Version 4.70

Part No. 315000-B Rev 00
February 2003

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Secure IP Services Gateway Release Notes

NORTEL NETWORKS™

Copyright © 2002 Nortel Networks

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

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

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, Bay Networks, Contivity, and Preside 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, Inc.

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 Inc. software license agreement

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

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

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

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

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

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

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

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

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

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

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

Contents

Preface

These release notes contain the latest information about the Nortel Networks* Contivity* Secure IP Services Gateway Version 4.70.

Before you begin

These release notes are intended for network managers who are responsible for the Contivity Secure IP Services Gateway. 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 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 workarounds.
- Configuring Basic Features for the Contivity Secure IP Services Gateway introduces the product and provides information about initial setup and configuration.
- Configuring Authentication and Certificates for the Contivity Secure IP Services Gateway provides instructions for configuring authentication services and digital certificates.
- Configuring Firewalls and Filters for the Contivity Secure IP Services Gateway provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- Configuring Tunneling Protocols and Advanced WAN Settings for the Contivity Secure IP Services Gateway provides instructions for configuring the tunneling protocols IPsec, L2TP, PPTP, and L2F, as well as instructions for configuring PPP, frame relay, PPPoE, and advanced WAN settings.
- Configuring Routing for the Contivity Secure IP Services Gateway provides instructions for configuring RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Managing and Troubleshooting the Contivity Secure IP Services Gateway* provides information about system administrator tasks such as backup and recovery, file management, and upgrading software, and instructions for monitoring gateway status and performance. Also, provides troubleshooting information and interoperability considerations.
- *Reference for the Contivity Secure IP Services Gateway Command Line Interface* provides syntax, descriptions, and examples for the commands that you can use from the command line interface.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. 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* Acrobat 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 the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

You can purchase printed books and documentation sets from Vervante. To order printed documentation, go to Vervante at the www.vervante.com/nortel URL.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
Overview

The Contivity Secure IP Services Gateway Version 4.70 release includes bug fixes and new features added since the release of the Contivity Secure IP Services Gateway Version 4.50. These release notes contain the latest information about the Contivity Secure IP Services Gateway. Version 4.70 incorporates all changes made in V04.06.130, V04.07.021, and V04.50.376. Later versions, such as V04.55, are not included in this release. Version 4.70 supports upgrades from Versions 4.50, 4.07, and 4.06. If you are running an older version, you need to upgrade to a supported version before you upgrade to Version 4.70.

Refer to your Contivity hardware installation guide for instructions on getting your gateway up and running. After you configure an IP address, a subnet mask, and a gateway address (if applicable), you can view online Help from the management interface.

Version 4.70 new features

This section highlights the new Contivity Secure IP Services Gateway features that are supported in Version 4.70. For additional information, refer to the documentation set or the online Help.

- WAN as private interface
  - — Allows the gateway to make a clear text (non-tunneled) connection over a WAN interface
  - — Used only within secure or trusted networks
  - — Uses Layer 2 protocols: point-to-point protocol (PPP) and frame relay
  - — Supports Layer 3 routing: static routing, RIP, and OSPF
  - — Routing functionality is the same as for LAN interfaces
  - — The firewall functions over private WAN interfaces

  - — The Contivity Stateful Firewall must be turned on and the interface filter must be activated for routing to function over WAN interfaces
  - — VRRP mastership can only be configured on LAN interfaces, not private WAN interfaces; however, a private WAN interface can be added to an interface group for VRRP critical interface fail-over
- Frame relay
  - — Switched Layer 2 data transport “fast packet” service
  - — Contivity gateway functions as frame relay DTE or FRAD
  - — Contivity implementation supports PVCs only, not SVCs
  - — Allows the Contivity device to act as a gateway between a newer VPN or public tunneled network and an existing frame relay network
- Contivity 1700 and 2700 support
- Licensing enhancements
  - — Contivity 1700 and 2700 available with low cost router (five VPN tunnel) base unit options
  - — VPN tunnel licensing upgrade options for the Contivity 1000 (up to 30 tunnels), 1700 (up to 500 tunnels), and 2700 (up to 2000 tunnels)
  - — Contivity 600 now supports up to 50 tunnels (no upgrade options available)
- Features from Contivity 1010/1050/1100 release

Nortel Networks CD

The Nortel Networks CD contains all the software files you need to configure and manage your Contivity gateway. The directories on the CD are described in the following sections.

The directory named V04_70.119 contains the Nortel Networks Contivity Secure IP Services Gateway software. You would use this directory to upgrade your gateway from an older version of the product.

Doc (Documentation) directory

The doc directory contains the documentation set for the Contivity Secure IP Services Gateway. These guides are provided in Adobe Acrobat PDF format. The documentation set provides configuration, monitoring, administration, and troubleshooting information.

The documentation directory also contains the management information base (MIB) files.

LDAP (Netscape) directory

The LDAP directory contains the Netscape Directory Server* 4.5 software (d45diu.zip for the domestic kit and d45eiu.zip for the international kit). To install the software, unzip the .zip file and click on Setup.exe.

Tools directory

The tools directory contains the Nortel Networks IP Address Configuration Utility.

The Ie5 subdirectory contains the ixtNetIP.exe file, which is for Microsoft* Internet Explorer, Version 5.5. This file starts the Internet Explorer installation procedure, then links to the Microsoft Web site to download the full Internet Explorer Version 5.5 software. Therefore, you must have Internet access when you run this setup program in order to complete the Internet Explorer installation. You can install this browser or use a different browser of your choice.

