Version 2.00

Part No. 317522-A Rev 00
December 2003

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity 221 VPN Switch Release Notes

NORTEL NETWORKS™

Copyright © 2003 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* VPN Switch Version 2.00.

Before you begin

These release notes are intended for network managers who are responsible for the Contivity 221 VPN 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 192.168.1.12`**
`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 221 VPN Switch, 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.
- *Contivity 221 VPN Switch Quick Start Guide* introduces the product and provides information about initial setup and configuration.
- *Configuring and Troubleshooting the Contivity 221 VPN Switch* provides compete information about installation, configuration, administration, and troubleshooting.

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

Technical Solutions Center	Telephone
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

These release notes contain the latest information about the Nortel Networks Contivity 221 VPN Switch version 2.00.

Refer to your *Configuring and Troubleshooting the Contivity 221 VPN Switch* 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.

Nortel Networks CD

Doc (Documentation) directory

The doc directory contains the documentation set for the Contivity 221 VPN Switch. The guides are provided in Adobe Acrobat PDF format.

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 2.00 release of the Contivity 221 VPN switch.

Fixed in this release

As this is the first software release for the Contivity 221 VPN Switch, there are no fixes to report. In future software releases, this section of the release notes will highlight the fixes that are supported in the corresponding software release.

Product considerations

The following sections discuss product considerations or limitations.

Only one administer login at a time

A user can only either use the WebGUI, telnet or a console connection, but cannot be logged in to any two simultaneously.

Closing a user interface without properly logging out of the Contivity 221, may result in an inability to log back into the system until the previous session times out (maximum five minutes) or the system is rebooted.

Precautions for using email alerting

In the log settings, having the System Errors or Attacks checked under "Immediate Alerts," result in many emails being sent as the system will send an email every time there is an event that does not match a firewall rule. This can result in an email flood to the receiving device.

Cannot add static route in first entry

The first static route entry is reserved for system use and thus is read only.

Configuring the IP address ranges in the VPN setup

When configuring the NAT range in a VPN rule, you must configure the actual range and not subnet mask.

Configuring VPN tunnel with multiple VPN tunnels established

When multiple VPN tunnels are already established and passing traffic and you try to configure another VPN tunnel, some packets may be dropped while the Contivity 221 is savng the configuration.

Configuring Multiple DNS Servers

Configure DNS servers that are accessible through a VPN tunnel first in the priority order on the DNS server page.

Asymmetric Branch Office Tunnels

Contivity ABOT tunnels are Aggressive mode tunnels. Be sure to configure tunnels to be used for ABOT as Aggressive mode in the Contivity 221.

Documentation notes

None to note at this time.

Known anomalies

Unable to set SA Idle timer from the WebGUI (Q00789921)

Currently, the SA idle timer for tunnel on the Contivity 221 is set to disabled. This timer is based upon inbound traffic and can be used to remove SA's after a certain period of inactivity, if desired. This timer affects both Branch Office (on demand) and Client emulation (manual) tunnels. For Client emulation tunnels this will cause the user to select the "Connect" button to reconnect. It is recommended that this be used for Branch Office tunnels only where automatic recovery is required in the event of a central site device failure. The Client emulation feature allows for keep-alive configuration that will remove the SA if the central site device fails.

In order to enable this, the user must go through the following steps:

- Connect to the SMT menu via Telnet or the Console Port
- Select option 24 "System Maintenance"
- Select option 8 "Command Interpreter Mode"
- At the CLI prompt, invoke 'ipsec timer chk_input <time_in_minutes>'

N.B: the default for <time_in_minutes> is 0 (disable)."

Cannot escape from error message (Q00759278)

While configuring the Dial Backup feature with the current software release, if there is a Dial Backup Call Control value error, an error message comes up on the screen, but there is no OK or Cancel button. To proceed simply close the window and continue. Any changes made on this menu not saved before the error will not be saved.

WAN priority (metric) does not save (Q00737553)

When changing the WAN priority (metric) using the WebGUI, it is necessary to also put in the WAN IP address in order for this menu to save. If you do not put in the WAN IP, it will say that the setting has been saved, however when you go back to the menu, the setting will revert back to its previous setting.

Apply Trigger port entry with blank name, says OK but isn't saved (Q00785724)

If you specify a Trigger Port table entry that has valid incoming and trigger port ranges but has a blank name, and then you Apply, you get a "configuration updated successfully" message. However, if you leave the tab and then return to the table, the entry is gone.

Static routes added via CLI is not displayed the WebGUI (Q00770700)

If static routes are added via CLI may not display in the WebGUI static route page.

