Version 4.85

Part No. 315000-E Rev 02
December 2003

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Secure IP Services Gateway 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, 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 19

Before you begin 19
Text conventions 19
Related publications 21
How to get help 22

Chapter 1
Overview 23

Version 4.85 new features 23
Contivity gateway hardware and software compatibility 25
Tunnel licensing 26
Nortel Networks CD 27
Doc (Documentation) directory 28
Tools directory 28
Restricted product - export license requirement 28

Chapter 2
Considerations and issues 31

Fixed in this release 31
Product considerations 34
Number of versions 34
Support considerations 34
Monitoring hard disk usage 35
Configurable MTU with Bay RS and Contivity gateway 35
Load-balancing and hardware encryption accelerator cards 35
BIS using dial interface with CHAP authentication 36
Multiple BIS interfaces using the same primary interface 36
Dial interfaces LCP Echo Request settings 36

PPP multi-link with BayRS over dial interfaces 36
Legacy option cards not supported in Contivity 5000 37
Valid local address required for branch office tunnel 37
NAT policy considerations 37
SSL administration configuration 38
Backing up your configuration 38
DHCP server assigns leases when neither CSF or interface filters enabled 38
NetBIOS NAT ALG 39
Certificate subject names 39
Enabling manageability mode may affect performance 39
RADIUS server disabled when upgrading 39
Asynchronous branch office tunnel with nailed-up option enabled 40
Branch office support for state and cost 40
NAT traversal port numbers 40
Recovery floppy diskette 40
Downgrading from previous versions 40
RADIUS-supplied attributes 41
PPTP and L2TP MPPE 128-bit encryption keys 41
Browser considerations 41
Viewing and calculating memory usage 42
IPTunnel SNMP MIB 43
Gateway disconnects with PC client through LinkSys 43
Windows 2000 client using L2TP over IPSec 44
Contivity Stateful Inspection firewall UI 44
Using OSPF virtual links 44
Post implied rules tab removed 45
Branch office test fails when traffic is passed over non-nailed up tunnel 45
Inactive PPP connection through LMC 1200 board 45
Changing an interface card that has many branch office tunnels 45
Obsolete CLI commands 46
Documentation notes 48
Enabling and disabling ICMP filter (Q00809341) 48
Upgrading TCP-MSS Clamping (Q00808395-02) 48
Outbound packet counter set to zero (Q00804640) 48
Using dial interface as backup in BIS (Q00701773) 48

Sharing external LDAPs causes instability (Q00701008) 49
Firewall shows interface not present (Q00697364) 49
Provisioning time (Q00627570) 49
Dial interface correction (Q00725400) 49
NTP server replies ignored (Q00713605) 50
Public address table works only when Firewall/Interface filters are disabled (Q00676509) 50
Misleading branch office information (Q00461065-01) 50
Default Configuration for 1010, 1050, and 1100 51
Known anomalies 51
CLI issues 51
Provisioning with external LDAP and show running-config (Q00725303) 51
Managing entity names that begin with a CLI keyword (Q00633489-01) 52
Frame relay circuit issue when editing unrelated WAN card (Q00562810) . . . 52
Show Logging Events command (Q00488571-02) 52
Editing user accounts created in CLI from UI (Q00255043-01) 52
Caching configuration screens (Q00207522-01) 53
CLI network command (Q00072440-01) 53
Routing issues 53
Dynamic changes to CAR options incorrect in routing table (Q00708960) . . . 53
OSPF DD packets with incompatible MTU size accepted (Q00657955-01) . . 54
Configuring two interfaces within same subnet (Q00559903) 54
Responder tunnels cannot use multicast boundary list (Q00537232-01) 54
Multicast boundary list cannot be enabled or disabled (Q00535443-01) 54
Exiting browser during VRRP configuration (Q00458703-01) 54
Verify changes to RIP configuration (Q00281283-02) 55
Two unique LSIDs must exist in backbone area (Q00067571-02) 55
Authentication and certificate issues 55
RADIUS authentication of Contivity VPN Client requires PAP or CHAP (Q00693226) 55
Compatibility between versions when using AES with group 5 (Q00609054) . 56
Windows 2000 VPN server (Q00228485) 56
Using certificate RDN fields for a remote identity (Q00154595-01) 56
NAT and Contivity Stateful Firewall issues 56
Firewall Policy Rules disappear when moved and copied (Q00722486-01) . . 56
SNMP traps affected when NAT policy modified (Q00660225) 57

Enabling NAT and then firewall (Q00626964) 57
International characters in group names (Q00039540-01) 57
Contivity 1010/1050/1100 issues 57
Deleting previous version before upgrade (Q00536634) 57
Incorrect restart system message (Q00457593-01) 58
General issues 58
Possible hang with V.35 WAN links (Q00808698) 58
Windows 2000 PPP/L2TP multi-link (Q00727615) RTV* 58
Boot drive selection on Contivity 5000 (Q00725494) 58
BIS ping trigger on networks with devices that disallow Ethernet broadcast (Q00725466) 59
Using square brackets in event logs (Q00725362) 59
Restoring a backup image from recovery disk (Q00721362-01) 59
Using PPPoE as secondary On Demand circuit (Q00719478) 59
Setting WAN PPP IP via serial menu (Q00696510-01) 59
Changing from dynamic to static branch office tunnel (Q00692438) 60
L2TP/IPSEC IPsec Transport Mode Connections (Q00671793) 60
Status Health Check and SNMP Trap screens (Q00634001-01) 60
Changing branch office tunnel type (Q00627074-01) 60
Incorrect WAN status in system report (Q00560429) 60
Error message when adding branch office groups (Q00548286-01) 61
Some DHCP server options are not configurable (Q00532773) 61
Using comma with network name (Q00532630) 61
Enabling SNMP MIB through the UI (Q00440453-01) 61
Editing last name for user profile causes errors (Q00435962-01) 61
Cannot cancel upgrade in progress (Q00433348-01) 61
Branch office tunnel filters not working properly (Q00418382-02) 62
Incorrect error message for excess rates (Q00289581-02) 62
Serial console issues with system reset menu options (Q00284339-02) 62
File retrieval counter increments FTP failure attempts (Q00250467-01) 62
Setting LDAP to an unreachable external server (Q00155644-02) 62

Chapter 3
Configuration changes for interfaces and tunnels 63

Interfaces 63

Tunnels 63
Configuring the interface MTU and the TCP MSS 64
Configuring the MTU on an interface 65
Displaying the MTU and TCP MSS values of an interface 66
Configurable TCP MSS clamping 67
Resetting the TCP MSS on an interface 67
Enabling TCP MSS clamping 68
Interface MTU and TCP MSS configuration commands 69
mtu (interface) 69
Syntax 69
Parameters 70
Default 70
Command mode 70
Next command mode 70
Required privileges 70
Related commands 71
Example 71
tcp-mss 71
Syntax 71
Parameters 72
Default 72
Command mode 72
Next command mode 72
Required privileges 72
Related commands 72
Examples 72
tcp-mss enable 73
Syntax 73
Parameters 73
Default 73
Command mode 73
Next command mode 74
Required privileges 74
Related commands 74
Examples 74

Tunnel MTU and IPsec DF bit configuration commands 74
mtu (branch office tunnel) 75
Syntax 75
Parameters 75
Default 75
Command mode 75
Next command mode 75
Required privileges 75
Related commands 76
Example 76
mtu enable 76
Syntax 76
Parameters 76
Default 77
Command mode 77
Next command mode 77
Required privileges 77
Related commands 77
Example 77
df-bit 78
Syntax 78
Parameters 78
Default 78
Command mode 79
Next command mode 79
Required privileges 79
Related commands 79
Example 79

Chapter 4
Using packet capture (PCAP) 81

PCAP overview 81
PCAP features 82
Security features 82
File format 83

Capture types 83
Physical interface captures 84
Tunnel captures 84
Global IP captures 85
Filters and triggers 85
Capture filters 86
Triggers 86
Saving captured data 87
Memory considerations 87
Performance considerations 87
Enabling and configuring packet capture 88
Enabling packet capture on a Contivity gateway 88
Sample packet capture objects 91
Physical interface 91
Tunnel capture 92
Global IP capture 93
Sample show capture commands 93
Viewing a packet capture output file on a PC 94
Installing Ethereal software 94
Saving, downloading, and viewing PCAP files 95
Viewing a PCAP file with Sniffer Pro 96
PCAP commands 97
capture 98
Syntax 98
Parameters 98
Default 98
Command mode 98
Next command mode 98
Required privileges 99
Prerequisites 99
Warning messages 99
Related commands 99
Example 99
capture add 100
Syntax 100

Parameters 100
Default 100
Command mode 101
Next command mode 101
Required privileges 101
Warning messages 101
Related commands 101
Example 101
capture enable 102
Syntax 102
Parameters 102
Default 102
Command mode 103
Next command mode 103
Required privileges 103
Prerequisites 103
Warning messages 103
Related commands 103
Example 104
capture save 104
Syntax 104
Parameters 104
Default 104
Command mode 105
Next command mode 105
Required privileges 105
Prerequisites 105
Warning messages 105
Related commands 105
Example 106
capture start 106
Syntax 106
Parameters 106
Default 106
Command mode 106

Next command mode . . . 106
Required privileges . . . 107
Prerequisites . . . 107
Warning messages . . . 107
Related commands . . . 107
Example . . . 107
capture stop . . . 108
Syntax . . . 108
Parameters . . . 108
Default . . . 108
Command mode . . . 108
Next command mode . . . 108
Required privileges . . . 108
Prerequisites . . . 108
Warning messages . . . 109
Related commands . . . 109
Example . . . 109
clear capture . . . 109
Syntax . . . 109
Parameters . . . 109
Default . . . 110
Command mode . . . 110
Next command mode . . . 110
Required privileges . . . 110
Prerequisites . . . 110
Warning messages . . . 110
Related commands . . . 110
Example . . . 111
direction . . . 111
Syntax . . . 111
Parameters . . . 111
Default . . . 111
Command mode . . . 111
Next command mode . . . 111
Required privileges . . . 112

Prerequisites 112
Warning messages 112
Related commands 112
Example 112
filter 113
Syntax 113
Parameters 113
Default 113
Command mode 114
Next command mode 114
Required privileges 114
Prerequisites 114
Warning messages 114
Related commands 114
Example 115
length 115
Syntax 115
Parameters 115
Default 115
Command mode 116
Next command mode 116
Required privileges 116
Prerequisites 116
Warning messages 116
Related commands 116
Example 116
persistent 117
Syntax 117
Parameters 117
Default 117
Command mode 117
Next command mode 117
Required privileges 118
Prerequisites 118
Warning messages 118

Related commands 118
Example 118
promiscuous 119
Syntax 119
Parameters 119
Default 119
Command mode 119
Next command mode 119
Required privileges 119
Prerequisites 120
Warning messages 120
Related commands 120
Example 120
remoteip 120
Syntax 121
Parameters 121
Default 121
Command mode 121
Next command mode 121
Required privileges 121
Prerequisites 121
Warning messages 121
Related commands 122
Example 122
show capture 122
Syntax 122
Parameters 122
Default 123
Command mode 123
Next command mode 123
Required privileges 123
Warning messages 123
Related commands 123
Example 124
trigger 126

Syntax 126
Parameters 126
Default 127
Command mode 127
Next command mode 127
Required privileges 127
Prerequisites 127
Warning messages 127
Related commands 127
Example 128
type 128
Syntax 128
Parameters 129
Default 129
Command mode 129
Next command mode 129
Required privileges 129
Prerequisites 129
Warning messages 130
Related commands 130
Example 130
userid 131
Syntax 131
Parameters 131
Default 131
Command mode 131
Next command mode 131
Required privileges 131
Prerequisites 132
Warning messages 132
Related commands 132
Example 132
wrapping 133
Syntax 133
Parameters 133

Default 133
Command mode 133
Next command mode 133
Required privileges 133
Prerequisites 134
Warning messages 134
Related commands 134
Example 134

Chapter 5
Using forced logoff 135

forced-logoff 135
Syntax 135
Parameters 135
Default 136
Command mode 136
Next command mode 136
Required privileges 136
Warning messages 136
Related commands 136
Example 137
forced-logoff 137
Syntax 137
Parameters 137
Default 137
Command mode 137
Next command mode 138
Required privileges 138
Example 138

Appendix A
Firewall and Filters Example. 139

Preface

These release notes contain the latest information about the Nortel Networks* Contivity* Secure IP Services Gateway Version 4.85.

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 and Filters for the Contivity Secure IP Services Gateway* provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- *Configuring Tunneling Protocols and Advanced WAN Settings for the Contivity Secure IP Services Gateway* provides instructions for configuring the tunneling protocols IPsec, L2TP, PPTP, and L2F, as well as instructions for configuring PPP, frame relay, PPPoE, and advanced WAN settings.
- *Configuring Routing for the Contivity Secure IP Services Gateway* provides instructions for configuring RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Managing and Troubleshooting the Contivity Secure IP Services Gateway* provides information about system administrator tasks such as backup and recovery, file management, and upgrading software, and instructions for monitoring gateway status and performance. Also, provides troubleshooting information and 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.

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 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 4.85 release includes new features added since the release of the Contivity Secure IP Services Gateway Version 4.80. These release notes contain the latest information about the Contivity Secure IP Services Gateway.

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

Version 4.85 new features

This section highlights the new Contivity Secure IP Services Gateway features that are supported in Version 4.85. For additional information, refer to the documentation set or the online Help.

- Configurable maximum transmission unit (MTU) specifies the largest packet that can be sent out on an interface. If a packet to be sent is larger than the MTU configured for the interface, the packet is fragmented or dropped. See Chapter 3, “Configuration changes for interfaces and tunnels,” on page 63.
- Packet capture (PCAP) allows you to troubleshoot networking problems. It saves captured traffic to a file on the disk for downloading and off-line analysis. See Chapter 4, “Using packet capture (PCAP),” on page 81.
- Forced logoff provides the ability to log off end users and branch office connections either by the individual connection or by logging of all connections at once through the CLI. See Chapter 5, “Using forced logoff,” on page 135.