The Java* subdirectory contains the installation files for the Sun Microsystems* Java Runtime Environment (JRE) Version 1.3.0. This application is needed to load the Policy Manager configuration utility. The JRE should automatically be installed when these Java applets are first accessed; however, the installation files are included on this CD to allow for manual installation.

Restricted product - export license requirement

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

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

Pursuant to such license, the product can be marketed and sold only to a limited class of international users. Any entity, other than Nortel Networks, 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 describe issues and considerations that apply to the Version 4.70 release of the Contivity Secure IP Services Gateway.

Fixed in this release

Table 1 lists customer issues from previous releases that are fixed in this release.

Table 1 Fixed issues

Q00552796	IPSec branch office and PPTP nested tunnels terminate on same Contivity box.
Q00533241	MLPPP option needed on Contivity 1100.
Q00527721-01	Groups and users lost after loading CLI script and then power OFF/ON.
Q00524162	Dashes not accepted in DHCP domain name attribute.
Q00516186	CLI not showing proper information for PPPoE.
Q00498165	Set password length to 32 characters or more for IPSec user tunnels.
Q00494324-02	IPX does not work properly after upgrade.
Q00486667	Unable to change or edit DHCP server option 3 (router).
Q00475362-02	Auto Backup fails with unable to change directory.
Q00456996	GUI Quick Start: Static address overwritten if there is a DHCP server.
Q00435996	Changes to default filters on public side.
Q00432781-01	Corrupted npbuf causes crash.
Q00431557	Quick Start does not work when ISP is not using DHCP.
Q00102956-02	Added source address for traceroute tool in GUI and CLI.
Q00094136-04	Authentication fails when removing delimiter in the LDAP.

Product considerations

The following sections discuss product considerations or limitations.

Number of versions

Nortel Networks recommends that you maintain no more than two versions of the software on your gateways in addition to the version that is currently running.

Support considerations

- This release incorporates all changes made in V04.06.130, V04.07.021, and V04.50.376. Later versions, such as V04.55, are not included in this release.
- Version 4.70 supports upgrades from Versions 4.50, 4.07 and 4.06. If you are running an older version, you need to upgrade to a supported version before you upgrade to Version 4.70.
- The minimum memory requirement is 128 MB.
- The Contivity 1500, 2000, 2500, and 4000 hardware platforms are not supported for V4.70 and subsequent releases.
- Version 4.07 software provides support only for the Contivity 1010/1050/ 1100 series. Version 4.70 will also support this series.
- Version 4.06_120 and subsequent releases provide support for the Contivity 1700 and 2700.
- Versions 3.50, 3.60, 4.0, 4.50 and 4.70 do not work on the Contivity 1000.
- Shasta Server Farm is not supported by Version 4.70.
- A T1 interface does not support packets larger than 47 KB.

Asynchronous branch office tunnel with nailed-up option enabled

If a nailed-up asynchronous branch office tunnel initiator tunnel is configured, a tunnel disconnects after three minutes the first time it connects. Because the tunnel is nailed-up the connection is automatically be re-established.

Branch office support for state and cost

You can share state and cost in Branch Office→Accessible Network→Remote Endpoint with previous versions through LDAP. Nortel Networks recommends that you do not share an external LDAP server between different versions of the Contivity Secure IP Services Gateway.

NAT traversal port numbers

Nortel Networks strongly recommends that you use port 10001 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.

Recovery floppy diskette

Any recovery floppy diskette that you created prior to release Version 4.0 will not work on a system that runs Version 4.0, 4.5 or 4.70 software. Nortel Networks recommends that when you upgrade to Version 4.0, 4.50 or 4.70 software, you create a recovery floppy diskette as soon as you complete the upgrade. This version of the recovery floppy diskette works on systems running any release up to and including Version 4.50. You must use a formatted diskette when creating the recovery diskette.

Downgrading from previous versions

You must disable the Contivity Stateful Firewall before you downgrade to any version prior to Version 3.50 of the Contivity Secure IP Services Gateway. If you fail to disable the firewall, you may encounter unexpected results when you reboot for the downgrade.

RADIUS-supplied attributes

Contivity 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, if any.

Browser considerations

You should be using the latest version of your browser to ensure accurate screen displays of the Web interface for the gateway.

- Internet Explorer 5.5 or 6.0 and Netscape* 4.79 or 6.2 are the supported Web browsers. You should be using the latest version of your browser to ensure accurate screen displays of the Web interface for the gateway.
- Both Internet Explorer and Netscape browsers cache user ID and password information. If you have caching enabled in your browser, Nortel Networks recommends that you close the browser when you finish making changes to the gateway.
- America Online* (AOL*) V5.0 Web browser is not supported.

Viewing and calculating memory usage

The minimum memory requirement for Version 4.70 is 128 MB.

Due to the complexity involved in the formula for memory calculation (which was provided with earlier versions of the release notes), a new Memory Calculator tool is now available. The Memory Calculator tool is a Microsoft Excel spreadsheet that provides information on determining the memory requirements for a Contivity system based on the configuration of tunneling, routing, and firewall. The configuration values can be input 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.

Nortel Networks recommends that you evaluate the memory requirement using the Memory Calculator tool to ensure that sufficient memory is installed for the configuration prior to upgrading to Version 4.50. Contact your Nortel Networks sales representative if your configuration requires additional memory.

