Version 7.0

Part No. NN46110-403
315000-R Rev 01
February 2007
Document status: Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Release Notes — Server Software Release 7.0

Copyright © 2007 Nortel Networks. All rights reserved.

Trademarks

Restricted rights legend

Statement of conditions

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

Preface

These release notes contain the latest information about the Nortel VPN Router Version 7.0. 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 are responsible for the VPN Router. They assume that you have experience with windowing systems or graphical user interfaces (GUIs) and familiarity 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`**.

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.

Related publications

For more information about the VPN Router, refer to the following publications:

- Release notes provide the latest information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *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 for configuring services on the SSL VPN Module 1000, including authentication, networks, user groups, and portal links.
- *Nortel VPN Router Security—Servers, Authentication, and Certificates* (NN46110-600) provides instructions for configuring authentication services and digital certificates.
- *Nortel VPN Router Security—Firewalls, Filters, NAT, and QoS* (NN46110-601) provides instructions for configuring the Nortel VPN Router Stateful Firewall and Nortel VPN Router interface and tunnel filters.
- *Nortel VPN Router Configuration—Advanced Features* (NN46110-502) provides instructions for configuring advanced LAN and WAN settings, PPP, frame relay, PPPoE, ADSL and ATM, T1CSU/DSU, dial services and Demand Services, DLSw, IPX, and SSL VPN.
- *Nortel VPN Router Configuration—Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, L2TP, PPTP, and L2F.
- *Nortel VPN Router Configuration—Routing* (NN46110-504) provides instructions for configuring BGP, RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Nortel VPN Router Troubleshooting* (NN46110-602) provides information about system administrator tasks such as backup and recovery, file management, and upgrading software, and instructions for monitoring gateway status and performance. This book also provides troubleshooting information and interoperability considerations.
- *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.

- *Nortel VPN Router Configuration—Client* (NN46110-306) provides information for setting up client software for the Nortel VPN Router.
- *Nortel VPN Router Configuration—TunnelGuard* (NN46110-307) provides information about configuring and using the TunnelGuard feature.

Hard copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to www.nortel.com/support, 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 Adobe Systems 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 latest 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 latest 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 Router** software
Latest documentation	Nortel page for **VPN Router** documentation

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:

- 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:

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 latest information about the Nortel VPN Router version 7.0. They support the first release of the VPN Router Model 2750 and the VPN Router 5000E and address customer-found software issues.

The Contivity Secure IP Services Gateway and the Contivity hardware is rebranded to Nortel VPN Router. The Contivity VPN Client is rebranded to Nortel VPN Client.

As well as the rebranding changes for version 7.0, the model number is changed from CESxxx to NVRxxx. Any external user scripts that look up the model number may no longer work. This change includes the VPN Router Configuration Manager. When upgrading to version 7.0, the system descriptor located in flash is upgraded and is not reversible when downgrading to an older version.

You may still see the name Contivity in the hardware or the software. For example, the MIB, the CLI commands and their outputs, and the CES> prompt are not rebranded.

Note: The rebranding changes in the flash are not seen unless you update the flash. An upgrade is not required for functional reasons.

Refer to the Nortel VPN Router hardware installation guide for instructions on 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 or graphical user interface (GUI). 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.

Nortel VPN Router version 7.0 supports the following application software versions:

- Nortel VPN Client: NVC V05.01, NVC V06.01 and NVC V07.01

Note: Client versions V05.01, V06.01, and V07.01 only were tested with Nortel VPN Router software version 7.0. Although earlier versions of the client may work with NVR 7.0, they were not tested.

- TunnelGuard: TG_1.0.0.0, TG_2.0.0.0 and TG_3.0.0.0
- Nortel VPN Gateway (NVG): NVG 5.1.7 (or greater), 6.0.1 (or greater)

Note: If the NVG card is running a version less than 5.1.7, you must upgrade to 5.1.7 or greater before upgrading the VPN Router software to V7.0.

- VPN Router Multi-Element Manager (formerly Contivity Configuration Manager): V2.3.1.0 (minimum). For a list of all available software for the VPN Router Multi-Element Manager, go to https://app33.nortelnetworks.com/go/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=11402

Note: VPN Router Multi-Element Manager (VRMM) version 2.3.1.0 allows VRMM to discover VPN Routers that are running version 7.0. VRMM 2.3.1.0 does not support new features in version 7.0. VRMM support for version 7.0 features will be available in a later release.

Version 7.0 features

New hardware features

Version Version 7.0 of the VPN Router supports the following new hardware features:

- VPN Router 2750
- VPN Router 5000E

VPN Router 2750

The VPN Router 2750 is the Restriction of Use of Certain Hazardous Substances (RoHS) compliant version of the VPN Router 2700. The performance of the VPN Router 2750 is identical to that of the VPN Router 2700. The VPN Router 2750 provides the same virtual private networking and routing for medium-sized business sites as the VPN Router 2700.

The VPN Router 2750 has an additional LAN port that provides an extra slot for optional input/output (I/O) cards. The system has four Peripheral Component Interconnect (PCI) expansion slots that can support VPN Router I/O option cards.

The VPN Router 2750 supports the following:

- 2 000 simultaneous Nortel VPN Client connections with each connection running Tunnel Guard with five rules
- 2 000 simultaneous static route Branch Office tunnels with no client connections
- 750 simultaneous dynamically routed Open Shortest Path First (OSPF) Branch Office tunnels with five simultaneous client connections with a single Tunnel Guard rule
- 250 Frame Relay permanent virtual circuits (PVC) per WAN Interface
- 256 802.1Q VLANs per Ethernet interface

The VPN Router 2750 accepts incoming traffic through authenticated, tunneling connections using the following protocols:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Forwarding (L2F), IPsecurity (IPsec)
- Layer 2 Tunneling Protocol (L2TP).

