Document changes

The following sections are updated for this release:

Preface

These release notes contain the most recent information about the Nortel VPN Router Version 8.00. The Nortel VPN Router was formerly known as the Contivity Secure IP Services Gateway. These release notes also refer to Nortel VPN Client, formerly known as Contivity VPN Client.

Before you begin

These release notes are intended for network managers who manage the VPN Router. This document assumes that you have experience with windows-based systems or graphical user interfaces (GUIs) and that you are familiar with network management.

Text conventions

This guide uses the following text conventions:

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

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

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

Related publications

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

- Release notes provide the most recent information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Nortel VPN Router Configuration — Client* (NN46110-306) provides information to install and configure client software for the 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 1000 Module, 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.
- *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.

Chapter 1
Overview

These release notes contain the most recent information about the Nortel VPN Router version 8.00.

See the Nortel VPN Router hardware installation guide for instructions about getting the VPN Router up and running. You must configure an IP address, a subnet mask, and a gateway address (if applicable).

You can view online Help from the Nortel VPN Router management interface (the VPN Router graphical user interface). To view online Help for the VPN Router 1010, 1050, or 1100, enter the location of the Help files on the CD or on a server.

To take full advantage of this release, Nortel recommends that you use the following versions for the related products. These versions are only a recommendation; this release is compatible with all supported versions:

- Nortel VPN Client 8.01
- Nortel VPN Client 7.01.250
- Nortel Tunnel Guard Agent 4.5
- Nortel VPN Gateway 6.0.1

Nortel VPN Router Version 8.00 supports the following application software versions:

- Nortel VPN Client (NVC): NVC V6.0x, NVC V7.0x, NVC 8.01, and NVC 10.01

Note: Client versions V6.01, V6.07, and V7.01 were tested with Nortel VPN Router software version 8.0. Although earlier versions of the client may work with 8.0, they were not tested.

- Tunnel Guard: TG_1.0.0.0, TG_2.0.0.0, TG_3.0.x.0, and TG_4.5.0.0
- Nortel SSL VPN 1000 Module: 5.1.7 (or greater), 6.0.1 (or greater), 7.0.1

Note: If the Nortel SSL VPN 1000 Module runs a version less than 5.1.7, you must upgrade to 5.1.7 or greater before you upgrade the VPN Router software to V8.0.

- VPN Router Multi-Element Manager (formerly Contivity Configuration Manager): V2.3.1.0 (minimum) or V2.3.3 (recommended).

Note: VPN Router Multi-Element Manager (VRMM) version 2.3.1.0 allows VRMM to discover VPN Routers that run version 7.0x. VRMM 2.3.1.0 does not support features introduced in version 7.0x.

This chapter includes the following topics:

New software features

Version 8.00 of the VPN Router supports the following new software features:

Banner message

The Nortel VPN Router supports a custom banner message that appears on admin access screens prior to a user attempt to log on the Nortel VPN Router. For more information, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500).

The 8.0 document suite includes a feature introduced in Release 7.0, a banner message for client tunnels. For more information, see *Nortel VPN Router Configuration — Tunneling Protocols* (NN46110-503).

Branch office tunnel NAT Traversal

Release 8.0 introduces Network Address Translation (NAT) Traversal for branch office tunnels between VPN Routers when one router is in a private network that uses one or more NAT devices. For more information, see *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508).

Certificate cross certification

Release 8.0 supports two types of cross certification: hierarchical and peer-to-peer. For more information, see *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600).

DHCP changes

If you use an IP address pool on an external Dynamic Host Configuration Protocol (DHCP) server, the pool name on the external server must match the pool name you configure for the group on the VPN Router. 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. For more information, see *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600).

Forced logoff timer

Release 8.0 increases the upper bounds of the forced logoff timer to 120 hours (5 days). For more information, see *Nortel VPN Router Configuration — Tunneling Protocols* (NN46110-503).

HP Openview discovery

This feature enables the Discovery feature in HP Openview to determine the loopback address of a VPN Router. For security, discovery operates over private interfaces.

HTTP retrieval for CRL

Release 8.0 introduces HTTP retrieval of certificate revocation lists (CRL) to supplement the current Lightweight Directory Access Protocol (LDAP) CRL distribution retrieval method for certificate authentication. For more information, see *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600).

