Version 4.90

Part No. 315000-F Rev 00
April 2004

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Secure IP Services Gateway Release Notes

NORTEL NETWORKS™

Copyright © 2004 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, and Contivity are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

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

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

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

Netscape, Ntescape Communicator, Netscape Directory Server, 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 **7**

Before you begin 7
Text conventions 7
Related publications 9
Hard-copy technical manuals 10
How to get help 10

Chapter 1
Overview **11**

Version 4.90 feature summary 12
Version 4.85 feature summary 17
Nortel Networks CD 20
Doc (Documentation) directory 20
Tools directory 20
Restricted product - export license requirement 20

Chapter 2
Considerations and issues **23**

Version 4.90 Considerations 23
General product considerations 24
Documentation notes 33
Failover using DNS remote end-point for ABOT 34
MIBs and OIDs documentation 35
Known anomalies 35
Customer issues fixed in this release 35
General anomalies 36
ADSL anomalies 38
DNS anomalies 39

Security anomalies 39
Show running config (SRC) anomalies 39
Tunnel anomalies 40

Preface

These release notes contain the latest information about the Nortel Networks* Contivity* Secure IP Services Gateway Version 4.90.

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 TunnelGuard for the Contivity Secure IP Services Gateway* provides information about configuring and using the TunnelGuard feature.
- *Configuring Authentication and Certificates for the Contivity Secure IP Services Gateway* provides instructions for configuring authentication services and digital certificates.
- *Configuring Firewalls, Filters, NAT and QoS for the Contivity Secure IP Services Gateway* provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- *Configuring Advanced Features 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 inter operability 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.

Hard-copy technical manuals

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.

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 Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

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 4.90 release contains the latest information about the Contivity Secure IP Services Gateway.

Refer to your Contivity hardware installation guide for instructions on getting your Contivity 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. When you click on the Help menu from the UI on the Contivity 1010, 1050, and 1100 systems, you can enter the location of the help files on the CD or on a server.

Version 4.90 adds the following capabilities that were available in version 4.85, but now ships with the Contivity gateway for the first time. These features include:

- Configurable MTU and configurable TCP/MSS clamping
- Packet capture
- Diffserv-based ingress traffic conditioning controls

Version 4.90 also provides a complete series of new WAN interface cards, as well as new client and server software features. These features include:

- ADSL PCI option card
- 1000BaseSX PCI option card
- 1000BaseT PCI option card
- Contivity Security Accelerator (CSA)
- AES client support
- 802.1Q VLAN routing
- Serviceability enhancements

Support considerations for Version 4.90 include:

- Supported platforms include the Contivity 1010, 1050, 1100, 600, 1600, 1700, 1740, 2600, 2700, 4500, 4600, and 5000.
- New I/O modules will not be supported on all systems, (see I/O Matrix).
- The Contivity 1010 and 1050 do not have I/O option slots.
- The Contivity 1010, 1050, and 1100 require a 64 M/byte flash drive and 128 M/byte of memory.
  - — All systems were upgraded as of Version 4.80 out of the factory on July 2003.
  - — Any system with the quiet fan has 64/Mb flash.
  - — Flash must be pre-programmed with Contivity image so retail off-the-shelf flash cannot be used.

Version 4.90 feature summary

The following sections describe features that are new for Version 4.90.

ADSL Option Card

Version 4.90 introduces an ADSL option card that is supported on the Contivity 1100, 600, 1700, 1740, 2700 and 5000. The ADSL card is a ½ height card that can be used in slot 3 on an 1100. The card supports ITU G.922 standards for ADSL over analog and ADSL over ISDN. The Annex B variation of the ADSL card supports DTAG UR-2 requirements.

Table 1 Maximum ADSL cards supported

Hardware platform	Maximum ADSL cards
600	1
1100	2
1700	2
1740	4
2700	4
5000	5

Functionally the ADSL capability in Release 4.90 supports

- ITU G.992.2 (G.Lite).
- ITU G.992.1 Annex A.
- ITU G.992.1 Annex B.
- ANSI T1.413 Issue 2.
- DSL Forum document TR-042 ATM Transport over ADSL.
- Support splitter operation as described in G.992.1 and G.992.2, as in a splitter between the ADSL and the Telco network in order to split analog voice or ISDN away from the ADSL signal. One output from the splitter goes to the analog POTS equipment or ISDN equipment the other goes to the Contivity ADSL card. Splitter not provided by Nortel.
- ATM AAL5 over ADSL.
- ATM UBR Class of Service.
- Support a single ATM VC (VCI/VPI).
- VPI/VCI user-configurable, default 0/32.
- RFC 2364 PPP over AAL5.
- RFC 2684 Multiprotocol Encapsulation over ADLS (MPoA) Routed encapsulation.
- Contivity gateway QoS capabilities available as of Version 4.80, legacy forwarding, bandwidth management and Diffserv.
- Support British Telecom SIN 329 broadband IP products requirements for end user NTE equipment, where the router and ADSL modem functions are both integrated into the Contivity gateway.
- Support for Deutsche Telekom U-R2 interface specification.
- ADSL over ISDN circuits.
- PPPoE is the only protocol that supports RFC 2684 bridged mode.