The parameters affecting Contivity memory usage are:

- Contivity software version
- Single or dual CPU (if single CPU model or dual CPU model Contivity Secure IP Services Gateway)

- Internal or External LDAP shows whether internal or external LDAP configured
- Number and type is the number and type of branch office and user tunnels
- Static routes is the number of static route entries in the IP routing table
- RIP routes is the number of RIP route entries in the IP routing table
- OSPF Routes is the number of OSPF route entries in the IP routing table
- Redistributed OSPF and RIP Routes is the number of routes redistributed into RIP and OSPF Routing protocols
- FW/NAT Max connections is the maximum number of connections as configured from Services→Firewall/NAT→Edit screen
- FW/NAT Number of Sessions is the total number of Firewall/NAT sessions
- BO NAT number of Sessions is the number of Branch Office NAT sessions
- CSFW Enabled shows if CSIF (Contivity Stateful Firewall with Interface Filter) is on
- Interface NAT Enabled shows if Interface NAT is on
- Antispoofing Enabled shows if Antispoofing is on

The Memory Calculator Tool is available at:

www.nortelnetworks.com/documentation

Select Data and Internet and Contivity Secure IP Services Gateway Portfolio. Go to Technical Support Documentation and Engineering Notes and Guidelines.

To view the Contivity system memory status, use the Status→System screen. The Memory field under System Hardware displays the total amount of memory provisioned, as well as how much memory is currently free.

IPTunnel SNMP MIB

If the IPTunnel SNMP MIB is currently enabled in Version 3.50 or Version 3.60 software, it will be disabled after you upgrade to Version 4.0 or higher. You can reenable it on the Admin→SNMP screen.

Gateway disconnects with PC client through LinkSys

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 gateway, then one or both of these PCs will be disconnected and/or their communications disrupted unless NAT Traversal mode is used on the gateway. (The client monitor will continue running and will 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 screen, which activates NAT Traversal and allows multiple PCs behind the NAT box to function properly.

Windows 2000 client using L2TP over IPSec

You cannot run the Windows* 2000 client using L2TP over IPSec if the Contivity 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 screen 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.

Online Help files

You can print the online Help files by going to Help→Help Contents and selecting the topic that you want to print.

Contivity Stateful Inspection firewall UI

The Contivity Stateful Inspection Firewall Java UI requires Version 1.3.0 of the Java Runtime Environment for proper operation. The JRE 1.3.0 is distributed with the Contivity Secure IP Services Gateway image; it can also be downloaded from Sun Microsystems, Inc.

Using OSPF virtual links

Because Version 3.*x* does not support OSPF vlinks, you must turn on or off a flag using the CLI **`Compat_3_6 enable`** command. However, this flag does not permit gateways running Version 4.0 to form a virtual link over tunnels.

If all the gateways in the network are running Version 4.0, then Nortel Networks recommends that you use the no Compat_3_6 enable flag on all of the gateways. Even if only one gateway running Version 3.*x* participates in OSPF through tunnels, then every gateway with Version 4.0 needs to be set with the Compat_3_6 enable flag.

For example, if end-point A is running Version 4.0 and end-point B is running Version 3.*x*, end-point A should have the Compat_3_6 flag enabled for OSPF to work properly. However, if both end-point A and end-point B are running Version 4.0 and both have enabled the Compat_3_6 enable flag, OSPF will work properly, but vlink over this tunnel may not work properly. Also, if you set the flag for end-point A to Compat_3_6 enable and end-point B to no Compat_3_6 enable, OSPF may not work properly.

If you set the flag for end-point A to no Compat_3_6 enable and set end-point B to no Compat_3_6 enable, OSPF and vlink will both work properly over this tunnel.

Branch office test fails when traffic is passed over non-nailed up tunnel

Testing a branch office tunnel might fail if the tunnel is being initiated from both side at the same time. This occurs when the initiation is due to live traffic or a test button tunnel initiation.

Inactive PPP connection through LMC 1200 board

If you are using an LMC 1200 board (V.35) and you suspect that your PPP connection is not working properly, perform the following steps to check the connection. The connection might appear to be working (for example, the board's LEDs might be active) but no data is being passed through.

1 Go to your gateway’s System→WAN screen. Select the Statistics button for the interface.

2 On the Statistics screen, check the IP Packets Sent field. If the field shows that zero packets have been sent, this indicates that the PPP connection is not active.

You must re-initialize the board to activate the PPP session: power off the gateway, wait a few seconds, and then power it back on.

Documentation notes

The following sections describe items that will be added to future versions of the documentation.

Restoring LDAP database causes the Start/Stop button to disappear

The Start/Stop button disappears when you restore the LDAP database. If you need to refresh the screen after the restore completes and the restore status popup is dismissed, you can reselect the screen using the menu item selection.

Asynchronous branch office tunnels over private interfaces

Asynchronous branch office tunnels only work on public interfaces.

Reboot when changing PPP to or from frame relay

If you reconfigure the interface type from PPP to frame relay, you must reboot the gateway for the change to take effect.

PPPoE static default route does not appear

When PPPoE is configured, a default route is added to the route table. However, this route is not viewable on the Routing→Static Routes screen. As a result, the Enable Static Routes button may accidentally be disabled, which deletes the default route and stops packet forwarding. Be sure that Static Routes are enabled if you use PPPoE.