IGMP Proxy

The VPN Router uses Internet Group Management Protocol (IGMP) Proxy to appear to an IGMP client as an IGMP router. In turn, the VPN Router appears to the multicast network as an IGMP client. The VPN Router proxies IGMP requests to the network on behalf of the IGMP client. For more information, see *Nortel VPN Router Configuration — Routing* (NN46110-504).

Management access filters

You can now use management access filters to block HTTPS and SSH. For more information, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500).

NTP changes

With Release 8.0, you can now use the Network Time Protocol (NTP) on all public and private interfaces. For more information, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500).

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 *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600).

PassGo Defender

Release 8.0 adds support for PassGo Defender, formerly called Axent Defender, token authentication. For more information, see *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600), *Nortel VPN Router Configuration — Tunneling Protocols* (NN46110-503), and *Nortel VPN Router Using the Command Line Interface* (NN46110-507).

SFTP server

Secure File Transfer Protocol (SFTP) is a secure version of the File Transfer Protocol (FTP). SFTP uses FTP commands to transfer files securely between accounts on different machines. The SFTP provides secure file transfer functionality over any reliable data stream; it is the standard file transfer protocol for use with the SSH2 protocol. For more information, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500).

TunnelGuard 4.5

Release 8.0 enhances the TunnelGuard feature. In prior releases, you implemented and bundled a third-party API to make TunnelGuard work in your implementation. TunnelGuard now supports preconfigured Software Requirement Set (SRS) that you can modify. For more information about preconfigured SRS and the changes in the TunnelGuard applet, see *Nortel VPN Router Configuration — TunnelGuard* (NN46110-307).

Tunnel upgrade for the 1750

The minimum number of tunnels for VPN Router 1750 is now 50. For more information, see *Nortel VPN Router Installation — VPN Router 1750* (NN46110-316).

Two factor authentication

Beginning with Release 8.0, you can select two methods of IPsec authentication for a branch office or user tunnel connection. The available authentication methods for tunnels remains the same, 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. For more information, see *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600) and *Nortel VPN Router Configuration — Client* (NN46110-306).

Certificate authentication is the primary authentication with username and password as the secondary authentication. Currently, Radius soft tokens and hard tokens are not supported as part of the secondary authentication method. Therefore they are not supported by the Two Factor Authentication feature.

4096 bit certificates

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

Restricted product—export license requirements

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

A product that incorporates encryption with a key length up to 56 bits can be eligible for international shipment pursuant to a license exception. However, any product that incorporates encryption technology exceeding 56 bits will require an export license from the US Department of Commerce.

Pursuant to such license, the product can be marketed and sold only to a limited class of international users. Any entity, other than Nortel, Inc., that wants to export this product must first obtain license approval from the US Department of Commerce.

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

Chapter 2
Considerations and issues

The following sections contain customer issues fixed in this release and general considerations for this product. This chapter includes the following topics:

Customer issues fixed in this release

"Issues fixed for V8.00" on page 26 lists customer issues from the V7.05.300 software stream that are fixed for V8.00.

Table 1 Issues fixed for V8.00

CR number	Description
Q01717623	The Nortel VPN Router does not send a request to the RADIUS authentication server.
Q01300169	In ABOT Tasman as Initiator contivity is converting ID payload based on types. Therefore, it is converting type 1 as well.

Version 8.00 known anomalies

The following describes the known anomalies for Nortel VPN Server version 8.00.

Q01506432—NAT translations do not show the correct destination addresses for RTP and RTCP streams

NAT translations show the destination addresses for RTP and RTCP streams in the flow cache as the Call Server and not the actual endpoint IP addresses.

Q01721633-01—Knova: DHCP Server on Sub-Interface stops DHCP Relay on LAN Interface

Enabling and configuring DHCP Server on a LAN subinterface prevents DHCP Relay from working on the main LAN interface. The documentation states that the use of DHCP server and Relay on the same physical interface are mutually exclusive but was not clear if a subinterface was considered a separate interface for the purposes of DHCP server and Relay.

Q01808947-02—CMP Request with large reference number and large authorization code results in NVR crash

NVR crashes when it performs a CMP request with a large reference number and authorization code.

Q01870898—Public side Management Protocol inconsistent behavior compared to private side

When configuring Management Protocols using VPN Router Interface Filters for Firewall on the NVR to manage the unit, you will see inconsistent behavior between private & public interfaces.

