Version 6.05.140

Part No. NN46110-403
315000-P Rev 02
December 2006

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Release Notes

NORTEL

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

America Online and AOL are trademarks of America Online, Inc.

iPlanet, Java, and Sun Microsystems are trademarks of Sun Microsystems.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Netscape, Netscape Communicator, Netscape Directory Server, and Netscape Navigator are trademarks of Netscape Communications Corporation.

Steel-Belted Radius is a trademark of Funk Software, Inc.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

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

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

Statement of conditions

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

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

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

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

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

Nortel Networks software license agreement

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

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

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

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

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

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface 7

Before you begin 7
Text conventions 7
Related publications 9
Printed technical manuals 10
How to get help 11
Finding the latest updates on the Nortel Web site 11
Getting help from the Nortel Web site 11
Getting help over the phone from a Nortel Solutions Center 12
Getting help from a specialist by using an Express Routing Code 12
Getting help through a Nortel distributor or reseller 12

Chapter 1
Overview 13

Version 6.05.140 features summary 13
New hardware features 13
VPN Router 2750 14
VPN Router 5000E 15
New software features 16
Integrated Services Digital Network 17
Lightweight Directory Access Protocol 19
Certificate Revocation List 25
Restricted product—export license requirement 28

Chapter 2
Considerations and issues 29

Customer issues fixed in this release 29
Version 6.05.140 product considerations 32

Version 6.05.140 known anomalies 34
Demand Services 34
Q01141767—If Demand is enabled for the first time from CLI, an error message appears 34
Multinetting 34
Q01191923—TCP MSS options not configurable under secondary multinet interfaces 34
Q01193299—CLI mode permits adding of multiple secondary IP addresses from the same network 34
Others 35
Q01128397—Ping to validate default route: static route not installed 35
Q01167469—Errors and incorrect messages in event log after Reboot 35
Q01190797—Applet for configuring Firewall and NAT policies does not work with Opera browser 35
Q01191261—Netdirect subnet error log on NVR is incorrect 36
Q01201847—OSPF Announce access-lists do not work in some cases 36
Documentation change 36

Preface

These release notes contain the latest information about the Nortel VPN Router 6.05.140. The Nortel VPN Router is formerly known as the Nortel Contivity Secure IP Services Gateway. These release notes also refer to the Nortel VPN Client, formerly known as the Contivity VPN Client.

Before you begin

These release notes are intended for network managers who are responsible for the VPN Router. The release notes assume that you have experience with windowing systems or graphical user interfaces (GUI) 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, formerly known as the Contivity Secure IP Services Gateway, 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 work arounds.
- *Nortel VPN Router Configuration — Basic Features* introduces the product and provides information about initial setup and configuration.
- *Nortel VPN Router Configuration — SSL VPN Services* 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* provides instructions for configuring authentication services and digital certificates.
- *Nortel VPN Router Security — Firewalls, Filters, NAT, and QoS* provides instructions for configuring the Nortel VPN Router Stateful Firewall and Nortel VPN Router interface and tunnel filters.
- *Nortel VPN Router Configuration — Advanced Features* 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* provides configuration information for the tunneling protocols IPsec, L2TP, PPTP, and L2F.
- *Nortel VPN Router Configuration — Routing* 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* 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* provides syntax, descriptions, and examples for the commands that you can use from the command line interface.

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

Printed 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 the VPN Router 2750, click one of the following links:

Link to	Takes you directly to the
Latest software	Nortel page for the **VPN Router** 2750 software located at: www130.nortelnetworks.com/go/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=17381
Latest documentation	Nortel page for the **VPN Router 2750** documentation located at: www130.nortelnetworks.com/go/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=17381

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 6.05.140. Version 6.05.140 is a software maintenance release to Version 6.00.310. These release notes support the first release of the VPN Router Model 2750 and the VPN Router 5000E. Also, these release notes address customer-found software issues.