Unable to access UI after disabling branch office with VRRP running

If a critical interface for a VRRP interface goes down, the VRRP interface is also brought down (this is how critical interface functions). Therefore, if VRRP is configured on the management subnet interface, the management interface is brought down if any critical interface is down. When this happens, the gateway cannot be managed through the management interface. This occurs only if the VRRP interface is the interface with the same subnet as the management interface.

Close browser after upgrade

After you successfully upgrade your system, log off from the Web Management UI, close the browser, then log on again to continue managing the box. Closing browser session ensures that the latest version of the management UI is used to manage the box.

Disabling interface NAT does not impact branch office NAT

Interface Nat only applies to clear text traffic (non-tunneled, routed through the gateway) and branch office NAT only applies to specific branch office tunnel traffic. If you disable interface NAT, it does not impact branch office NAT.

Asynchronous branch office tunnels do not support responder for interface groups

Asynchronous branch office tunnels do not support responder for interface groups. Therefore responder does not appear as a choice under Available Interfaces. VRRP critical interfaces do not support this type of tunnel as a critical interface.

Known anomalies

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

CLI issues

The following sections describe issues that apply to the command line interface (CLI).

Using comma delimiter in user name (Q00564649-01)

When using the CLI to create an account name, do not use a comma to split the user name.

Frame relay circuit goes down when editing unrelated WAN card (Q00562810)

Editing an unrelated WAN card causes a virtual connection to go down and if a card is already disabled, config commands are not disabled or ignored. You can configure the CSU/DSU from the CLI on cards that do not have on board CSU/DSU (the WANic 400 and LMC 1000). The second problem is that if you make changes to a card that does have on board CSU/DSU (LMC 1200), it brings down a frame relay VC on an unrelated card. CLI should configure CSU/DSU only on the cards that allow it.

show ip route displays incorrect default route for RIP (Q00549724)

The **`show ip route`** command behaves in the same way as the **`show ip route all`** command. In addition to displaying best routes, it displays suboptimal routes as well. To see best routes per protocol (RIP, OSPF, static or utunnel) use the **`show ip route protocol`** command.

Firewall support using show running-config (Q00545275)

The CLI **`show running-config`** command does not support the Contivity Stateful Firewall.

Using UI and CLI at same time (Q00536184)

If you are using CLI and UI at the same time and if CLI displays configuration information before the UI completes it (when protocol on WAN is changed to frame relay but not yet configured), you will see a CLI error message. To avoid this problem, do not have two or more UI or CLI sessions open at the same time.

Provisioning branch office tunnels using CLI scripts (Q00534229)

If you use a CLI script to provision large numbers of branch office tunnels, the physical interfaces for the local endpoints of the tunnels must be installed and configured for IP to ensure optimal provisioning performance.

Disabling Contivity tunnel filter from the CLI (Q00533335)

The Contivity tunnel filter can only be disabled when the Contivity Stateful Firewall is enabled. If you disable the stateful firewall and from the CLI type **`no firewall tunnel-filter`**, the tunnel filter is disabled even though the stateful firewall is disabled.

Inconsistency with number of characters for CLI and GUI (Q00523488 and Q00523479)

There is an inconsistency with the number of characters you can enter within the UI and CLI for the branch office group and branch office connection names. When you create a branch office group, you can only enter 30 characters, but with CLI you can enter over 100 characters for a branch office group name. For branch office connection, you can only enter 16 characters for the name, but with CLI you can have 130 characters for a name. Also, for Add Group name, you can only enter about 40 characters, but using the CLI you can enter 120 characters for the group.

Using no ip helper command changes server address (Q00507033)

The **`no ip helper`** command can change the server address; this should only be accomplished using the **`ip helper`** command and the **`no`** version should not accept the IP address of the server

Using show running routing dhcp-relay command (Q00506537)

If you use the **`show running routing dhcp-relay`** command with DHCP relay globally configured or with it disabled but still configured for the same interface, it does not show the configuration. The command should configure the feature and then disable or enable it based on its status.

Misleading error message (Q00505908)

The **`no ipx interface`** command displays a misleading error message when applied to an interface that is not present in the box. The error message `%devloc` should be `%Interface` *`slot/port`* `does not exist`.

RADIUS groups configuration (Q00495080)

RADIUS groups are based upon group level authentication. Except for RADIUS groups, all authentication types for group authentication are located within group ipsec/Base auth *xxxx*. Because group level RADIUS is located in auth RADIUS, you cannot provision groups with the **`show running-config`** command.

CLI ftp-coredump command (Q00483131)

If you issue the **`ftp-coredump`** command and do not use the full syntax (**`ftp-coredump host`** *`x.x.x.x`* **`path`** `core` *`x.x.x.x`*), you receive an index out of range error message. Be sure to enter the full syntax including the path.

CLI no lease default and no lease maximum values zeroed (Q00456725)

The CLI commands **`no lease default`** and **`no lease maximum`** should reset values back to the default values. To work around this problem, avoid using the no commands or if you use them, be sure that the lease default and lease maximum values are set to any reasonable value greater than zero, such as 1 day and 12 hours.

CLI shows disabled IPSec encryption as enabled (Q00447373)

If you globally disable all IPSec encryption from the CLI and then execute the **`show bo-group /Base`** command, the last IPSec encryption that was disabled shows as enabled. The UI shows all encryption for /Base as disabled.

CLI changes to branch office groups (Q00438531)

If you make changes to the IPsec encryption level to a group with active tunnels using the CLI, the tunnels do not bounce and then come back. The changes do not take effect until the tunnel is logged off and then reinitiated.