Q01871415-01—Nortel VPN Router (NVR) stops sending OSPF hellos when saving firewall

When you log in using stateful firewall with rules defined for the group, open the firewall policy that is running, and save the firewall. During the save, NVR stops sending OSPF hellos. If the save takes longer than 40 seconds, all the adjacencies go down.

Q01873871—NVR does not respond the same way to snmpget and snmpbulkget queries

NVR does not respond the same way to snmpget and snmpbulkget queries for versions after V07_00.031. This affects the interaction with HPOV software which uses both commands.

Q01881747—Sub-interfaces do not appear in the NTP

Sub-interfaces do not appear in the NTP private combo box. A configuration attempt from CLI returns an error message stating that the IP address is not existent. Configure an NTP server and try to choose the sub-interfaces IP from the private combo box.

Q01885012—Inheritance allows temporarily prohibited modifications in subgroups

The IP Address Source or the Pool Name assigned to a group that has connected users should not change. Currently there is no mechanism for continuously checking the group's inheritance and for preventing modifications on parent groups while subgroups inherit attributes.

Q01891331—Two-factor session should not go to phase 2 if only one endpoint has two-factor authentication

When trying to establish a BO tunnel between two endpoints in which only one has dual authentication enabled and the other uses Certificates authentication, the session should be closed at phase I. This prevents the session from appearing as up at any time on the NVR that uses Certificates authentication.

Q01919421—Client NAT Traversal issue after upgrade to V08_00

Clients accessing the contivity from behind a NAT device are unable to connect after the contivity has been upgraded from V07_05 to V08_00.

Q01942839—VPNR 8 beta rev 43–VRRP critical interface

The problem is that the interface group which includes the tunnels goes down but the interface tracking the group does not go down.The critical interface state is down but the operational state still displays Master. Only after disabling or re-enabling the administrative state does the Master status goes critical.

Q01942959—TA NVR 8.0 - VRRP cannot ping

A client PC at the branch office can always ping the VRRP address where as a PC from the head office cannot ping. If the VRRP master is the contivity that is used to route to the head office via, pinging the VRRP fails. Until now eight sites have been upgraded and all are facing the same issue.

VPN Router upgrade considerations

The following sections contain upgrade considerations for this product.

- Release 8.0 operates with 128 MB RAM memory configurations.
- VPN Router 1010, 1050, and 1100 require a 64 MB flash disk.
- Version 8.0 supports upgrades from Versions 5.05.330, 6.0.310, 6.05.140, 6.05.210, 7.00.062, and 7.05.330. If you run an older version, you may have to upgrade to a more recent version before you upgrade to Version 8.0.
- The amount of disk space required to upgrade to the latest version is configuration-specific. If you receive disk space error messages, you must remove unnecessary files from your VPN Router.
- A recovery floppy diskette that you created prior to Release Version 4.0 does not work on a system that runs Version 4.0 or later software.
- Nortel recommends that, when you upgrade to Version 8.0 software, you create a recovery floppy diskette as soon as you complete the upgrade. You must use a formatted diskette when you create the recovery diskette.
- Nortel recommends that you maintain no more than two versions of the software on the VPN Router in addition to the version that is currently running.
- After you upgrade to 8.0, if you enable two factor authentication for a parent group, this configuration propagates to children groups, regardless of the inheritance configuration.

VPN Router recommendations

Nortel recommends that you:

- Use the automatic backup feature to back up your current configuration on the VPN Router for later restoration. It functions by saving all of the contents of the VPN Router file system from the /ide0/system point down. The contents of the flash memory are not saved as part of this process.

- Monitor the amount of space remaining on the hard disk drives, because a full file system produces unexpected behavior. To check the hard disk usage level, choose Status, Health Check. Because log files can consume a significant amount of disk space, especially in large configurations, you should periodically remove old log files.

VPN Router considerations

Note the following information:

- When you configure two VPN Routers back-to-back with an E1 interface and one side is disabled physically, the other side stays up. This leads to routing issues because the route is not removed from the router whose interface is up. This happens because the E1 driver cannot generate AIS in a back-to-back scenario. The workaround is to administratively disable both sides to manage the network stability.
- If you use a Simple Traversal of UDP through NAT (STUN) client and server to determine the type and capabilities of local NAT, the reported type can be incorrect when you use Branch Office NAT.
- Asynchronous branch office tunnel (ABOT) definitions do not support multinet addresses as initiators.
- The saved event log file contains binary data and is only readable by a dump log utility, Dumplog.exe. This utility takes a binary log file and converts it to American Standard Code for Information Interchange (ASCII) text. Dumplog.exe requires the evl.txt file from the VPN Router /system/log directory. Dumplog.exe is in VPN Router \tools directory.