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

Version 6.05.140 features summary

Version 6.05.140 of the VPN Router supports the following new features:

- "New hardware features" on page 13
- "New software features" on page 16

New hardware features

Version 6.05.140 of the VPN Router supports the following new hardware features:

- "VPN Router 2750" on page 14
- "VPN Router 5000E" on page 15

VPN Router 2750

The VPN Router 2750 is the 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 Restriction of Use of Certain Hazardous Substances (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 on page 16 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 CES 5000 350W Spare Power Supply **Note:** Identified by a label on the power supply as: DPS-350	**VPN Router 5000** • DM1401117 CES 5000 128BIT LAN & GIG ENET • DM1401118 CES 5000 56BIT LAN, GIG, ENCRYPT ACCL • DM1401153 CES 5000 128BIT LAN, CSA • DM1401154 CES 5000 56BIT LAN, CSA • DM0011091 CES 5000 128 BIT CHASSIS SPARE • DM0011092 CES 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 6.05.140 of the VPN Router supports the following new software features:

- "Integrated Services Digital Network" on page 17
- "Lightweight Directory Access Protocol" on page 19
- "Certificate Revocation List" on page 25

To configure all of the following software features with the command line interface (CLI), use the VPN Router in Global Configuration mode. To set the Global Configuration mode, see *Nortel VPN Router Using the Command Line Interface*.

Integrated Services Digital Network

This section about the Integrated Services Digital Network (ISDN) discusses "ISDN Terminal Endpoint Identifier processing" on page 17.

Note: 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 12.

ISDN Terminal Endpoint Identifier processing

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.

Configuring the calls per TEI with the GUI

To configure the calls per TEI:

1. From the **Navigational** menu, select **SYSTEM**.

   The SYSTEM menu appears.

2. From the **SYSTEM** menu, select **DIAL INTERFACE**.

   The DIAL INTERFACE window appears.

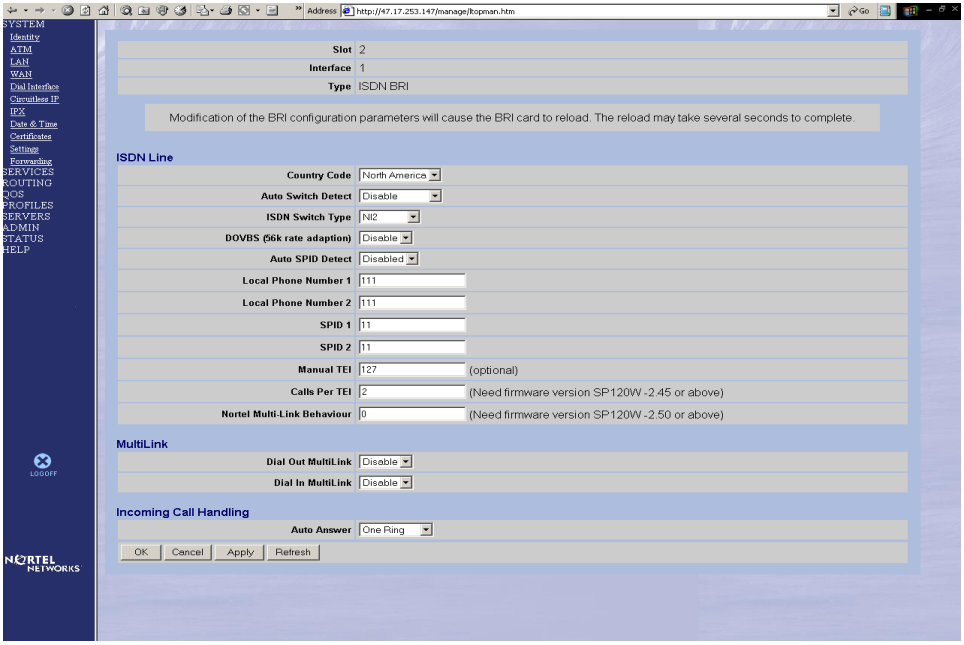
3. In the **DIAL INTERFACE** window, select the **ISDN BRI** type interface.
4. Click **OK**.