You can maintain traffic privacy with authentication services such as:

- internal or external Lightweight Directory Access Protocol (LDAP)
- Remote Authentication Dial-In User Service (RADIUS)
- NT Domains
- Token Cards encryption algorithms

With filters, you can create a unique profile that determines the performance level, type of access and level of security. With the management features you can jointly manage the VPN Router 2750 between the organization's network administrator and a service provider. The VPN Router 2750 provides a log of all transactions and it supports industry standard PPTP clients from Microsoft and other third party vendors. The VPN Router 2750 provides 128 Bit encryption support.

VPN Router 5000E

The VPN Router 5000E complies with the RoHS requirements. The VPN Router 5000E uses a 500-watt power supply because production of the 350-watt power supply has ended. The VPN Router 5000 supports only the 350-watt power supply and the VPN Router 5000E supports only the 500-watt power supply.

When you order a replacement or spare power supply for the VPN Router 5000 or 5000E, order only the 350-watt power supply model for the VPN Router 5000, and order only the 500-watt power supply model for the VPN Router 5000E. You must not install an unsupported power supply in the VPN Router 5000 or in the VPN Router 5000E.

Table 1 shows the model number for each chassis that supports either the 350-watt or 500-watt power supply.

Table 1 Model number for each chassis that supports either the 350-watt or 500-watt power supply

Power supply model numbers	**Power supply chassis model numbers**
350-watt (nonRoHS) DM0005005 NVR 5000 350W Spare Power Supply **Note:** Identified by a label on the power supply as: DPS-350	**VPN Router 5000** • DM1401117 NVR 5000 128BIT LAN & GIG ENET • DM1401118 NVR 5000 56BIT LAN, GIG, ENCRYPT ACCL • DM1401153 NVR 5000 128BIT LAN, CSA • DM1401154 NVR 5000 56BIT LAN, CSA • DM0011091 NVR 5000 128 BIT CHASSIS SPARE • DM0011092 NVR 5000 56 BIT CHASSIS SPARE
500-watt (RoHS) DM0005022E5 VR5000E Spare Power Supply **Note:** Identified by a label on the power supply as: DPS-500	**VPN Router 5000E** • DM1401167E5 5000E 128BIT LAN, CSA • DM0011158E5 VR5000 128 BIT CHASSIS FRU

New software features

Version 7.0 of the VPN Router provides the following new software features:

Note: All new features are configured using the NNCLI. The existing features are still configured using the CLI.

Note: There is no 56 bit version of the 7.0 software.

- UNISTIM Virtual ALG for firewall
- LDAP proxy password management support for Active Directory
- LDAP 3DES password encryption
- LDAP user configurable encryption key
- LDAP optimization scheduling
- RADIUS dynamic filtering
- SNMP traps when an IP address pool reaches the configured threshold
- Automatic backups
- PCAP enhancements
- SNMP interface index (IfIndex) enhancement
- Configuring the SSH server
- Custom API
- Network Time Protocol support for Daylight Saving Time 2007 change
- Systemlog lifetime or disk size limit usage option
- FTP server passive mode parameter
- Restricting source IPs access to management
- Respond ICMP Packets option in VRRP configuration
- Preempt Mode in VRRP configuration
- Customizing FWUA login and status window
- ISDN Terminal Endpoint Identifier processing
- Certificate Revocation List Update Specific Time

The following sections describe each of these features in more detail.

UNISTIM Virtual ALG for firewall

A Virtual ALG is a syntax-independent application level gateway (ALG) for firewall traversal that works for both encrypted and nonencrypted UNISTIM signaling, which is a VoIP protocol. A Virtual ALG works only with UNISTIM signaling. Virtual ALG is based on a trust model that assumes that the phone authenticates itself with the call server, and that continuous detection of signaling traffic between the phone and the call server allows media to or from the phone to traverse the firewall. Continuous communication implies that the call server trusts the endpoint and that it would not communicate constantly with the endpoint device if it was not authorized to send media through the firewall. The controlling entity does not acknowledge any requests from unauthorized devices.

For more information, see *Nortel VPN Router Security — Firewalls, Filters, NAT, and QoS* (NN46110-601).

LDAP proxy password management support for Active Directory

The Microsoft Active Directory is a server type that is selected on the Servers > LDAP Proxy window to manage passwords. With this option, if an end user’s password is expired, a popup window opens, forcing the user to change the password. The end user does not receive a notification when the password is about to expire. To change the password, you must have an SSL connection between the VPN Router and Active Directory. The feature extends the LDAP Proxy password management function to Active Directory.

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

LDAP 3DES password encryption

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

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

When you enable 3DES, the LDAP is automatically updated. Each VPN Router that enables the feature checks the LDAP to ensure that all passwords are in 3DES (external LDAP only).

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

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

LDAP user configurable encryption key

In previous releases, passwords stored in LDAP were encrypted with same encryption key across all VPN Routers. This enhancement provides more security on the VPN Router by allowing you to enter a desired encryption key for passwords. If you use an external LDAP server, all VPN Routers using the same external LDAP server must use the same encryption key.

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

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

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

LDAP optimization scheduling

With the LDAP optimization scheduling option, the VPN Router administrator can configure the time and day that the LDAP database is optimized.

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

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

RADIUS dynamic filtering

The Nortel VPN Router offers several methods to control network access for authenticated users. One such mechanism is the tunnel filter. Tunnel filters are applied at the group level and control access to network resources as well as management access to the VPN Router. When a user is authenticated, they are assigned to a group. Part of the group profile specifies that you apply a filter. Dynamic filters provides a means of distributing filters for IPsec user tunnels via a RADIUS return attribute. Depending on the configuration of the RADIUS server, these filters can vary by individual user, or apply to an entire class of users.

➡ **Note:** These filters apply only to IPsec user tunnels. They do not apply to branch office tunnels, or non-IPsec tunnels.