Editing user accounts created in CLI from UI (Q00255043)

If you add a user using CLI without any parameters and then use the UI to add an IPSec username and password, it does not work and the no entries found IPsec error message appears.

WAN interfaces not supported through CLI (Q00246541)

The current release of the gateway does not support CLI for a WAN interface. Consequently, features that depend on configuration of a WAN port will not be provisioned with a script generated with **`show running-config`** commands. For example, if static routes through a WAN port are configured, you cannot provision them without first configuring a WAN IP address. If you want to use a **`show running-config`** generated script to provision a box with a WAN interface, be sure that all WAN parameters are first configured through the UI.

Unable to view an invalid default route through serial menu or CLI (Q00227717-01)

Because invalid default routes do not appear either with CLI or through the serial menu, they cannot be deleted. However, they can be viewed and deleted through the UI.

Caching configuration screens (Q00207522)

Your Internet browser might be caching configuration screens. This becomes an issue if another UI session or CLI session is changing parameters displayed on the same screen. In this case, refreshing the screen might not display the latest version of these parameters.

To ensure that the latest values are displayed, you can either disable browser caching or restart the management session by logging out and logging in again.

You should check how many management sessions are open before making any critical configuration changes. Two users modifying the same functional area simultaneously could lead to an inconsistent configuration.

Branch office encryption levels (Q00206309)

The UI does not display proper information about branch office connection encryption levels. The encryption level setting is not propagated automatically to all branch office connections. To change the branch office tunnel encryption level:

1. Disable the tunnel.
2. Change the encryption level (Services→L2TP).
3. Change the branch office connection parameters (other than encryption); for example, temporarily change the user name.
4. Enable the tunnel.

Boot system version command does not work (Q00173683)

The CLI **`boot system`** `[<version>]` command does not work. Instead of rebooting the device it displays warning message indicating that reboot is not possible because there are users logged on to the gateway. Use the **`boot system`** `[<version>]` **`recurse`** command to reboot the device through the CLI interface (Telnet or serial connection).

show running-config enables RIP (Q00173630)

The default value for redistribution is to enable static routes into RIP. However, when you use the **`show running-config routing`** command, the CLI **`router rip`** command executes, which enables RIP.

Incorrect master-delay output (Q00173616)

The **`show running-config vrrp`** command does not produce correct output for master-delay parameters. It always displays the delay as 00:00:00 regardless of what is actually configured on the box. If a script generated this way is used to provision other boxes, you have to manually insert the proper value.

VRRP configuration support (Q00173612)

CLI does not support full configuration of VRRP. You can configure either master delay mode or authentication, but not both of these features. Configuring master-delay mode time removes authentication settings and configuring authentication resets master delay mode time. You can use the UI to configure either delay mode or authentication.

SNMP enable traps command (Q00156156-01)

The SNMP **`enable traps`** command is missing the hardware accelerators and HSSI cards options. You cannot enable or disable traps for these types of hardware using the CLI. The **`show running-config`** command will also not configure these traps. You must use the UI to configure them.

Configuring parameters spanning multiple lines (Q00156117-01)

CLI does not allow you to configure parameters that span multiple lines. In addition, the lines cannot be longer than 255 characters. The UI allows you to configure multiple lines of description, for example group banners. If you have configured multiple line descriptions using the UI, you cannot replicate them using the **`show running-config`** command. If you attempt to do this, only the first line will be configured on a destination device instead of the entire banner.

CLI network command (Q00072440)

For the CLI **network** {*<network-address>*} {*<wildcard-mask>*} **area** {*<area-id>*} command, the network address on the gateway refers to an actual IP address on a physical interface.

For example, if the gateway has three IP interfaces defined as 192.32.54.37, 192.32.54.65, and 192.32.54.97, you need to use the following three commands for all the interfaces to be configured in area 0.0.0.0:

```
network 192.32.54.37 0.255.255.255 area 0.0.0.0
network 192.32.54.65 0.255.255.255 area 0.0.0.0
network 192.32.54.97 0.255.255.255 area 0.0.0.0
```

Routing issues

The following sections describe issues related to routing.

Changing the management IP address and mask through serial (Q00573391)

You must enable OSPF and VRRP on the management interface before you change the management IP address and mask through the serial interface.

Deleting active interface group (Q00564615)

If you delete an interface group, VRRP switching does not work correctly. You must go to the UI Routing→Interfaces→Configure screen and then click OK or use the CLI Config Term | Interface Fastethernet 0/1| Ip Vrrp command.

VRRP with critical interface (Q00565798)

If you bring up the VRRP interface after the critical interface, the routes for the VRRP interface are not placed in the routing table. Disable and re-enable interface to re-establish traffic.

Loss of connectivity to default route IP with VRRP (Q00565661)

When using a branch office tunnel, the Contivity does not take the backup default route for the IP address of the primary default route if the interface for the primary default route goes down.

Modifying subnet mask does not update routing table (Q00561804)

If you change the IP mask or IP address on a frame relay VC, the direct route to the replaced address remains in the routing table until the Contivity is rebooted. If the original address or subnet is used, it might cause routing problems.

Configuring two interfaces within same subnet (Q00559903)

To avoid routing problems, be sure that you do not have two interfaces in the same subnet.