   The ISDN BRI interface window appears.

5. From the **ISDN BRI Interface** window, click **Configure BRI**.

   The Configure BRI window appears (Figure 1).

Figure 1 Configure BRI window



6 In the **Calls per TEI** box, type **1** to permit only one bearer call per TEI or type **2** to permit two bearer calls on a single TEI. Two bearer calls per TEI is the default.

Configuring the calls per TEI with the CLI

To configure the calls per TEI, use the following command:

```
interfaces bri isdn calls-per-tei <1|2>
```

where:

- 1 permits only one bearer call per TEI.
- 2 permits two bearer calls on a single TEI. This is the default value.

Lightweight Directory Access Protocol

This section about the Lightweight Directory Access Protocol (LDAP) discusses the following topics:

- "LDAP 3DES password encryption" on page 19
- "LDAP user configurable encryption key" on page 21
- "LDAP optimization scheduling" on page 23

LDAP 3DES password encryption

The administrator of the Nortel VPN Router can use this option to secure user and application passwords with Triple Data Encryption Standard (3DES) encryption, which is a more secure algorithm than the current DES. In a world where system security is the highest of priorities for businesses, the administrator must keep the encryption used to secure these systems up to date.

If you use an external LDAP, you must upgrade all VPN Routers in the network to 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. If you attempt to log on to a system not running 6_05.140 with an LDAP that was converted from DES to 3DES, you get a password failure.

When you enable 3DES encryption, 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).

Caution: Nortel recommends that you back up your LDAP and Config before you enable this feature.

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

Enabling LDAP 3DES password encryption with the GUI

To enable LDAP 3DES password encryption:

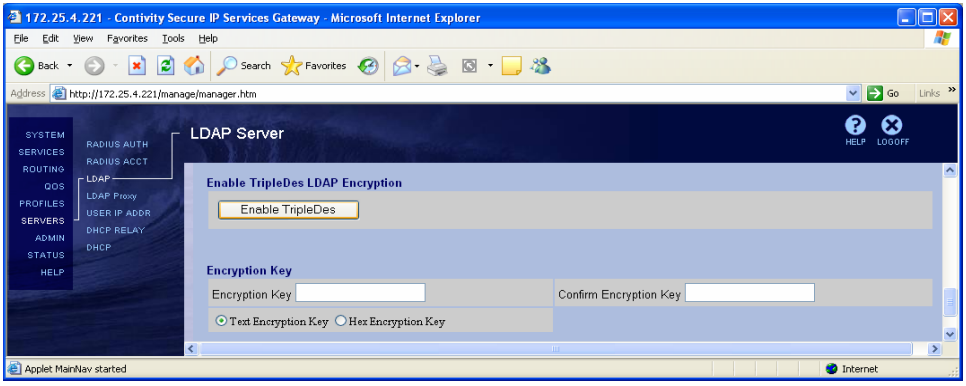
1. From the **Navigation** menu, choose **SERVERS.**

   The Servers menu appears.

2. From the **Servers** menu, choose **LDAP.**

   The LDAP Servers window appears (Figure 2).