1000BaseSX and 1000BaseT Option cards

This is the release of two different Gig-Ethernet cards that can be supported in a Contivity platform. The 1000BaseSX provides a short haul fiber optic PHY using an LC type connector. The 1000BaseSX card is capable of supporting segments up to 550 Meters (1800 feet) using multimode fiber cables. The 1000BaseSX card operates over 1000Mbps link speeds only.

The 1000BaseT card supports 10/100/1000 Mbps Ethernet rates over Category 5 cables. The card can auto-sense the link rate. The functionality of the 1000BaseT card is identical to that of the on-board 1000BaseT port on the Contivity 5000.

Up to a maximum of 2 Gigabit Ethernet cards can be supported in any of the Contivity 1740, 2600, 2700, 4600 or 5000 platforms. With the 1000BaseT port in base 5000, up to 3 Gigabit Ethernet ports can operational on a Contivity 5000.

The existence of multiple Gigabit Ethernet Interfaces on a Contivity platform does not imply 1000Mbps throughput between Gigabit interfaces on the same Contivity. Gigabit Ethernet Interfaces are being provided in order to provide connectivity between Contivity and Gigabit LAN switches. Refer to 4.90 design guidelines for detailed performance characteristics of the various Contivity systems. The 4.90 design guidelines will be available approximately 1 quarter after the release of 4.90.

Contivity Security Accelerator

Contivity Security Accelerator (CSA) is the next generation hardware accelerator for Contivity platforms. The new capability unique to the CSA card are hardware assist for Security Association establishment and Advanced Encryption Standard (AES) can now have a hardware assist. The CSA is based on Hifn 7854, and supports Advanced Encryption Standard (AES) algorithm. The CSA provides acceleration of Security Association establishment, and speeds up tunnel establishment.

Contivity provides an automated load balancing technique to share the encryption/ decryption load between software based and hardware based services. The performance of the system is optimal when utilizing the automated load balancing.

CSA performance

- Boost to 3DES throughput, ~380Mbps on Contivity 5000.
- Approximately 25% improvement for AES over software only and greater when compressed.
- When running high tunnel counts, allows the Contivity gateway to manage load balancing between hardware and software encryption.

- CSA card is offered as a base element of the Contivity 5000 or as an option for the Contivity 4600, 2700, and 1740. The Contivity 5000, 4600 and 2700 can support up to two CSA cards. The Contivity 1740 can support a single CSA card. The first generation hardware accelerator, known as the “Hardware Accelerator” card will continue to be available either as an upgrade or as a base element of the Contivity 5000.

AES Client

Advanced Encryption Standard (AES) is a FIPS approved cryptographic algorithm providing stronger security and greater computational efficiency than the commonly used 3DES algorithm. AES offers longer key lengths than DES and 3DES. While 3DES provides adequate security and is approved for most if not all security applications, AES is widely deployed within the VPN market. Up until now Contivity has offered AES for branch office tunnels but not for user tunnels.

Contivity 4.90 in conjunction with Contivity VPN Client (CVC) version 4.91 provide support for client tunnels using AES. The AES client tunnels can also operate in 256-bit mode in addition to 128-bit. Branch Office Tunnels will continue to be supported at 128-bit level at this time.

The server can also support third-party clients that also support AES. Version 4.90 has been verified with Safenet Softremote and Certicom Movian

DNS Enhancements

Starting with release V04_90, Contivity allows for VPN DNS and Round Robin DNS. VPN DNS provides the ability for IPSec ABOT tunnels, on Contivity, to be configured to use the DNS name of a remote peer rather than the IP address. Consider a situation where a Contivity Initiator from the Branch Office brings up a tunnel to Contivity Responder in Central Office. Without the VPN DNS, the initiator needs to know the IP address of the responder and must reconfigure the address every time address changes. With VPN DNS, the initiator can refer to the remote side by its name, thus when IP changes no reconfiguration on the initiator site is required. This reduces the configuration time and simplifies the management. Contivity VPN client already supports this feature and now the client may use Contivity's domain name when bringing up IPSec user tunnel.

Round Robin DNS is used in IP networks to provide a form of load balancing/ failover. Services on the Internet typically have more than one server that is public facing to share the load. Each of these servers has a unique IP address, but shares a common DNS name. A DNS server will be aware of all the IP addresses that correspond to a particular domain name. When a user requests a lookup for that domain name, the DNS server will provide all the known addresses in a random/ round-robin order. The user can now pick one of the addresses to communicate with the service. The Contivity gateway always uses the first address from the list. If the first address is unresponsive, the Contivity gateway performs a new query. A variety of simple load balancing and failover scenarios can be implemented based on this round robin behavior of the DNS servers.