Multicast traffic causes OSPF to stop receiving hello packets (Q00557579)

You must use stateless mode for L2TP tunnels if you have an environment where packets might be lost. Stateful mode forces the tunnel to drop more packets once a packet loss is detected. Multicast does not work over a Contivity OSPF L2TP tunnel through a Cisco router.

RIP learned routes not displayed (Q00549153)

Only one RIP learned route and its cost is displayed when you use the **`show ip route rip all`** command.

VRRP interface group reported incorrectly (Q00538784)

When you assign a tunnel to an interface group even though the branch office tunnel is not up, the interface group operational state is reported as up in both the UI and at the CLI

Responder tunnels cannot be used with multicast boundary list (Q00537232)

You can only use the multicast boundary list on a interface that has an IP address. Asynchronous branch office responder tunnels do not have an IP address and therefore cannot use the multicast boundary list.

Multicast boundary list cannot be enabled or disabled (Q00535443)

You cannot disable multicast boundary through the Add Multicast Boundary screen, but you can use the Enable and Disable buttons on the Routing→Multicast screen.

VRID set to 0 if browse to another screen while in VRRP create (Q00458703)

If you start to configure VRRP and instead of cancelling the configuration, exit the browser (click on the back button), the UI creates OM records and leaves it in a default state (0 for VRID). This creates unusable records that are never cleaned unless you specifically remove them. However, it does not prevent the application from running properly.

Incorrect routing error message (Q00447493)

The UI incorrectly informs you that a license key is required to change Default Route Preference option located on Routing→Configure page. If you need to change this option, you can ignore this warning.

Changes to RIP configuration don't always take effect when they should (Q00281283-01)

When making changes to the RIP configuration using the UI, you may need to click on the OK button more than once for your changes to take effect. To verify that your chances have take effect, go back to the RIP configuration screen.

Displaying private default routes (Q00173694-01)

After you change the IP address of the private interface, the UI Routing screen may not display private default routes correctly. (This does not prevent routing from functioning properly.) Instead of displaying the private interface name, it displays the public interface name. The IP Address column shows the proper (private interface) address. Alternatively, you can use the CLI to verify that the default route is set up correctly.

Two unique LSIDs must exist in backbone area (Q00067571)

RFC 2328 supplies an algorithm for the assignment of LSIDs for more specific/less specific routes. For example, if IP address (a) 192.50.10.66/27 is in OSPF area 2.0.0.0 and IP address (b) 192.50.10.67/26 is in OSPF area 2.0.0.0, address (a) has 30 possible host addresses and address (b) has 62 possible host addresses. Both (a) and (b) need to have entries in the OSPF backbone to ensure full connectivity. Therefore, for the backbone area to differentiate the same summary network (in this case, 192.50.10.64), two unique LSIDs must exist in the backbone area. This functionality is supported for AS external-LSAs but not for summary-LSAs.

Authentication and certificate issues

The following sections describe issues that apply to authentication.

Change in parent group values breaks subgroups inherit setting (Q00517065)

There are two problems when a subgroup is set to inherit a value from its parent after the parent values are changed from the original inherited value. First, the corresponding field in the subgroup is no longer set to inherit (the field is now a live field). And second, the subgroup's value is not updated to the new value.

Group certificate assignment fails if only /Base group exists (Q00456110)

Group Certificate Assignment fails if only group /Base exists. If the group /Base exists with no other groups and if you attempt to assign a server certificate to this group for authentication, the certificate will not be associated with group /Base.

CRL retrieval does not work with external Iplanet directory server (Q00418932-01)

CRL retrieval does not work with iPlanet* Version 5.0. Nortel Networks recommends that you use Version 4.0.

PPTP and L2TP MPPE 128-bit encryption keys (Q00285658)

PPTP and L2TP MPPE 128-bit encryption keys do not work properly in the gateway 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 Networks 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 gateway if PPTP or L2TP MPPE-based 128-bit encryption is required.

Interpretability issue between Versions 4.5 and 4.0 (Q00281646-03)

When using Triple DES with Group 7 (ECC 163-bit field) for IKE encryption and Diffie-Hellman Group, Version 4.0 and Version 4.70 will not interoperate. The tunnels come up but the data traffic is dropped as authentication failures. The workaround is to disable PFS.

Windows 2000 VPN server (Q00228485)

For the current release of the Windows 2000 VPN server, you must disable IPSec compression (LZS) in the branch office group to allow the gateway to successfully initiate branch connections with Windows 2000.

Using certificate RDN fields for a remote identity (Q00154595)

If you are using RDN fields to identify a certificate user (either branch office or user), you must clear the current contents of all RDN fields, save the empty values, and then enter correct values.

NAT and Contivity Stateful Firewall issues

The following issues pertain to Network Address Translation and Contivity Stateful firewall.

Firewall anti-spoofing requires reboot message (Q00428120-01)

If you use CLI to enable firewall anti-spoofing, it does not tell you that you need to reboot to enable the anti-spoofing, but the UI tells you to reboot in order for changes to take effect.

Establishing control tunnels using NAT and firewall (Q00103770)

Control tunnels cannot establish a connection when the Contivity Stateful Firewall is enabled when using the Autodetect IPSec capable NAT feature. To establish a control tunnel over a NAT connection, use IPSec capable NAT.

Dynamic routing for branch office tunnels using NAT (Q00087586)

Dynamic routing (RIP or OSPF) will not work over branch office tunnels using NAT. Support for this feature will be included in a future release.