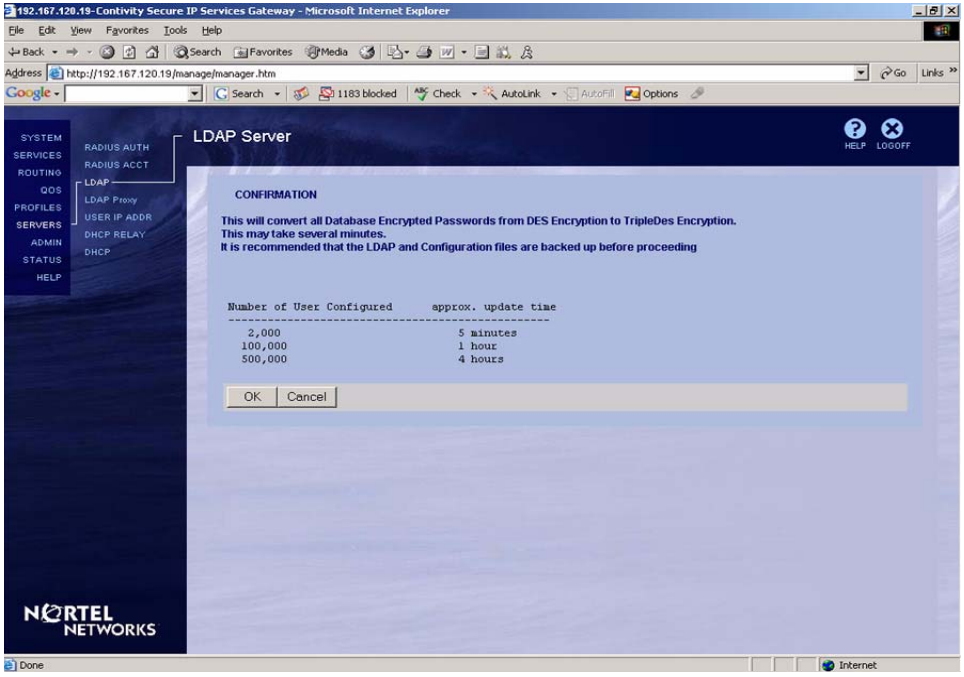
Figure 2 LDAP Server window



3. Click **Enable TripleDes**.

   The confirmation window appears (Figure 3).

Figure 3 Confirmation window



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

Enabling LDAP 3DES password encryption with the CLI

To enable LDAP 3DES password encryption, use the following command:

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

LDAP user configurable encryption key

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

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

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

Configuring the hash key with the GUI

To configure the LDAP user configurable hash key:

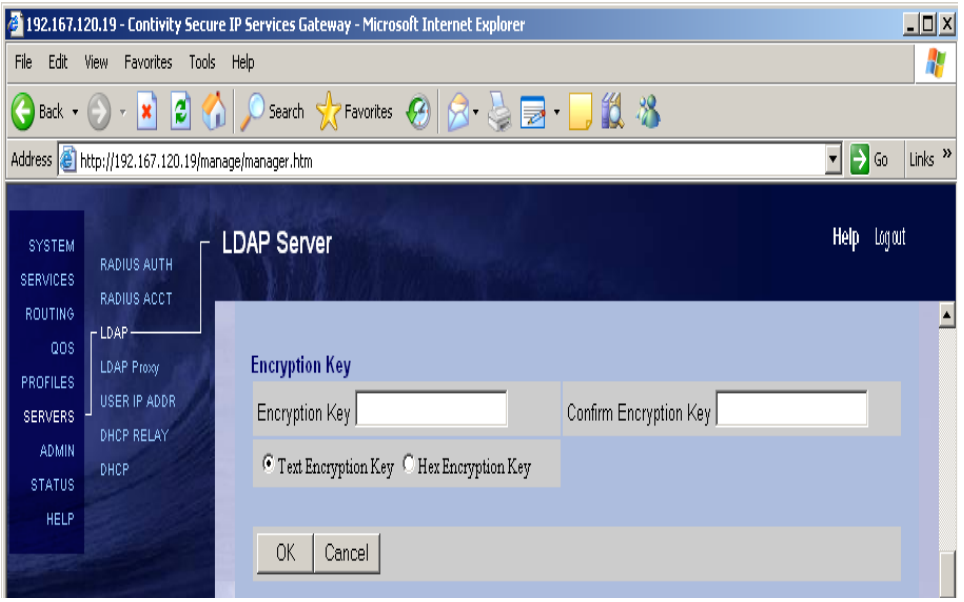
1 From the **Navigation** menu, choose **SERVERS**.

The SERVERS menu appears.

2 From the **Servers** menu, choose **LDAP**.

The LDAP Server window appears (Figure 4).