  Usage: dumplog [options] <evl_file> <log_file>

  The following options are currently available:

  -e <Entity> Only display messages for this entity/subentity

  -c <Code> Only display messages with the specified code

  -s <Severity> Only display messages with specified severity

  Severities are specified as follows:

  (E)mergency

  (A)lert

(C)ritical

E(R)ror

(W)arning

(N)otice

(I)nfo

(D)ebug

-a <Directory> All autolog files are treated as a single saved log.

Autolog files are stored in <Directory>

-t <Time> Print log starting at this time (24 hour time)

-d <Date> Print log starting at this date

- If the BGP local preference is 0, the BGP routing table does not accept any remote routes and, therefore, those routes are not advertised to the other neighbors.
- H.323 does not work when NAT is enabled, nor does H.323 video traffic pass with an allow H.323 only policy.
- The applet to configure NAT and Firewall policies no longer works with Opera browser. A custom Event Queue replaces the SystemEventQueue of the Java Virtual Machine (JVM). Opera is written in Java and uses its own instance of JVM. When Opera tries to open an applet, it uses the browser JVM for the applet, not a different instance. The function getSystemEventQueue from the Java API returns the SystemEventQueue if no security policy is defined, or if a security policy that allows the execution of the function is defined. Opera has a security policy that does not permit the above mentioned function to return the SystemEventQueue. To permit the function to return the SystemEventQueue, add the following line in the grant section (default permissions granted to all domains) of the file opera.policy found in the {Opera installation directory}\classes directory: permission java.awt.AWTPermission "accessEventQueue".
- In the CLI, if you switch IP addresses between public and private and set the default gateway in the new private network, the value for the default gateway keeps the old value instead of the new one. You must reboot the VPN Router for the change to take effect.
- Use one of the following methods to select either English or Japanese as the default language:

  Using the GUI, choose the following:

Admin, Administrator, Default Language, Japanese (Shift-JIS)

Using the CLI, enter the following command in the Global Configuration mode:

```
# default language japanese
```

Note: Nortel VPN Router Software Release 7.0 and later no longer supports Japanese as the default language. If you use Japanese as the default language, some display issues can occur.

- You cannot select a Point-to-Point Protocol Over Ethernet (PPPoE) interface when you create an interface group for a demand profile if the local IP address in the interface PPPoE settings is 0.0.0.0 (Dynamic). The interface is not available in Routing, Interface Grp due to its particular value (0.0.0.0).

  If an interface included in an interface group is deleted or changes its IP, that interface is removed from the interface group and not updated, even if the interface was acquired dynamically using Dynamic Host Configuration Protocol (DHCP).
- When you upgrade to version 6.0 or later, the passive FTP service is disabled by default. The default in earlier versions was enabled. If your configuration uses passive FTP, be sure to enable the option after you upgrade.
- CLI (Python) scripts dynamically allocate memory upon execution of the script. The Python interpreter does not have a garbage collection mechanism within it, so the only way to reclaim the memory is to exit the current CLI session. Nortel recommends that you exit the current CLI session after you execute large scripts.

Viewing and calculating memory usage

The minimum memory requirement for Version 8.0 is 128 MB. The Memory Calculator tool is a Microsoft Excel spreadsheet that helps determine the memory requirements for a VPN Router based on the tunneling, routing, and firewall configuration. You can enter the configuration values in the Memory Calculator tool to determine the base memory recommended for the specified configuration. Given the dynamic nature of memory usage, the result provided by the tool is only an estimate. The Memory Calculator tool is found at the following location:

www.nortel.com/support.

Click on Support & Training from the top menu bar and then select Technical Documentation. Select Security & VPN, VPN Router 1750 and in the Documentation section, click Show All. In the Contains Term(s) box, type Nortel Networks Contivity Memory Calculator, and then click Apply Filters.