802.1Q VLAN Routing

Release 4.90 provides 802.1Q VLAN Routing Phase 1. 802.1Q is an IEEE standard for tagging of Ethernet frames for the purpose of logically segmenting LAN traffic at OSI Layer 2. Most all LAN switches support 802.1Q tagging, which allows the switch to segment traffic by 802.1Q tag IDs. The Contivity gateway routing provides VLAN to VLAN connectivity.

The specific feature details are:

- Support for routing between Subnet-Based VLANs fits into the IP Services and IP Layer applications focus of the Contivity devices.
- Support for 802.1Q Tagging on Fast Ethernet and GigE interfaces
- Tagging on public and private interfaces
- Static, RIP and OSPF routing per VLAN
- 802.1P static mapping to/from Diffserv Code Points
- Uses Nortel Networks mapping defaults - supported in BayStack, Passport etc.
- Ability to turn mapping on or off
- 6 VLANS per interface on “branch” site Contivity, i.e. 1000 series and 600
- 20 VLANS per interface on “HQ” site Contivity, i.e. 1700……5000
- Tunneling over VLANs
- Statistics per VLANs
- DHCP per VLAN

Serviceability Enhancements

Version 4.90 delivers two principle NNCLI enhancements: configurable CLI prompt and user-friendly mode for the show running config command. The configurable CLI prompt allows you to modify the standard CLI prompt from CES > to a 32-character ASCII string of your choice.

User-friendly show running configuration is a mode that can be typed into the show running configuration parameter to provide a clearer description of the information presented in show running configuration. The output from user friendly show running configuration can not be used to provision the Contivity, it is intended for users that are trying to check a section of their configuration or troubleshoot a system.

Version 4.85 feature summary

The following sections list Version 4.85 features that have been included in Version 4.90.

Configurable MTU and configurable TCP/MSS clamping

Networking is the transmission of information packets between two network attached entities. All the various network mediums (Ethernet, Frame Relay etc.) have restrictions with regard to the minimum and maximum size of packets. Although these issues can apply to any protocol type, these new tools are commonly required in a PPPoE environment.

These tools allow you to control packets sizes transmitted and to provide tuning efficiency to avoid issues in the Internet where certain downstream networks may mishandle or drop large packets. Configurable MTU provides the network manager with the ability to set the MTU to the optimum value for their environment.

When two network attached entities establish a TCP session, one of the parameters that are exchanged is the Maximum Segment Size (a.k.a. MSS), in most cases the MSS value is 1460 bytes, the Ethernet maximum adjusted for IP and TCP headers. This MSS value becomes the largest packet size that the entities will use during their communication session. The end stations are unaware of any

packet size restrictions that may exist between themselves, or any additional overhead that may be applied by network devices such as IPsec and or PPPoE headers. The TCP MSS/Clamping tool allows the Contivity to intercede in the MSS exchange between peers adjusting the MSS value to predetermined value.

Configurable MTU/MSS clamping features include:

- Egress packet size (MTU, Max Transmission Unit) configurable for interfaces and VPN tunnels.
- Default behavior for tunnel MTU is enabled at 1788 bytes.
- Interception and adjustment of negotiated packet size for the TCP session per interface. When enabled, the TCP MSS value is derived from the interface MTU. This value can also be configured.
- Provides a configurable option for DF (Don't Fragment) bit value to be set, copied, or cleared. When enabled, the TCP MSS value is derived from the interface MTU. This value can also be configured.
- Compliance with Path MTU Discovery Router Specification (RFC1191) for sending ICMP message with correct MTU value when dropping packets due to MTU Too Large And DF Set.

Packet Capture

Packet capture is a utility in Contivity that allows a network administrator to capture packets moving through Contivity to a file. The purpose of the tool is to assist network administrators in trouble shooting remote networks. The network administrator configures PCAP filters on the Contivity to trigger what types of packets they desire to capture. The captured packets are written to a file on the Contivity FLASH or hard disk in the form of a TCPDUMP/LIBPCAP format. The file can be read using Ethereal (http://www.ethereal.com/), or similar tools that can read a TCPDUMP format.

In order to avoid security concerns of a hacker gaining access to the PCAP utility, some particular constraints have been placed on the configuration and use of PCAP in Contivity.

PCAP must be enabled through physical access to the com port. It only needs to be enabled once; captures can be started and stopped remotely using CLI. When the PCAP feature is enabled, the user must configure a PCAP password. The PCAP password is used to encrypt the captured packets file. When the file is transferred off the Contivity, the PCAP password is required to decrypt the file. The PCAP password can only be configured through physical access to the com port.