Figure 4 LDAP Server window



3 From the **Encryption Key** options, select **Text Encryption Key** or **Hex Encryption Key**.

4 In the **Encryption Key** box, type the desired encryption key.

5 In the **Confirm Encryption Key** box, retype the desired encryption key.

6 Click **OK**.

Configuring the LDAP hash key with the CLI

To configure the LDAP user configurable text hash key, use the following command:

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

where:
password is an eight-byte character string.

To configure the LDAP user configurable hex hash key, use the following command:

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

where:
password is a 16-byte hexadecimal value.

LDAP optimization scheduling

With this option, the administrator of the Nortel VPN Router can configure the time and day that the LDAP database is optimized.

LDAP optimization frees all unused memory blocks and deletes any deleted LDAP data structures, which makes the LDAP database lookups faster and more efficient. The optimization process has disadvantages because it is run at the LDAP priority and is very CPU intensive. In environments with heavy volume traffic and very large LDAP databases, the optimization process can cause timeouts and data drops. The administrator can use this option to schedule these events.

You can use the GUI or the CLI to configure LDAP Optimization Scheduling.

Configuring LDAP Optimization Scheduling with the GUI

To configure LDAP Optimization Scheduling:

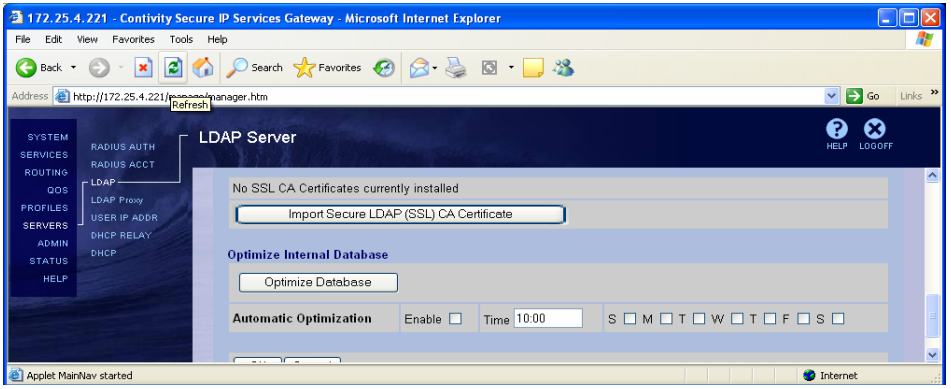
1. From the **VPN Router** menu, choose **SERVERS.**

   The SERVERS menu appears.

2 From the **SERVERS** menu, choose **LDAP**.

The LDAP Server window appears (Figure 5).

Figure 5 LDAP Server window



3 Select the **Automatic Optimization Enable** box.

4 In the **Automatic Optimization Time** box, type the desired time.

5 In the **Automatic Optimization Days of the week** options, select the desired days.

Enabling LDAP Optimization Scheduling with the CLI

To enable LDAP Optimization Scheduling, use the following command:

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

To disable LDAP Optimization Scheduling, use the following command:

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

To enable LDAP Optimization Scheduling everyday at a specific time, use the following command:

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

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

To disable LDAP Optimization Scheduling everyday at a specific time, use the following command:

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

To enable LDAP Optimization Scheduling on specific days of the week at a specific time, use the following command

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

where:

- *days of the week* are the specific days for enabling LDAP Optimization Scheduling.
- *hh:mm* is the hour (00–24) and the minutes of the specific time.

To disable LDAP Optimization Scheduling on specific days of the week, use the following command:

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

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

Certificate Revocation List

This section about the Certificate Revocation List (CRL) discusses "CRL Update Specific Time" on page 25.

CRL Update Specific Time

With this option, the administrator of the Nortel VPN Router 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.

You can use the GUI or the CLI to configure CRL Retrieval Scheduling.

