Version 7.05.300

NN46110-403 02.01
315000-T Rev 01
November 2007
Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Release Notes — Server Software Release 7.05.300

NORTEL

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 details what's new in *Nortel VPN Router Release Notes — Server Software Release* (NN46110-403) for Release 7.05.300.

Features

See the following section for information about feature changes.

1000BASE-T (GT 1000) Ethernet card

The 1000BASE-T (GT 1000) card replaces the nonRoHS-compliant 10/100 Ethernet module. See "1000BASE-T (1000 GT) Ethernet card" on page 17.

24-byte LDAP encryption keys

In this release, you can configure a 24-byte encryption key for LDAP passwords. See "LDAP encryption keys" on page 18.

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:

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, go to:

www.nortel.com/support

Select Security & VPN and then, in the section called Virtual Private Networking (VPN), IPSEC, and SSL, click the appropriate VPN Router product.

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.

Preface

These release notes contain the latest information about the Nortel VPN Router Version 7.05.300. 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—Tunnel Guard* (NN46110-307) provides information about configuring and using the Tunnel Guard 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.

Chapter 1
Overview

These release notes contain the latest information about the Nortel VPN Router version 7.05.300. They support the software maintenance release and address customer-found software issues.

As well as the rebranding changes for version 7.0x, 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 7.0x, 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 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, the following versions are recommended for the related products. This is only a recommendation; this release is compatible with all supported versions:

- Nortel VPN Client 7.01.250

- Nortel VPN Client 6.07
- Nortel Tunnel Guard Agent 3.0.1.0_004
- Nortel VPN Gateway 6.0.1

Nortel VPN Client Version 5.01.103 and above is required to obtain the full benefit of Entrust Roaming Profiles and Entrust Link Certificates.

Nortel VPN Router Version 7.05.300 supports the following application software versions:

- Nortel VPN Client (NVC): NVC V5.01, NVC V6.01 and NVC V7.0x

Note: Client versions V5.01, V6.01, V6.07, and V7.01 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.

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

Note: If the Nortel SSL VPN module 1000 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).

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

New hardware features

Version 7.05.300 of the VPN Router supports the following new hardware feature:

1000BASE-T (1000 GT) Ethernet card

The 1000BASE-T (1000 GT) Ethernet card is a Restriction of Use of Certain Hazardous Substances (RoHS)-compliant Ethernet module.

The 1000BASE-T (1000 GT) Ethernet card provides 10BASE-T, 100BASE-TX, and 1000BASE-T Ethernet services and supports autonegotiation. The card supports the IEEE 802.3ab standard and provides RJ-45/CAT 5 interconnection. It can operate in either full or half duplex mode at 10/100 Mbit/s, and in full duplex mode at 1 Gbit/s..

Note: The 1000BASE-T (1000 GT) Ethernet interface card can only operate at 10/100 Mbit/s on the VPN Router 600, 1100, 1600, and 2600.

The VPN Router 600, 1100, 1600 and 2600 only support 10/100 Mbit/s operation for the 1000BASE-T (1000 GT) Ethernet card. To ensure reliable speed/duplex operation on these platforms, Nortel recommends that both the interface and the attached devices are hard-coded to the appropriate matching 10/100 speed and duplex settings.

The 1000BASE-T (1000 GT) Ethernet card supports 10/100/1000 Mbit/s operation in the VPN Router 1700/1740/1750, 2700/2750, 4600, and 5000.

For the 10/100/1000 Ethernet card to be recognized by the system, the minimum required VPN Router operating software is:

- 5.05.330
- 6.05.140 and all subsequent versions
- 7.00.062
- 7.05.100 and all subsequent versions (FIPS branch)
- 7.05.300 and all subsequent versions

New software features

For the 7.05.300 release, you can use either a user-defined or a default LDAP encryption key. This key can either be 8 bytes (DES) or 24 bytes (3DES) in length.

For more information, see the following section.

LDAP encryption keys

In Versions 6.05.170 and later (including Version 7.05.300), you can configure a 24-byte encryption key for passwords stored using the Lightweight Directory Access Protocol (LDAP).

By default, the VPN Router uses the Data Encryption Standard (DES), and therefore an 8-byte key for LDAP-stored passwords. To use a 24-byte key, you must first enable Triple DES (3DES) encryption. If you enable 3DES, a 24-byte password is required.

Only passwords stored in the LDAP file are affected by this new feature. Any passwords stored in the configuration file remain unchanged and are encrypted as in previous software versions.

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

Configuration information

Internal and external LDAP keys are stored in flash memory. A hash is calculated from the user-defined key and stored in the LDAP file.