- QOS enhancements provide the option of dropping data that exceeds configured Traffic Conditioning Assured Forwarding rates. This allows for guaranteed bandwidth based on Diffserv code points that guarantees a fixed percentage of total bandwidth to each of several applications.

  The QoS main menu has been reorganized. The previous QOS Menu included:

  — Classifiers
  — QOS Interfaces
  — Bandwidth Management - Contained selections to enable bandwidth management and the unrelated Admission Control function.
  — Bandwidth Rates

  The new QOS Menu includes:

  — Classifiers (unchanged)
  — QOS Interfaces
  — Bandwidth Management - Contains selection to enable bandwidth management and incorporates the Bandwidth Rates screen.
  — Call Admission (renamed from Admission Control) Contains selection to enable Call Admission

  The QOS Interfaces screen has been reorganized. The previous QOS Interfaces screen included:

  — Bandwidth Management- Contained Interface Shaping (Ethernet only) and Call Admission data
  — Diffserv Edge
  — Egress (Outbound) Queueing Mode
  — The new QOS Interfaces screen includes:
  — Interface Shaping (Ethernet only)
  — Bandwidth Management
  — Call Admission
  — Diffserv Edge
  — Egress (Outbound) Queueing Mode

A configuration option has been added.The Assured Forwarding queues can be configured to drop data exceeding the configured rate. (EF excess data is always dropped.) Such data is dropped on ingress and never enqueued. With that done, if the configured data rates for the Assured Forwarding queues are based on the interface shaping rate, which is based on the downstream data rate, the queues will be of appropriate size.

- Nested tunnels allow you to create a PPTP end user tunnel inside an IPSec branch office tunnel or an asynchronous branch office tunnel. You can have a nested tunnel from within the private network or from the public side. You can individually log off nested tunnel sessions from the Status > Sessions > Active Session screen.
- Encrypted password for administrative user account for the CLI show running config command.
- Increased the IP address pool blackout interval between reassigning IP addresses to a maximum value of 24 hours (84600 seconds).

Contivity gateway hardware and software compatibility

Table 1 shows Contivity Secure IP Services hardware and software compatibility.

Table 1 Hardware platform and server software compatibility

	Software version and release date						
Hardware platform	**4.06_180** **11/8/02**	**4.07** **6/20/02**	**4.50** **9/11/02**	**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** **4.85** **8/08/03**
1010		X			X	X	X
1050		X			X	X	X
1100		X			X	X	X
600	X		X	X	X	X	X
1500	X						
1510	X						
1600	X		X	X	X	X	X
1700	X		X	X	X	X	X

Table 1 Hardware platform and server software compatibility (continued)

	Software version and release date						
Hardware platform	**4.06_180** **11/8/02**	**4.07** **6/20/02**	**4.50** **9/11/02**	**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** **4.85** **8/08/03**
1740							X
2000	X		X	X			
2500	X		X	X			
2600	X		X	X	X	X	X
2700	X		X	X	X	X	X
4000	X		X	X			
4500	X		X	X	X	X	X
4600	X		X	X	X	X	X
5000			X			X	X
	Minimum memory required (MB)						
	64	128	128	128	128	128	128

Tunnel licensing

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 gateway model.
- VPN bundle option supports the maximum number of tunnels for the Contivity gateway model.

Table 2 lists the maximum number of tunnels for each Contivity gateway model and indicates whether each model has a five-tunnel base unit version.

Table 2 Maximum number of tunnels by Contivity gateway model

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

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_85.101 contains the Nortel Networks Contivity Secure IP Services Gateway software. You would use this directory to upgrade your gateway from an older version of the product.

Note: The Contivity gateway release image is now available in an optimized file (V04_85.101.tar.gz) located on the CD. The Contivity gateway decompresses the image as it retrieves it so that each individual file no longer downloads separately. You must then apply the new image. You can only use this file if you are upgrading from Version 4.80 or later. For further information on upgrading your system, see the "Upgrading the software" section in Chapter 3 of the *Managing and Troubleshooting the Contivity Secure IP Services Gateway* book.

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 following items:

- IP address configuration utility (ExtNetIP.exe) that configures the management IP interface on a newly installed Contivity gateway. After you run this utility, you can configure and manage the gateway using a Web browser from a PC.
- The Java* subdirectory 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 4.85 release of the Contivity Secure IP Services Gateway.

Fixed in this release

Nortel Networks* Contivity* Secure IP Services Gateway sustaining release Version 4.85_101 resolves the following issues.

Table 3 lists customer issues from previous releases that are fixed in this release.

Table 3 Fixed in this release

Q00285651-03	Parser error on routing screens when using Japanese as default language.
Q00511528-01	Changes to allow a maximum value of 24 hours (in seconds=84600) for the DHCP blackout interval for the remote user IP address pools.
Q00605498	ABOT tunnel configured as Initiator would accept incoming connections and act as a Responder. For example, initiator Contivity gateway accepts incoming peer-to-peer connections.
Q00610979-01	Multiple logins circumvented via prefix stripping feature.
Q00655781-02	CLI show running config command does not display the group level RADIUS server configuration. CLI commands for the prefix-delimiter, prefix-remove and suppress-service-type options have been added: o CES(config)#radius-server group "groupName" prefix-delimiter o CES(config)#radius-server group "groupName" prefix-remove o CES(config)#radius-server group "groupName" primary suppress-service-type enable
Q00655981-02	SNMP trap branch office link up/down trap ifIndex is always 0.
Q00698551-03	Main mode branch office tunnels not recovering after the idle timeout has been reached.

Table 3 Fixed in this release

Q00698937-01	Contivity server certificate request fails to be signed by OpenSSL certification authority.
Q00708877-01	Memory leak with L2TP/IPSec branch office tunnels if branch office disable/enable script is run many times.
Q00722486-01	Firewall policy rules disappear when moved and copied.
Q00726913	Performing a MIBwalk or GetNext MIB command to the Contivity switch may time out.
Q00727615-01	PPTP/L2TP/L2F user tunnels could not be established if client has a multilink negotiation turned on as LCP Echo request enabled by default on Contivity gateway V04.80. Configuration option for LCP-Echo request for PPTP, L2TP, and L2F tunnel types has been added to GUI and CLI: o CES(config)# pptp lcp-echo enable o CES(config)# l2tp lcp-echo enable o CES(config)# l2f lcp-echo enable
Q00729201-01	Diffie-Hellman group mismatch produces core if CRL is required. CRLs are not present on the Contivity gateway and LDAP to obtain CRL is not reachable. Core dump occurs on the Contivity gateway when Contivity VPN Client attempts to log in using certificates and all of the following conditions are met: o CES has no CRLs in LDAP; o CRL required is set to TRUE; o There is Diffie-Hellman group mismatch between Contivity Client and Contivity o CRLs can not be obtained successfully from CA
Q00729841	Contivity Stateful Firewall logging security requirements addressed.
Q00732207-01	Memory leak condition with CRL retrieval enabled.
Q00735688-01	Using certificates with a long identification string causes a buffer overflow condition resulting in a core.
Q00736323-01	Contivity cores when Contivity Stateful Firewall reuses existing connections.
Q00745594-01	Switching Connection Port for the external LDAP to or from SSL Port takes 9 minutes; Contivity gateway cores if tunnels present.
Q00745692-01	Removal of a Wan interface with frame relay enabled causes core.
Q00745752-01	AES forwarding performance optimization.
Q00749158-01	Contivity gateway cannot handle multiple Frame Type AVPs from L2TP tunnel request, which results in interoperability problems between Contivity gateway and Cisco 5300 and 5400.

Table 3 Fixed in this release

Q00749182-01	Contivity gateway did not support the user ID component in subject DN. As a result the Full DN starting with UID in user profile was not saved, making it impossible to add users.
Q00752138-04	LDAP server memory leaks have been fixed.
Q00754901-01	Contivity gateway cores if CA certificate with CRL optimization enabled is deleted via CLI.
Q00758259-01	The CLI show running config command produced incorrect output for the outbound interface filters causing problems with provisioning.
Q00759098-01	Console port PPP does not recognize the carrier detect sent by the modem and therefore never recognize that the connection is up not work on the 1010. 1050, and 1100 platforms.
Q00760279-01	Adding a user to base group and a user account for FWUA later breaks show running-config command and causes errors with CLI provisioning.
Q00760888-01	The “show run server radius” command produces an error for the group-level RADIUS server.
Q00761120-01	The “show run profile bo-conn” command produces a “% bad argument” error.
Q00763073	Ability to specify a TunnelGuard agent minimum version has been added to the Contivity.
Q00763184-01	Branch office static routes did not appear in the routing forwarding table after a reboot.
Q00763617-01	When provisioning with CLI show running config command, an error referenced to the dynamic DNS was produced as no CLI command for the client’s default dynamic DNS existed.
Q00763927	Latest version of Open SSL was incorporated into Contivity gateway to address OpenSSL vulnerabilities per CERT Advisory CA-2003-26 http://www.cert.org/advisories/CA-2003-26.html.
Q00764698	Contivity gateway core due to buffer overflow when there are a large number of network objects in the group object.
Q00768944-03	Retransmissions do not work correctly when there is an FTP failure.
Q00769218-01	Cannot ping public interface of the Contivity gateway if the source IP is registered with control tunnel.
Q00770530-02	BOOTP requests not recognized by Contivity and thus dropped.
Q00774317	The 5000 LED Fail LED does not clear after the LED has been turned on by the failure and the failure has been addressed.
Q00777712	HTTP out of sequence TCP FIN frame is dropped with stateful firewall enabled.
Q00779748	The secondary disk drive removal and insertion on 5000 failed with the error message “Unable to attach to the device”.

Table 3 Fixed in this release

Q00781788	A core dump may occur when HTTP and SIP-upd or SIP-tcp traffic go through the stateful firewall.
Q00784351-01	NTP was not releasing UDP sockets.
Q00785286-01	Reverse (wildcard) subnet mask considered non-continuous and therefore disallowed.
Q00785510	The Contivity switch may core dump if Tunnelguard is configured along with branch office tunnels.
Q00788452	DHCP Request packets do not conform to RFC2131.
Q00791328-02	LDAP could be deleted and set to default at reboot in V04.80_124 if firewall policy has been recently edited.
Q00793835	Received stale CRL was not stored in LDAP.
Q00803032	The Contivity switch may core if a user tunnel is being established when the LDAP is stopped.
Q00808350-01	Incorrect link for the CA certificate installation on the Servers > LDAP Proxy screen in the V04_80 code.
Q00811642	Request to have the current client version logging and Tunnelguard logging collected in the syslog instead of the eventlog.

Product considerations

The following sections discuss product considerations or limitations.

Number of versions

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

Support considerations

- Version 4.85 does not support Check Point Firewall-1.
- Diffie-Hellman Group 5 functionality does not exist in Version 4.0 so therefore Diffie-Hellman Group 5 does not interoperate with Version 4.0. Version 4.85 Diffie-Hellman Group 5 interoperates with Version 4.70 Diffie-Hellman Group 5.

- Version 4.85 supports upgrades from Versions 4.50, 4.07, 4.06, 4.70 and 4.80. If you are running an older version, you must upgrade to a supported version before you upgrade to Version 4.85.
- 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 gateway system.
- 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 4.85.
- A T1 interface does not support packets larger than 47 KB.
- The Contivity gateway UI and CLI support only 7-bit ASCII characters.
- The Contivity gateway works with all RFC-compliant FTP servers.
- The Contivity gateway 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.

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.

Configurable MTU with Bay RS and Contivity gateway

If you are having problems configuring OSPF adjacency between a Bay RS router and a Contivity gateway system, be sure that the MTUs match.

Load-balancing and hardware encryption accelerator cards

When one or two optional hardware encryption accelerator cards are installed, Contivity gateway 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.

BIS using dial interface with CHAP authentication

When using dial interfaces as backup interfaces in BIS and using CHAP authentication, you must configure the username and password in the Dial Interface Configuration screen. The username and password configured under the BIS configuration only works when using PAP authentication.

Multiple BIS interfaces using the same primary interface

Multiple BIS interface configurations that point to the same primary interface or use the same primary interface as the triggering interface is not supported. Do not configure multiple BIS interface in that manner. It will cause BIS to not function correctly.

Dial interfaces LCP Echo Request settings

The default setting for LCP Echo Request over dial lines is set such that Contivity gateway sends out echo-requests every 10 seconds and an echo-response is expected back by the Contivity gateway in 20 seconds. If no response is received within 20 seconds, the Contivity gateway will drop the call. If you run into call drops because of “Excessive Lack of LCP Echo replies” you may want to increase the fault threshold value accordingly. Alternatively, LCP Echo Requests can be completely turned off by setting the Echo Interval to 0.

PPP multi-link with BayRS over dial interfaces

When using PPP multi-link to connect to a BayRS router, turn LCP Echo requests off on the Contivity gateway dial interface by setting the LCP Echo Interval to 0. There is an issue with BayRS software that causes the LCP replies to not get sent out correctly when multi-link is active. This will result in the call getting dropped if the LCP echo requests are not turned off on the Contivity gateway.

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 gateway 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)

  This card can no longer be ordered. However, you can install existing dual V.35 cards in slots 3, 4, and 5 only.

Valid local address required for branch office tunnel

You must have the proper local end point defined while configuring a branch office tunnel. If invalid addresses (addresses that are not one of the Contivity interface or CLIP addresses) are used in heavy traffic conditions, performance may suffer substantially.

NAT policy considerations

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 Java GUI. You will see an (old format) text message to alert you to the change. The Version 4.70 policies will still be translated, 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.

SSL administration configuration

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 CES securely using Admin SSL.

1. Make an entry in the hosts file corresponding to your Contivity gateway management IP address.
2. Import the root certificate that issued your Contivity gateway server certificate into your browser store.
3. Import the root certificate that issued your Contivity gateway server certificate into your JRE.

To satisfy a further name check by Netscape browsers, the Contivity gateway 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.

