Version 4.07

Part No. 314963-A Rev 00
June 2002

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity 1010/1050/1100 Release Notes (V4.07)

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, and Contivity are trademarks of Nortel Networks.

3Com is a trademark of 3Com Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

AIX is a trademark of International Business Machines Corporation (IBM).

America Online is a trademark of America Online, Inc.

Certicom is a trademark of Certicom Corp.

Entrust is a trademark of Entrust Technologies United.

Hummingbird FTP Server is a trademark of Hummingbird Communications Ltd.

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

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

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

On-Net is a trademark of On-Net Internet Services, Inc.

Peerlogic is a trademark of Peerlogic, Inc.

Red Hat is a trademark of Red Hat, 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.

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* 1010/1050/1100.

Before you begin

These release notes are intended for network managers who are responsible for the switch. 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`**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is **`more disk`***`n`***`:`***`<directory>`***`/...`***`<file_name>`**, you enter **`more`** and the fully qualified name of the file.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **`ping`** *`<ip_address>`*, *`ip_address`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`

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

Related publications

For more information about the switch, refer to the following publications:

- *New Features for the Contivity 1010/1050/1100* (part number 315535-A) describes the new features for the Contivity 1010/1050/1100 series of switches.
- *Installing the Contivity 1010/1050/1100* (part number 314961-A) provides instructions on how to install the Contivity 1010, 1050, and 1100 and includes technical specifications.
- *Configuring the Contivity VPN Switch* (part number 311642-D) provides procedural information to help you configure, monitor, and troubleshoot your switch.
- *Reference for the Contivity VPN Switch Command Line Interface* (part number 311645-C) describes the commands that you can use from the command line interface.
- *Connecting for Internet Access* (part number 314962-A) describes how to set up your Contivity 1010, 1050, or 1100 at the branch office site.

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* at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader*.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/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

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 www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1
Overview

Version 4.07 provides software support only for the Contivity 1010/1050/1100 series of switches. These release notes contain the latest information about the Contivity 1010/1050/1100. Refer to your Contivity *Installation* guide for instructions on getting the Contivity 1010/1050/1100 switch up and running.

Version 4.07 new features

This section highlights the new Contivity VPN Switch features that are supported in Version 4.07. For additional information, refer to the documentation set or on-line help.

This release of the Contivity 1010/1050/1100 will include for the following:

- Point to Point Protocol over Ethernet (PPPoE) allows PPP to run over Ethernet. Typically, PPP runs over serial interfaces and in most cases runs over phone lines connected to a server.
- Dynamic Host Configuration Protocol (DHCP) dynamically assigns configuration parameters to hosts and provides for centralized network administration. DHCP pushes configuration information to clients, including network address parameters and standard options and provides for interaction with DNS.
- DNS proxy acts as a DNS server to the private side. It resolves host names for both locally connected hosts and those from other DNS zones.
- Unique default configuration that allows public network access without any initial configuration. This allows non-technical users to set up the switch at a branch office location.
- Compact flash disk for long term storage needs.
- Support for optional PCI cards: 10/100 Ethernet card and T1 and X.21/V.35 WAN cards for the Contivity 1100.
- A four-port Ethernet switch for the Contivity 1050 and 1100.

Nortel Networks CD

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

Doc (Documentation) directory

The doc directory contains the documentation set for the Contivity VPN Switch. These guides are provided in Adobe Acrobat PDF format. The documentation set provides configuration, monitoring, administration, and troubleshooting information as follows:

- *New Features for the Contivity 1010/1050/1100 (V4.07)* (features.pdf) provides information about features that are unique to the Contivity 1010/ 1050/1100 series of switches.
- *Configuring for Internet Access* (Int_access.pdf) describes how to connect the Contivity 1010/1050/1100 to the Internet at the local branch office.
- *Installing Contivity 1010/1050/1100* (1010.pdf) provides hardware overview, instructions on how to install and replace option cards in the Contivity 1100, and technical specifications.
- *Configuring the Contivity VPN Switch* (cesproc.pdf) provides procedures for configuring, monitoring, administering and troubleshooting the Contivity VPN switch at the central office or network operations center.
- *Reference for the Contivity VPN Switch Command Line Interface* (clirefgd.pdf) provides information about the Command Line Interface (CLI). The CLI enables you to access the switch using a telnet session.
- HTML files that consist of the on-line help.