The parameters that affect VPN Router memory usage are:

- VPN Router software version
- Single or dual CPU
- Internal or External LDAP (shows whether internal or external LDAP is configured)
- Number and type (the number and type of branch office and user tunnels)
- Static routes (the number of static route entries in the IP routing table)
- RIP routes (the number of RIP route entries in the IP routing table)
- BGP routes (the number of BGP route entries in the IP routing table)
- OSPF Routes (the number of OSPF route entries in the IP routing table)
- Redistributed OSPF, BGP and RIP Routes (the number of routes redistributed into RIP, BGP, and OSPF Routing protocols)
- FW/NAT Max connections (the maximum number of connections configured on the Services > Firewall/NAT > Edit window)
- FW/NAT Number of Sessions (the total number of Firewall/NAT sessions)
- BO NAT Number of Sessions (the number of Branch Office NAT sessions)
- SFW Enabled [shows if the Stateful Firewall with Interface Filter (SIF) is enabled]
- Interface NAT Enabled (shows if Interface NAT is enabled)
- Antispoofing Enabled (shows if Antispoofing is enabled)

Software and hardware compatibility

Nortel no longer supports the following products:

- Nortel VPN Router software versions 5.00 and 5.05. You must upgrade to version 6.05, 7.05, or 8.0 for a fully-supported software release.

- Nortel VPN Client 5.01. Nortel VPN Router software version 8.0 supports Nortel VPN Client versions 6.01 and higher.
- Contivity 1600, 2600, and 4600 platforms. While Nortel supports VPN Router 8.0 on these Contivity platforms, be aware that support for the hardware may not be available. Contact your Nortel sales representative if you have questions or concerns.

"Hardware platform and server software compatibility" on page 34 shows VPN Router hardware and software compatibility. An X in the table indicates which platforms were qualified for the version of the VPN Router software.

Note: You can install the SSL VPN 1000 Module only in the VPN Router 1740, 1750, 2700, 2750, and 5000 platforms.

All platforms are available in RoHS and non-RoHS versions, only the 2750 and 5000E are unique to RoHS.

Table 2 Hardware platform and server software compatibility

Hardware platform	Server software compatibility				
	6.00	6.05.140	7.00	7.05.300	8.00
1010	X	X	X	X	X
1050	X	X	X	X	X
1100	X	X	X	X	X
600	X	X	X	X	X
1600	X	X	X	X	X
1700	X	X	X	X	X
1740	X	X	X	X	X
1750	X	X	X	X	X
2600	X	X	X	X	X
2700	X	X	X	X	X
2750		X	X	X	X
4600	X	X	X	X	X
5000	X	X	X	X	X
5000E		X	X	X	X

Load-balancing and hardware encryption accelerator cards

When you install one or two optional hardware encryption accelerator cards, VPN Router software tries to ensure optimal tunnel throughput by balancing tunnels across available system resources, such as the CPUs and the hardware encryption accelerator cards. Several parameters, such as the number of active tunnels and the current load on the resources, are evaluated during new tunnel establishment or rekeys to determine the assignment of a new tunnel.

After you assign a tunnel to a hardware encryption accelerator card or to the CPU, the VPN Router does not dynamically reassign the tunnel to a new resource due to the dynamic nature of the load balancing algorithm. Therefore, you may see some tunnels assigned to software (to a CPU) even if there are hardware encryption accelerator cards available.

General support considerations

General support considerations include the following:

- The output generated by the CLI command **`show running-config`** (SRC) command does not always produce usable scripts that can be applied directly to provision a VPN Router. This applies both to the use of SRC within an affected software version and across versions. You should not use the output from SRC without inspection and, if necessary, editing and reordering the output to provision a VPN Router. For further information about SRC, see *Nortel VPN Router Using the Command Line Interface* (NN46110-507).
- Gigabit Ethernet (GbE) fiber and copper cards do not fit into the connector on slot 4 on the VPN Router 4600.
- If more than 10 Certificate Management Protocol (CMP) enrollments occur at the same time, the administrative functions of the VPN Router (GUI/CLI) can be nonresponsive for short periods of time.
- Shasta Server Farm is not supported by Version 8.0.
- The VPN Router GUI and CLI support only 7-bit ASCII characters.
- The VPN Router works with all RFC-compliant FTP servers.