Backing up your configuration

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

DHCP server assigns leases when neither CSF or interface filters enabled

A change to the interaction of the DHCP server and firewalls will now allow DHCP clients to obtain IP addresses when no firewall is enabled. This new behavior does not in any way enable clear text traffic to egress a public interface; it merely allows private side DHCP clients to obtain an IP address from the pool.

NetBIOS NAT ALG

The NAT ALG for NetBIOS packets supports datagram packets only; it does not have support for name service datagrams.

Certificate subject names

- 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 the Contivity gateway 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 gateway as identical to: ou=contivity, o=nortel, c=us, cn=joe Rearranging the order allows the Contivity gateway to correctly process certificates generated by CAs with differing DN encoding orders.

Enabling manageability mode may affect performance

When manageability mode is enabled from the System > Settings > Enable Manageability Mode screen, the priority of the HTTP management tasks is given higher priority to ensure manageability. However, the performance of the Contivity gateway may be impacted when management access is ongoing, due to it's high priority, and other services (such as routing or tunnel creation) may not occur in a timely manner. Also, CPU or I/O intensive management operations such as secure management access (SSL enabled HTTP), and viewing large event logs will increase the possibility of service disruption.

RADIUS server disabled when upgrading

When you upgrade to Version 4.85, 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.

Asynchronous branch office tunnel with nailed-up option enabled

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

Branch office support for state and cost

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

NAT traversal port numbers

Nortel Networks strongly recommends that you use port 10001 for NAT Traversal. Do not use L2TP/L2F port 1701 or General Packet Radio Service (GPRS) port 3386. Make sure that any port you select does not conflict with any ports that you are already using.

Recovery floppy diskette

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

Downgrading from previous versions

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

RADIUS-supplied attributes

Contivity gateway 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.

PPTP and L2TP MPPE 128-bit encryption keys

PPTP and L2TP MPPE 128-bit encryption keys do not work properly in the Contivity gateway if they were obtained during RADIUS authentication with a Funk Software, Inc. Steel-Belted Radius* Server Version 2.2 or later. This problem also applies to other RADIUS servers derived from Steel-Belted Radius, including the Bay Networks* BSAC RADIUS server Version 2.2 and later and the Nortel Networks Preside* RADIUS server Version 1.0.49 and later.

In addition, the Microsoft RADIUS server exhibits this problem when doing MS-CHAP authentication that returns MPPE keying information. PPTP and L2TP MPPE based 40-bit encryption is unaffected by this problem. Do not use the noted RADIUS servers with the gateway if PPTP or L2TP MPPE-based 128-bit encryption is required.

Browser considerations

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

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

- 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.

Viewing and calculating memory usage

The minimum memory requirement for Version 4.80 is 128 MB.

The Memory Calculator tool is a Microsoft Excel spreadsheet that provides information on determining the memory requirements for a Contivity gateway system based on the configuration of tunneling, routing, and firewall. The configuration values can be input in the Memory Calculator tool to determine the base memory recommended for the specified configuration. Given the dynamic nature of memory usage, the result provided by the tool is only an estimate.

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

The parameters affecting Contivity gateway memory usage are:

- Contivity gateway software version
- Single or dual CPU (if single CPU model or dual CPU model Contivity Secure IP Services Gateway)
- Internal or External LDAP shows whether internal or external LDAP configured
- Number and type is the number and type of branch office and user tunnels
- Static routes is the number of static route entries in the IP routing table
- RIP routes is the number of RIP route entries in the IP routing table
- OSPF Routes is the number of OSPF route entries in the IP routing table
- Redistributed OSPF and RIP Routes is the number of routes redistributed into RIP and OSPF Routing protocols
- FW/NAT Max connections is the maximum number of connections as configured from Services > Firewall/NAT > Edit screen

- FW/NAT Number of Sessions is the total number of Firewall/NAT sessions
- BO NAT number of Sessions is the number of Branch Office NAT sessions
- CSFW Enabled shows if CSIF (Contivity Stateful Firewall with Interface Filter) is on
- Interface NAT Enabled shows if Interface NAT is on
- Antispoofing Enabled shows if Antispoofing is on

The Memory Calculator Tool is available at:

`www.nortelnetworks.com/documentation`

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

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

IPTunnel SNMP MIB

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

Gateway disconnects with PC client through LinkSys

If you are using a Linksys Etherfast Cable/DSL router in IPSec passthru mode, and if two or more PCs connect through it to a gateway, then one or both of these PCs will be disconnected and/or their communications disrupted unless NAT Traversal mode is used on the gateway. (The client monitor will continue running and will not display a message that the connection is disconnected or disrupted.) This occurs because the LinkSys does not support more than one IPSec session. To prevent this, select the Auto-Detect NAT option on the Profiles > Groups > *GroupName* > Edit IPsec screen, which activates NAT Traversal and allows multiple PCs behind the NAT box to function properly.

Windows 2000 client using L2TP over IPSec

You cannot run the Windows* 2000 client using L2TP over IPSec if the Contivity VPN Client is installed. The IPSec driver conflicts with the native IPSec driver in Windows 2000. You must disable the Windows 2000 IPSec driver, which effectively prevents the use of the Windows 2000 Client using L2TP/IPSec. If you go to the Services > IPSec screen and change the IPSec Policy Manager setting from Disabled to Automatic and reboot the system, the client detects the loading of the Windows 2000 IPSec driver and disables the client's IPSec driver.

Contivity Stateful Inspection firewall UI

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.

Using OSPF virtual links

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

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

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

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

Post implied rules tab removed

The Post implied rules tab of the Contivity Stateful Firewall was removed in Version 4.80. This was done, without loss in functionality, to present a less complicated firewall configuration environment.

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

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

Inactive PPP connection through LMC 1200 board

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

1. Go to your gateway's System > WAN screen. Select the Statistics button for the interface.
2. On the Statistics screen, check the IP Packets Sent field. If the field shows that zero packets have been sent, this indicates that the PPP connection is not active.

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

Changing an interface card that has many branch office tunnels

If you remove or move to another slot an interface card that has hundreds or thousands of branch office tunnels configured on it (that is, the local tunnel end point is configured on that card), an extended delay may occur when you reboot the system as the gateway attempts to initialize the branch office tunnels using the nonexistent local end-point IP address.

To avoid a lengthy delay after moving or removing an interface card:

1. Before you move or remove the interface card, enable manageability mode.

   On the Web management interface, choose System > Settings. Or, from the CLI Global Configuration mode, enter this command:

   ```
   CES(config)# scheduler manageability enable
   ```

2. Shut down the gateway and then move or remove the interface card.
3. Restart the gateway.
4. While the gateway is rebooting, configure the proper interface IP address so that the branch offices can be initialized in the normal time frame.

Obsolete CLI commands

Table 4 lists the CLI commands that are not displayed in interactive mode. These commands are supported and continue to function properly when used in scripts.

Table 4 Obsolete CLI commands

# show running-config server address-pool	Displays pool configuration information
(config/rule)# use dest-port eq WORD	PortName
(config/rule)# use src-port eq WORD	PortName
(config)# control create WORD WORD A.B.C.D A.B.C.D A.B.C.D A.B.C.D A.B.C.D	Remote network subnet mask
(config)# control help	Description of the control tunnel help system
(config)# control show	Displays current control tunnels defined
(config)# ip default-route-preference private default	Defines that public routes will be preferred as default routes
(config)# ip dhcp address-release	Enables the address release policy
(config)# policy nat enable	Enable Interface NAT.
(config)# policy nat interface disable	Disable Interface NAT.
(config-group/ipsec)# default encryption 3des-md5	Triple DES with MD5 Integrity
(config-group/ipsec)# default encryption des40-md5	40bit DES with MD5 Integrity
(config-group/ipsec)# encryption ike 128aes-group5	AES 128 with Group 5 (1536-bit prime)
(config-if)# no ppp ip local negotiated	Specifies rejection of a negotiated local IP address
(config-if)# no ppp remote authentication chap	Disables CHAP authentication

(config-if)# ppp remote authentication chap	Enables CHAP authentication
(config-if)# ip rip export-bo-static-metric 0	Disables export branch office static route metric
(config-if)# ip rip export-static-metric 0	Disables export static route metric
(config-if)# ppp ip rip export-bo-static-metric 0	Disables export branch office static route metric
(config-if)# ppp ip rip export-static-metric 0	Disables export static route metric
(config-car)# summarization	Enables the network routes of client address to be injected to routing table for redistribution
(config-subif)# encapsulation PPPoFR	Configures PPPoFR encapsulation
(config-subif)# ip rip export-bo-static-metric 0	Disables export branch office static route metric
(config-subif)# ip rip export-static-metric 0	Disables export static route metric

Documentation notes

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

Enabling and disabling ICMP filter (Q00809341)

The Contivity gateway can filter ICMP traffic to its interfaces and management IP address. You can use the check boxes on the Services > Available > ICMP screen to filter this traffic on both public and private interfaces. If you use services such as LDAP, RADIUS or CMP that rely on ICMP traffic, the filter on the public interface, which is enabled by default, must remain enabled. If the filter is not checked, these services will not work because the Contivity gateway needs to ping these servers and it is filtered on the public interface and dropped.

Upgrading TCP-MSS Clamping (Q00808395-02)

If you previously configured TCP-MSS Clamping on PPPoE interfaces, you need to reconfigured it in V04_85.

Outbound packet counter set to zero (Q00804640)

If you have branch office tunnels set up with two-way traffic to form multiple IPsec security associations (SAs), there is one transmit SA and one receive SA. The packet counters on the Status > Sessions screen are derived from both SAs for transmit and receive traffic. If you have multiple IPsec SAs, the outbound traffic counter is set to zero because the traffic will be re-routed over the existing SA, which has an outbound packet count of zero.

Using dial interface as backup in BIS (Q00701773)

To use a dial interface as the backup interface in BIS, you must configure the PPP Authentication protocol under the Dial Interfaces PPP configuration. You must configure the user-name and password parameters under the BIS configuration.

Sharing external LDAPs causes instability (Q00701008)

When multiple systems share an external LDAP, any parameters added or removed from the external database by one system are not visible to the other system until the database caches are flushed. The cache flush is a timed interval.

Firewall shows interface not present (Q00697364)

When you create a firewall rule, under Interface Specific Rules, it lists Slot 7 Interface 1, which is the serial port. The serial port listing does not appear on versions of Contivity gateway prior to Version 4.80.

Provisioning time (Q00627570)

If you configure an external LDAP proxy server that is unavailable, you will experience delays in Contivity gateway provisioning times.

Dial interface correction (Q00725400)

In Chapter 3 Configuring Dial Interface of the *Configuring Tunneling Protocols and Advanced WAN Settings for the Contivity Secure IP Services Gateway* book, the screen shots and the description under the “Configuring Dial Interfaces” subsection, pertains to the configuration of the Contivity gateway's serial (COM) port as a dial interface. The V.90 configuration and screen shots have not been included separately. However, the configuration of V.90 interface is similar to the configuration of the Serial Port except in the following:

- For a V.90 interface, there is no Port Mode configuration parameter. V.90 can only be used for PPP.
- For a V.90 interface there is no Baud Rate parameter. The V.90 interface auto-negotiates baud rates down starting from 56K as needed

NTP server replies ignored (Q00713605)

Previously the NTP server would open the NTP port for the management IP rather than the filter. Now if the Management IP address is higher than the LAN IP and an NTP server is configured as accessible from the private network, NTP operates properly, but the local address will show up as 0.0.0.0 on the Status > Statistics > NTP Stats screen.

Public address table works only when Firewall/Interface filters are disabled (Q00676509)

Because there are no routing protocols (RIP, etc.) running on the untrusted interfaces, there is no way to know how to route packets to the appropriate trusted interfaces. The IP public address table (PAT) provides the needed routing information. Because the sources are not trusted using this interface, the IP PAT is used to limit unauthorized sources. PAT is disabled when either the Contivity Stateful Firewall or filter firewall is enabled to provide better policy-based security.

When the firewall is disabled, PAT applies only to packets received on a public interface. PAT has a list of trusted sources that includes the remote client or branch office tunnel end point, remote Radius/CMP/CRL server address (if on the public side). PAT does not limit the packets from any of those trusted sources. For packets coming from any address that is not in the trusted source list, a rate limit (6 packet/10 second) is applied based on the source address.

The Contivity Stateful Firewall public address table information is not related to network address translation (NAT) or network address port translation (NAPT), which is often referred to as port address translation (PAT).

Misleading branch office information (Q00461065-01)

Branch office session information can be misleading on the Status > Accounting screen because re-keyed branch office tunnels are displayed as separate entries. RADIUS accounting records are not sent to external servers for branch office connections.

Default Configuration for 1010, 1050, and 1100

The 1010, 1050, 1100 default configuration is set up to meet requirements for the majority of small office connections. This configuration includes a public interface configured for IP and can receive an address via DHCP from the ISP. The private side has the DHCP server enabled and the DHCP address pool set to 192.168.1.1/24. If you require a configuration such as PPPoE, you must first delete the IP protocol and a drop down list appears. Available configuration details do not appear on the default configuration screen unless this is deleted first.

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. For TunnelGuard related issues and considerations, see *tg_relnotes.pdf*.

CLI issues

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

Provisioning with external LDAP and show running-config (Q00725303)

When you provision a Contivity gateway using **show running-config** and an external LDAP, it does not enable all Services > IPSec encryptions. Also it disables all encryptions for /Base on Profiles > Branch Office group configuration screen.

Managing entity names that begin with a CLI keyword (Q00633489-01)

You cannot use the CLI to manage entities with names that begin with the same letters as a CLI keyword. For example, you cannot edit connections (branch office tunnels) whose names begin with “a,” “ad,” or “add,” because “add” is the CLI keyword used to add tunnels. You can create a branch office connection whose name begins with these letters, but when you try to edit the connection, an error message appears. The CLI parser does not recognize the input as data even if you enclose the name in quotation marks.

```
CES(config)#bo-c add add /Base
CES(config)#bo-c add /Base
                     ^
% Incomplete command. See '^' marker.
CES(config)#
```

As a workaround, use the Web GUI to rename tunnels whose names begin with “a,” “ad,” or “add” if you need to manage such tunnels with the CLI.