Configuring CRL Retrieval Scheduling with the GUI

To configure CRL retrieval scheduling:

1. From the **VPN Router** menu, choose **SYSTEM** .

   The SYSTEM menu appears.

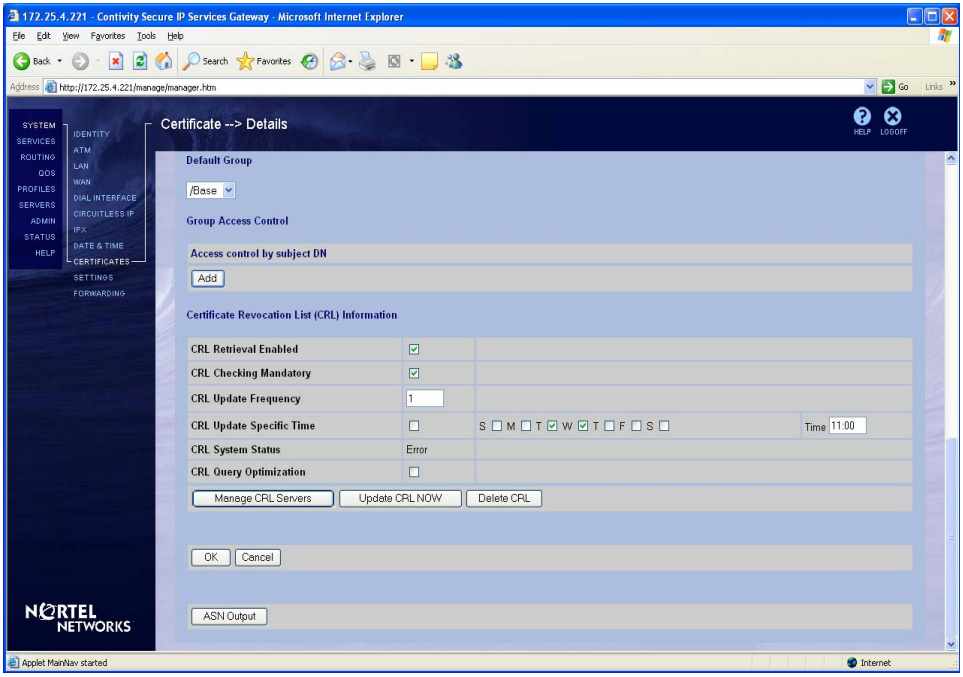
2. From the **SYSTEM** menu, choose **Certificates**.

   The Certificates window appears.

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

   The Certificate Details window appears (Figure 6).

Figure 6 Certificate Details



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

6 In the **Time** box, type the desired time.

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

8 Click **OK**.

Configuring the CRL Update Specific Time with the CLI

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

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

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

This command has the following options:

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

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

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

This command has the following options:

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

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

```
crl update now
```

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 64 bits can be eligible for international shipment pursuant to a license exception. However, any product that incorporates encryption technology exceeding 64 bits requires 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 general considerations for this product.

Customer issues fixed in this release

Table 2 lists customer issues from previous releases that are fixed in the V6.05.140 release.

Table 2 V6.05.140 release

CR number	Description
Q01044305_01	The Nortel VPN Router discarded non-standard FTP packets when NAT was applied to Branch Office Tunnels.
Q01044727-01	The RADIUS Diagnostic Report on the Nortel VPN Router may show erroneous configuration errors when the group setting in Profiles->Groups->Base->IPSEC is configured for Group Level Radius.
Q01079892-01	The Nortel VPN Router cores when a task a Radius Server is contacted at the same time as the Radius Server is deleted.
Q01127098-01	The Nortel VPN Router lacks a CLI command that could disconnect a specific session for a particular user.
Q01221722	The Nortel VPN Router may core when viewing the Event Log because of special characters displayed in Event Log.
Q01231980-01	When multiple Frame Relay Virtual Circuits were configured on a Nortel VPN Router, the ifSpeed MIB value displayed the same value for all the Virtual Circuits.
Q01243188	The Nortel VPN Router may return an incorrect next-hop value when performing Traceroute from the VPN client.
Q01257496-01	The Nortel VPN Router may attempt to connect to a certificate server on the private interface even if CMP is disabled on the interface.
Q01263131	The Nortel Router fails to send RIP updates on the Primary Branch Office Tunnel after BIS rediscovery occurs.