Content Filter keyword limit error (Q00780399)

The maximum character length for key words entered into the content filtering list is 31, but the Help reports 64 chars and the entry field will allow 127 character (but will only save the first 31 charactes).

Default gateway configuration issue in SMT (Q00737589)

The Default Static Route (0.0.0.0/0.0.0.0) is reserved for use by the WAN interface. The WebGUI protects against creating a default route entry in the Static Route Table, but this is not protected in the SMT menu. If you create a default static route via the SMT, this will result in connectivity problems when you modify any of the WAN configuration parameters. Non-Default Route Static Route configuration works fine.

Default gateway is reserved for Table index #1 (Q00737604)

The Contivity 221 reserves the first entry in the IP Static Route table for use by the WAN configuration screens. When defining static routes, start adding them in entry #2 of the Static Route Table; this should be followed even if Entry #1 is blank. If a Static Route is added in Entry #1, any subsequent configuration changes within the WAN screens will over write Entry #1.

Changing WAN encapsulation type MAY effect LAN remote subnet connectivity if default route is used on LAN (Q00755252)

The Contivity 221 reserve the first entry in the IP Static Route table for use by the WAN configuration screens. When defining static routes, start adding them in entry #2 of the Static Route Table; this should be followed even if Entry #1 is blank. If a Static Route is added in Entry #1, any subsequent configuration changes within the WAN screens will over write Entry #1.

Configuration cannot be save using Netscape (Q00765988)

While managing a Contivity 221 with a Netscape Browser, you are unable to save the configuration file via the Backup button under the Configuration Tab within the Maintenance WebGUI screen. The workaround is to use the Xmodem functionality via the SMT menu screen. Internet Explorer does not exhibit this issue.

Phase 1 and Phase 2 SA lifetimes must match(Q00769514)

Within the VPN-Branch Office-Advanced page, do not configure the Phase 1 SA Lifetime to be a different value than the Phase 2 SA Lifetime. Configuring these values to be different numbers can result in periodic outages of your tunnel equivalent to the difference between these 2 lifetimes.

SNMP and Trap can't be configured from WebGUI (Q00777190)

In order to configure SNMP and Traps, you must use the SMT menu. Configuration of these parameters is not presently available via the WebGUI.

At the main SMT menu, select 22 (SNMP Configuration) to configure SNMP and Traps.

SUA Server ports cannot include port 1026 (Q00778521)

Port 1026 cannot be used when configuring Port Forwarding via the SUA/NAT SUA Server section. You can define two ranges, up to 1025, and then starting with 1027 on upwards, but you will not be able to configure a range that includes port 1026.

VPN Remote networks do not appear in the routing table (Q00778963)

Remote networks specified in the Branch Office - IP Policy screen are not advertised by the Contivity 221 via RIP, and they are not included in the Contivity 221 Routing Table. They can be viewed using the following SMT command:

C221> ipsec show spd

Traffic crosses the tunnels and forwarding to these remote networks works fine.

Domain names added to Content Filters cannot have spaces (Q00786225)

When configuring Content Filters, you cannot list a domain that has spaces. The Contivity 221 only checks the Domain part of the URL. In order to check a full URL, you must enable directory and file checking. Any space within a file name must be filled in with a %20.

WebGUI incorrect when WAN interface changed to DHCP (Q00790762)

When you receive the Default Route via DHCP on the WAN interface, the WebGUI will not display the Default Route in its Static Route Table. Also, if you change your WAN interface from a Statically defined IP Address to DHCP, the old statically defined Default Route will still be present in the Static Route Table page in the WebGUI.

This is purely a cosmetic issue, the proper routes are inserted into the devices routing table, and traffic is properly routed via the correct default route.

CVC emulated tunnel tear down (Q00791160)

When using Client Emulation mode on the Contivity 221, the recommendation is that you do not configure a re-key value on the remote Contivity of less than one hour.

"-" can't be included in the User Name field in WAN setup (Q00782127)

You cannot use the character "-" in the User Name field when configuring the WAN interface.

Filter configuration for IP Alias is needed on WebGUI (Q00777264)

You cannot configure Incoming/Outgoing protocol filters for the IP Alias via the WebGUI on the Contivity 221. You will need to configure this via the SMT Menu.

Choose 3 (LAN Setup), 2 (TCP/IP and DHCP Setup), Toggle Edit IP Alias to be true, Enter, then you are brought to the IP Alias Setup menu where you can configure the Incoming/Outgoing Protocol filters.