Diffserv Based Ingress Traffic Conditioning Controls

One of Contivity's Quality of Service features is traffic conditioning. Traffic conditioning uses a three color marker to police traffic rates (see RFC2697 for background on three color markers). With Release 4.85, Contivity now has the option to either mark or drop traffic for all supported Diffserv Code Points based on a bandwidth profile per Diffserv Code Point.

Traffic conditioning with Contivity allows the user sets a bandwidth policy in bits per second for tunnels, interface level ingress traffic. The bandwidth policy is applied against traffic classes based on Diffserv Code Point. For example you might want the Contivity to insure that 100Kbps be available to EF traffic.

Contivity supports CS7 (network control traffic), EF, AF4, AF3, AF2, AF1 and DF (best effort) Diffserv per hop behaviors. In previous releases of Contivity the user was able to configure a rate at which the traffic received against a particular per hop behavior was considered excessive. The configurable items were the rate and the action, where the only action was mark. This feature adds the ability to set the action to either mark or drop for all the supported per hop behaviors. If the action is set to mark, any traffic that is received outside of the bps profile will be marked with green (in profile) or red marker (outside profile). If the egress port is experiencing congestion, the packets marked with red will be dropped until the congestion situation eases. If there is no congestion at the egress port, the Contivity scheduler will send red marked packets. If the action is set to drop, any traffic received outside of the bps profile will be immediately dropped by the Contivity. This drop capability is useful if the user wants to guarantee that a particular traffic class (by per hop behavior) does not exceed a particular bit-per-second rate. This capability could be used to guarantee the egress bandwidth availability to a particular application or applications.

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_90.264 contains the Nortel Networks Contivity Secure IP Services Gateway software. It also contain the V04_90.264.tar.gz file. You would use this file 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.

Tools directory

The tools directory contains the Java* subdirectory, which contains the installation files for the Sun Microsystems* Java Runtime Environment (JRE) Version 1.4.1_02. 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 4.90 release of the Contivity Secure IP Services Gateway.

Version 4.90 Considerations

ADSL Considerations

The asymmetric nature of ADSL means that the downstream data rate is approximately 10 times greater than the upstream rate. The data rates are specific to the physical environment and can vary accordingly. Because of this, PPP keep-alive packets may be lost when the low-speed ADSL upstream receives a large number of data packets from FTP sessions. You can adjust the keep-alive parameters to minimize the keep-alive packet loss.

802.1Q Considerations

- DHCP client/server and firewall are not supported over 802.1q VLANs for this release
- We do not support 802.1Q over fast ethernet interfaces that have the Intel i82557 chip set. You get a configuration error if you attempt to enable 802.1Q on interfaces with these chipsets (the ethernet device information under System->LAN->Statistics has information on what chipset is used on the interface). The 82557 10/100 PCI card was used in the Contivity Configurable MTU with Bay RS and Contivity. If you are having problems configuring OSPF adjacency between a Bay RS router and a Contivity system, be sure that the MTUs match.

Configurable MTU / MSS clamping considerations

- For Tunnels, the tunnel MTU can be configured or derived from the interface MTU. The tunnel adjusts for encapsulation so that the packets in the tunnel are not larger than the MTU. By default, configured tunnel MTU is enable at 1788
- IPSEC DF Bit in the outer IPSec header is determined from the configuration. The original DF Bit is stored in and used if COPY is specified.
- PMTUD (Path MTU Discovery) should be disabled on Solaris workstations. Their non-standard implementation of PMTUD causes issues with the Contivity gateway, BayRs, Passport and Cisco. To disable Solaris 8 (and previous versions):

```
$ ndd -set /dev/ip ip_path_mtu_discovery 0
Set Maximum MSS to 1460:
$ ndd -set /dev/tcp tcp_mss_max 1460
```

- There is an issue when the tunnel peer is on a V04_80 or earlier Contivity gateway and the firewall is enabled and tunnel compression is ON and packets larger than 1540 bytes are transferred. There is an issue in the V04_80 and earlier that only decompresses packets up to 1540 bytes. The solution is to set the tunnel MTU to 1540 bytes or less.
- OSPF now uses the interface MTU in DD packets as specified in RFC 2178. You may have to adjust interface MTU values to create an adjacency.
- When using Windows 2000 or Windows XP, some Web sites may be unreachable when connected to a Contivity gateway via L2F tunnels (dial access). The work around is to enable the TCP MSS option and lower the TCP MSS value to 1400 from the default.

General product considerations

The following sections contain general considerations for this product.

Upgrade Procedure Considerations

- The Contivity 1010, 1050, and 1100 require 64 Mb flash disk.
- Version 4.90 supports upgrades from Versions 4.50, 4.70 and 4.80. If you are running an older version, you may have to upgrade to a later version before you upgrade to Version 4.90.