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). You must first purchase a license to use this software. To install the software, unzip the .zip file and click on Setup.exe.

Tools directory

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. For installation instructions, please view the Policy Manager getting started documentation in the *Configuring the Contivity VPN Switch* book.

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 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 4.07 release of Contivity 1010/1050/1100.

Product considerations

The following sections discuss information that you should consider before using your Contivity 1010/1050/1100.

Public MAC address

If your ISP requires a MAC address to establish a connection, you need to provide them with the LAN 1 (public) MAC address for your Contivity 1010/1050/1100. This address is located on the back of your unit.

Number of versions on switches

Nortel Networks recommends that you maintain at most two versions on your Contivity 1010/1050/1100, including the version that is currently running.

NAT traversal port numbers

Nortel Networks 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.

CMP Auto enrollment issues

- You must wait for 2 minutes after rebooting the switch to use the CMP automatic enrollment facility.

- When you use the CMP feature, only the reference number and authorization code are required for enrollment with Entrust Certificate Authority.
- The CA must be located on a publicly accessible IP address.

Very large packets over T1 interface

A T1 interface does not support packets larger than 47KB.

Entrust SSL certificates

Entrust* certificates are supported when hashing method MD5 is selected by the Certificate Authority. Hashing method SHA-1 is not supported.

Browser considerations

- Internet Explorer 5.5 or 6.0 and Netscape 4.7.*x* 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 switch.
- For the Help Contents path, location field, and the associated links to work properly, you must not disable accepting Cookies from your Web browser.
- 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 switch.
- America Online* (AOL) V5.0 Web browser is not supported.

Switch 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 switch, then one or both of these PCs will be disconnected and/or their communications disrupted unless NAT Traversal mode is used on the switch. (The client monitor will continue running and will not display a message that the connection is disconnected or disrupted.) This occurs because the LinkSys router 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.

Contivity Stateful Inspection Firewall UI

The Contivity Stateful Inspection Firewall Java UI requires version 1.3.0 of the Java Run Time Environment for proper operation. The JRE 1.3.0 is distributed with the Contivity Extranet Switch image; it can also be downloaded from Sun Microsystems.

Known anomalies

The following sections describe issues that Nortel Networks has determined will not be fixed in the current release. These include new issues identified with V4.07 and legacy issues. Version V.07 is only available for the Contivity 1010/1050/1100. If you have other Contivity units running other software versions, refer to the appropriate release notes to determine any open or fixed issues.

New V4.07 issues

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

Unable to delete files that contain spaces for characters (Q00458351)

The switch cannot delete any files that contain a space instead of a character. For example if you FTP a file to the switch that contains spaces in the file name, you cannot subsequently remove the file.

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.

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

The CLI commands no lease default and no lease maximum should return 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.

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.

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.

OSPF router ID summary displays incorrectly (Q00448190)

When the OSPF router ID summary is set to 0.0.0.0, the UI reports the correct lowest IP address, but the change is not passed to OSPF.

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.

Incorrect 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.

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.

Adding and deleting users (Q00447205)

Adding and deleting significant numbers of users and groups can reduce the size of the available space on the compact flash disk.

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.

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.

Load balance feature not functional (Q00436831)

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

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.

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.

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.

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.

RIP routes not added to routing table (Q00431986-01)

RIP routes are not added to the routing table when you use an asynchronous branch office tunnel from the initator side, .

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.

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 side network is not updated. To complete the branch office configuration, you need to change the private side addresses,and add the new DHCP range of addresses.