To restore a VPN Router to the default internal key:

- the VPN Router must be set to factory default (this clears the key saved in flash), and
- the configuration and LDAP files to be restored must be ones that were saved before any user defined keys were applied.

External LDAP key information

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

To change the key, the VPN Router must be configured with the last saved key.

Keys on all routers that use a shared LDAP must match before any router can change the key; and if one router changes the key, all the others must have matching keys configured. For example, if two routers, VPN Router1 and VPN Router2, use the same external LDAP, and VPN Router1 sets a user-defined key, then VPN Router2 cannot set any key except the one that matches the key of VPN Router1. After VPN Router2 sets a key that matches, then VPN Router2 can configure a new key. If VPN Router 2 sets a new key, then VPN Router1 must configure a matching key before authentication is successful.

After VPN Router1 sets a key, the LDAP passwords are encrypted using the key. When VPN Router2 sets the same key, there is no change to the LDAP passwords.

Changing from DES to 3DES

For internal and external LDAP, 3DES uses the default internal key unless a user key is defined. After 3DES is used, the VPN Router processes the entire LDAP, field by field, and sets a flag for every password that is encrypted by 3DES.

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

3DES external LDAP information

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

After a VPN Router enables 3DES, the LDAP passwords are encrypted using 3DES. When another VPN Router that shared the LDAP enables 3DES, no changes are made to the LDAP stored passwords.

3DES external LDAP proxy information

If an external LDAP proxy is used, the VPN Router (which has its own internal LDAP file) does not touch or modify the external LDAP database. However, the VPN Router modifies the Bind Password that is attached to the Bind Name (under LDAP Proxy Servers).

Configuration scenarios

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

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

Consider the following scenario:

- A VPN Router with V6.05.140 (a version that supports only 8-byte keys) is configured with:
  - 3DES encryption enabled
  - an 8-byte LDAP user encryption key.
- The VPN Router is upgraded to V7.05.300 and the 24-byte user encryption key is not configured.

This is a supported configuration, and the running configuration and LDAP files can still be modifed as required. Automatic backups and LDAP saves for the purposes of disaster recovery are recommended.

If this VPN Router must be replaced with a new VPN Router, or factory-defaulted and reloaded to a full V7.05.300 version, the following steps must be performed to restore the previously saved backup/LDAP:

1. Configure the management and interface addresses.
2. On the Servers > LDAP window, configure the original 8-byte encryption key.

Note: Do not select 3DES encryption. After 3DES is enabled, a 24-byte key is required.

3 Restore the saved V7.05.300 configuration file

4 Reboot the VPN Router.

5 Restore the saved V7.05.300 saved LDAP.

After you perform these steps:

- 3DES is enabled;
- the original 8-byte encryption key is used;
- tunnels operate.

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

Case 2—Upgrades and unknown key lengths

When 3DES is enabled, software versions prior to 6.05.170 only allow an 8-byte user key to be entered. In V6.05.170 and later, only 24-byte user encryption keys are permitted after 3DES LDAP encryption is enabled. The VPN Router software does not make a distinction between:

- an 8-byte key that was entered in an older version of code and upgraded to 6.05.170+; and
- a user key that was entered natively in 6.05.170+.

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

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

Customer issues fixed in this release

In version 7.05.300, you can now configure a 24-byte encryption key for LDAP passwords. See "New software features" on page 18.

Table 1 lists customer issues from the 6.05 to the 6.05.175 software stream that are fixed for V7.05.300.

Table 1 Issues fixed for V7.05.300.

CR number	Description
Q00924572	A Nortel VPN Router user with view-only rights is only able to display the first page of a group.
Q01155571	The Nortel VPN Router console may hang momentarily after it adds non-reachable SNMP Trap/Get hosts.
Q01165684	An incorrect line speed for the Nortel VPN Router LMC 1000 card may appear during interface configuration.
Q01184732	Nortel VPN Router VRRP may fail due to incorrect Critical Interface function.
Q01204638	L2TP may drop multiple tunnels when one tunnel sends a disconnect request to the Nortel VPN Router.
Q01251562	One cannot install a server certificate for https management on the Nortel VPN Router.
Q01267714	The MTU reverts to default after DHCP renewal on the Nortel VPN Router.
Q01284522	On the VPN Router, remote networks may become unreachable if the default route is through a dynamic branch office tunnel.

Table 1 Issues fixed for V7.05.300.