- The VPN Router supports the current version and generally the two previous versions of the Nortel VPN Client. If you have any concerns, contact Nortel support for the latest information.
- If you use a Linksys Etherfast Cable/DSL router in IPsec passthru mode, and if two or more PCs connect through it to a VPN Router, then one or both of these PCs can be disconnected or their communications disrupted unless you use NAT Traversal mode on the VPN Router. (The client monitor continues to run and does not display a message that the connection is disconnected or disrupted.) This occurs because the LinkSys does not support more than one IPsec session. To prevent this, select Auto-Detect NAT from Profiles, Groups, Edit, IPsec Configure, NAT Traversal, which activates NAT Traversal and allows multiple PCs behind the NAT box to function properly.
- You cannot run the Windows 2000 client using Layer 2 Tunneling Protocol (L2TP) over IPsec if the Nortel VPN Client is installed. The IPsec driver conflicts with the native IPsec driver in Windows 2000. You must disable the Windows 2000 IPsec driver, which effectively prevents the use of the Windows 2000 client using L2TP over IPsec. On the PC, right-click My Computer, and then choose Manage. Choose Services and Applications, Services. Double-click IPSEC services, change the Startup type from Disabled to Automatic, and then restart the system. The client detects the loading of the Windows 2000 IPsec driver and disables the client IPsec driver.
- The VPN Router supports RADIUS-supplied attributes, such as IP address and MPPE key and additional specific attributes, if they are returned from a RADIUS server; any other returned attributes are ignored. The specific attributes are detailed in Microsoft documentation and defined in RFC 2548. This data overrides the corresponding data stored in LDAP.
- You can use any unused UDP port for NAT Traversal except the L2TP and Layer 2 Forwarding (L2F) port 1701 or General Packet Radio Service (GPRS) port 3386. Make sure that the port you select does not conflict with ports that you already use.
- Route policy configuration is lost after an upgrade from V04_7x to the latest version. You must re-enter the settings manually.

VPN Router admin browser considerations

The following considerations pertain to administrative users:

- Internet Explorer 6.0 or 7.0, and FireFox 2.0 and 3.0 are the supported Web browsers. Use the latest version of your browser to ensure accurate screen displays of the Web interface for the VPN Router.
- You must install Java Runtime Environment 1.6.0_u6 to manage the SSL VPN and the Stateful Inspection Firewall UI. The JRE 1.6.0_u6 is distributed with the VPN Router image; it can also be downloaded from Sun Microsystems, Inc.
- A Microsoft issue in Internet Explorer 6.0 SP1 creates problems when you attempt to launch the SSL VPN Manager over HTTPS. Internet Explorer SP2 corrects this issue.
- The off-line Help stored on local computers cannot be accessed from the links in the Help page due to security constraints that are implemented in Netscape 4.1 or higher and Internet Explorer 6.0 SP1, which have hotfixes. There are two workarounds
  - — Add the site to the trusted zone of IE
  - — Add the machine name to the URL
- Netscape 4.79 incorrectly does not prevent users from launching multiple copies of VPN Router Firewall Configuration tool. If you click Manage Policies twice or more without waiting for the configuration tool to appear, multiple copies of the tool are launched, which leads to runtime errors. If this happens, you must close all active browser windows and start a new management session.
- When you use HTTPS to secure administrator access to the VPN Router, Netscape Communicator and Internet Explorer perform differing security checks. Nortel recommends that you use the following configuration to obtain the best performance when you administer the VPN Router securely using Admin SSL:
  - — In the hosts file, make an entry that corresponds to your VPN Router management IP address.
  - — Import the root certificate that issued your VPN Router server certificate into your browser store.
  - — Import the root certificate that issued your VPN Router server certificate into your JRE.
- To satisfy a further name check by Netscape browsers, the VPN Router server certificate common name (filled in when you create the certificate request from System, Certificates, PKCS#10 Certificate Request) must be either a DNS name that resolves to the management IP address or the actual management IP address.

- Using Internet Explorer Version 6.0.2800.1106IC on Windows NT 4.0, the GUI presents inconsistent information in the firewall java section.
- If you launch two Java applets from one Web GUI session on the same PC, it can cause inconsistencies with firewall policy rules.