Frame relay circuit issue when editing unrelated WAN card (Q00562810)

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

Show Logging Events command (Q00488571-02)

The CLI event log may have missing events when under extremely heavy load.

Editing user accounts created in CLI from UI (Q00255043-01)

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

Caching configuration screens (Q00207522-01)

Your Internet browser might be caching configuration screens. This becomes an issue if another UI session or CLI session is changing parameters displayed on the same screen. In this case, refreshing the screen might not display the latest version of these parameters. To ensure that the latest values are displayed, you can either disable browser caching or restart the management session by logging out and logging in again. You should check how many management sessions are open before making any critical configuration changes. Two users modifying the same functional area simultaneously could lead to an inconsistent configuration.

CLI network command (Q00072440-01)

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

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

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

Routing issues

The following sections describe issues related to routing.

Dynamic changes to CAR options incorrect in routing table (Q00708960)

You can switch freely between the various CAR modes (disabled, host only, static aggregation, and dynamic aggregation). However, this can create some unpredictable behavior in the routing table. For example, if one or more clients were already logged in when you switched from static aggregation to host only mode, the aggregated route would remain and the host routes would not be added to the table. In this situation, only new client logins would get their host routes added to the routing table.

OSPF DD packets with incompatible MTU size accepted (Q00657955-01)

RFC 2178 specifies that when a device (such as a router or gateway) receives an OSPF database description (DD) packet that advertises an MTU larger than the device can receive, the router or gateway should drop this packet to prevent an OSPF adjacency from forming. However, the Contivity gateway does not drop such DD packets and instead tries to form an OSPF adjacency.

Configuring two interfaces within same subnet (Q00559903)

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

Responder tunnels cannot use multicast boundary list (Q00537232-01)

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

Multicast boundary list cannot be enabled or disabled (Q00535443-01)

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

Exiting browser during VRRP configuration (Q00458703-01)

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

Verify changes to RIP configuration (Q00281283-02)

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

Two unique LSIDs must exist in backbone area (Q00067571-02)

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

Authentication and certificate issues

The following sections describe issues that apply to authentication.

RADIUS authentication of Contivity VPN Client requires PAP or CHAP (Q00693226)

When you configure RADIUS authentication from the Servers > Radius Auth screen, you must enable PAP or CHAP for successful authentication of the Contivity VPN Client over RADIUS. Support for conversion to MSCHAP will be in a future release.

Compatibility between versions when using AES with group 5 (Q00609054)

If you configure AES group 5 within a branch office group between two Contivity gateways, and only one of the gateways is running Version 4.76, the two gateways will not interoperate. If you configure AES group 5 on a gateway that is running a software version earlier than Version 4.76, that gateway will not work with third-party devices or with a Contivity gateway running Version 4.76. (A gateway running Version 4.76 and AES group 5 will work with third-party devices.) Nortel Networks recommends that you use AES group 8 instead of group 5.

Windows 2000 VPN server (Q00228485)

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

Using certificate RDN fields for a remote identity (Q00154595-01)

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

NAT and Contivity Stateful Firewall issues

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

Firewall Policy Rules disappear when moved and copied (Q00722486-01)

When the rule is cut and pasted, the parenthesis is removed from the key word, resulting in an error when the policy is copied. You can use either of the following ways to work around this issue:

- Use the save policy as option instead of copy from the Firewall - Select Policy screen.

- Change the event log type from none to brief, detail, or trap to correct the missing parenthesis.

SNMP traps affected when NAT policy modified (Q00660225)

If you modify a NAT policy to a new translated NAT address or apply a new NAT policy, the traps sent use the original NAT address. The active NAT policy shows the correct NAT translation, but the NAT cache has to be flushed before the modified NAT policy works correctly. Traps are only sent from the first applied NAT policy.

Enabling NAT and then firewall (Q00626964)

If you are running an a slower version of Windows, the rate of refresh may give you time to re-select some check boxes and click on OK again during the refresh process. This will cause incorrect behavior if you are trying to enable NAT and then the firewall.

International characters in group names (Q00039540-01)

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

Contivity 1010/1050/1100 issues

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

Deleting previous version before upgrade (Q00536634)

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

Incorrect restart system message (Q00457593-01)

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.

General issues

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

Possible hang with V.35 WAN links (Q00808698)

In an unstable network over V.35 WAN links, the Contivity gateway may hang if the instability lasts for more than an hour.

Windows 2000 PPP/L2TP multi-link (Q00727615) RTV*

The Contivity gateway sends the LCP echo requests but does not recognize the LCP replies received from the tunnel and determines that no replies were received. To work around this issue, you need to turn of multi-link negotiation on the client:

1. Right click on the Windows 2000 client and select Properties.
2. Under the Networking tab, select Settings.
3. Check to be sure that “Negotiate multi-link for single link connections” is disabled.

Boot drive selection on Contivity 5000 (Q00725494)

A software error will result during a disk synchronization operation if ide1 is selected for the boot drive. Ide0 is the default boot drive and should remain so unless a hardware failure of ide0 necessitates the use of ide1 for boot.

BIS ping trigger on networks with devices that disallow Ethernet broadcast (Q00725466)

BIS Ping trigger cannot be used where the primary (source) interface is an Ethernet interface that connects to a networks device that does not allow forwarding of Ethernet (MAC level) broadcast packets. Use another BIS trigger instead of Ping Trigger in such situations.

Using square brackets in event logs (Q00725362)

Do not use strings that contains square brackets [] in the Sorting Key Words field on the Status > Event Log screen.

Restoring a backup image from recovery disk (Q00721362-01)

An extra slash (/) character is erroneously appended to the beginning of the backup path every time an auto-backup occurs. This error does not impact the successful completion of the auto-backup, but you need to adjust the path and remove the extra characters before executing a Restore Backup from the recovery image/disk.

Using PPPoE as secondary On Demand circuit (Q00719478)

If you use a PPPoE interface as the backup interface in BIS, you must disable the On Demand parameter of PPPoE. Configuring PPPoE as a backup interface with On Demand enabled causes BIS to repeatedly bounce the circuit.

Setting WAN PPP IP via serial menu (Q00696510-01)

You must configure a WAN PPP interface through the CLI or GUI. If you attempt to configure a WAN PPP interface through the serial menu, the IP address will create a core situation.

Changing from dynamic to static branch office tunnel (Q00692438)

When you change from a dynamic to a static branch office tunnel and enter the remote network, the tunnel goes down. The tunnel should stay up until you are entirely finished with the branch office configuration and not when you configure the routing part of the branch office tunnel.

L2TP/IPSEC IPsec Transport Mode Connections (Q00671793)

If you use inheritance to enable IPsec Transport Mode Connections, the L2TP authentication never takes place and the end user connection attempt times out. The IPsec transport connection is established, but the L2TP authentication never occurs. If you do not use inheritance on the group and IPsec Transport Mode Connections is explicitly enabled on the group, the tunnel is established.

Status Health Check and SNMP Trap screens (Q00634001-01)

To display the most recent status, some management screens perform network activity before the display. For example, the Health Check screen tries to contact servers, such as DNS and SNMP, before it displays the server status. Displaying such screens could be delayed if there is a network problem or if the servers do not respond within a time limit.

Changing branch office tunnel type (Q00627074-01)

If you configure a branch office for a tunnel type of IPsec or L2TP over IPsec and then later change the tunnel type to L2TP or PPTP, ISAKMP still comes up if the remote peer tries to initiate it.

Incorrect WAN status in system report (Q00560429)

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

Error message when adding branch office groups (Q00548286-01)

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

Some DHCP server options are not configurable (Q00532773)

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

Using comma with network name (Q00532630)

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

Enabling SNMP MIB through the UI (Q00440453-01)

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

Editing last name for user profile causes errors (Q00435962-01)

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

Cannot cancel upgrade in progress (Q00433348-01)

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

Branch office tunnel filters not working properly (Q00418382-02)

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.

Incorrect error message for excess rates (Q00289581-02)

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

Serial console issues with system reset menu options (Q00284339-02)

For the recovery image, the Normal or Safe text string for the current mode is missing “System Reset Menu Options. System is currently in mode.”

File retrieval counter increments FTP failure attempts (Q00250467-01)

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

Setting LDAP to an unreachable external server (Q00155644-02)

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

Chapter 3
Configuration changes for interfaces and tunnels

This chapter describes the configuration changes for interfaces and tunnels

Interfaces

For interfaces, you can configure the following parameters for interfaces:

- MTU (maximum transmission unit)
- TCP MSS (maximum segment size) clamping and value

The MTU sets the maximum size of a data packet transmitted from the interface. It does not affect the size of a packet accepted by the interface. Packets larger than the MTU are either fragmented or dropped. The DF (don't fragment) bit in the IP header determines what action is taken.

For better network performance, configure the largest MTU value possible. Certain network topologies do not handle large packets, in which case you may want to decrease the size of the packets you send by lowering the MTU.

Tunnels

For tunnels, you can configure the following:

- For all tunnels, tunnel MTU may be enabled and configured.
- For IPsec tunnels, DF (don't fragment) Bit behavior may be configured.

Tunnel MTU determines the largest size packet than can be sent through the tunnel. This size includes all Layer 2 encapsulations dictated by the tunnel type. The default behavior is to enable tunnel MTU at the maximum value of 1788 bytes. If tunnel MTU is disabled, the tunnel MTU is derived from the interface.

For IPsec tunnels, the DF bit in the outer IP header is now configurable. The default behavior is to CLEAR the bit. The user may SET the bit or COPY the bit from the inner header.

Configuring the interface MTU and the TCP MSS

The default MTU value for each interface is based on the media type adjusted for Layer 2 encapsulation (Table 5).

Table 5 Default MTU by interface media type

Media/interface	Default MTU (bytes)
Ethernet	1500
Frame relay	1496
ISDN	1500
PPPoE	1492
Serial	1500
WAN (T1/T3)	1500

You can reset the MTU on each interface to these values:

- For LAN interfaces: 576 through 1500 bytes
- For PPPoE interfaces: 576 through 1492.
- For WAN interfaces: 576 through 1788 bytes

Note: Nortel Networks recommends that you do not change the MTU if you are running IPX.

Configuring the MTU on an interface

To change the MTU on an interface through the GUI:

- For a LAN interface, go to the System > LAN screen, select Configure, and enter the MTU value.
- For a WAN interface, go to the System > WAN screen, select Configure > Configure, and enter the MTU value.

To find out the current MTU of the interface through the CLI, use the **`show interface`** command (see "Displaying the MTU and TCP MSS values of an interface" on page 66). To change the MTU on an interface, navigate to the interface and execute the **`mtu`** command.

1. Access the command line interface in one of two ways:
   - Connect a terminal or PC to the serial port on the gateway. From the Serial Port menu, enter **`L`** to access the command line interface.
   - Establish a Telnet session with the gateway's management IP address.
2. At the Login prompt, log in to the gateway using an account with administrator privileges, for example:

   ```
   Login: admin
   Password:<password>
   CES>
   ```

3. At the User EXEC mode prompt (`CES>`), go to Privileged EXEC mode and then to Global Configuration mode.

   ```
   CES> enable
   Password:<password>
   CES# configure terminal
   CES(config)#
   ```

4. Navigate to the interface whose MTU you need to change.

   In this example, you go to Ethernet interface 1/1.

   ```
   CES(config)# interface fastethernet 1/1
   ```

5 Set the MTU to the new value in bytes.

```
CES(config-if)# mtu 1500
CES(config-if)# exit
CES(config)#
```

To reset the MTU on an interface to its default value, navigate to the interface and use the **no mtu** command. In the following example, you go to ISDN BRI interface 3/1.

```
CES(config)# interface bri 3/1
CES(config-if)# no mtu
CES(config-if)#
```

Displaying the MTU and TCP MSS values of an interface

To see the value of the MTU, use the **show interface** command. The syntax of this command is as follows:

show interface *<interface-type> <slot>*/*<port>*

For example, to display configuration parameters (including the MTU) for the Ethernet interface in slot 1 port 1, enter the following command:

```
CES# show interface fastethernet 1/1
Fastethernet Interface 1/1 Configuration
  Description                      : PPPoE
  DHCP-relay                       : Disabled
  Duplex                           : AutoNegotiate
  Filter                           : permit all
  IP Address                       : 1.1.1.1
  MAC-pause                        : Disabled
  MTU [bytes]  : 1200
  PPPoE                            : Enabled
  Public/Private                   : Public
  Service (DHCP)                   : Enabled
  Status                           : Up
  Speed [Mbps]                     : AutoNegotiate
  TCP-Maximum Segment Size Clamping: Enabled
  TCP-Maximum Segment Size [bytes] : 1460
CES#
```

Configurable TCP MSS clamping

You can configure the TCP maximum segment size (MSS) on all interfaces. The TCP MSS specifies the largest TCP packet that can be sent between TCP peers. You configure the TCP MSS independently from the MTU size.

Note: On most PCs and the Contivity gateway, the default value for the TCP MSS is MTU – 40 bytes.

TCP MSS *clamping* is the substitution of a configured MSS for the MSS value negotiated with the TCP peer. To implement TCP MSS clamping, you must configure it on the interfaces that will receive or transmit the plain-text packets. When you configure TCP MSS clamping, the packets affected are already "clamped" when they go through a tunnel.

Resetting the TCP MSS on an interface

To change the current TCP MSS of an interface through the GUI:

- For a LAN interface, go to the System > LAN Edit screen, select tht Enabled or Disabled option, and enter the TCP MSS value.
- For a WAN interface, go to the System > WAN > Configure > Configure screen, select the TCP MSS Option (enabled or disabled), and enter the TCP MSS value.

To find out the current TCP MSS of an interface through the CLI, use the **`show interface`** command (see "Displaying the MTU and TCP MSS values of an interface" on page 66).

To change the TCP MSS on an interface, navigate to the interface and execute the **`tcp-mss`** command.