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

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

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

There are many available RADIUS servers, each with different specifics for configuring return attributes. Regardless of how you configure return attributes, they always use the following AV-Pair to define and transmit attribute/value pairs:

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

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

SNMP traps when an IP address pool reaches the configured threshold

You can configure the VPN Router to make an SNMP trap send a notification about an exhausted pool when a defined IP address pool reaches a configurable limit. The list of IP address pools is periodically traversed and if any pool is over the quota, a trap is sent. You can set the limit and the default is 70%.

For more information, see *Nortel VPN Router Troubleshooting* (NN46110-602).

Automatic backups

You can now back up a file or a directory, as well as trigger a backup, when a file changes. Previously, you could only back up system, configuration, and log files. You can use either the GUI or the CLI to configure automated backup.

You can also now use a Secure File Transfer Protocol (SFTP) client as well as FTP to transfer backup files. You can use either the GUI or the CLI to activate SFTP.

For more information, see *Nortel VPN Router Troubleshooting* (NN46110-602).

PCAP enhancements

The packet capture (PCAP) enhancement enables you to capture packets to disk files. Previously, capture packets were captured to random access memory (RAM) only. The buffer acted as a ring and you configured PCAP to continue writing to the buffer indefinitely, or to stop when the buffer was full. You can now choose to continue capturing packets by writing them to files in a circular buffer of maximum 999 files, or to stop when the specified maximum number of files is reached.

There are two ways to capture packets:

- No packet loss—captures all packets. If the RAM buffer is full, a forced flush to disk occurs.
- Packet loss—skips some packets. If the RAM buffer is full, packets are dropped. A malformed packet is inserted in the place where packets were not captured. The number of dropped packets is stored in this malformed packet.

There are 5 new commands for the Command Language Interface (CLI) of the VPN Router. You must use the CLI to configure PCAP.

Note: You can perform PCAP to RAM on multiple interfaces at the same time, but you can perform PCAP to file on only one interface at a time. You can perform a combination of multiple PCAP to RAM and one PCAP to file at the same time.

For more information, see *Nortel VPN Router Troubleshooting* (NN46110-602).

SNMP interface index (IfIndex) enhancement

Third party Network Management Systems (NMS) rely on IfIndex numbers to monitor and gather statistics on devices through SNMP. These locally significant numbers are assigned to the physical and virtual interfaces on the device and enable the NMS to associate statistics with interfaces. Previously, when a branch office tunnel came up, it was assigned a dynamic IfIndex number. Only up tunnels were reported; any down tunnels were not reported.

With the enhancement, each branch office has a static IfIndex assigned to it, the IfIndex is saved in LDAP, and tunnels are reported even when they are down or disabled.

Note: When upgrading to V7.0, the branch office tunnels come up but then restart when the SNMP process assigns the static IfIndex. This behavior does not occur on subsequent reboots.

For more information, see *Nortel VPN Router Troubleshooting* (NN46110-602).

Configuring the SSH server

You can now enable an SSH server on the VPN Router that allows secure CLI sessions to the VPN Router. You also have the option of enabling the private and public interface filters, set the port for the SSH server, and restart the server. You can use either the GUI or the CLI to configure the SSH server.

The following table shows the list of verified SSH clients.

Table 2 SSH clients

Client	Operating System	Version	Encryption type
Putty .56	Windows 2000	0.56	AES256, 3DES, Blowfish
Linux redhat	Linux redhat	OpenSSH_3.5p1	3DES, Blowfish
Solaris 2.8	Solaris 2.8	OpenSSH_3.0.2p1	AES128, AES256, 3DES
Fedora core	Fedora core	OpenSSH_3.9p1	3DES, AES128, AES256

For more information, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500).

Custom API

In Version 7.0, the VPN Router supports a third party encryption Application Programing Interface (API) that adds supports to other encryption types, such as GOST. Because of legal restrictions regarding the source of the encryption code and/or existence of certain encryption types, this API provides a way for third party entities to add country-specific encryption types to the platform. For example, a GOST encryption module developed in one country does not work in another country. Each module must be country-specific.

The API communicates with an encryption module that the third party vendor provides and installs. Nortel verifies and adds a digital signature on the module. Only modules with the Nortel digital signature are recognized by the VPN Router. As of Version 7.0 VPN Router software, a module is available through CAN LLC in Moscow, Russia, which enables GOST to be used over branch to branch tunnels. The GOST module is only available from and must be installed by CAN.

For more information, see *Nortel VPN Router Configuration — Tunneling Protocols* (NN46110-503).

Network Time Protocol support for Daylight Saving Time 2007 change

Network Time Protocol (NTP) supports the 2007 Daylight Saving Time change in the USA and various Canadian provinces. In 2007, Daylight Saving Time begins at 2AM on the second Sunday in March and ends on 2AM on the first Sunday in November.

NTP also supports time zones and Daylight Saving Time for places other than North America, such as India time and British summer time.

For more information, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500).

Systemlog lifetime or disk size limit usage option

The VPN Router allows you to choose between setting a log file disk size limit or a log file lifetime for the Systemlog. Previous versions of VPN Router only allowed the Systemlog to have a lifetime specified (default 60 days).

For more information, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500).

FTP server passive mode parameter

There is a new checkbox called **FTP server passive mode** found in System > Settings in the Router Settings section.

When you enable this parameter, passive ftp connections can connect to the unit, perform directory listings, and upload and download files. If this checkbox is not enabled, you can still use passive ftp connections to connect to the unit but you cannot perform directory listings or upload and download files.

For more information, see *Nortel VPN Router Configuration — Basic Features* NN46110-500).

Restricting source IPs access to management

With this release, an administrator has more control over management services by restricting source IPs connections for management purposes through Access Lists (ACL).

For more information, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500).

Respond ICMP Packets option in VRRP configuration

When you enable the Respond ICMP Packets option, an address which has been taken over by the VRRP Master router accepts and responds to ICMP packet requests sent by the router.

For more information see *Nortel VPN Router Configuration — Routing* (NN46110-504).