- The amount of disk space required to upgrade to the latest version is configuration specific. If you receive disk space error messages, you need to remove any unnecessary files from your Contivity system.
- Any recovery floppy diskette that you created prior to release Version 4.0 will not work on a system that runs Version 4.0 or later software.
- Nortel Networks recommends that when you upgrade to Version 4.90 software, you create a recovery floppy diskette as soon as you complete the upgrade. You must use a formatted diskette when creating the recovery diskette

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.

Backing up your configuration

The automatic backup feature is provided as a way to backup your current configuration on the Contivity for later restoration. It functions by saving all of the contents of the Contivity file system from the /ide0/system point down. The contents of the flash memory are not saved as part of this process.

Monitoring hard disk usage

Monitor the amount of space remaining on the hard disk drives; a full file system will produce unexpected behavior. To check the hard disk usage level, choose Status > Health Check. Because log files can consume a significant amount of disk space, especially in large configurations, remove old log files periodically.

Viewing and calculating memory usage

The minimum memory requirement for Version 4.90 is 128 MB. 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 4.90. Contact your Nortel Networks sales representative if your configuration requires additional memory. The Memory Calculator tool is available at:

www.nortelnetworks.com/documentation

Scroll to Contivity Secure IP Services Gateways Portfolio, click on the Documentation link, and select Contivity Memory Calculator V4.90.

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

Software and hardware compatibility

The minimum Contivity VPN Client version that is supported by Version 4.90 is 4.65.

Table 2 shows Contivity Secure IP Services hardware and software compatibility. An X in the table indicates which platforms support this version of the Contivity gateway software.

Table 2 Hardware platform and server software compatibility

Hardware platform	**4.50 4.55_120 9/11/02 12/09/02**	**4.70 4.75 12/20/02**	**4.76 5/23/03**	**4.80 8/08/03**	**4.90 05/04**
1010		X	X	X	X
1050		X	X	X	X
1100		X	X	X	X
600	X	X	X	X	X
1500					
1510					
1600	X	X	X	X	X
1700	X	X	X	X	X
1740				X	X
2000	X				
2500	X				
2600	X	X	X	X	X
2700	X	X	X	X	X
4000	X				
4500	X	X	X	X	X
4600	X	X	X	X	X
5000			X	X	X

Load-balancing and hardware encryption accelerator cards

When one or two optional hardware encryption accelerator cards are installed, Contivity software tries to ensure optimal tunnel throughput by balancing tunnels across available system resources, that is, the CPUs and the hardware encryption accelerator cards. Several parameters, such as the number of active tunnels and the current load on the resources, are evaluated during new tunnel establishment or rekeys to determine the assignment of a new tunnel.

After a tunnel has been assigned to a hardware encryption accelerator card or to the CPU, the gateway does not dynamically reassign the tunnel to a new resource due to the dynamic nature of the load balancing algorithm. Therefore, you may see some tunnels assigned to software (to a CPU) even if there are hardware encryption accelerator cards available.

Legacy option cards not supported in Contivity 5000

The Contivity 5000 does not support the following legacy option cards (neither of which is now sold):

- Ethernet LAN cards with the 82557 and 82558 chip sets
- Original Contivity hardware encryption accelerator card (order numbers DM0011041 and DM0011042)

The Contivity 5000 supports the following option cards in slots 3, 4, and 5 only:

- HSSI WAN option card (order numbers DM2104003 and DM2111003)
- Dual V.35 option card (order numbers DM2104001 and DM2111001)

General support considerations

General support considerations include the following:

- Support of E1 functionality on both the LMC1200 (current single port T1 card) and the Quad T1/E1 card will not be included in this release. Both of these will be supported in Version 5.00. Any references to either of these in the documentation should be ignored for this release.

- The output generated by the CLI command show running-config (SRC) does not always produce usable scripts that can be applied directly to provision a Contivity gateway. This applies both to the use of SRC within an affected software version and across versions. You should not use the output from SRC without inspection and if necessary, editing and reordering the output to provision a Contivity gateway. For further information about SRC, see Reference for the Contivity Secure IP Services Gateway Command Line Interface.
- Version 4.90 does not support ExtNetIP as the console menu replaces this function. The ExtNetIP.exe file has been removed from the Tools directory.
- GigE fiber and copper cards will not fit into the connector on slot 4 on the Contivity 4600.
- The Contivity gateway does not currently support Chap authentication on ISDN interfaces.
- If more than approximately 10 CMP enrollments occur at the same time, the administrative functions of the Contivity gateway (GUI/CLI) may be non-responsive for short periods of time.
- Version 4.90 supports upgrades from Versions 4.50, 4.70 and 4.80. If you are running an older version, you must upgrade to a supported version before you upgrade to Version 4.90.
- The amount of disk space required to upgrade to the latest version is configuration specific. If you receive disk space error messages, you need to remove any unnecessary files from your Contivity system.
- Any recovery floppy diskette that you created prior to release Version 4.0 will not work on a system that runs Version 4.0 or later software. Nortel Networks recommends that when you upgrade to Version 4.0, 4.50, 4.70, 4.80 or 4.90 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 4.90. You must use a formatted diskette when creating the recovery diskette
- Windows 95 does not support JRE 1.4.1_02 and therefore, Version 4.70 and subsequent releases do not support running the UI on Windows 95.
- Shasta Server Farm is not supported by Version 4.90.
- The Contivity UI and CLI support only 7-bit ASCII characters.
- The Contivity works with all RFC-compliant FTP servers.
- The Contivity supports the current version and generally the two previous versions of the Contivity VPN Client. If you have any concerns, contact Nortel Networks support organization for the latest information.