Large packets fail with NAT traversal (Q00431240)

Large packets of 2048 bytes fail with NAT traversal active and compression disabled for IPSec users.

Turning off firewall affects existing client tunnels (Q00430477)

If you turn off the firewall, several minutes later the ICMP traffic become sporadic and the client tunnel eventually comes down. You must reboot the switch when the firewall is turned off.

PPPoE MTU setting (Q00429500)

If you are using PPPoE, be sure that the Maximum Transmission Unit (MTU) setting on the PC is set to 1492 or lower.

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.

IPSec keepalive not supported (Q00426585-01)

The IPSec keepalive feature is not supported for this release.

Editing default NAT rule (Q00420765)

You cannot edit the default NAT rule. If you go to Services→Firewall/NAT screen and then edit the default NAT rule, you receive the “Failure - encountered a problem editing this rule” error.

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.

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.

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

The Contivity 1100 is a five port switch. 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 switch 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.

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 to127 characters.

Restoring LDAP database causes the Start/Stop button to disappear (Q00323610)

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.

Disabling interface NAT does not impact branch office NAT (Q00322927)

Contivity VPN Switches has interface Nat, which only applies to clear text traffic (non-tunneled, routed through the switch) and branch office NAT, which only applies to specific branch office tunnel traffic. If you disable interface NAT, it does not impact branch office NAT.

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 10MB 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 7MB and 10MB of traffic destined for the branch office tunnel; lower traffic rates work properly.

Delay restoring PPPoE (Q00281350)

When there is a loss of PPPoE service using dynamic IP addressing on the Contivity 1010/1050/1100, the remote route is removed from the IP forwarding table. When PPPoE is restored and reconnected, the Contivity 1010/1050/1100 obtains a new public source IP address and any packets are temporarily sent out the PPPoE interface because the remote static route is no longer available. After 3-4 minutes the Contivity 1010/1050/1100 adds the asynchronous branch office tunnel static remote networks to the routing table. The delay occurs when Interface NAT is disabled. However, with Interface NAT enabled there is no recovery unless the tunnels on both sides are disable and re-enabled.

Editing asynchronous branch office connection type (Q00281201)

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

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.

File retrieval counter increments FTP failure attempts (Q00250467)

When you upgrade the switch 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.

PPPoE static default route does not appear (Q00230542)

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.

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.

No duplicate IP error message for the 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.

Legacy issues

The following sections describe issues from prior releases.

CLI issues

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

CLI show users command not working (Q00293267)

The switch UI incorrectly accepts an invalid slash (/) character when you specify group names. Groups with names that contain a slash are functional but are not properly recognized by CLI. CLI might show such groups are empty or present misleading error messages. To avoid this issue, rename groups using the UI.

Editing or deleting accounts without user first names (Q00175932)

When creating a user account, you can specify both first name and last name to identify the user, but specifying the first name is optional. However, because of a minor LDAP database change between Versions 3.6 and 4.0 or higher there are some problems with removing or editing an account where the first name has not been specified. If accounts without first names are already created, sharing the LDAP database between Version 3.6 and 4.0 or higher (or using a database created with Version 3.6 by Version 4.0 or higher) might cause some problems:

You cannot edit or delete user accounts without a first name that were created in the Version 3.6 UI using the Version 4.0 or 4.07 CLI. To access these accounts through CLI, you must add an extra space in front of the name; for example:

`user " Smith" /Base` (to open configure mode for user Smith)
`no user "Smith" /Base` (to delete user Smith)

Nortel Networks recommends that you specify both the first and last name when creating user accounts and use CLI only to edit accounts that do not have a first name.