Preempt Mode in VRRP configuration

The Preempt Mode feature allows a higher priority backup router to preempt a lower priority Master router, even if the higher priority router is not the address owner. The router with the highest priority becomes Master. This is important in failover situations, and allows the before-failure Master router to become Master again after coming back online.

For more information see *Nortel VPN Router Configuration — Routing* (NN46110-504).

Customizing FWUA login and status window

You can customize the FWUA login and status windows by creating a custom.gif to replace the standard Nortel logo. You can also use style sheets to customize other elements of the window.

For more information on customizing FWUA, see *Nortel VPN Router Security — Firewalls, Filters, NAT, and QoS* (NN46110-601).

ISDN Terminal Endpoint Identifier processing

The new ISDN features require version 2.45 of the microcode. To obtain version 2.45 of the microcode, see "Getting help over the phone from a Nortel Solutions Center" on page 13.

With ISDN Terminal Endpoint Identifier (TEI) processing, the Nortel VPN Router ISDN module, by default, sends two 64K bearer calls on a single TEI. Some older ISDN providers do not support two bearer calls on a single TEI; therefore, Nortel added this option to support these older providers.

You can use the graphical user interface (GUI) or the command line interface (CLI) to configure the calls per TEI.

For more information about Terminal Endpoint Identified processing, see *Nortel VPN Router Configuration — Advanced Features* (NN46110-502).

Certificate Revocation List Update Specific Time

The new feature for the Certificate Revocation List is CRL Update Specific Time. With this feature, the Nortel VPN Router administrator can configure the time and day that a CRL request is sent to the CRL Server.

This CRL process has disadvantages because it is run at the LDAP priority and it is very CPU intensive. In environments with heavy volume traffic and very large LDAP CRLs, the CRL process can cause timeouts and data drops. The administrator can use the CRL Update Specific Time to avoid these timeouts and data drops.

For more information about the Certificate Revocation List, see *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600).

Restricted product - export license requirement

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 section contains customer issues fixed in this release and general considerations for this product.

Customer issues fixed in this release

Table 3 lists customer issues from previous releases that were fixed in V6.05.100 release.

Table 3 V6.05.100 release

CR number	Description
Q01060298	The Nortel VPN Router no longer returns only the first 64 entries of the routing table for MIB-II IP Route Table SNMP polls.
Q01193293	On a Nortel VPN Router, changing the mask of an interface from the serial menu with a value that made the IP address equal with the network address of the subnet no longer causes the following error message to appear: *Couldn't set the Subnet Mask value*.
Q01199301	An upgrade from V04_85 to V06_00 on the Nortel VPN Router no longer results in the loss of Firewall objects.
Q01246301	On the Nortel VPN Router, there is a public default gateway in in the route table when the public interface obtains the IP address from a DHCP server.
Q01247735-01	On a Nortel VPN Router, the default route over a T1 PPP link is added to the routing table after a restart.
Q00987742-02	On the Nortel VPN Router, the Circuitless IP page in the GUI is available if the IP address is given in a nonstandardized format.
Q01116006-01	The Nortel VPN router no longer cores while passing traffic over tunnels. The issue happened only when using external LDAP.
Q01119969	On a Nortel VPN Router, the first failure of a Fiber Gig Ethernet link terminates the interface group.

Table 3 V6.05.100 release (continued)

CR number	Description
Q01140430	A Memory leak no longer occurs on the Nortel VPN Router when using Certificates for Authentication on user tunnels.
Q01174599-01	On the VPN Router, CLI support for V.90 card now exists for the following commands: snmp-server enable traps hardware ? no snmp-server enable traps hardware ?
Q01175788-01	The Nortel VPN router no longer cores when multiple users employ a single configured L2TP user account for tunneling.
Q01218846-01	On a Nortel VPN Router with dual disks, hot-swapping a drive but not clicking Enable after reinstalling the drive no longer causes the VPN system to halt processing when a format or list directory contents command is performed on the remounted drive.
Q01219475-01	The Nortel VPN Router no longer experiences a QoS: GUI: *Parser Error* problem when attempting to display QoS statistics and the line of data exceeds 100 characters in length.
Q01246607-01	A VPN router with GMT +1 (Europe) now stops Daylight Saving Time on the last Sunday of October, according to EU regulations.
Q01251107	The Nortel VPN router no longer drops packets over a VPN client tunnel after re-establishing a connection if the previous tunnel terminates ungracefully. This issue occurred when RADIUS authentication was used and no firewall was enabled.
Q01039888-01	On a Nortel VPN Router, logging for NTP is no longer incorrect. Erroneous log messages stated that the NTP clock was adjusted every hour.
Q01185011-01	For an ASDL interface on a Nortel VPN Router, changing the IP address source selection from *Negotiated* to *Specified*, or vice versa, no longer causes a VPN system to halt processing or core.
Q01248693	On a Nortel VPN Router, a user logged in through a Control Tunnel with Restricted Mode enabled no longer prevents all other user tunnels from connecting.
Q01267137-01	If the WAN link on a Nortel VPN Router is configured with Frame Relay, IP packets between the size of the interface MTU and the interface MTU minus four are now forwarded from the Frame Relay link.
Q01275587-01	L2TP data packets transmitted from a Nortel VPN Router do not have sequence numbers unless requested.
Q01044727-01	On the Nortel VPN Router, the Radius diagnostic report showed incorrect information when using group level Radius.