1 Access the command line interface in one of two ways:

   - Connect a terminal or PC to the serial port on the gateway. From the Serial Port menu, enter **`L`** to access the command line interface.
   - Establish a Telnet session with the gateway's management IP address.

2 At the Login prompt, log in to the gateway using an account with administrator privileges, for example:

```
Login: admin
Password:<password>
CES>
```

3 At the User EXEC mode prompt (CES>), go to Privileged EXEC mode and then to Global Configuration mode.

```
CES> enable
Password:<password>
CES# configure terminal
CES(config)#
```

4 Navigate to the interface whose TCP MSS you need to change.

In this example, you go to Ethernet interface 1/1.

```
CES(config)# interface fastethernet 1/1
```

5 Set the MSS to the new value in bytes (from 536 through 1748).

```
CES(config-if)# tcp-mss 1500
CES(config-if)#
```

To reset the TCP MSS on an interface to its default value, navigate to the interface and use the **no tcp-mss** command. In the following example, you go to serial interface 4/1 and reset the MSS to the default value (1460).

```
CES(config)# interface serial 4/1
CES(config-if)# no tcp-mss
CES(config-if)#
```

Enabling TCP MSS clamping

To find out the whether TCP MSS clamping is enabled on an interface, use the **show interface** command (see "Displaying the MTU and TCP MSS values of an interface" on page 66).

To enable TCP MSS clamping on an interface, navigate to the interface and execute the **tcp-mss enable** command.

1 Navigate to the interface where you will enable TCP MSS clamping.

In this example, you go to Ethernet interface 1/1.

```
CES(config)# interface fastethernet 1/1
```

2 Enter the following command:

```
CES(config-if)# tcp-mss enable
CES(config-if)#
```

To disable TCP MSS clamping on an interface, navigate to the interface and execute the **no tcp-mss enable** command.

```
CES(config)# interface serial 4/1
CES(config-if)# no tcp-mss enable
CES(config-if)#
```

Interface MTU and TCP MSS configuration commands

This section describes the interface MTU and TCP MSS configuration commands.

mtu (interface)

Use this command to reset the maximum transmission unit (MTU) of an interface. Use the **no** form of the command to reset the MTU value to its default value (see Table 6 on page 70).

The MTU specifies the largest packet that can be sent out an interface; if a packet to be sent is larger than the MTU configured for the interface, the packet is fragmented or dropped. You can reset the MTU value as follows:

- For LAN interfaces: 576 through 1500 bytes
- For PPPoE interfaces 576 through 1492
- For WAN interfaces: 576 through 1788 bytes

Syntax

mtu *<bytes>*
no mtu

Parameters

bytes	Specifies the maximum transmission unit in bytes. For an Ethernet interface, enter a value from 576 through 1500; for a PPPoE interface enter a value from 576 through 1492; for other interfaces, enter a value from 576 through 1788.

Default

The default MTU value for each interface is based on the media type minus the Layer 2 encapsulation (Table 6).

Table 6 Default MTU by interface

Media/interface	Default MTU (bytes)
Ethernet	1500
Frame relay	1496
ISDN	1500
PPPoE	1492
Serial	1500
WAN (T1/T3)	1788

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show interface
tcp-mss
tcp-mss enable

Example

The following example sets the MTU for Ethernet interface 2/1 to 1400 bytes.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# mtu 1400
CES(config-if)#
```

The following example resets the MTU size to its default value (for an Ethernet interface, 1500 bytes).

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no mtu
CES(config-if)#
```

tcp-mss

Use this command to configure the TCP maximum segment size (MSS) on an interface. The TCP MSS specifies the largest TCP packet that can be sent between TCP peers. You configure the TCP MSS independently from the MTU size.

Use the **no** form of the command to reset the TCP MSS to its default value. (On most PCs and the Contivity gateway, the default value for the TCP MSS is MTU – 40 bytes.)

Syntax

tcp-mss *<bytes>*
no tcp-mss

Parameters

bytes	Specifies the maximum amount of TCP data in bytes. For an Ethernet interface, enter a value from 536 through 1460; for other interfaces, enter a value from 536 through 1748.

Default

1460

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

mtu
show interface
tcp-mss enable

Examples

The following example sets the TCP MSS to 1400 bytes on Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# tcp-mss 1400
CES(config-if)#
```

The following example resets the TCP MSS on serial interface 4/1 to its default value (1460).

```
CES(config)# interface serial 4/1
CES(config-if)# no tcp-mss
CES(config-if)#
```

tcp-mss enable

Use this command to enable TCP MSS clamping. TCP MSS clamping is the substitution of a configured MSS for the MSS value negotiated with the TCP peer. To implement TCP MSS clamping, you must configure it on the interfaces that will receive or transmit the plain-text packets. When you configure TCP MSS clamping, the packets affected are already "clamped" when they go through a tunnel. Use the **no** form of the command to disable TCP MSS clamping.

Syntax

```
tcp-mss enable
no tcp-mss enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

mtu
show interface
tcp-mss

Examples

The following example enables TCP MSS clamping on serial interface 4/1.

```
CES(config)# interface serial 4/1
CES(config-if)# tcp-mss enable
CES(config-if)#
```

The following example disables TCP MSS clamping on serial interface 4/1.

```
CES(config)# interface serial 4/1
CES(config-if)# no tcp-mss enable
CES(config-if)#
```

Tunnel MTU and IPsec DF bit configuration commands

This section describes the tunnel MTU and IPsec DF bit configuration commands.

mtu (branch office tunnel)

Use this command to reset the maximum transmission unit (MTU) for a branch office tunnel. The MTU specifies the largest packet that can be sent over the tunnel; if a packet to be sent is larger than the configured MTU, the packet is fragmented or dropped. Use the **no** form of the command to reset the MTU value to its default value (1788 bytes).

Syntax

```
mtu <bytes>
no mtu
```

Parameters

bytes	Specifies the maximum transmission unit in bytes. Enter a value from 576 through 1788 bytes.

Default

1788

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

mtu enable
show bo-conn

Example

The following example sets the MTU for the branch office tunnel “test” to 1400 bytes.

```
CES(config)# bo-conn test /Base
CES(config-bo_conn)# mtu 1400
CES(config-bo_conn)#
```

The following example resets the MTU size for the branch office tunnel “test” to its default value (1788 bytes).

```
CES(config)# bo-conn test /Base
CES(config-bo_conn)# no mtu
CES(config-bo_conn)#
```

mtu enable

Use this command to enable a user-configured maximum transmission unit (MTU) for a branch office tunnel. The MTU specifies the largest packet that can be sent over the tunnel; if a packet to be sent is larger than the configured MTU, the packet is fragmented or dropped. Use the **no** form of the command to disable the use of a configured MTU value over the branch office tunnel.

Syntax

mtu enable
no mtu enable

Parameters

None

Default

Enabled

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

mtu
show bo-conn

Example

The following example disables the use of a configurable MTU for the branch office tunnel “test.”

```
CES(config)# bo-conn test /Base
CES(config-bo_conn)# no mtu enable
CES(config-bo_conn)#
```

The following example sets the MTU for the branch office tunnel “test” to 1500 bytes and enables the use of the edited MTU.

```
CES(config)# bo-conn test /Base
CES(config-bo_conn)# mtu 1500
CES(config-bo_conn)# mtu enable
CES(config-bo_conn)#
```

df-bit

Use this command to set the don't fragment (DF) bit in the outer IP header of an IPsec-encapsulated packet. Depending on the setting of the DF bit in the IP header, packets larger than the MTU configured for the tunnel are either fragmented or dropped.

By default, the gateway clears the DF bit in the outer IP header to allow fragmenting (and sending) of packets that are larger than the MTU. You can configure the gateway to set the DF bit in the outer IP header or to copy the value for the DF bit that is specified in the inner IP header.

Note: The DF bit setting specified in this configuration mode overrides any other DF bit settings configured in other modes.

Syntax

```
df-bit {clear | copy | set}
```

Parameters

clear	Specifies that the outer IP header will have the DF bit cleared and that the gateway may fragment the packet to add the IPsec encapsulation.
copy	Specifies that the gateway will copy the DF bit setting in the original packet to the outer IP header.
set	Specifies that the outer IP header will have the DF bit set; however, the gateway may fragment the packet if the original packet had the DF bit cleared.

Default

clear

Command mode

Branch Office Group IPsec Configuration

Next command mode

Branch Office Group IPsec Configuration

Required privileges

System Management - None
User Management - Manage

Related commands

None

Example

The following example sets the DF bit on all packets that traverse IPsec tunnels created for the group /Base/test.

```
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# df-bit set
CES(config-bo_group/ipsec)#
```

The following example copies the DF bit from the inner IP header to the outer header on all packets that traverse IPsec tunnels created for the group /Base/test.

```
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# df-bit copy
CES(config-bo_group/ipsec)#
```

The following example clears the DF bit from the outer IP header of all packets that traverse IPsec tunnels created for the group /Base/test.

```
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# df-bit clear
CES(config-bo_group/ipsec)#
```

Chapter 4
Using packet capture (PCAP)

Packet capture (PCAP) allows network administrators and customer support personnel to remotely troubleshoot various Contivity gateway and network problems. Packet capture is especially useful with a gateway such as the Contivity 1100, which is typically located in a small office where no technical expertise may be available.

This chapter contains the following topics.

Command	Page
PCAP overview	81
Enabling and configuring packet capture	88
Viewing a packet capture output file on a PC	94
PCAP commands	97

PCAP overview

Packet capture is a troubleshooting tool that you can use in conjunction with other tools, such as statistics, logging, network analyzers, and testers. Using packet capture, a network manager or support engineer can capture packets traversing the Contivity gateway and write them to disk in a format that can be read with common packet analyzer tools such as the Network General Sniffer.

Packets are captured in a PCAP buffer in memory and are not written to the disk until you stop the capture and save the captured data to a file on the disk. You can then download the file and analyze the contents offline using one of many available tools.

This section contains the following topics.

Command	Page
PCAP features	82
File format	83
Capture types	83
Filters and triggers	85
Saving captured data	87
Memory considerations	87
Performance considerations	87

PCAP features

The Nortel Networks implementation of packet capture enables the Contivity gateway to perform the following tasks:

- Simultaneously capture network traffic at different sources (Ethernet and serial interfaces, tunnels, and the gateway as a whole).
- Limit the traffic to be captured by using traffic filters.
- Automatically start and stop packet capture with triggers.
- Provide gzip compression of captured data when saving it to the disk.

Security features

Following are security features for packet capture:

- Packet capture is disabled by default. You can enable packet capture using the CLI through the serial port only.
- To enable packet capture, you must configure a separate capture password. You must enter the capture password to decrypt the data.
- When you save a capture buffer to a file on disk, the file is encrypted; the capture password is encrypted with the file.

- To open a capture file, you can use a tool called **`openpcap`** that is shipped with Contivity software (in the tools directory on the software CD). It is built for both 128-bit and 56-bit versions. The tool uses the same cryptographic library that the server code uses. The **`openpcap`** tool prompts you for a password.
- Packet capture configuration is not saved in LDAP or in the configuration file. When you reboot the gateway, the packet capture configuration is lost.

File format

Packets are stored in PCAP/TCPDUMP file format. This file format is recognized by many tools.

- PCAP format has a header that specifies the link type of saved packets. All packets in one file must be of the same link type.
- Packet is saved with the following additional information:
  - Timestamp of the packet
  - Length of the portion of the packet present in the PCAP file
  - Length of the entire packet as it was received/sent on the wire

The following restrictions apply:

- You cannot save packets from different types of interfaces in one file.
- Multiple packet capture objects can exist for the same source (for example, an interface or tunnel), but only one object can run at any one time. However, objects on different sources can be run at the same time.

Capture types

The Nortel Networks implementation of packet capture enables the Contivity gateway to capture packets from the following sources:

- Physical interfaces, including the following:
  - Fast Ethernet and Gigabit Ethernet, including traffic that is not directed to the Contivity gateway (promiscuous mode)
  - Dial (V.90 and asynchronous PPP)
  - ISDN BRI

  - — Serial
- Tunnels
  - — Branch offices
  - — Asynchronous branch offices
  - — User tunnels
- All IP traffic on the gateway

The following sections describe each type of capture.

Physical interface captures

Packet capture of traffic on a physical interface can help you to troubleshoot Layer 2 issues, connectivity issues, and performance issues. The Layer 2 header is saved in the PCAP file for each packet. PCAP files that contain traffic captured on a physical interface can be converted to most file formats including Sniffer.

Tunnel captures

Packet capture of traffic over tunnels can help you to troubleshoot a specific tunnel problem. For example, you could create a tunnel capture object to diagnose the following types of problems: a protocol not working for a particular user; performance issues for a particular user; OSPF not working properly inside a specific branch office tunnel. Raw IP encapsulation is used.

You can configure a capture object for an existing tunnel or for tunnels that have yet to be initiated. You can also enable *persistent mode* for tunnel capture objects. When persistent mode is enabled and a captured tunnel disconnects, packet capture restarts automatically when it encounters another tunnel that matches the capture criteria. Tunnel capture criteria include the following:

- Tunnel type: user tunnel, branch office, ABOT initiator, ABOT responder, IPsec, L2TP, PPTP, or L2F
- IP address of the peer on the tunnel session
- User ID (or another criterion to specify the user)

If you start a tunnel capture object and more than one tunnel matches the capture criteria, only the first tunnel is captured. If no tunnel matches the criteria, packet capture waits for a tunnel that matches the criteria. If you configure more than one capture object with the same criteria, the first matching tunnel uses the first PCAP object, and the next matching tunnel uses the other capture object. In this way, you can capture a set of tunnels with the same criteria in different capture files.

For performance reasons, only one capture object can be running at one time for a specific tunnel. Multiple tunnel capture objects can run at the same time, but each object must capture different tunnels.

Global IP captures

Global (raw) IP packet capture captures all IP traffic traversing any physical interface or tunnel on the gateway. Only one global IP capture object can run at one time. Packets are captured as they are encapsulated or decapsulated (depending on the capture direction that you configure). To restrict the amount of traffic captured by a global IP capture, configure filters (see "Filters and triggers" on page 85).