If you are going to use LDAP database with Version 4.0 or higher devices only, you should remove and add all users that do not have a first name defined as follows:

1 Create file containing user information.

```
CLI# show running-config file-url usr.cli profiles users
```

The following is an example of the usr.cli file can be found in the /system/runconf directory:

```
! User Groups Configuration
! User configuration for group "/Base"
user add " Smith" "/Base"
user " Smith" "/Base"
l2tp uid "smith" password "yyy"
no ipsec-credentials
exit

user add "John Doe" "/Base"
user "John Doe" "/Base"
l2tp uid "johnd" password "abc"
no ipsec-credentials
exit
```

2 FTP the file to the workstation and open it using an editor (such as Notepad).

3 Remove all of the text from records that pertain to users with first and last names that do not have the extra space before the last name.

4 Add the user records that contain the first and last name.

5 Add standard login prolog and epilog for provisioning scripts (`enable, setup, config terminal` at the beginning and `exit, exit, exit` at the end). This results in the following file:

```
! standard prolog
enable
setup
config terminal
! User Groups Configuration
!
! User configuration for group "/Base"
no user " Smith" "/Base"    - this line has been added to remove “old” - Smith user
user add "John Smith" "/Base" - this line and the next line has been edited - space
remove
user "John Smith" "/Base"
l2tp uid "smith" password "yyy"
no ipsec-credentials
exit
! standard epilog
exit
exit
exit
```

6 FTP the file back to the device provisioning directory (/system/prov).

If you are going to use the LDAP database with Version 3.6 and 4.0 or higher devices, Nortel Networks recommends that you define a first name for all your user accounts.

Caching configuration pages (Q00207522)

Your Internet browser might be caching configuration pages. This becomes an issue if another UI session or CLI session is changing parameters displayed on the same screen. In this case, refreshing the page 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.

Timing problem using automated CLI scripting via telnet (Q00175882)

When you are using automated CLI scripts via telnet, problems could arise if the telnet session is exited before the previous command's output is displayed. To prevent this, be sure that there is a delay between the last command and the exit command that is sufficient to allow all pending output to be displayed. Note that this value will vary between switches with different processor speeds.

For example, if you are using "TCL/Expect" the sequence would be:

```
expect "CES(config)#"  ; send "exit\r"
sleep 5
expect "CES#"  ; send "\r"
sleep 5
expect "CES#"  ; send "exit\r"
expect "CES>"  ; send "\r"
sleep 5
expect "CES>" ; send "exit\r"
```

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 switch. Use the `boot system [version] recurse` command to reboot the device through the CLI interface (telnet or serial connection).

Incorrect Identification output for show running-config service available (Q00317410)

The `show running-config service available` command does not produce correct output for Identification. If you use a script generated this way to provision other boxes, you must manually insert the `[no] identification enable` command.

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.

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.

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.

Using spaces in VRRP authentication passwords (Q00173642)

CLI allows you to use spaces in a VRRP authentication password. CLI syntax allows you to enclose multi word parameters (such as passwords) in quotation marks. However, if you need to use the `show running-config` command to duplicate configurations that have multi word passwords with spaces, you need to add the quotation marks. The `show running-config` command does not automatically generate them.

Configuring parameters spanning multiple lines (Q00156117)

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.

Creating branch office tunnels through UI and CLI (Q00156156)

If you use the UI (user interface) to partially create a branch office tunnel definition, you will not be able to display or configure it using the CLI. However, after you complete the configuration of branch office tunnels through the UI, you can use the CLI to display and reconfigure them. This does not occur when you use only the CLI or only the UI to configure the switch.

SNMP enable traps command (Q00156522)

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. `Show running config` will also not configure these traps. You must use the UI to configure them.

Configuring VRRP through the CLI (Q00153242)

When configuring VRRP from the CLI, you need to add the following lines to the script after the second `exit` line to complete the configuration:

```
no router vrrp
router vrrp
```

Group IPSec configuration and branch office tunnel configuration (Q00154008)

Currently, there is no CLI command to configure Allow IPSec Data Protection or to modify the parent group for the branch office connection.