Table 2 V6.05.140 release

CR number	Description
Q01272710-02	The OSPF LSDB on the Nortel VPN Router may not be correctly updated after an area range is removed.
Q01278185-01	The Call Admission Priority for Groups on the Nortel VPN Router will function even though 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” did not recover if the Dial on Demand interface started or stopped too fast.
Q01284522-01	The IpForwardTable on the Nortel VPN Router 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 cannot be configured via CLI.
Q01312474-01	The VPN Router built-in DHCP server does not reply to requests if the User Class option is specified by the client but not recognized by the server.
Q01324536	The Nortel VPN Router 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 permits the upgrade to a FIPS compatible version that does not contain the desmac.dat file. This may result in a continuous crash.
Q01344462	Nortel VPN Router may core within TunnelGuard after a connection error occurs connecting to the PC Agent.
Q01354195-01	The Nortel VPN Router timers act erratically after 414 days from the last reset because of the timers' representation limitation.
Q01355028	When a port of the Quad T1 interface card receives a Blue Alarm Indication (or AIS), the Nortel VPN system may demonstrate high CPU Utilization, even after traffic destined for the affected port ceases or the link is disconnected.
Q01366666-02	The Nortel VPN Route may core when referencing the routing table after an interface goes down.
Q01367218	The Nortel VPN Router 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 does not download when the next user attempts to login. This occurs 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 unreachable.

Table 2 V6.05.140 release

CR number	Description
Q01369393	When using a NAT rule to translate an internal address to the "Public Interface" address, the Nortel VPN Router will not translate the source address if the ultimate destination of the connection is another internal address.
Q01370768	The Re-key Timeout on the Nortel VPN Router cannot be disabled by entering the value 00:00:00 as specified in the documentation.
Q01371631	After a reboot on a Nortel VPN Router, the HTTP sessions would stop responding after the first attempt to manage the SSL VPN card. This occurred when the Stateful Firewall and Enforce TCP Conversation Rules were enabled.
Q01373095	The Nortel VPN Router may display an error when either the default or the maximum lease time for DHCP is configured. This occurs when the value for these parameters is set to infinite.
Q01374435-01	The Nortel VPN Router may experience 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 may still boot from the named config file.
Q01388055-01	The Nortel VPN router reports an incorrect source address in ICMP unreachable packets.
Q01389415-01	An external DHCP sever cannot be configured through the GUI on the Nortel VPN Router.
Q01392155	The PPP implementation for the Nortel VPN Router allowed PPP interfaces to have endpoint IP addresses that were from a different subnet. When such a situation was encountered, a configuration warning was posted on the Event Log and the subnet mask for the local endpoint was changed to 255.255.255.255.
Q01394814-01	The Nortel VPN Router may fragment large uncompressed packets by IP after encryption.
Q01395708	The Nortel VPN Router may experience 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 displayed for the CLIP interface even when CLIP is not configured on the router. This may result in problems with management software due to the possible duplication of MAC addresses.
Q01403240-01	The Nortel VPN Router may lock up when using the Hardware Accelerator and throughput is higher that normal.
Q01406461	The display format of the SNMP Link UP and Link Down traps was not the same, which made it difficult to monitor those traps on a standard tool.

Table 2 V6.05.140 release

CR number	Description
Q01407495	The Nortel VPN Router did not display the learned IP address when dynamic PPPoE was set for the public interface.
Q01414706-01	During log on the Nortel VPN Router, the user attempted to log on three times before gaining access when using Entrust certificates with CDP authentication.
Q01415415	During interface configuration, the Nortel VPN Router cored when the Multi-Field Classifier was enabled or disabled.
Q01418676	On the Nortel VPN Router, when no Egress Multi-Field Classifier was configured, the show qos interfaces command displayed "Ingress (Inbound) Multi-Field Classifier: None" instead of "Egress (Outbound) Multi-Field Classifier: None."
Q01422229-01	The Nortel VPN router cored after performing an LDAP search.