Table 3 V6.05.100 release (continued)

CR number	Description
Q01251562-01	The Nortel VPN Router no longer requires root CA and complete certificate chain installation to successfully install a server certificate for HTTPS management.
Q01275951-01	On a Nortel VPN Router, user tunnels are no longer forced to the secondary VNR when load balancing was enabled.
Q01285754-01	The VPN Router no longer sends wrong *Certificate Request payload* during BOT certificate authentication.
Q01242299	Nortel VPN Router no longer cores when checking the system log after removing all files from the system/log directory.
Q01213277-01	The Nortel VPN Router event log now shows which certificate belongs to which Branch Office Tunnel if an error occurs.
Q01292571	On a Nortel VPN Router, a user that has administrator rights set to *view and view* can no longer modify LDAP Proxy settings, which affects user tunnel authentication.
Q01225876-01	On the Nortel VPN Router, logging in to HTTP admin with a backslash (\) prefix no longer cores the router.
Q01187605-01	On the Nortel VPN Router, a DLSw remote peer configured with address 0.0.0.0 no longer causes a core when a connection is initiated with this peer.
Q01169205-01	The Nortel VPN Router no longer stops processing when the allocation of a PPTP connection fails.
Q00996298-01	The Nortel VPN Router no longer cores during an IPSEC user logoff if an account that was previously deleted is referenced.
Q01202623-01	The Nortel VPN Router no longer erroneously reports a Health Check WARNING when RADIUS authentication and accounting servers are disabled.
Q01259481	The Nortel VPN Router no longer cores when a network definition contains an unmatched parenthesis.
Q01271104-01	On a Nortel VPN Router, FTP PORT transfers from a server behind NAT/CSFW now work.
Q01306856	On the Nortel VPN Router, the VRRP deactivate option is no longer missing from the output of the show running-config command.
Q01176372-01	The Nortel VPN Router no longer displays erroneous Tunnel Guard error messages in the event log at the recheck interval when no problem exists with software versions.

Table 3 V6.05.100 release (continued)

CR number	Description
Q01244857	The Nortel VPN Router the CLI command *show running-config system wan* now contains the *line-encoding* command.
Q01306264	On the Nortel VPN Router, the *show running config routing vrrp* command output no longer contains unnecessary information about the interface RIP and OSPF configuration.
Q01185103-03	On the Nortel VPN Router, if a TunnelGuard error message occurs, the message now shows the SRS policy name in the message.
Q01306267	On Nortel VPN Router, the *show running configuration routing vrrp* command output no longer misses the configured critical-interface-group for one of the configured interfaces.
Q01308134	The Nortel VPN router now has a CLI option to disable IP-directed broadcasts.
Q01306270	On the Nortel VPN Router, some configuration combinations for the policy object groups no longer lead to invalid *show running config service policy* output.
Q01305147	On the Nortel VPN Router, the *show running config service policy* no longer generates commands longer than 480 characters causing provisioning to fail.
Q01276638	On the Nortel VPN Router, a DLSw peer is now re-established after a restart if the peer is configured over a Frame Relay circuit.
Q01310093	On a Nortel VPN Router, when a subinterface is deleted from the CLI, the subinterface no longer appears in the configuration as well as *show ip int* and *show ip int brief*.
Q01252376-01	The Nortel VPN Router DHCP server now issues an IP address to a PC that previously had an IP obtained from another DHCP server.
Q01316605-01	If QoS filters are changed on any interface through the GUI, the Nortel VPN router no longer cores.
Q01277898	On the Nortel VPN Router, an ACCEPT policy for OSPF no longer generates a core when the policy is configured from CLI.
Q01297464	Load balancing on the Nortel VPN Router now works after an upgrade to V06_00 from any release prior to V06_xx.xx.
Q01295471	Enabling Equal Cost MultiPath on the Nortel VPN Router with NAT policies configured no longer causes inappropriate NAT translations.
Q01326645	On the Nortel VPN Router, the ENABLE status for Direct Nets and Direct Hosts are no longer reversed by the BGP show command *show ip bgp redistribution*.

Table 3 V6.05.100 release (continued)

CR number	Description
Q01208524-01	The Nortel VPN Router no longer cores during a connection attempt through a telnet session.
Q01334191-01	Processing SIP calls no longer cause a memory leak on the Nortel VPN Router.
Q01283462-01	On the Nortel VPN Router, UDP NAT entries now time out after the documented three-minute time interval. Subsequently, these entries are deleted from the NAT translation table.
Q01274933-01	On the Nortel VPN Router, a user is no longer bound to the wrong group when using an LDAP Proxy with Certificates.
Q01229607	On the Nortel VPN Router, a user can now configure RADIUS authentication on a WAN interface.
Q01292662	A core no longer occurs on the Nortel VPN Router if two OSPF interfaces are configured with different costs.
Q01353264	Admin HTTP sessions on the Nortel VPN Router can now idle out or be logged off from the Management GUI.
Q01326075-01	The Nortel Router no longer stops processing after selecting Routing > Static Routes from the Management GUI.

Table 4 lists customer issues from previous releases that were fixed in the V6.05.140 release.

Table 4 V6.05.140 release

CR number	Description
Q01044305_01	The Nortel VPN Router no longer discards non-standard FTP packets when NAT was applied to Branch Office Tunnels.
Q01044727-01	The RADIUS Diagnostic Report on the Nortel VPN Router no longer shows erroneous configuration errors when the group setting in Profiles->Groups->Base->IPSEC is configured for Group Level Radius.
Q01079892-01	The Nortel VPN Router no longer cores when a task is created at the same time another task is deleted.
Q01127098-01	The Nortel VPN Router no longer lacks a CLI command that can disconnect a specific session for a particular user.
Q01221722	The Nortel VPN Router no longer cores when viewing the Event Log because of special characters displayed in Event Log.