LDAP authentication uid command (Q00152801)

The `LDAP authentication uid` command specifies attributes that are used as user entries for username and password in the LDAP directory for the external LDAP authentication server. The syntax is:

authentication ldap-server uid *username* password *secret* [ldap-filter *filter*]

The *username* and *secret* parameters are mandatory.

The UI allows you to have only the UID parameter and not specify the password parameter. If you do not specify both of these parameters using CLI, the `show running-config server authentication ldap-server` command displays missing fields as empty quotes. To provision the switch using the CLI, you must specify both parameters.

CLI network command (Q00072440)

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

For example, if the switch 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.

Changes to RIP configuration do not always take effect (Q00281283)

When making changes to the RIP Configuration screen using the UI, it is sometimes necessary to press the OK button more than once for your changes to take effect. (It is necessary to press OK again if pressing OK has not returned you to the Routing Interfaces page.)To verify that your changes have taken effect, return to the RIP Configuration page.

Incorrect error message in OSPF interface configuration (Q00252840)

When configuring an OSPF interface, an erroneous message COST: Value out of defined range (1 - 65535) appears even when the cost is within this range. The OSPF interface is still configured correctly and comes up when enabled.

Redistribution into the OSPF domain (Q00107804)

You must enable the firewall on the switch where redistribution is done to distribute tunnel end points into the OSPF domain. To enable the firewall, go to Services→Firewall NAT and click on Contivity Interface Filter, click on OK and reboot the switch.

When the firewall is disabled, the switch does not distribute any static routes. However, you must also use the Permit All Filter on the Private Interface.

Displaying private default routes (Q00173694)

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.

ECMP same cost multiple default routes (Q00155923)

Nortel Networks recommends that you do not use ECMP with multiple default routes of the same cost. However, if your switch is misconfigured, you may see that the route table does not contain proper default routes even though the user interface shows the correct one. To correct this, go to the Routing→Static Routes screen and disable and then enable the global flag.

Branch office tunnels with dynamic routing (Q00089544)

Branch office tunnels with dynamic routing may not come up properly if RIP is globally enabled and you then define a dynamic branch office tunnel (either RIP or OSPF). You must disable and reenable the tunnel from the Profiles→Branch Office→Edit Configuration screen.

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.

WAN-based static routes (Q00170449)

Static routes based WAN links may not come properly during an upgrade. To work around this issue, disable and then enable the global flag on the Routing→Static Routes screen.

WAN-based static branch office tunnel (Q00176521)

When the physical WAN link is disabled and then enabled, the branch office tunnel configured over this link may not come up properly. To work around this issue, disable and then enable the global flag on the Routing→Static Routes screen.

Authentication issues

The following sections describe issues that apply to authentication.

IPSec DH Group 7 interoperability issue (Q00281646-01)

When using Triple DES with Group7 (ECC 163-bit field) for IKE encryption and Diffie-Hellman Group, V04_00.891 and V04_07.xxx will not interoperate. The tunnels would come up but data traffic will be dropped as authentication failures. Disabling PFS is a workaround.

40-bit DES not supported (Q00278068)

You cannot configure 40-Bit DES encryption with this version of software.

Errors when make changes in LDAP authentication (Q00254257)

LDAP authentication page does not function properly when the internal LDAP server is stopped or when an external LDAP server is not accessible. Instead of displaying an informative error message, internal errors are presented.All LDAP related screens only work properly when internally all external LDAP servers are accessible.

RADIUS accounting time-out interval (Q00280211 & Q00281978)

The Radius Accounting time-out value is now configurable.This value should only be changed if the default time-out of 3 seconds is not sufficient, such as if you are connecting over a WAN link. If you change this value, you should set to no longer than 60 seconds. This parameter is configurable only through the UI.

BSAC or Funk Steel Belted Radius version 3.0 (Q00225619)

If you are using BSAC or Funk Steel Belted Radius Version 3.0 (or any RADIUS server that acknowledges the Service-Type attribute with a value of 8), return list attributes will not be sent back to the switch upon authentication

CRL and CMP traffic on public side (Q00173677)

For CRL and CMP traffic to exit or enter a public interface, you must configure the following:

- Services→Available must have the appropriate checkbox selected.
- Either interface filters or the Contivity Stateful inspection Firewall must be enabled.