CR number	Description
Q01335175	Nortel VPN Router Time of Day Master Delay mode may work properly after the gateway reboots.
Q01357308	An Interface Group that is down, and contains Dynamic BOOT, may incorrectly report as up on the Nortel VPN Router.
Q01369393	NAT may not translate an address when using the Nortel VPN Router Public Interface object.
Q01402258	The Nortel VPN Router may core when it tries to change an IP address that is configured for VRRP.
Q01413140	The Nortel VPN router may attempt to access a RADIUS Accounting Log file before it has been created. This results in an error in the event log.
Q01474068	The Serial Data Rate cannot be set to 2048K from the Nortel VPN Router CLI.
Q01491598	Nortel VPN Router VRRP stops advertising when a BOOT is enabled and disabled.
Q01497838	If an interface has no IP address configured on the physical interface, but an IP address is configured on an 802.1Q sub-interface, a Health Check Warning: "Device fei1 has no IP address" is shown.
Q01524262	Nortel VPN Router Tunnel Guard SRS Rule failure details are not logged in switch event logs.
Q01537523	The Nortel VPN Router LAN interface counters roll-over.
Q01542582	A Nortel VPN Router may core after an upgrade if it encounters failed RADIUS authentication attempts.
Q01546621	The GUI HTTP server on the Nortel VPN Router is in violation of RFC 1945 in the way that it treats HEAD and GET commands.
Q01548743	There may be a slow menu refresh when using Internet Explorer 6 to access the Nortel VPN Router.
Q01557483	Nortel VPN Router authentication fails when "User must change password at next logon" is enabled on an active directory host.
Q01570229	A Nortel VPN Router branch office tunnel may not recover when an T1/E1 link fails and recovers.
Q01574790	There is no sysObjectId in the Newoak MIB for the Nortel VPN Router 2750 platform.
Q01580009	Multimedia Client does not work for multiple clients over BOT/NAT with port mapping NAT on the Nortel VPN Router.
Q01582318	Additional logging requirements are added to the Nortel VPN Router to pass ICSA IPSec 1.0D testing.

Table 1 Issues fixed for V7.05.300.

CR number	Description
Q01584141	The Nortel VPN Router Initial Contact Message does not work as expected in ICSA Lab environment.
Q01585474	The Nortel VPN Router may core during IP phone use with TCP fragmentation enabled.
Q01587291	OSPF Adjacency drops in 6.05.140 on the Nortel VPN Router.
Q01588320	The Nortel VPN Router may core when two telnet sessions are established simultaneously.
Q01588523	LAN utilization statistics may be incorrect on the Nortel VPN Router.
Q01588979	The ROUTING VRRP configuration screen may show errors after LDAP stops or starts on the Nortel VPN Router.
Q01592255	The PCAP utility may not be accessible to manage users who are not administrators on the Nortel VPN Router.
Q01592714	Nortel VPN Router primary administrator password change does not generate any log messages.
Q01595733	The Nortel VPN Router may not preserve the configuration of a V.35 PCI card after it is replaced with a newer revision of the module.
Q01596270	Upgrading the Nortel VPN Router may result in cores when a large number of Tunnel Guard sessions disconnect.
Q01597911	In V06_05.140, the Nortel VPN Router OSPF LSA max age increments faster than it should.
Q01602630	The Nortel VPN Router BGP peer up-time may not be accurate after an upgrade to V07_00.062.
Q01613867	The "No response from client - logging out" message no longer appears in the System Log on the Nortel VPN Router.
Q01616048	Port NAT is not aged out of the NAT table if the source port is not mapped to the original port on the Nortel VPN Router.
Q01616289	The Nortel VPN Router may core when a large number of Tunnel Guard sessions terminate due to a socket error.
Q01617010	Multiple viewing of a large system log may hang HTTP on the Nortel VPN Router.
Q01618871	Auto backup does not delete log files on the Nortel VPN Router.
Q01619835-01	One is unable to access LAN0 after upgrading from saved config version 05_05. Applying a config file saved in V05_05 to a Contivity running V06_05 may leave LAN0 inaccessible.
Q01637372	CSU Loop Back recognition fails on the Nortel VPN Router.
Q01637538	The Nortel VPN Router may core if the IP Tunnel MIB is enabled.

Table 1 Issues fixed for V7.05.300.