- If you are using a Linksys Etherfast Cable/DSL router in IPSec passthru mode, and if two or more PCs connect through it to a 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.
- The Contivity Stateful Inspection Firewall Java UI requires Version 1.4.1_02 of the Java Runtime Environment for proper operation. The JRE 1.4.1_02 is distributed with the Contivity Secure IP Services Gateway image; it can also be downloaded from Sun Microsystems, Inc.
- 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.
- If you are currently running Contivity Secure IP Services Version 4.70 with NAT policies applied to branch offices, the policies will appear as read only in the Version 4.80 or later Java GUI. You will see an (old format) text message to alert you to the change. The Version 4.70 policies are translated, but you can no longer edit them. If you want to edit a Version 4.70 policy or use the CLI show running config command to export the NAT rules, you must launch the Java GUI, select the (old format) policy, select copy and save as, and apply the new policy to the branch office
- When you upgrade to Version 4.80 or later, the RADIUS service is disabled by default even if it was previously enabled. If your configuration is using RADIUS, be sure to re-enable RADIUS service after upgrading
- 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.

- 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

Browser considerations

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.

- The off-line help stored on local computer cannot be accessed from the links in the help page due to security constraints which are implemented in Netscape 4.1 or higher and Internet Explorer 6.0 SP1 which have hotfixes. regarding this issue. (Q00818628) There are two workarounds;
  - — Add the site to the trusted zone of IE
  - — Add machine name to the URL
- 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.
- Netscape 4.79 incorrectly does not prevent users from launching multiple copies of Contivity Firewall Configuration tool. If you click on the Manage Policies button twice or more without waiting for the configuration tool to appear, multiple copies of the tool will be launched and lead to runtime errors. If this happens, you must close all active browser windows and start a new management session.
- When using certificates, Netscape Communicator and Internet Explorer perform various and differing security checks. The following configuration is recommended to obtain the best performance when administering the Contivity gateway securely using Admin SSL.
  - — Make an entry in the hosts file corresponding to your Contivity management IP address.
  - — Import the root certificate that issued your Contivity server certificate into your browser store.
  - — Import the root certificate that issued your Contivity server certificate into your JRE.

- To satisfy a further name check by Netscape browsers, the Contivity server certificate common name (filled in when you create the certificate request on System > Certificates > pkcs#10 certificate request) should be either a DNS name that resolves to the management IP address or the management IP address. For further information about Netscape certificates, go to http:/ home.netscape.com/eng/security/comm4-cert-download.html.
- Using Internet Explorer Version 6.0.2800.1106IC on Windows NT 4.0, the GUI presents inconsistent information in firewall java section.
- If you launch two Java applets from one Web GUI session on the same PC, it can cause inconsistencies with firewall policy rules.

Tunnel considerations

- Testing a branch office tunnel might fail if the tunnel is being initiated from both sides at the same time. This occurs when the initiation is due to live traffic or a test button tunnel initiation.
- For nailed-up connections, the IPSec SA may go down due to inactivity. Only the ISAKMP SA stays up all of the time.
- PPTP and L2TP MPPE 128-bit encryption keys do not work properly in the Contivity 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
- The following tunnel licensing options are available for the Contivity 1010, 1050, 1100, 1700, and 2700:
  - Base unit (low-cost router option) supports five tunnels. You can upgrade the license to support the maximum possible number of tunnels for the Contivity model.
  - VPN bundle option supports the maximum number of tunnels for the Contivity model.

- Table 3 lists the maximum number of tunnels for each Contivity model and indicates whether each model has a five-tunnel base unit version.

Table 3 Maximum number of tunnels by Contivity model

Contivity model	Maximum number of tunnels	Five-tunnel base unit available? (Yes/No)
1010, 1050, 1100	30	Yes
600	50	No
1700, 1740	500	Yes
2700	2000	Yes
4600	5000	No
5000	5000	No

Certificate considerations

VeriSign certificates use a unique e-mail identifier that is different from Microsoft and Entrust so you must use the full subject distinguished name when configuring branch office connections authenticated using certificates.