Table 4 V6.05.140 release (continued)

CR number	Description
Q01231980-01	When multiple Frame Relay Virtual Circuits are configured on a Nortel VPN Router, the ifSpeed MIB value no longer displays the same value for all the Virtual Circuits.
Q01243188	The Nortel VPN Router does not return an incorrect next-hop value when performing Traceroute from the VPN client.
Q01257496-01	The Nortel VPN Router does not attempt to connect to a certificate server on the private interface, even if CMP is disabled on the interface.
Q01263131	The Nortel Router now sends RIP updates on the Primary Branch Office Tunnel after BIS rediscovery occurs.
Q01272710-02	The OSPF LSDB on the Nortel VPN Router now correctly updates after an area range is removed.
Q01278185-01	The Call Admission Priority for Groups on the Nortel VPN Router no longer functions if the Advanced Routing key is not installed and QOS->Call Admission is DISABLED.
Q01284128-01	An ABOT configured on the Nortel VPN Router with the local gateway as *AutoSelect* now recovers if the Dial on Demand interface starts or stops too fast.
Q01284522-01	The IpForwardTable on the Nortel VPN Router no longer shows the next-hop as 0.0.0.0 when the next-hop interface is a Branch Office endpoint.
Q01292501-01	When using certificates with an AltSubjectName for Branch Office authentication on the Nortel VPN Router, the AltSubjectName for the Local Identifier type IP can now be configured via CLI.
Q01312474-01	The VPN Router built-in DHCP server now replies to requests if the User Class option is specified by the client but not recognized by the server.
Q01324536	The Nortel VPN Router now installs a default route when PPP is configured on a T1 interface with the Remote IP Address set to *Accept Negotiated*.
Q01342308-01	The Nortel VPN Router no longer permits the upgrade to a FIPS compatible version that does not contain the desmac.dat file. This resulted in a continuous crash.
Q01344462	Nortel VPN Router no longer cores within TunnelGuard after a connection error occurs connecting to the PC Agent.
Q01354195-01	The Nortel VPN Router timers no longer act erratically after 414 days from the last reset because of the timers' representation limitation.

Table 4 V6.05.140 release (continued)

CR number	Description
Q01355028	When a port of the Quad T1 interface card receives a Blue Alarm Indication (or AIS), the Nortel VPN system no longer demonstrates high CPU Utilization, even after traffic destined for the affected port ceased or the link is disconnected.
Q01366666-02	The Nortel VPN Route no longer cores when referencing the routing table after an interface goes down.
Q01367218	The Nortel VPN Router no longer writes the system log file to disk even though the radial *Write System Log to File* is disabled.
Q01367613	When a CRL is deleted on a Nortel VPN Router, it now downloads when the next user attempted to login. This occurs even if the user has Group Level Authentication configured and uses LDAP proxy.
Q01368558	When a customer enables Restricted Mode via the CLI, all backend servers (Radius, LDAP, DHCP and so on) are now reachable.
Q01369393	When using a NAT rule to translate an internal address to the *Public Interface* address, the Nortel VPN Router now translates the source address if the ultimate destination of the connection is another internal address.
Q01370768	Users can now disable the Re-key Timeout on the Nortel VPN Router by entering the value 00:00:00 as specified in the documentation.
Q01371631	After a reboot on a Nortel VPN Router, the HTTP sessions no longer stop responding after the first attempt to manage the SSL VPN card, even when the VPN Router Stateful Firewall and Enforce TCP Conversation Rules are enabled.
Q01373095	The Nortel VPN Router no longer displays an error when either the default or the maximum lease time value for DHCP is set to infinite.
Q01374435-01	The Nortel VPN Router no longer experiences a core when backing up the LDAP if NAT or Firewall policies are configured.
Q01376689	After canceling a scheduled reboot from a named config file, the Nortel VPN Router no longer boots from the named config file.
Q01388055-01	The Nortel VPN router no longer report an incorrect source address in ICMP unreachable packets.
Q01389415-01	A user can now configure an external DHCP server through the GUI on the Nortel VPN Router.
Q01392155	The Nortel VPN Router PPP implementation allows PPP interfaces to have endpoint IP addresses that are from a different subnet. When such a situation is encountered, a configuration warning is posted on the Event Log and the local endpoint's subnet mask is changed to 255.255.255.255.
Q01394814-01	The Nortel VPN Router no longer fragments large uncompressed packets by IP after encryption.

Table 4 V6.05.140 release (continued)

CR number	Description
Q01395708	The Nortel VPN Router no longer experiences a core after upgrading to Release V06_05.100.
Q01396909	When an *SNMP get interface* is performed on a Nortel VPN Router, an address is no longer displayed for the CLIP interface when CLIP is not configured on the router. This resolves the issues with management software due to the possible duplication of MAC addresses.
Q01403240-01	The Nortel VPN Router no longer locks up when using the Hardware Accelerator and throughput is higher than normal.
Q01406461	The display format of the SNMP Link UP and Link Down traps is now the same, which makes it easier to monitor those traps on a standard tool.
Q01407495	The Nortel VPN Router now displays the learned IP address when dynamic PPPoE is set for the public interface.
Q01414706-01	When logging on to the Nortel VPN Router, the user no longer has to log on three times before gaining access when using Entrust certificates with CDP authentication.
Q01415415	During interface configuration, the Nortel VPN Router no longer cores when the Multi-Field Classifier is enabled or disabled.
Q01418676	On the Nortel VPN Router, when no Egress Multi-Field Classifier is configured, the show qos interfaces command no longer displays *Ingress (Inbound) Multi-Field Classifier: None* instead of *Egress (Outbound) Multi-Field Classifier: None*.
Q01422229-01	The Nortel VPN router no longer cores after performing an LDAP search.

Version 7.0 product considerations

- 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. The reason for this is that 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.
- Nortel no longer supports Axent defender. It was removed from the management GUI.

- If you use a 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.
- ABOT's 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 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 set to 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 for configuring 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. The workaround is: 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, select the following:

  ADMIN > Administrator > Default Language > Japanese (Shift-JIS)

  Using CLI, enter the following command:

  ```
  # default language japanese
  ```

Note: Nortel VPN Router software release v7.0 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 PPPoE interface when creating an Interface Group for a Demand profile if the local IP Address in Interface PPPoE settings is set to 0.0.0.0 (Dynamic). The interface is not available in Routing > Interface Group 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 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 is using Passive FTP, be sure to enable the option after upgrading.
- 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. It is recommended that this be done after executing large scripts.

Version 7.0 known anomalies

The following sections describe issues that Nortel has determined need to be corrected in a future release, but are not fixed in the current release.