A global IP capture object captures packets beginning from the IP header; no Layer 2 header is saved in the capture file. Because both encrypted and decrypted packets can be captured, global IP packet capture can be useful in troubleshooting certain VPN issues.

Note: If capture objects for physical interfaces or tunnels are running at the same time as a global IP capture object, performance on the gateway will be affected.

Filters and triggers

Existing interface filters can be applied to a capture object as a capture filter, a start trigger, or a stop trigger. You configure capture filters, start triggers, and stop triggers independently.

Capture filters

To apply a filter to a capture object, you must first stop the capture object if it is running. When applied, filters are compiled. When you delete a capture object or change the filters on an object, the old filters are freed.

No non-IP frames will match any filter or trigger. For example, if you configure a capture object with a filter for a serial interface configured with PPP, no LCP traffic will match filter criteria on a capture object. You can configure the capture object to always capture non-IP frames or always discard them.

Triggers

You can configure existing interface filters as triggers for capture objects. A trigger causes a capture object to start or stop automatically when certain packets are received. (By default, the system saves frames to the capture buffer as soon as capture is started.)

- A start trigger causes the system to wait for a specific packet before it starts saving packets to the capture buffer.
- A stop trigger causes the system to stop saving traffic in the capture buffer after a specific packet matching the stop trigger is encountered. Capture, however, is not fully stopped.

The use of a start and a stop trigger allows capturing specific transaction-oriented traffic. Triggers can also be used with filters to allow still greater flexibility. The packets that triggered the capture object to start or stop are also captured if they match capture filters (if any). If you set both a start and a stop trigger, the start trigger can reenable saving traffic to a capture buffer.

A trigger works only for the direction that the capture is configured for. For example, if you enable a capture for outgoing traffic only, and the type of packet that triggers the capture to start or stop arrives only in incoming packets, the trigger will never work. In the absence of a start trigger, a stop trigger will not work. A start trigger and a stop trigger can both be activated on the same packet. In this case, only one packet ia captured. Triggers never match non-IP frames.

Saving captured data

The command **`capture save`** is used to save captured network traffic from buffer in memory to a disk file. Capture must be stopped before this command can be used.

Memory considerations

The number of packet capture objects that can be allocated on a Contivity gateway is limited by the amount of contiguous memory available on the gateway. When you create a capture object, you can specify the capture buffer size (the default buffer size is 1 MB).

You can create new capture objects until the maximum block size reaches 25 MB. The gateway does not allow you to reduce the maximum block size to less than 25 MB. If you allocate too much memory to packet capture buffers, a buffer will not be allocated and you will see an error message suggesting a smaller buffer size.

To check the maximum block size, go to the GUI page Status > Statistics and click on Memory in the Resources section of the page. Scroll to the bottom of the page to find the maximum block size. The output looks similar to this:

```
Shared Heap Statistics:
 status   bytes    blocks   ave block  max block
 ------ --------- -------- ---------- ----------
current
   free  40542960       18    2252386  39532912
  alloc  64815872      135     480117         -
```

You can display the same information by executing the command **`show status statistics resources memory`**.

Performance considerations

Enabling packet capture may have an effect on Contivity performance. For this reason, packets are saved in the capture buffer and only written to disk when you stop and save the file.

Only one capture object can be running at one time for a specific source (interface or tunnel). Multiple capture objects can exist on the same source, but only one object is allowed to start. Capture objects on different sources can be running at the same time with no limitations.

To reduce the effect on gateway performance, use packet capture for troubleshooting only and observe the following guidelines:

- Configure the capture object to capture less data (only the first *n* bytes of the packet).
- Configure filters and triggers to capture only relevant traffic (see "Filters and triggers" on page 85).
- When you no longer need a capture object, delete it to free up disk space.
- Do not run capture objects for physical interfaces or tunnels at the same time as a global IP capture object (some packets will be captured more than once).

Enabling and configuring packet capture

Enable and configure packet capture as described in the following sections.

Enabling packet capture on a Contivity gateway

A serial connection is required to enable packet capture; you cannot do enable capture via a Telnet session. To prepare to run packet capture on the gateway:

1. If the administrator password on the gateway is still set to its default value, change the password.
   - From the GUI, choose Admin > Administrator.
   - From the command line interface, execute the command **`adminname`** *`<admin_name>`* **`password`** *`<new_password>`*

Caution: Make sure to remember the new administrator password. If you lose it, you will not be able to manage the gateway.

2. If necessary, boot the gateway with a software version that has the PCAP feature.

3 Turn on the terminal or PC.

The terminal or PC should be configured as follows:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No flow control

4 Connect the serial cable (supplied with the gateway) from the gateway's serial port to a terminal or to the communications port on a PC.

5 On the PC, start HyperTerminal* or another terminal emulation program and press Enter.

The Welcome screen appears.

```
Welcome to the Contivity Secure IP Services Gateway
Copyright (c) 1999-2003 Nortel Networks, Inc.

Version:              V04_90.155
Creation date:        May 27, 2004, 20:51:06
Date:                 05/27/2004
Unit Serial Number:   317563

Please enter the administrator's user name:
```

6 Enter the administrator's user name and password.

```
Please enter the administrator's user name: admin

Please enter the administrator's password: *****
```

The serial main menu appears.

```
Main Menu: System is currently in NORMAL mode.

   1) Interfaces
   2) Administrator
   3) Default Private Route Menu
   4) Default Public Route Menu
   5) Create A User Control Tunnel(IPsec) Profile
   6) Restricted Management Mode FALSE
   7) Allow HTTP Management TRUE
   8) Firewall Options
   9) Shutdown
   B) System Boot Options
   P) Configure Serial Port
   C) Controlled Crash
   L) Command Line Interface
   R) Reset System to Factory Defaults
   E) Exit, Save and Invoke Changes

   Please select a menu choice (1 - 9,B,P,C,L,R,E): L
```

7 Access the command line interface by typing the letter “L” (uppercase or lowercase) at the prompt.

The User EXEC prompt appears:

```
CES>
```

8 Enter Privileged EXEC mode and type **`capture enable`**.

```
CES>enable
Password:
```

9 Enable packet capture globally on the gateway and create the capture password. You use this password to open capture files with the **`openpcap`** utility. Enter at least eight characters for the capture password and include at least one number.

```
CES#capture enable
Please specify password for encrypting capture files.
Password: ********
Reenter password: ********
```

10 If you want, you can now change the gateway administrator password.

```
CES#configure terminal
Enter configuration commands, one per line.  End with
Ctrl/z.
```

```
CES(config)#adminname <admin_name> password <new_password
CES(config)#exit
CES#
```

You can now configure and start packet capture objects.

Sample packet capture objects

This section provides examples of capture objects. For complete information about the packet capture commands, see "PCAP commands" on page 97. Commands are shown for creating, starting, stopping, and saving a PCAP object.

Physical interface

The following example configures a capture object for the Ethernet interface 0/1. The commands create the object (called "ether0"), navigate to Capture Configuration mode, display all commands in Capture Configuration mode, start the capture object, stop it, save the buffer to a file called ether0.cap, and finally clear the capture buffer.

Note: The **promiscuous** parameter is available only for Ethernet capture objects.

```
CES#capture add ether0 fastether 0/1
CES#capture ether0
CES(capture-ethernet)#?
Packet capture mode
  direction        Captures in one direction
  exit             Exits capture mode
  filter           Applies interface traffic filter to capture only
                   matching traffic
  length           Specifies how many octets to capture for every packet
  no               Disables features and settings
  promiscuous      Enables promiscuous mode when capture is running.
  Trigger          Enables triggers
  wrapping  Continues capturing when buffer gets full
CES#capture ether0 start
CES#capture ether0 stop
CES#capture ether0 save ether0.cap
CES#clear capture ether0
```

Tunnel capture

The following example configures a capture object for a tunnel. The commands create the object (called “bot1”), navigate to Capture Configuration mode, display all commands in Capture Configuration mode for tunnel objects, start the capture object, stop it, save the buffer to a file called bot1.cap, and finally clear the capture buffer.

Note: A tunnel capture object has several parameters (**persistent**, **remoteip**, **type**, and **userid**) available only for tunnel objects.

```
CES#capture add bot1 tunnel
CES#capture bot1
CES(capture-tunnel)#?
Packet capture mode
  direction   Captures in one direction
  exit          Exits capture mode
  filter        Applies interface traffic filter to capture only
                matching traffic
  length       Specifies how many octets to capture for every packet
  no            Disables features and settings
  persistent  Restarts capture on session disconnect.
  Remoteip    Captures sessions from this ip
  trigger       Enables triggers
  type          Captures only sessions of specific type
  userid        Captures sessions from this user
  wrapping   Continues capturing when buffer gets full
CES(capture-tunnel)#type peer2peer
CES#capture bot1 start
CES#capture bot1 stop
CES#capture bot1 save bot1.cap
CES#clear capture bot1
```

Global IP capture

The following example configures a capture object for global IP on the gateway. The commands create the object (called “global”), navigate to Capture Configuration mode, display all commands in Capture Configuration mode for global IP objects, start the capture object, stop it, save the buffer to a file called rawip1.cap, and finally clear the capture buffer.

```
CES#capture add rawip1 global
CES#capture rawip1
CES(capture-global)#?
Packet capture mode
  direction    Captures in one direction
  exit            Exits capture mode
  filter         Applies interface traffic filter to capture
only matching traffic
  length      Specifies how many octets to capture for every
packet
  no             Disables features and settings
  trigger       Enables triggers
  wrapping   Continues capturing when buffer gets full
CES#capture rawip1 start
CES#capture rawip1 stop
CES#capture rawip1 save rawip1.cap
CES#clear capture rawip1
```

Sample show capture commands

Following are examples of the **show capture** command. In this example, the command is entered with no parameters to display a list of all the capture objects configured on the gateway.

```
CES# show capture
Name        Type                  Size     Buffer use   Count     State
bot1        TUNNEL                1048576     0%          0       EMPTY
ether0      ETHERNET              1048576     7%          984     STOPPED
rawip1      GLOBAL              1048576     0%         0       EMPTY
```

The first example shows the type of output you see when you enter the **show capture** command for a specific capture object.

```
CES# show capture bot1
Capture state:                              EMPTY
Capture buffer size:                        1048576
Capture type:                               TUNNEL
Restarting capture on tunnel logoff:        DISABLED
Capturing MAX octets per frame:             4096
Captured frames:                            0
Capture buffer utilization:                 0%
Capturing direction:                        BIDIRECTIONAL
Capture buffer wrapping:                    DISABLED
Capture buffer wrapped:                     FALSE
CES#
```

Viewing a packet capture output file on a PC

After you save a capture buffer to a file on the gateway disk, you can download the file to a workstation and analyze the contents offline using one of many available tools. The Contivity gateway does not provide a utility to analyze packet capture data; however, it provides a utility called **openpcap** that you use to view the file.

- To view a packet capture file with Ethereal* software, you can use the **openpcap** utility supplied with the Contivity software.
- To view a packet capture file with Sniffer Pro* software, you can use the **openpcap** utility supplied with the Contivity software along with the Ethereal **editpcap** utility.

Installing Ethereal software

To install Ethereal (free of charge):

1. Log on to www.ethereal.com and click on Download.
2. Locate the Microsoft Windows row and click on “local archive.”
3. Click on ethereal-setup-*n.nn.n*.exe.
4. Click on a download site and save the executable file on your hard drive.

5 Double-click on the executable file to install Ethereal software in the c:\Program Files\Ethereal directory.

6 After you install the software, click on the Ethereal application to open Ethereal window.

Saving, downloading, and viewing PCAP files

To save and download a PCAP file and view it using the Contivity **`openpcap.exe`** utility and Ethereal software:

1 On your PC, create a PCAP directory called **`c:\pcap`**.

2 In the **`c:\pcap\`** directory, copy the **`openpcap.exe`** file that is provided with the Contivity packet capture software.

3 On the gateway, stop the packet capture object and save the output to a file, for example:

```
CES#capture ethernet1 stop
CES#capture ethernet1 save ethernet.cap
Saving capture ethernet to file /ide0/ethernet.cap
please wait . . 82 frames written successfully.
```

Note: If you are running PCAP on a gateway that has two hard drives, PCAP files may be saved to directory **`/ide1`**.

4 On the PC, use FTP software to connect to the Contivity gateway and copy the **`ethernet.cap`** file located in the **`/ide0/`** directory to the **`c:\pcap`** directory on the PC.

5 Open a DOS window and from the **`c:\pcap`** directory, open the PCAP file **`ethernet.cap`** by using the **`openpcap`** executable. For example, enter this command (syntax is **`openpcap`** *<input_file> <output_file>*):

```
openpcap ethernet.cap ether1.cap
```

You are prompted for a password.

6 Enter the password that was set when packet capture was initially enabled.

Note: If you plan to use Sniffer Pro to view the capture file, go to the next section, "Viewing a PCAP file with Sniffer Pro" on page 96).

7 From the open Ethereal GUI window, disable Enable network name resolution by clicking on the checkbox.

If this parameter is enabled, a large PCAP file will take a long time to open because every address captured will try to perform name address resolution.

8 Open the packet capture file (for example, **`ethernet.cap`**).

Viewing a PCAP file with Sniffer Pro

Because Sniffer Pro is not free shareware, it is assumed that you have already installed the software on the PC.

1 Install Ethereal software as described in "Installing Ethereal software" on page 94.

2 Save the packet capture file and download it to the PC as described in steps 1-6 of "Saving, downloading, and viewing PCAP files" on page 95.

You must install the Ethereal software to view the PCAP file with Sniffer Pro.

3 Open a new DOS window and change directory to the c:\Program Files\Ethereal directory to access the **`editcap`** command.