If you select No Firewall, CMP and CRL traffic will be blocked on public interfaces.

Using certificate to authenticate branch office tunnels (Q00153406)

When using certificates to authenticate branch office tunnels, be sure that the sequence of the DNs in the Full DN field are ordered in exactly the same way as the presented certificate. Failure to do this will result in a “ghost” tunnel being created that uses the incorrectly ordered DN. Examine the event log to verify that the sequence is correct.

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.

Windows 2000 VPN server (Q00228485)

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

NAT and Contivity Stateful Firewall issues

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

Establishing control tunnels using NAT and Stateful Firewall (00103770)

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.

Applying new or changing NAT policies (Q00039476)

New or changed NAT policies only affect sessions or connections established after the policy change. Existing sessions or connections continue to use the old NAT policy until they either terminate or time out.

Deleting NAT sets (Q00093676)

Attempting to delete a NAT set when only one NAT set is defined will fail. You must create a new NAT set, which can be empty of NAT rules, and then you can delete the original NAT set.

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

You cannot configure interface-specific rules from the Java GUI for groups with international characters in their name. The rule appears to be configured and saved successfully, but packet matching will not work correctly. If you need to use international characters, you can correctly configure and save these interface-specific rules through the CLI.

Browser issues

The following sections describe issues with Internet Explorer and Netscape browsers.

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

Internet Explorer issues (Q00086814, Q00093915, & Q00093920)

- Internet Explorer 5.01 Service Pack 2 is not supported by the Contivity VPN Switch. Nortel Networks recommends that you upgrade to a newer version of Internet Explorer.
- Problems have been observed managing the switch using Internet Explorer 5.5 while managing the firewall policy manager. Nortel Networks recommends that you upgrade to a newer version of Internet Explorer.
- When using Internet Explorer Version 5.0 to manage several different switches simultaneously, you may see problems with multiple windows not all responding correctly. To avoid this, upgrade to Internet Explorer Version 5.5 or greater.

Netscape Communicator issue (Q00032009)

Occasionally Netscape Communicator* 4.75 will stop responding when you are closing the Graphing utility located on the Status→Reports screen. In order to recover from this situation, you need to go to the Windows Task Manager screen, select the Netscape application, and click on the End Task button to stop the process.

General switch issues

The following release notes apply to the Contivity VPN Switch.

Serial console issues with System Reset Menu Options (Q00284325, Q00284339, Q00301428)

- Recovery image: Resetting into Normal mode does not reboot the switch box. A workaround is to reset the box manually.
- Recovery image: Resetting into Safe mode neither changes the switch box into Safe mode nor reboots it. After a manual reboot, it is still be in Normal mode. There is no work around for this.
- Recovery image: The Normal or Safe text string for the current mode is missing “System Reset Menu Options. System is currently in mode.”
- Operational image: When you reset the switch into Safe mode, it reboots in Normal mode and does not change to Safe mode. To work around this issue, set the switch to Safe mode from the UI screen.

No warning when deleting a BO group with subgroups & active tunnels (Q00305208)

If you delete a branch office group, you also delete all subgroups and tunnels, even if the tunnels are active during 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.

Moving asynchronous branch office connection to new group (Q00305202)

If you change the group that an asynchronous branch office tunnel belongs to, you must reboot the switch.

Max Number of Logins Attempt value does not work from UI (Q00277875)

You cannot use the UI to change the value of Max Number of Login Attempts. You must use CLI to change this parameter.

Error message in Groups connectivity screen (Q00289581)

An incorrect error message is displayed if you enter an excess rate smaller than the committed rate for group connectivity. The message should say `Excess rate must be greater than or equal to committed rate` rather than `Error 0`.