International characters in branch office and user group names (Q00039540)

Do not use non-ASCII (US) characters in the names of branch office groups, user groups, firewall and NAT rules or other named entities.

Contivity 1010/1050/1100 issues

The following describe issues that were identified with the Contivity 1010/1050/1100.

Deleting previous version before upgrade (Q00536634)

Because the Contivity 1010, 1050, and 1100 are diskless systems with limited storage space, you must delete the last non-loaded version of code on the box before you can upgrade.

Incorrect restart system message (Q00457593)

When running the recovery process on a Contivity 1010/1050/1100, the restart system description incorrectly states “To restart the system, remove the diskette and press the Reset button on the back of the Switch.” These units do not have a diskette and you just need to turn the power off and on again.

Creating the quick start tunnel in the /Base group (Q00447587)

Branch office quick start creates tunnel in the /Base group. If you need to modify any parameters for /Base group, first move automatically created tunnels to another group.

Load balance feature not functional (Q00436831)

The Contivity 1010/1050/1100 does not perform load balancing.

Private network not updated when branch office fails (Q00431668)

When the Branch Office Quick Start successfully creates the branch office tunnel, but fails the branch office test, the private interface configuration is not updated. To complete the branch office configuration, you need to change the private interface addresses, and add the new DHCP range of addresses. When BOQS fails to complete configuration because of the connectivity problems or invalid data entry, it is always safe to rerun BOQS.

Ethernet connection at full duplex when connected to hub (Q00389709)

The Contivity 1100 is a five port gateway. Ports 1-4 are external; port 5 is an internal port wired to the internal Ethernet MAC on the motherboard. Therefore, the internal port will always read 100 Full Duplex Interface because it is point-to-point to port 5 of the gateway regardless of how the external ports are configured through auto-negotiation. You cannot read the state of the four external ports because they are not managed.

General gateway issues

The following release notes apply to the Contivity Secure IP Services Gateway.

Incorrect WAN status in system report (Q00560429)

The system report for WAN cards for frame relay interfaces incorrectly reports that the card is local when it is public, and public when it is private (local). Also, the IP address is not displayed and the mask is incorrect. PPP WAN interfaces are shown correctly.

Next hop table terminology for routes learned over private frame relay (Q00553851)

When routing over private frame relay virtual circuits while also having a branch office connection defined over that frame relay virtual circuit, the terminology for the next-hop table is deceiving. Under Linked, the table should say Frame Relay instead of Tunnelled.

Ping reports ICMP failure yet echo replies received at public WAN interface (Q00553090)

If you specify the public interface address as the source when you use the management interface address **`ping`** command, the ICMP is successful. When you add a public default route to either the Fast Ethernet interface or the public WAN interface, the public WAN interface behaves differently from the Fast Ethernet interface when public default routes are bonded to those interfaces. ICMP echo replies reach the device, but it reports no answer after changing whether the pings are sent with or without a source.

Error message when adding branch office groups (Q00548286)

You cannot add multiple branch office connections using the Apply button in the GUI. After a connection is added, click on OK and proceed to configure the connection. Once the connection is fully configured, click on Add to configure additional branch office connections.

Switching internal LDAP to external LDAP (Q00546864)

When you switch between internal LDAP and external LDAP, you should reboot your Contivity. When you shut down the internal LDAP server for backup, you should do so when the Contivity has only the management session running that you use to stop the server and when tunnel traffic volume is low.

DHCP IP ADDR POOL rejects logins when cache size is small (Q00541564)

Tunnel creation fails when the cache is exhausted and because of lack of available IP addresses while the cache was being refilled. To work around this issue, use a cache size greater than or equal to the number of user tunnels.

Changing authentication requires restarting PPPoE (Q00541099)

When PPPoE is in the up state changes, you can edit the PAP or CHAP UID and password on the Authentication screen. However, the changes will not take effect until the PPPoE is restarted.

Quick start shows empty field (Q00539650)

You can use the Quick Start to configure a private default route; however, if you run it again after the initial configuration is complete, you will be unable to see it. The route is configured correctly and can be seen and changed using the GUI screens or CLI.

Unable to delete UDP port for NAT traversal (Q00533495)

You cannot delete or remove the NAT traversal setting for UDP port. The Contivity stores the UDP port number even when you remove it from the UI.

DHCP option lengths not configurable (Q00532773)

DHCP Policy Filter Option requires a list of IP address and mask combinations. DHCP Static Route Option requires a list of pairs of IP addresses. For both options the length must be 8 bytes or multiples of 8 bytes. At present neither of these options are configurable.

Using comma with network name (Q00532630)

Do not use comma in network names. If you create a new network that has a comma in its name, you get error message when you add new subnet and the network name isn't saved in the network list.

Changing parent group value breaks subgroups inherit setting (Q00517065)

When a subgroup for certificates is set to inherit a value from its parent after the parent values are changed from the original inherited value, the corresponding field in the subgroup is no longer set to inherit (a live field). Also, the value of the subgroup is not updated to the new value.

Configuring virtual interfaces on LAN (Q00503364-01)

If you go to the System→LAN screen to create a virtual interface for an interface that already is configured using DHCP client, the virtual interface will replace the already configured interface with static IP. Although the gateway supports multiple IP addresses on an interface, DHCP does not support this.

Health check warning with fragmented LDAP database (Q00476718)

With the repeated addition and deletion of hundreds of LDAP entries, the LDAP database can become fragmented. This will adversely affect the performance of LDAP operations on the gateway. If this occurs, you can increase performance either by exporting the database to an LDIF format and then importing the LDIF file or restarting the device.