- All characters of the certificate subject and issuer DN are case insensitive. The subject DN o=nortel is considered equivalent to o=Nortel. This complies with RFC 3280 4.1.2.4 and 4.1.2.6.
- When a user enters a full DN, the order of the individual components is no longer important because Contivity stores it in a predetermined order. For example, if you enter the DN of cn=joe, ou=contivity, o=nortel, c=us, this is viewed by the Contivity as identical to: ou=contivity, o=nortel, c=us, cn=joe Rearranging the order allows the Contivity to correctly process certificates generated by CAs with differing DN encoding orders.

Documentation notes

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

Failover using DNS remote end-point for ABOT

When a responder Contivity gateway that goes down without informing the initiator, the initiator has no way to know it so the session is not deleted on the initiator. The session stays up until it is removed by one of the following:

- Idle-timeout -- If the initiator tunnel is not nailed-up (meaning it is on-demand), the session goes away due to an idle-timeout (default 15 minutes). Another tunnel setup attempt is required on the initiator to detect that the remote end-point is not available. After this failed connection attempt, the initiator forces a new DNS query for the DNS name. The response to this query contains the active responder address as the first IP address in the list (due to the round-robin DNS responses). The initiator then establishes the tunnel and the failover action is complete. The time it takes to idle-timeout depends on the idle time-out setting. The time it takes to attempt a connection depends on when a data packet becomes available. This in turn depends on the type of routing used for the tunnel. With static routing, the tunnel connection attempt depends on data packets. With dynamic routing, RIP or OSPF packets periodically force the tunnel connection attempt. Even though the failover will work, the response time is slower.
- Nailed-up connections -- If the initiator tunnel is nailed-up, it brings down the session because the responder does not respond to keep-alives (or rekeys if the responder is running Version 4.50 or earlier). Once the session goes down, the nailed-up mechanism tries again to bring up the tunnel. After this failed connection attempt, the initiator forces a new DNS query for the DNS name. The response to this query contains the active responder address as the first IP address in the list (due to the round-robin DNS responses). The Initiator then establishes the tunnel and the failover action is complete. The failover response time can change from 15 or more minutes to two or three minutes.
- On-demand connections with keepalive enabled -- If the initiator tunnel is on-demand and if on-demand keep-alives are enabled, the initiator can detect that the remote end is unavailable in several seconds. The standards-based dead peer detection (DPD) allows you to configure the number of missed keep-alives and the retransmission interval. (The responder must be running Version 4.70 or later to support keep-alives.) The failover response time can be brought down to one or two minutes, depending on the settings for the keepalive (which in turn depends on network characteristics).

MIBs and OIDs documentation

For a detailed description of the latest MIBS and OIDs, go to:

`http://www142.nortelnetworks.com/bvdoc/contivity/doc_pdf/mibs.xls`

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.

Customer issues fixed in this release

Version 4.90 contains all known anomalies through Version 4.85.120. Table 4 lists customer issues from previous releases that are fixed in this release.

Table 4 Fixed customer issues

Q00693226	Group level RADIUS authentication server doesn't perform CHAP authentication.
Q00732525-01	Core dump InitSSL.
Q00763937-01	Core dump when using parenthesis for the user name.
Q00764306-01	Core DnCls.cpp:500.
Q00769544	CLI banner-fragment command does not add line feed.
Q00772289-01	BIS ping beyond local broadcast subnet
Q00810153-02	Branch office test automation fails during ABOT test cases between 4.80 and 4.90.
Q00817738	Administrator name can be set by user with manage switch rights.
Q00829151	tPPP takes up 90-99% of utilization on a V.35 card with LCP echo request.
Q00831593	Bad fragmentation makes domain login impossible for Contivity VPN client.
Q00839257	Contivity gateway hangs, when deleting CA certificate with Optimize on.
Q00843158-02	Provisioning running slow.
Q00844593-01	Changes to MTU size on FastEthernet are not retained through reboots.

Table 4 Fixed customer issues

Q00846105-01	When unchecked, Services > Available ICMP on private should drop on private interface.
Q00850854	Core dump when modifying and saving TunnelGuard rule.
Q00854300	Users unable to connect with uncommon DN.
Q00855248	Using a percent sign (%) in the IPSec user ID (UID) causes a core.
Q00857233	If SNMP ALG disabled, traps are no longer sent over branch office tunnel.
Q00858176-01	Output errors increment upon unanswered ARP
Q00861210	Enhancement to increase RADIUS response timeout interval maximum from 10 to 30.
Q00861774	Non-primary administrative users can reset primary administrative user name and password to 0.
Q00862458-02	Serial UI system boot banner copyright includes year 2004.
Q00862694	Certificates unable to use the "-" in the e-mail address when defining the remote
Q00864731	Allow the "@" symbol to be used in the initiator ID of an asynchronous branch office configuration.
Q00870869-01	Compressed IPSec tunnels have MTU interoperability problem.
Q00873373	Need to upgrade to latest version of OpenSSL.
Q00873635	Contivity gateway sends ICMP Need to Fragment packet out o incorrect interface.
Q00885036-01	Tunnel packets not routing to Public Interface with Cfg=Tunnel/Public.