PROFILE→USERS screen does not correctly show users (Q00254855)

The Profile→Users screen will display an error message that there are more than 2000 users in the group even if there are not that many. As a workaround, either enter a search criteria or enter a * to display all users.

Number of users in user groups (Q00041269)

The Contivity VPN Switch supports up to 4000 users for each user group. If you add more users in a single group, this could affect the performance and responsiveness of the UI management interface.

Improperly reporting of hardware L2 cache size (Q00086173)

The Status→Statistics→Flash Contents screen displays the incorrect hardware cache size. Go to the Status→Reports→System Report screen to obtain the correct information.

Simultaneous searches on the Status→Accounting page (Q00208655)

The results of accounting record searches from the Status→Accounting page may be incorrect if another search is initiated by another administrator before the first search has completed. Therefore, ensure that not more than one administrator is searching accounting records at one time.

Enabling MSCHAP V2 before creating branch office tunnels (Q00175537)

You cannot create branch office tunnels if MSCHAP V2 is disabled. To create new branch office tunnels through the UI, you must first enable MSCHAP V2 on the Services→L2TP and Services→PPTP screens and then create the tunnels. This restriction applies also to IPSec tunnels. Alternatively, you can use CLI to create these tunnels.

Editing a user record (Q00154383)

The first and last name fields of user records cannot be edited from the CLI or UI. To change a first or last name, you must delete the entire user record and add it again. User records cannot be edited or deleted from the UI if the first or last name fields were edited prior to V03_65.14.

Error message when editing branch office connections (Q00153391)

After opening the Edit screen for an existing profile from the Profiles→Branch Office screen and clicking on the OK button, you may see the error message `Subject Distinguished Name already defined for this account type`. If this occurs, change the Common Name, click on OK, reopen the Edit screen, and revert to the original Common Name.

Windows 2000 client using L2TP over IPSec (Q00059655)

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.

Ping and traceroute issues (Q00080227)

If a DNS server is configured from the System→Identity page 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.

NTP broadcast mode error message in event log (Q00093553)

When you configure NTP in broadcast mode, the following error message appears in the event log:

```
NTP [13] bind() fd 55, family 2, port 123, addr 10.118.255.255,
in_classd=0 flags=1 fails: S_errno_EADDRINUSE
```

You can ignore this message. It appears when broadcast packets (one for the interface address and one for the management IP address) are sent out on two logical interfaces connected to the same LAN.

Changing NAT traversal parameter while session connected (Q00081099)

If you change the NAT traversal parameter for a group from allowing NAT traversal to not allowing it, while a session is connected with a user login that is in the group, the session stops when the next rekey occurs. If you change the encryption type (3DES to DES 56) or compression (enabled to disabled) in the group, these changes have no effect when a rekey occurs.

NAT traversal with UDP port number change (Q00081100)

If you change the UDP port from the Services→IPSec screen when using NAT traversal, you should receive a warning message that sessions will be disconnected. However, this message does not appear.

Removing DNS domain name with DNS server (Q00046262 & Q00046267)

If the Primary DNS Server Address is specified on the System→Identity screen, you cannot delete the DNS Domain Name. The error message `DNS Domain Name Error: The primary DNS server is specified` appears. However, if you modify the DNS domain name, you do not receive this message. Once it is changed, you cannot point to the switch through the DNS host name. This problem occurs on both the GUI and the CLI.

Inactive PPP connection through LMC 1200 board (Q00020224)

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 switch's System→WAN page. Select the Statistics button for the interface.
2. On the Statistics page, 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 switch, wait a few seconds, and then power it back on.

Branch Office support for state and cost (Q00049775)

You can share state and cost in Branch Office→Accessible Network→Remote Endpoint with previous versions through LDAP. For example, Version 3.60 can read the LDAP file from Version 4.0 or higher. If new remote endpoints are updated through the V3.60 switch, the state and cost information is lost. Nortel Networks recommends that you do not share an external LDAP server between different versions of the Contivity VPN Switch.