Q01078645 — Incorrect message when IP of private interface is set as external IP address source

If you create a user tunnel, using a VPN Router configured as DHCP as the User IP Address Source, and the IP of a private interface as the Specified External Server, the tunnel comes up and there appears to be no problems. However, the NVR the clients use displays an incorrect notification of No recent offers received from this DHCP server, instead of the correct message of Configured.

Q01142400 — DHCP Server always offers packets with management IP as source

When a relay is used, the DHCP client gets its address from the DHCP server through the relay. The server provides the client with a default gateway. All DHCP packets received by the client from the server have the server’s management IP address as source, and the server identifier field is set to the server’s management IP address, regardless of the physical interface the server sent the packets through. Halfway through the lease’s duration, the client tries to renew its lease by sending unicast requests to the server’s management IP address. DHCP clients are unable to renew their lease because the DHCP request packets sent by the client are trying to directly reach the DHCP server management IP address, which is unreachable.

You can renew your lease if the default gateway used by the DHCP clients can reach the management IP address of the VPN Router that acts as the DHCP server. Otherwise, you remain without your IP address for a few seconds until new IP addresses are negotiated with the DHCP server through the DHCP relay.

Q01191261—Netdirect subnet error log on VPN Router is incorrect

The VPN Router event log says *SSL-VPN netdirect address (xx.xx.xx.xx) must be in the 192.32.18.0 space* even though it is the front-end interface and should not be in the same subnet as the backend interface.

Q01191923—TCP MSS options not configurable under secondary multinet interfaces

TCP MSS options are available only for the primary interface. You cannot configure the secondary multinet interfaces.

Q01229904—Route table lost after reboot if more than 507 VLANs are configured on VPN Router

If more than 507 VLANs are configured on the VPN Router, the route table is lost after a reboot (empty route table). If the number of VLANs is equal to 507 or less, there is no problem if the VPN Router is rebooted.

Q01449017-01—QoS: Call Admission does not work correctly

QoS: Call Admission (not Call Admission Priority) does not work correctly in V06_00.310, V06_05.123 and V07_00.031 of the code. In these code versions, when Bandwidth Management and Call Admission are enabled and there is a tunnel established with a Branch Office Bandwidth policy of 10mbps for the committed & excess rate, the other incoming tunnel connections are denied when they should be accepted.

Q01468605—Not all NAT routes are redistributed in BGP

When you apply a pooled NAT policy to translate many Classes (to simulate many hosts) on Interfaces and redistribute NAT routes on BGP, not all of the NAT routes are redistributed.

Q01471112—Summarized NAT routes are not redistributed in BGP until they are enabled or disabled

If you redistribute some NAT host routes in BGP and then activate the summarization for those host routes, the summarized routes are not redistributed in BGP unless you disable and reenable the redistribution of NAT routes in BGP.

Q01482188—Configured description for virtual circuits on WAN interface not displayed on snmpwalk

On a WAN interface (PPP protocol), you can configure a description for logical circuits. However, snmpwalk on ifName and ifDescr displays default values instead of configured values.

Q01483342—CORE in scaling rack when 7854 HWA disabled with 2500 BOT's and then enabled

If you disable and then enable the 7854 HWA card with 2500 ABOT tunnels, it produces a core on the VPN Router.

Workaround: Wait at least 3 minutes before re-enabling the HWA card to allow time for the tunnels to be swapped over to the software.

Q01497139-03—Cannot log onto VPN Router with a digital certificate when CRL Query Optimization is enabled

If CRL Query Optimization is enabled, you cannot use a digital certificate to log onto the VPN Router. You receive a message saying "Login Failure due to: Remote host not responding".

Q01500817—Critical interface issues when associated with Master Delay

When an interface group is disabled and reenabled and the VRRP interface goes from Critical state to Backup state (because of Master Delay), the default route is lost, which causes you to lose management of the VPN Router. This happens because the VRRP interface is not up when the Interface goes from Critical to Backup. The default route is back in the routing table when VRRP interface goes in Master state (after the delay time).

The default route is lost from the beginning if the interface group is down twice and the VRRP interface goes to Critical state a second time. The default route is not lost from the beginning if the interface group is down for the first time after you configure the feature on the VPN Router.

Q01500838—Subinterface with VRRP remains in INIT after disabling and reenabling within Time of Day interval

If you disable and then reenable a subinterface configured with VRRP and Master Delay mode set to Time of Day within the specified interval, the subinterface remains in INIT state. The subinterface should change to the Master state after you reenable it, but it does not. The state remains INIT even if the VRRP is restarted. The subinterface configured with VRRP assumes back the mastership only when you restart the VPN Router.

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

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

Q01511688—Value becomes empty when changing private VPN Router address

When you change the private VPN Router IP address, the IP address value becomes empty if you do not also change the cost.

Q01512149—Incorrect next hop recalculations when using PPP

When you use PPP and the negotiated IP addresses are not on the same subnet, the next hop recalculations for the best router can be incorrect, resulting in unreachable routes after a circuit goes down and comes back up.

Q01522262—Cannot make SSH connection after 8 invalid attempts

If a user attempts more than 8 invalid SSH connections either concurrently or serially, the server will not allow subsequent invalid or valid SSH connections.

The workaround is to restart the SSH server.

VPN Router considerations

The following sections contain general considerations for this product.

Upgrade procedure considerations:

- VPN Router 1010, 1050, and 1100 require a 64 Mb flash disk.
- Version 7.00 supports upgrades from Versions 4.70, 4,80, 4.90, 5.00, and 6.00. If you run an older version, you may have to upgrade to a later version before you upgrade to Version 7.00.
- 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 any unnecessary files from your VPN Router.
- Any 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 7.00 software, you create a recovery floppy diskette as soon as you complete the upgrade. You must use a formatted diskette when creating 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.

- The automatic backup feature is provided as a way to backup 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; a full file system produces unexpected behavior. To check the hard disk usage level, select 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.