The following considerations pertain to SSL VPN end users:

- To support the Telnet and SSH access, HTTP Proxy and Port forwarder features, Nortel recommends that you use the following browser and Java combinations:

  Windows:

  — Internet Explorer 5 or better with Sun JRE 1.3 or better
  — Internet Explorer 5 or better with Microsoft JVM 4 or better
  — Netscape Navigator 7 with Sun's JRE 1.3 or better
  — Mozilla 1.3 or better with Sun's JRE 1.3 or better

  Unix/Linux:

  — Netscape Navigator 7 with Sun JRE 1.3 or better
  — Mozilla 1.3 or better with Sun JRE 1.3 or better

  Configuration using the Browser-Based Management Interface is supported when you use the following browsers:

  Windows

  — Internet Explorer 5.5 or better
  — Netscape Navigator 7.1 or better
  — Mozilla 1.5 or better

  Unix/Linux

  — Netscape Navigator 7.1 or better
  — Mozilla 1.5 or better
- Both Internet Explorer and Netscape browsers cache user ID and password information. If you enable caching in your browser, Nortel recommends that you close the browser when you finish making changes to the VPN Router.
- America Online (AOL) V5.0 Web browser is not supported.

Tunnel considerations

- Testing a branch office tunnel can fail if the tunnel is initiated from both sides at the same time. This situation occurs when the initiation is due to live traffic or a test button tunnel initiation.
- For nailed-up connections, the IPsec security association (SA) can go down due to inactivity. Only the Internet Security Association and Key Management Protocol (ISAKMP) SA stays up all of the time.
- PPTP and L2TP MPPE 128-bit encryption keys do not work properly in the VPN Router if they were obtained during RADIUS authentication with a Funk Software, Inc. Steel-Belted Radius Server Version 2.2 or later. This problem also applies to other RADIUS servers derived from Steel-Belted Radius, including the Bay Networks BSAC RADIUS server Version 2.2 and later and the Nortel Preside RADIUS server Version 1.0.49 and later.
- In addition, the Microsoft RADIUS server exhibits this problem when doing MS-CHAP authentication that returns MPPE keying information. PPTP and L2TP MPPE based 40-bit encryption is unaffected by this problem. Do not use the noted RADIUS servers with the VPN Router if PPTP or L2TP MPPE-based 128-bit encryption is required.

Note: If you are using the 1750 five-tunnel base unit version, installing 8.00 will upgrade the minimum tunnel count to 50.

The following table lists the maximum number of tunnels for each VPN Router model and indicates whether each model has a five-tunnel base unit version.

Table 3 Maximum number of tunnels by VPN Router model

VPN Router model	Maximum number of tunnels	Five-tunnel base unit available? (Yes/No)
1010, 1050, 1100	30	Yes
600	50	No
1600 (discontinued)	200	No
1700 and 1740 (discontinued), 1750	500	Yes
2600 (discontinued)	1000	No
2700	2000	Yes

Table 3 Maximum number of tunnels by VPN Router model

VPN Router model	Maximum number of tunnels	Five-tunnel base unit available? (Yes/No)
2750	2000	Yes
4600	5000	No
5000	5000	No
5000E	5000	No

Nortel verifies VPN tunnel scaling in an optimal environment. Real world deployments should not expect to achieve these results for all VPN Router platforms. The VPN tunnel scaling and performance (properties) of a given system are highly influenced by platform configuration and its operating environment.

Certificate considerations

VeriSign certificates use a unique e-mail identifier that is different from Microsoft and Entrust, so you must use the full subject distinguished name (DN) when you configure branch office connections authenticated using certificates.

- The output of the certificate export must contain a blank line after the password hash information for the certificate to import successfully.
- All characters of the certificate subject and issuer DN are case insensitive. The subject DN o=nortel is considered equivalent to o=Nortel. This complies with RFC 3280 4.1.2.4 and 4.1.2.6.
- When a user enters a full DN, the order of the individual components is no longer important because the VPN Router stores it in a predetermined order. For example, if you enter the DN of cn=joe, ou=contivity, o=nortel, c=us, this is viewed by the VPN Router as identical to: ou=contivity, o=nortel, c=us, cn=joe Rearranging the order allows the VPN Router to correctly process certificates generated by CAs with differing DN encoding orders.

Documentation considerations

The following documentation issues will be fixed in future versions of the documentation.

- When configuring a critical interface or interface groups for critical interface failover (CIF), you cannot have VRRP configured on the interfaces. If you include an interface that is running VRRP as a critical interface or part of an interface group (for CIF), it is an unsupported configuration. Where VRRP is configured on the interface, there is already a failover/availability solution provided in case of loss of that interface.