CR number	Description
Q01639270	After a reboot of the Nortel VPN Router, all of the VPN Client tunnels may not connect properly.
Q01641163	The Nortel VPN Router may core while attempting to remove an aged next hop for a route which may have several potential new next hops to choose from.
Q01641580	The Nortel VPN Router may lose memory when the Hardware Accelerator statistics or status is queried.
Q01648941	The Nortel VPN Router 1100 show command may fail while displaying the information for a T1 CSU/DSU module.
Q01649116	Multiple Nortel VPN Router branch office sessions are created when responding to a single request from a Netscreen device.
Q01651667 Q01678906	Memory leak—the Nortel VPN Router may lose memory during RADIUS Authentication attempts.
Q01655695	The Nortel VPN Router may core when it looks at the details of the server certificate.
Q01663543	Nortel VPN Router 5000 may core when it accesses the Tunnel Guard client table for a user who disconnects due to a socket error.
Q01666914	The Nortel VPN Router log may contain "AddAttributeValue LDAP inconsistent - entry does not exist" messages when a RADIUS authentication attempt times out.
Q01675264	The Clear DF bit option does not work with Nortel VPN Router interface as it filters over HSSI interfaces.
Q01679839	The LDAP proxy authentication mode with digital certificates may not function properly on the Nortel VPN Router.
Q01684390	The Nortel VPN Router may core when it changes ECMP max path.
Q01687725	There may be a parser exception when Nortel VPN Router Tunnel Guard rule definitions are saved using Internet Explorer 6/Java 1.6.0.
Q01692038	The Nortel VPN Router CPU gets stuck at 100% when doing an auto backup with SFTP.
Q01693084	The Nortel VPN Router 1740 IKE setting for 128-bit AES group 2 is not available in v7.0.
Q01724507	The Nortel VPN Router RADIUS Accounting secret is not translated correctly when LDAP 3DES is enabled.
Q01726732	SFTP auto backup on the Nortel VPN Router no longer works after the SSH server bounces.
Q01726945	The Nortel VPN Router stays in a reboot loop if the DNS for the BOOT remote peer is the IP address of the static BOOT peer.

Version 7.05.300 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.

Q01717623—RADIUS authentication servers not working

A RADIUS authentication server's "status" blanks and the server does not work if /Base group level RADIUS parameters are configured prior to configuring a RADIUS authentication server.

If you upgrade with a preconfigured, working RADIUS authentication setup, you will not encounter this issue. Not all users who configure or add new RADIUS authentication server configurations experience this problem; it occurs only if specific sequences of steps are used to configure RADIUS authentication servers.

The problem occurs when RADIUS /Base group configuration parameters are added before general RADIUS authentication servers are added. The steps that lead to this scenario are:

1. Go to Profiles > Groups > Base edit > IPsec. Set a group IP address and Password, and select User name and Password. Click OK.
2. Go to Servers > Radius auth. Configure the external RADIUS server (IP and Password).

If these steps are followed, then the RADIUS authentication server status field is empty, and RADIUS authentication servers do not function correctly.

If this situation occurs, the workaround is:

1. Create a new dummy user group.
2. On the server's RADIUS Auth dialog box, toggle the "RADIUS Users Obtain Default Settings from the Group" to the new dummy user group.
3. Click OK.
4. Change the "RADIUS Users Obtain Default Settings from the Group" back to the original group.
5. Click OK.

After these steps are followed, the RADIUS authentication servers show the correct status and work correctly.

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.

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.

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.

Q01522262—Cannot make SSH connection after eight invalid attempts

If a user attempts more than eight 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 upgrade considerations

The following sections contain upgrade considerations for this product.

- VPN Router 1010, 1050, and 1100 require a 64 MB flash disk.
- Version 7.0x 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 7.0x.
- 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 7.0x 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.

VPN Router recommendations

Nortel recommends that you:

- Use the automatic backup feature 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.

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. 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 the CLI, enter the following command:

  ```
  # 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 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.

Viewing and calculating memory usage

The minimum memory requirement for Version 7.0x 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

Select Security & VPN, VPN Router 1750, and in the Documentation section, select Show All. Click the link called Nortel Networks Contivity Memory Calculator.

The parameters affecting 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

The minimum VPN Client version that is supported by Version 7.0x is 5.01.

Table 2 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, 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							
	4.76	4.80	4.90	5.00	6.00	6.05.140	7.00	7.05.300
1010	X	X	X	X	X	X	X	X
1050	X	X	X	X	X	X	X	X
1100	X	X	X	X	X	X	X	X
600	X	X	X	X	X	X	X	X
1500								
1510								
1600	X	X	X	X	X	X	X	X
1700	X	X	X	X	X	X	X	X
1740		X	X	X	X	X	X	X
1750					X	X	X	X
2000								
2500								
2600	X	X	X	X	X	X	X	X
2700	X	X	X	X	X	X	X	X
2750						X	X	X
4000								
4500	X	X	X	X				

Table 2 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**	**7.05.300**
4600	X	X	X	X	X	X	X	X
5000	X	X	X	X	X	X	X	X
5000E						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 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 7.0x.
- 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, 6.0, or 7.0, and Netscape 4.79 or 6.2 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.
- 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 3 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
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 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.