4 Find the appropriate example of how to use the **`editcap`** command so that Sniffer Pro can view the capture:

- D:\Program Files\Ethereal>editcap -T ether -F ngsniffer d:\pcap\ipsec.cap ipsec.enc (packet capture of an IPsec tunnel)
- D:\Program Files\Ethereal>editcap -T ether -F ngsniffer d:\pcap\rawip.cap rawip.enc (packet capture of global IP data)
- D:\Program Files\Ethereal>editcap -T ether -F ngsniffer d:\pcap\ether.cap ether1.enc (packet capture of an Ethernet interface)
- D:\Program Files\Ethereal>editcap -T ether -F ngsniffer d:\pcap\fr.cap frelay.syc (packet capture of a T1 frame relay interface)

- D:\Program Files\Ethereal>editcap -T ether -F ngsniffer d:\pcap\hssi.cap hssi.syc (packet capture of a HSSI PPP interface)

5 From Sniffer Pro, open the **`.enc`** file or the **`.syc`** file to view trace.

For a global IP trace or tunnel trace, you must perform an extra step on Sniffer Pro because only Layer 3 traffic is recorded in the PCAP capture.

6 Before opening a global IP or tunnel trace on Sniffer Pro, set the following option in Sniffer Pro: Click on Tools > Options > Protocol Forcing.

7 Click on Rule 1 and specify if <Frame Start>, Skip 0 bytes, then Internet Protocol.

8 Click on OK and then open the file.

This procedure allows you to view the correct Layer 3 information.

PCAP commands

This section describes packet capture commands.

Command	Page
capture	98
capture add	100
capture enable	102
capture save	104
capture start	106
capture stop	108
clear capture	109
direction	111
filter	113
length	115
persistent	117
promiscuous	119
remoteip	120

Command	Page
show capture	122
trigger	126
type	128
userid	131
wrapping	133

capture

Use this command to enter capture mode for an existing capture object. Use the **no** form of the command to delete the specified capture object.

Syntax

capture *<name>*
no capture *<name>*

Parameters

name	Specifies the name of an existing capture object.

Default

None

Command mode

Privileged EXEC

Next command mode

Capture Configuration (**capture** command)
Privileged EXEC (**no capture** command)

Required privileges

System Management - Manage
User Management - None

Prerequisites

To delete a capture object, you must first stop packet capture.

Warning messages

```
% Capture must be stopped first
% Capture object name does not exist
```

Related commands

capture add
capture enable
show capture

Example

The following example navigates to capture mode for the object “test.”

```
CES# capture test
CES(capture-ethernet)#
```

The following example deletes the capture object “test.”

```
CES# no capture test
CES#
```

capture add

Use this command to create a new capture object and to specify the size of the capture buffer for it (the default buffer size is 1 MB).

Syntax

capture add *<name>* {**bri** | **dial** | **fastethernet** | **gigabitethernet** | **serial**} *<slot>*/*<port>* [**size** *<octets>*]

capture add *<name>* {**global** | **tunnel**} [**size** *<octets>*]

Parameters

name	Specifies the name of the capture object to be created. This name must be unique on the gateway.
bri	Create a capture object for an ISDN BRI interface.
dial	Create a capture object for a dial interface.
fastethernet	Create a capture object for a Fast Ethernet interface.
gigabitethernet	Create a capture object for a Gigabit Ethernet interface.
serial	Create a capture object for a serial interface.
slot	For interface objects, specifies the slot of the interface card.
port	For interface objects, specifies the port on the interface card.
global	Create a capture object for all IP traffic traversing any physical interface or tunnel on the gateway.
tunnel	Create a capture object for a tunnel.
size	Specify the size of the capture buffer (default is 1 MB).
octets	Specifies the number of octets to allocate to the capture buffer. You can enter a value from 32768 through 268435456. The default value is 1 MB.

Default

Buffer size is 1 MB.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% add is not a valid name for capture object
% enable is not a valid name for capture object
% Capture object name already exists
% Console is not in PPP Async mode
% Interface x/y is not a dial interface
% Interface x/y is not a Fast Ethernet interface
% Interface x/y is not a Gigabit Ethernet interface
% Interface x/y is not an ISDN BRI interface
% Interface x/y is not a Serial interface
```

Related commands

capture
capture enable
show capture

Example

The following example creates a capture object named “test1” for Fast Ethernet interface 1/1 and allocates 128,000 octets to the capture buffer.

```
CES# capture add test1 fastethernet 1/1 size 128000
CES#
```

The following example creates a capture object named “test2” for a tunnel session.

```
CES# capture add test2 tunnel
CES#
```

The following example creates a capture object named “test3” to capture all IP traffic going through the gateway.

```
CES# capture add test3 global
CES#
```

capture enable

Use this command from the console port of the gateway to globally enable packet capture on the Contivity gateway. When you execute this command, you must enter a password to be used only by packet capture. This password must have at least eight characters and include at least one number.

Note: You must execute this command from the console port of the gateway before you can execute other packet capture commands from the command line interface.

Use the **no** form of the command to disable packet capture globally.

Syntax

```
capture enable
no capture enable
```

Parameters

None

Default

Disabled

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

You must change the administrator password from its default value before you execute the **`capture enable`** command.

Warning messages

```
% Administrator password must be changed first.
% Capture already enabled.
% Error reading password!
% Packet capture must be enabled from the console port.
% Passwords do not match!
% Weak password! Please try again.
```

Related commands

`capture add`
`capture start`
`capture stop`
`show capture`

Example

The following example enables packet capture globally. The password must have at least eight characters and include at least one number.

```
CES# capture enable
Please specify password for encrypting capture files.
Password: ********
Reenter password: ********
CES#
```

The following example disables packet capture globally.

```
CES# no capture enable
CES#
```

capture save

Use this command to save captured network traffic to the specified file on the Contivity system disk. The file is saved in encrypted form, along with the password you entered with the **`capture enable`** command.

Syntax

`capture` *<name>* **`save`** *<file-name>*

Parameters

name	Specifies the name of an existing capture object.
file-name	Specifies the name of the disk file to write network traffic to.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

You must stop the capture object before you can execute this command.

Warning messages

```
% Capture must not be running
% Capture buffer is empty, nothing to save
% Capture object name does not exist
```

Related commands

capture start
capture stop
clear capture
show capture

Example

The following example saves captured network traffic to the file eth-mgmt.cap on disk ide1.

```
CES# capture test save /ide1/eth-mgmt.cap
Saving capture test to file /ide1/eth-mgmt.cap please wait .
. .
112 frames written successfully.
CES#
```

capture start

Use this command to start capturing network traffic.

Syntax

capture *<name>* **start**

Parameters

name	Specifies the name of an existing capture object.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must already exist.

Warning messages

```
% Capture already running
% Capture object name does not exist
```

Related commands

capture add
capture enable
capture save
capture stop
show capture
trigger

Example

The following example starts packet capture on the gateway.

```
CES# capture test start
CES#
```

capture stop

Use this command to stop capturing network traffic.

Syntax

capture *<name>* **stop**

Parameters

name	Specifies the name of an existing capture object.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must have been started.

Warning messages

```
% Capture not running
% Capture object name does not exist
```

Related commands

capture add
capture enable
capture save
capture start
show capture
trigger

Example

The following example stops packet capture on the gateway.

```
CES# capture test stop
CES#
```

clear capture

Use this command to clear captured network traffic from the capture buffer of the specified capture object.

Syntax

clear capture *<name>*

Parameters

name	Specifies the name of an existing capture object.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
% Capture object name does not exist
% Packet capture must be enabled from the console port
```

Related commands

capture add
capture save
capture start
capture stop
show capture
wrapping

Example

The following example clears the capture buffer of the capture object “test.”

```
CES# clear capture test
CES#
```

direction

Use this command to set the direction of the traffic to be captured. If no direction is specified, PCAP will capture both inbound and outbound traffic. Use the **no** form of the command to reset packet capture to its default behavior, that is, capture both inbound and outbound traffic.

Syntax

```
direction {inbound | outbound}
no direction
```

Parameters

inbound	Capture inbound packets only.
outbound	Capture outbound packets only.

Default

Capture both inbound and outbound traffic.

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture
filter
length
show capture
trigger
wrapping

Example

The following example configures packet capture to capture inbound traffic only.

```
CES(capture-ethernet)# direction inbound
CES(capture-ethernet)#
```

The following example configures packet capture to capture outbound traffic only.

```
CES(capture-global)# direction outbound
CES(capture-global)#
```

The following example resets packet capture to its default behavior, that is, to capture both inbound and outbound traffic.

```
CES(capture-tunnel)# no direction
CES(capture-tunnel)#
```

filter

Use this command to apply an existing interface filter to a capture object. When you apply a filter, packet capture saves to its buffer only traffic that matches the filter. A filter matches IP traffic only.

By default, if a filter is set, non-IP traffic will not be saved to the capture buffer. However, if you set the **non-ip** parameter to **accept**, all non-IP frames are captured, as well as the IP frames that match the specified filter. (The default value for the **non-ip** parameter is **deny**.)

Use the **no** form of the command to reset packet capture to its default behavior, that is, to capture all traffic.

Syntax

```
filter <name> [non-ip {accept | deny}]
no filter <name>
```

Parameters

name	Specifies the interface filter to apply. Enter one of the following strings: deny-all, permit-all, permit-dns-tcp, permit-dns-udp, permit-entrust-ca, permit-finger, permit-ftp, permit-http, permit-ldap, permit-nntp, permit-ntp, permit-ping, or permit-telnet. You can also enter the name of a user-created filter.
non-ip	Specify whether packet capture will save non-IP packets when it applies this filter. By default, packet capture does not save non-IP packets when you apply a filter.
accept	Specify that non-IP packets are saved in the buffer, along with the IP packets specified by the filter.
deny	Specify that non-IP packets are not saved in the buffer.

Default

Capture all traffic.

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running

Warning: VJ compression may be negotiated on this interface.
Filters will not match on any VJ compressed frames.
```

Related commands

capture
direction
length
show capture
trigger
wrapping

Example

The following example applies the interface filter “permit ping” to the capture object.

```
CES# capture serial31
CES(capture-serial)# filter “permit ping”
CES(capture-serial)#
```

The following example disables the application of the interface filter and resets packet capture to its default behavior, that is, to capture all traffic.

```
CES(capture-ethernet)# no filter
CES(capture-ethernet)#
```

length

Use this command to specify the number of octets that are captured from every packet. Use the **no** form of the command to reset the length to the default value, 4096 octets.

Syntax

length *<length>*
no length

Parameters

length	Specifies the maximum number of octets to capture from each packet. Enter a value from 64 through 4096.

Default

4096 octets

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture
direction
filter
show capture
trigger
wrapping

Example

The following example sets the number of octets to capture from every packet to 1518.

```
CES(capture-ethernet)# length 1518
CES(capture-ethernet)#
```

The following example resets the number of octets to the default value, 4096.

```
CES(capture-ethernet)# no length
CES(capture-ethernet)#
```

persistent

Use this command to enable persistent mode for tunnel capture objects (persistent mode applies only to tunnels—user tunnels, branch office tunnels, and ABOTs). When persistent mode is enabled and a captured tunnel disconnects, packet capture restarts automatically when it encounters another tunnel that matches the capture criteria. Use the **no** form of the command to revert to the default behavior, that is, to stop packet capture when the tunnel disconnects.

Syntax

```
persistent enable
no persistent enable
```

Parameters

None

Default

Stop packet capture when the tunnel disconnects.

Command mode

Capture Tunnel Configuration

Next command mode

Capture Tunnel Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
remoteip
show capture
type
userid

Example

The following example enables persistent mode, which enables packet capture to restart when the captured tunnel disconnects so that another tunnel matching the capture criteria can be captured immediately.

```
CES(capture-tunnel)# persistent enable
CES(capture-tunnel)#
```

The following examples resets packet capture to its default behavior, that is, capture is stopped when the captured tunnel disconnects.

```
CES(capture-tunnel)# no persistent enable
CES(capture-tunnel)#
```

promiscuous

Use this command to enable promiscuous mode for an Ethernet interface capture object (promiscuous mode applies only to Ethernet interface capture objects). When promiscuous mode is enabled, the interface card will be configured to run in promiscuous mode—that is, traffic on the interface that is *not* directed to the gateway will be captured. Use the **no** form of the command to revert to the default behavior, that is, for promiscuous mode to be disabled when capture is started.

Syntax

```
promiscuous enable
no promiscuous enable
```

Parameters

None

Default

Disabled

Command mode

Capture Ethernet Configuration

Next command mode

Capture Ethernet Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
show capture

Example

The following example enables promiscuous mode for packet capture on an Ethernet interface.

```
CES(capture-ethernet)# promiscuous enable
CES(capture-ethernet)#
```

The following example disables promiscuous mode for packet capture.

```
CES(capture-ethernet)# no promiscuous enable
CES(capture-ethernet)#
```

remoteip

Use this command to specify the IP address of the remote tunnel end point for the tunnel capture object. When you execute this command, only traffic that goes through a tunnel with the specified remote tunnel end point will be captured. Use the **no** form of the command to revert to the default behavior, that is, to capture traffic from tunnels with any remote end point address.

Syntax

remoteip *<IP-address>*
no remoteip *<IP-address>*

Parameters

IP-address	Specifies the IP address of the remote tunnel end point; traffic traversing a tunnel with this remote IP address will be captured.

Default

Capture traffic from tunnels with any remote IP address.

Command mode

Capture Tunnel Configuration

Next command mode

Capture Tunnel Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
persistent
show capture
type
userid

Example

The following example sets the remote IP address from which the tunnel must come for it to be captured by this capture object.

```
CES(capture-tunnel)# remoteip 192.168.200.1
CES(capture-tunnel)#
```

The following example resets packet capture to its default behavior, that is, to capture tunnels from any remote IP address.