Restart DHCP service after adding DHCP pool (Q00456501)

When you add a new DHCP pool, you must restart the DHCP service to have the changes take effect. The UI does not send a message as notification to do this.

External LDAP causes permit all tunnel filter to disappear (Q00455434)

When you set the LDAP for External, the permit tunnel filter disappears and you must create a permit all filter. The interface filter for permit all is still there. Go to Profiles→Filters and create your own Permit All filter under the tunnel filters.

Restoring VRRP configuration file and LDAP (Q00433464)

You should first restore LDAP and then the VRRP configuration file. If you restore LDAP after the configuration file, then you may need to disable and re-enable VRRP for it to become operational. If some VRRP configuration information is in LDAP and not present when VRRP is enabled, then VRRP will not function.

DHCP Server options requiring multiple IP addresses (Q00432104)

You cannot configure DHCP server options that require multiple IP addresses through either the UI or CLI.

Enabling SNMP MIB through the UI (Q00440453)

If you enable the SNMP MIB through the UI and go to the Admin→Snmp screen, it does not show it as enabled. However, the CLI **`show snmp mib`** command shows that it is enabled.

Editing last name for user profile causes errors (Q00435962)

When you edit the user profile to change the user's last name, you will get a no entries found error message. This also occurs through the CLI, but no error messages appear. This occurs only if you leave the first name field empty. To workaround this, configure the user first name before changing the last name.

Cannot cancel upgrade in progress (Q00433348)

If you click on the Cancel button when an upgrade is in progress, the upgrade process does not cancel and the FTP continues.

Screen mismatch between group configure and group connectivity screens (Q00431944)

If you choose the default pool, the Profiles→Group screen correctly shows the default pool. However, if you click on Configure, the address pool name in the drop down list indicates “None defined on this switch” on the Profiles→Group Configure screen.

Branch office tunnel filters not working properly (Q00418382-01)

Filters for the branch office tunnel do not work unless you bring up all of the interface filters and modify them to add the rules to the tunnel filters.

Inconsistent sizes for branch office tunnel names (Q00386638-01)

When creating a branch office tunnel from the UI, you cannot use a branch office tunnel name of more than 25 characters. When using the CLI or BOQS, you can enter up to 127 characters.

CRL retrieval from MS AD is not working correctly for pkiCA object class (Q00322434)

CRL retrieval from Microsoft Active Directory will fail if the CRL is stored under an object class type of pkiCA. You should store CRLs under the object class crlDistriburionPoint.

Booting under load does not bring up branch office tunnels (Q00319718)

If you reboot the unit under load, the branch office tunnel does not come up until you stop the traffic. If you generate 10 MB of traffic from a host on the network to a host on another network, the traffic goes over the branch office tunnel as expected. If the traffic continues running and you reboot, the branch office tunnel does not become active after the reboot. This only occurs when you generate between 7 MB and 10 MB of traffic destined for the branch office tunnel; lower traffic rates work properly.

No warning when deleting a branch office group with subgroups and active tunnels (Q00305208)

If you delete a branch office group, you also delete all subgroups and tunnels, even if the tunnels are active during the delete operation. Because deleting active tunnels leads to connectivity failure, the UI should display a warning and ask for confirmation. However, an appropriate warning fails to display when an active tunnel resides in a subgroup of the group being deleted. (The warning is displayed when the tunnel is included directly in a group that is being deleted.) Verify that no active tunnels are present in the groups and all subgroups before you delete the group hierarchies.

Incorrect error message for excess rates (Q00289581-01)

When you change the excess rate in group connectivity to a value that is less than the committed rate value the “Error with 0: Excess rate must be greater than or equal to committed rate” error message is displayed. The message should say: “Excess rate must me greater than or equal to committed rate.”

Serial console issues with system reset menu options (Q00284339)

Recovery image: The Normal or Safe text string for the current mode is missing “System Reset Menu Options. System is currently in mode.”

Editing asynchronous branch office connection type (Q00281201)

You must delete the asynchronous branch office tunnel before you can edit the connection type.

File retrieval counter increments FTP failure attempts (Q00250467)

When you upgrade the gateway from an older version, a popup window tells you how many files have been transferred. However, if the retrieval is failing, the FTP tries three times to get a file until it quits and the counter in this window is counting these FTP attempts as actual files being transferred when they are not, which can be misleading.

No duplicate IP error message for DNS Server (Q00209618-04)

You can enter duplicate IP addresses for the DNS servers without any error messages stating that there are duplicate errors. This applies to both the UI and CLI interfaces.

Deleting a group with over 2000 users (Q00168861)

Contivity devices that have more than one hard drive installed and configured may experience problems when adding/deleting/modifying a large number of LDAP records via the HTTP or Telnet user interfaces. This occurs due to the disk synchronization process blocking LDAP from successfully modifying those records. While the major number of the example number (2000) of user records will be modified, some small percentage will fail.

Setting LDAP to an unreachable external server (Q00155644-01)

If you set LDAP to an external server that is unreachable through either the UI or CLI, LDAP hangs and takes several minutes to time-out.

Ping and traceroute issues (Q00080227)

If a DNS server is configured from the System→Identity screen and if the specified DNS server does not support reverse resolution queries (queries to map an IP address to a host name), **`ping`** and **`traceroute`** commands may take longer than expected and the behavior may be unpredictable.