Version 6.05.140 product considerations

Nortel no longer supports Axent defender. It has been removed from the management GUI.

If a STUN client and server are used to determine the type and capabilities of local NAT, the reported type can be incorrect when Branch Office NAT is used.

Multinet addresses are not supported as Initiators in ABOT’s definitions.

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 you are upgrading from Version 5.05 to Version 6.00, you must disable the demand interface before upgrading to the 6.00 version. Once the upgrade is completed, change the Ping source to IP, add the interface IP, and then enable the demand interface. A straight upgrade results in the backup connecting right away.

If the BGP local preference is set to 0, no remote routes are accepted into the BGProuting table 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.

Version 6.05.140 known anomalies

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

Demand Services

Q01141767—If Demand is enabled for the first time from CLI, an error message appears

When Demand is enabled for the first time from the CLI, an error message appears. Despite this error, Demand is enabled on the VPN Router (NVR) box.

Multinetting

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.

Q01193299—CLI mode permits adding of multiple secondary IP addresses from the same network

When you use the GUI to add more than one multinet IP from the same network, you get the error message: Error creating new record; IP address conflicts with:. However, from the CLI, you can add multiple secondary IP addresses from the same network without getting an error message.

Others

Q01128397—Ping to validate default route: static route not installed

When you use the feature Ping to Validate Default Route and the ping address is not on the local LAN, a static route is added to reach the destination. This works when creating the default route, ping destination. However, when the device is rebooted, an attempt is made to add the static route before the interface is up. The attempt fails and after several retries, the DUT stops trying to add the route. The interface then finishes coming up and the static routes are never installed. Since there is no route to the ping default route destination address, the ping fails and the default route is disabled. The workaround is bounce Ping to Validate Default Route.

Q01167469—Errors and incorrect messages in event log after Reboot

Incorrect messages are found in the event log when a newly installed NVR is rebooted. Some of these messages are marked as errors.

Q01190797—Applet for configuring Firewall and NAT policies does not work with Opera browser

The applet for NAT and Firewall policies configuration no longer works with Opera browser. A custom Event Queue replaces the SystemEventQueue of the Java Virtual Machine (JVM). Opera is written in Java and uses its own instance of JVM. When Opera tries to open an applet, it uses the browser JVM for the applet, not a different instance. The function getSystemEventQueue from the Java API returns the SystemEventQueue if no security policy is defined, or if a security policy that allows the execution of the function is defined. Opera has a security policy that does not permit the above mentioned function to return the SystemEventQueue.

To permit the function to return the SystemEventQueue, you must 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"

Q01191261—Netdirect subnet error log on NVR is incorrect

The VPN Router event log says "SSL-VPN netdirect address (33.33.33.33) must be in the 192.32.18.0 space," but that statement is incorrect. The 33.33.33.33 is the front-end interface and should not be in the same subnet as the back-end interface.

Q01201847—OSPF Announce access-lists do not work in some cases

There are scenarios when routes are advertised even though an access-list was created to block that range. However, if the access-list is applied globally (on all interfaces), the behavior is normal. The access-list also works correctly if the BO tunnel is disabled and the OSPF is bounced globally, or if the access-list is disabled and enabled again.

Documentation change

The documentation for Software Release 6.0 is missing the following information about the FTP server passive mode parameter:

There is a new checkbox called FTP server passive mode found under System > Settings > Switch Settings.

When you enable the FTP server passive mode, you allow passive FTP connections to connect to the unit, to perform directory listings, and to upload and download files. Without this checkbox enabled, if you use passive FTP connections, you can connect to the unit, but you cannot perform directory listings, or upload and download files.