```
CES(capture-tunnel)# no remoteip
CES(capture-tunnel)#
```

show capture

Use this command to show the status of existing capture objects.

Syntax

show capture [*<name>*]

Parameters

name	Specifies the name of an existing capture object.

Default

If no capture object name is specified, print out a summary of all capture objects.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% No capture objects found
```

Related commands

capture enable
capture save
capture start
capture stop
clear capture
show capture

Example

The following example lists and briefly describes all the capture objects configured on the gateway.

```
CES# show capture
Name        Type        Size        Utilization  Count      State
test        ETHERNET    1048576         100%     1282       BUFFER FULL
test2       ETHERNET    1048576           0%     0          EMPTY
test3       TUNNEL      1048576           0%     0          STOPPED
test4       GLOBAL      1048576          12%     232        RUNNING
```

The following example displays configuration parameters for the Fast Ethernet capture object “test.”

```
CES# show capture test
Capture state:                              BUFFER FULL
Capture buffer size:                        1048576
Capture type:                               ETHERNET
Capturing on interface:                     FastEthernet 0/1
Promiscuous mode is:                        DISABLED
Capturing MAX octets per frame:             4096
Captured frames:                            1282
Capture buffer utilization:                 100%
Capture direction:                          BIDIRECTIONAL
Capture buffer wrapping:                    DISABLED
Capture buffer wrapped:                     FALSE
Capture buffer last saved to:               /ide0/nn1
Frames saved:                               1281
```

The following example displays configuration parameters for the tunnel capture object “test3.”

```
CES# show capture test3
Capture state:                              STOPPED
Capture buffer size:                        1048576
Capture type:                               TUNNEL
Tunnel type to capture:                     IPSEC
Tunnel encapsulation to capture:            INITIATOR
Restarting capture on tunnel logoff:        DISABLED
Capturing MAX octets per frame:             4096
Captured frames:                            0
Capture buffer utilization:                 0%
Capturing direction:                        BIDIRECTIONAL
Capture buffer wrapping:                    DISABLED
Capture buffer wrapped:                     FALSE
Capture filter applied:                     permit all
Capture filter discards:                    0
Start trigger applied:                      permit all
Start trigger discards:                     0
Stop trigger applied:                       permit all
CES#
```

The following example displays configuration parameters for the global capture object “test4.”

```
CES# show capture test4
Capture state:                              RUNNING
Capture buffer size:                        1048576
Capture type:                               GLOBAL
Capturing MAX octets per frame:             4096
Captured frames:                            237
Capture buffer utilization:                 12%
Capturing direction:                        BIDIRECTIONAL
Capture buffer wrapping:                    DISABLED
Capture buffer wrapped:                     FALSE
```

trigger

Use this command to set start and stop triggers. Existing interface filters are used as start and stop triggers. By default, the system saves frames to the capture buffer as soon as capture is started.

- A start trigger causes the system to wait for a specific packet before it starts saving packets to the capture buffer (traffic encountered before the start trigger is encountered is discarded).
- A stop trigger causes the system to stop saving traffic in the capture buffer after a specific packet matching the stop trigger is encountered. Capture, however, is not fully stopped.

If you set both a start and a stop trigger, the start trigger can reenable saving traffic to a capture buffer. The use of a start and a stop trigger allows capturing specific transaction-oriented traffic. Triggers can also be used with filters to allow still greater flexibility. Use the **no** form of the command to revert to the default behavior, that is, to remove the start trigger, the stop trigger, or both.

Syntax

```
trigger {start | stop} <filter>
no trigger [start | stop]
```

Parameters

filter	Specifies the name of the interface filter to use as a start or stop trigger. Enter one of the following strings: deny-all, permit-all, permit-dns-tcp, permit-dns-udp, permit-entrust-ca, permit-finger, permit-ftp, permit-http, permit-ldap, permit-nntp, permit-ntp, permit-ping, or permit-telnet. You can also enter the name of a user-created filter.
start	Create a trigger that starts packet capture when the filter criteria are met.
stop	Create a trigger that stops packet capture when the filter criteria are met.

Default

None

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running

Warning: VJ compression may be negotiated on this interface.
Triggers will not match on any VJ compressed frames.
```

Related commands

capture
capture start
capture stop
direction
filter
length
show capture
wrapping

Example

The following example sets a start and stop trigger.

```
CES(capture-ethernet)# trigger start "permit ping"
CES(capture-ethernet)# trigger stop "permit ping"
CES(capture-ethernet)#
```

The following example removes the start trigger.

```
CES(capture-tunnel)# no trigger start
CES(capture-tunnel)#
```

The following example removes all triggers.

```
CES(capture-ethernet)# no trigger
CES(capture-ethernet)#
```

type

Use this command to specify the following criteria for tunnel capture objects:

- Type of tunnel: any type, user tunnel, branch office tunnel, or asynchronous branch office tunnel (responder side or initiator side)
- Tunneling protocol: IPsec, L2F, L2TP, or PPTP

When you execute this command, only traffic from the specified type of tunnel will be captured. Use the **no** form of the command to revert to the default behavior, that is, to capture packets that traverse tunnels of any type.

Syntax

```
type {any | initiator | peer2peer | responder | user}
{ipsec | l2f | l2tp | pptp}
no type
```

Parameters

any	Capture traffic from any type of tunnel.
initiator	Capture traffic from ABOT initiator tunnels only.
peer2peer	Capture traffic from peer-to-peer branch office tunnels only.
responder	Capture traffic from ABOT responder tunnels only.
user	Capture traffic from user tunnels only.
ipsec	Capture traffic from IPsec tunnels only.
l2f	Capture traffic from L2F tunnels only.
l2tp	Capture traffic from L2TP tunnels only.
pptp	Capture traffic from PPTP tunnels only.

Default

Capture packets from all tunnel types.

Command mode

Capture Tunnel Configuration

Next command mode

Capture Tunnel Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
persistent
remoteip
show capture
userid

Example

The following example configures packet capture to capture IPsec tunnels only.

```
CES(capture-tunnel)# type any ipsec
CES(capture-tunnel)#
```

The following example configures packet capture to capture only branch office tunnels running L2TP.

```
CES(capture-tunnel)# type peer2peer l2tp
CES(capture-tunnel)#
```

The following example configures packet capture to capture all types of tunnels.

```
CES(capture-tunnel)# no type
CES(capture-tunnel)#
```

userid

Use this command to specify the user name as the criterion that a tunnel capture object will use to capture packets. (For types of tunnels that do not have a user name, other information is used instead, for example, peer IP address for branch office tunnels.) When you execute this command, only traffic that goes through tunnels with the specified user name will be captured. Use the **no** form of the command to revert to the default behavior, that is, to capture traffic from tunnels with any user name.

Syntax

userid *<name>*
no userid

Parameters

name	Specifies the user name or other information for the tunnels.

Default

Capture tunnels with any user name.

Command mode

Capture Tunnel Configuration

Next command mode

Capture Tunnel Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
persistent
remoteip
show capture
type

Example

The following example configures packet capture to capture only tunnels with the user ID set to “test.”

```
CES(capture-tunnel)# userid test
CES(capture-tunnel)#
```

The following example configures packet capture to capture packets from all tunnels, regardless of user ID.

```
CES(capture-tunnel)# no userid
CES(capture-tunnel)#
```

wrapping

Use this command to allow the capture buffer to wrap when it fills up. By default, packet capture stops when the buffer fills up. If you execute this command, the oldest captured datagrams are discarded and new ones are saved in their place. With wrapping enabled, packet capture can run indefinitely regardless of the capture buffer size. Use the **no** form of the command to revert to the default behavior, that is, to stop capturing packets when the buffer is full.

Syntax

```
wrapping enable
no wrapping enable
```

Parameters

None

Default

Stop capturing when buffer is full.

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture
capture add
direction
filter
length
show capture
trigger
wrapping

Example

The following example enables the capture buffer to wrap when it gets full.

```
CES(capture-ethernet)# wrapping enable
CES(capture-ethernet)#
```

The following example disables wrapping; that is, packet capture stops when the buffer is full.

```
CES(capture-ethernet)# no wrapping enable
CES(capture-ethernet)#
```

Chapter 5
Using forced logoff

Forced logoff provides the ability to logoff end users and branch office connections either by the individual connection or by logging of all connections at once through the CLI.

forced-logoff

Use this command to log off a branch office tunnel or user tunnel immediately.

Syntax

forced-logoff boconn {**all** | *<bo_name> <bo_group_name>*}

forced-logoff user {**all-non-admin** | *<user_name> <group_name>*}

Parameters

all	Specifies that all branch office connections be immediately logged off.
bo_name	Specifies the name of the branch office tunnel connection that you want to log off. If the name includes spaces, enclose it in quotation marks.
bo_group_name	Specifies the name of the branch office group that the branch office connection belongs to. If the name includes spaces, enclose it in quotation marks.
all-non-admin	Specifies that all users who are not logged on as administrators be immediately logged off.

user_name	Specifies the name of the user that you want to log off. If the name includes spaces, enclose it in quotation marks.
group_name	Specifies the name of the user group that the user belongs to. If the name includes spaces, enclose it in quotation marks.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management – Manage
User Management – Manage

Warning messages

```
% Connection does not exist for BO <bo_name> in group
<group_name>
% Connection does not exist for user <user_name> in group
<group_name>
```

Related commands

kill
show sessions
who

Example

The following example immediately logs off the branch office tunnel Boston.

```
CES# forced-logoff boconn Boston "/Base/Branch1"
CES#
```

The following example immediately logs off user tunnel george123.

```
CES# forced-logoff user george123 "/Base/PQHQ"
CES#
```

forced-logoff

Use this command to force a group of user tunnels or branch office tunnels to log off at a specified time.

Syntax

forced-logoff *<hh:mm:ss>*

Parameters

hh:mm:ss	Specifies the time that the logoff will occur. Type the time in hours, minutes, and seconds, for example, 05:30:00 for 5:30 AM and 17:30:00 for 5:30 PM. You can enter time values from 00:00:01 through 23:59:59.

Default

00:00:00 (forced logoff is disabled)

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example logs off users in the group “testgroup” at 10:45 AM.

```
CES(config)# group connectivity “/Base/testgroup”
CES(config-group/con)# forced-logoff 10:45:00
CES(config-group/con)#
```

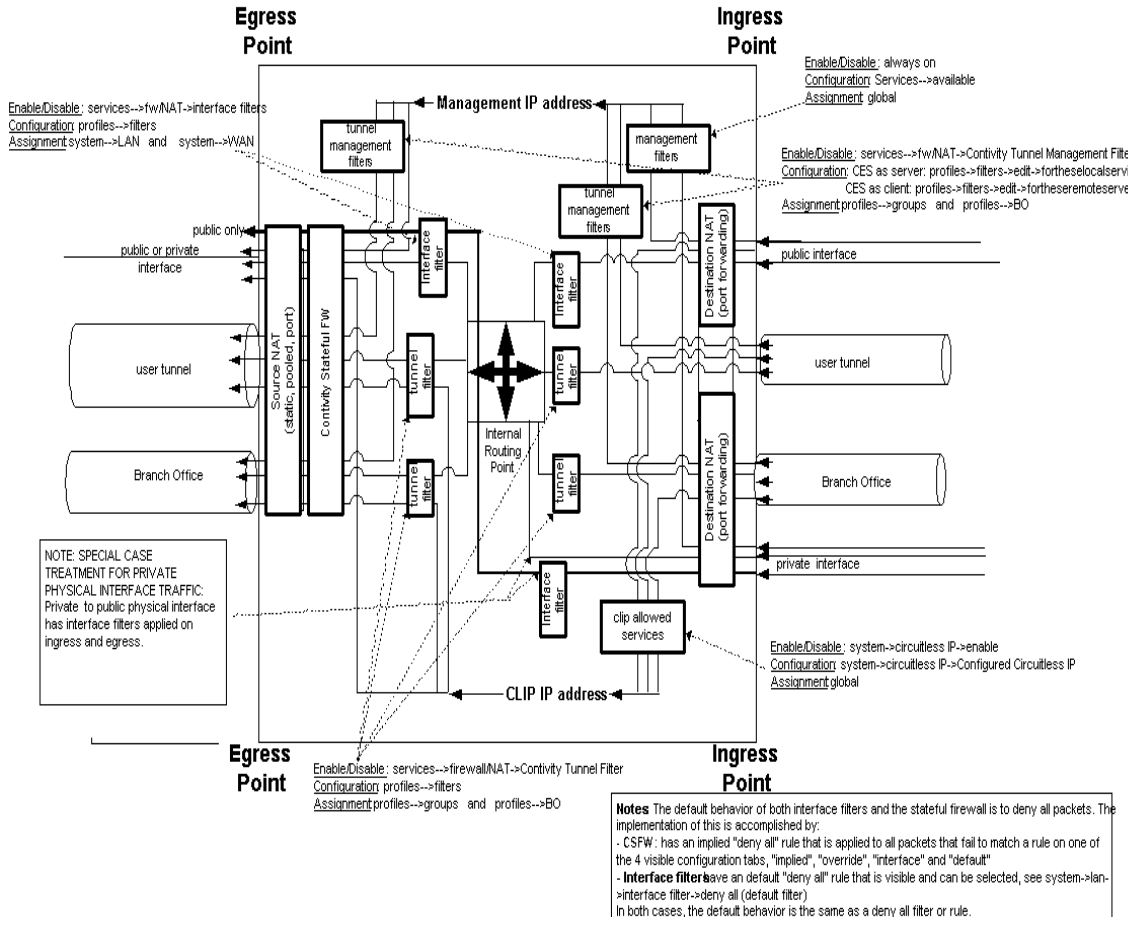
The following example logs off users in the branch office group “pubsgroup” at 10:45 PM.

```
CES(config)# bo-group connectivity “/Base/pubsgroup”
CES(config-bo_group/con)# forced-logoff 22:45:00
CES(config-bo_group/con)#
```

Appendix A
Firewall and Filters Example

Figure 1 shows the interaction between the Contivity Stateful Firewall and Contivity filters.

Figure 1 Sample firewall and filters configuration



In this figure, all traffic is shown as ingressing from the right side on one of four possible types of interfaces:

- User tunnel
- Branch office tunnel
- Private interface
- Public interface

After ingressing, the packet passes through the applicable services and then proceeds on to either the internal routing point or is terminated at an interface IP address, management IP address, or CLIP IP address.

All traffic egress points are shown as moving to the left, out the same four types of interfaces as the ingress point.