General anomalies

Q00776386 - Factory reset does not reset interface groups

If you set a Contivity 1100 back to the factory defaults, it requires two attempts before the unit is defaulted. The first time the operation is performed none of the settings are defaulted, but the second attempt is successful. This appears to be an intermittent occurrence.

Q00776386 - Fractional T1 interface serial menu

When setting the channel data rate for fractional T1 interfaces, the serial menu allows you to select arbitrary channels. The GUI and CLI require you to specify the first channel to be used (1 through 24) and the interface data rate in kilobits per second (Kb/s) to allocate to this connection (a multiple of 64 Kb/s-that is, 64 multiplied by the number of channels you are allocating). When you use the serial menu, Nortel Networks recommends that you select adjacent channels as required by the GUI and CLI.

Q00818628 - Contivity 1100 off-line Help file links launch incorrectly

The off-line Help stored on a local computer cannot be accessed from the links in the Help page due to security constrains that are implemented in Netscape 4.1 or higher and Internet Explorer 6.0 SP1, which have hotfixes regarding this issue. To work around this issue, either add the site to the trusted zone of IE or add the machine name to the URL.

Q00823565 - Incorrect message on firewall screen

The text hint on the bottom of the firewall applet screen is incorrect. It states, “Bold denotes that the policy is currently applied on the CES. Italics denotes that the policy is read-only.

Q00824093 - CLI Q key does not terminate log scrolling

With Terminal Paging = OFF, the Q (quit) key does not terminate scrolling of event log. Therefore, when log is full, you have to wait until it scrolls all the way through before gaining NNCLI control again.

Q00844301 - Provisioning ISDN interface missing exit command for SRC

When provisioning the ISDN interface using an SRC file, an exit command regarding the ISDN interface is missing.

Q00854946 - CLI updates to access list not applied

From the GUI, when you edit an existing access list it does not become active until you click on Close. When you click on Close, the added routes are removed from the RIP database. CLI does not have a similar function that allows edits to become active without having to bounce RIP.

Q00858553 - PPP Advanced Options 07 & 08

After an upgrade, if the ISDN MPPP Options 07 & 08 were configured to be enabled, they are displayed as DISABLED (False). This is a display issue only.

Q00871910 - ARP timeout feature missing from the GUI

The ARP timeout feature is missing for the GUI. However, it is available through the CLI.

Q00875394 - DHCP server not working after reload

Once the Contivity Firewall has been activated and the Contivity gateway has been rebooted, the DHCP server needs to be restarted to receive a DHCP address.

Q00881465-01 - Upgrade configuration parameter changed from enable to disable

During an upgrade, the “Enable the idle serial connection time out” parameter is disabled on the Admin > Upgrade screen. The upgrade should retain the original value.

ADSL anomalies

Q00865533 - PPPoEoA defaults MTU to 1500

Unlike other PPP interfaces, PPPoEoA, defaults to 1500. It is recommended that you manually set the MTU to 1492.

Q00867202 - No IP address received from service

The MAC CRC field can be set to either excluded or included. The default is included. The correct value depends upon your network configuration. If you have trouble getting an IP address from your ISP, try changing this setting.

DNS anomalies

Q00867485 - DNS server entries in System > Identify show error message

The resolver sends out DNS query packets of PTR type to the configured DNS servers. The resolver waits for a response from the DNS server to mark that server status as operational. If a response is not received from the DNS server before the resolver times out, then the DNS server status is marked as Error. For Win-2000 DNS servers, the reverse lookup zone must be configured for Win-2000 DNS servers to respond to the Contivity gateway (checking the status) within the timeout period.

Security anomalies

Q00822181 - Anti-Spoof should have the option to enable logging

To see the anti-spoofing incidents, you must go to Edit firewall and enable All for logging.

Show running config (SRC) anomalies

Q00829519 - Invalid pre-share key

Text pre-shared key 1234567890 should not be used to configure a static IPSec branch office tunnel. This key will cause an error if SRC is used for provisioning.

Tunnel anomalies

Q00831338 - Cannot change local network on control branch office tunnel

You cannot change the local network on a control branch office tunnel (BOT). If a control BOT with an auto-generated static NAT policy is created, saved, and working and you then disable the BOT and try to change the local network, the following error appears:

```
ERROR: NAT Policy definition is in use. Please refer to the
security log or event log for details.
```

This message is somewhat misleading because the NAT policy is not active (with the BOT being disabled). To change the local network, the entire branch office tunnel needs to be deleted and added again.