Viewing and calculating memory usage

The minimum memory requirement for Version 7.00 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 configuration of tunneling, routing, and firewall. 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/documentation

The parameters affecting VPN Router memory usage are:

- VPN Router software version.
- Single or dual CPU (if single CPU model or dual CPU model VPN Router).
- Internal or External LDAP shows whether internal or external LDAP configured.
- Number and type is the number and type of branch office and user tunnels.
- Static routes is the number of static route entries in the IP routing table.
- RIP routes is the number of RIP route entries in the IP routing table.
- BGP routes is the number of BGP route entries in the IP routing table.
- OSPF Routes is the number of OSPF route entries in the IP routing table.
- Redistributed OSPF, BGP and RIP Routes is the number of routes redistributed into RIP, BGP, and OSPF Routing protocols.
- FW/NAT Max connections is the maximum number of connections configured on the Services > Firewall/NAT > Edit window.

- FW/NAT Number of Sessions is the total number of Firewall/NAT sessions.
- BO NAT Number of Sessions is the number of Branch Office NAT sessions.
- SFW Enabled shows if SIF (Stateful Firewall with Interface Filter) is on.
- Interface NAT Enabled shows if Interface NAT is on.
- Antispoofing Enabled shows if Antispoofing is on.

Software and hardware compatibility

The minimum VPN Client version that is supported by Version 7.00 is 4.65.

Table 5 shows VPN Router hardware and software compatibility. An X in the table indicates which platforms support this version of the VPN Router software.

Note: The SSL VPN Module 1000 can be installed only in the VPN Router 1740, 1750, 2700, and 5000 platforms.

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

Table 5   Hardware platform and server software compatibility

Hardware platform	**Server software compatibility**						
	4.76	**4.80**	**4.90**	**5.00**	**6.00**	**6.05.140**	**7.00**
1010	X	X	X	X	X	X	X
1050	X	X	X	X	X	X	X
1100	X	X	X	X	X	X	X
600	X	X	X	X	X	X	X
1500							
1510							
1600	X	X	X	X	X	X	X
1700	X	X	X	X	X	X	X
1740		X	X	X	X	X	X
1750					X	X	X
2000							

Table 5 Hardware platform and server software compatibility

Hardware platform	Server software compatibility						
	4.76	**4.80**	**4.90**	**5.00**	**6.00**	**6.05.140**	**7.00**
2500							
2600	X	X	X	X	X	X	X
2700	X	X	X	X	X	X	X
2750						X	X
4000							
4500	X	X	X	X			
4600	X	X	X	X	X	X	X
5000	X	X	X	X	X	X	X
5000E						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 a tunnel is assigned 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) 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).
- GigE fiber and copper cards do not fit into the connector on slot 4 on the VPN Router 4600.
- If more than 10 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 7.00.
- 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 are using 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 and/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 the Auto-Detect NAT option on the Profiles > Groups > GroupName > Edit IPsec window, which activates NAT Traversal and allows multiple PCs behind the NAT box to function properly.
- You cannot run the Windows* 2000 client using 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/IPsec. If you go to the Services > IPsec window and change the IPsec Policy Manager setting from Disabled to Automatic and reboot the system, the client detects the loading of the Windows 2000 IPsec driver and disables the client's IPsec driver.

- If you are currently running VPN Router Version 4.70 with NAT policies applied to branch offices, the policies appear as read only in the Version 4.80 or later Java GUI. You will see an (old format) text message to alert you to the change. The Version 4.70 policies are translated, but you can no longer edit them. If you want to edit a Version 4.70 policy or use the CLI show running config command to export the NAT rules, you must launch the Java GUI, select the (old format) policy, select copy and save as, and apply the new policy to the branch office
- When you upgrade to Version 4.80 or later, the RADIUS service is disabled by default even if it was previously enabled. If your configuration is using RADIUS, be sure to reenable RADIUS service after upgrading
- 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. Do not use L2TP/L2F port 1701 or General Packet Radio Service (GPRS) port 3386. Make sure that any port you select does not conflict with any ports that you are already using.
- Any configuration of route policies 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 admin users:

- Internet Explorer 5.5 or 6.0 and Netscape* 4.79 or 6.2 are the supported Web browsers. You should be using the latest version of your browser to ensure accurate screen displays of the Web interface for the VPN Router.
- Java Runtime Environment 1.4.2_04 must be installed in order to manage the SSL VPN and the Stateful Inspection Firewall UI. The JRE 1.4.2_04 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 attempting 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 which 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 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 using HTTPS to secure administrator access to the VPN Router, Netscape Communicator and Internet Explorer perform various and differing security checks. The following configuration is recommended to obtain the best performance when administering the VPN Router securely using Admin SSL.
  - Make an entry in the hosts file corresponding 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 on System > Certificates > pkcs#10 certificate request) should be either a DNS name that resolves to the management IP address or the actual management IP address. For further information about Netscape certificates, go to http:/home.netscape.com/eng/security/comm4-cert-download.html.
- Using Internet Explorer Version 6.0.2800.1106IC on Windows NT 4.0, the GUI presents inconsistent information in 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/SSH Access, HTTP Proxy and Port forwarder features, the following browser and Java combinations are recommended:

  Windows:

  - Internet Explorer 5 or better with Sun's JRE 1.3 or better
  - Internet Explorer 5 or better with Microsoft's 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's JRE 1.3 or better
  - Mozilla 1.3 or better with Sun's JRE 1.3 or better

  Configuration via 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 have caching enabled 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 occurs when the initiation is due to live traffic or a test button tunnel initiation.
- For nailed-up connections, the IPsec SA can go down due to inactivity. Only the 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.
- Table 6 lists the maximum number of tunnels for each VPN Router model and indicates whether each model has a five-tunnel base unit version.

Table 6 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
1700, 1740, 1750	500	Yes
2700	2000	Yes
4600	5000	No
5000	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 configuring 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.