Version 4.90

Part No. 315900-C Rev 00
April 2004

600 Technology Park Drive
Billerica, MA 01821-4130

Managing and Troubleshooting the Contivity Secure IP Services Gateway

NORTEL NETWORKS™

Copyright © 2004 Nortel Networks

Trademarks

Restricted rights legend

Statement of conditions

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

Figures

Tables

Preface

This guide provides information about how to manage and troubleshoot the Nortel Networks* Contivity* Secure IP Services Gateway. Throughout this guide, the Contivity Secure IP Services Gateway is referred to as *the gateway.*

Before you begin

This guide is for network managers who monitor and maintain the Contivity Secure IP Services Gateway. This guide assumes that you have the following background:

- Experience with system administration
- Familiarity with network management

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **ping** <*ip_address*>, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off** | **on**}.

braces ({ })	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **`ldap-server source {external | internal}`**, you must enter either **`ldap-server source external`** or **`ldap-server source internal`**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **`show ntp [associations]`**, you can enter either **`show ntp`** or **`show ntp associations`**. Example: If the command syntax is **`default rsvp`** [**`token-bucket`** {**`depth`** | **`rate`**}], you can enter **`default rsvp`**, **`default rsvp token-bucket depth`**, or **`default rsvp token-bucket rate`**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is **`more disk`***n*`:`*<directory>*`/...`*<file_name>*, you enter **`more`** and the fully qualified name of the file.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **`ping`** *<ip_address>*, *ip_address* is one variable and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`
separator (>)	Shows menu paths. Example: Choose Status > Health Check.

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

Acronyms

This guide uses the following acronyms:

ARP	Address Resolution Protocol
CA	certificate authority
CHAP	Challenge Handshake Authentication Protocol
CMP	Internet Control Message Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Certificate Management Protocol
IKE	IPsec Key Exchange
IP	Internet Protocol
IPsec	IP Security
IPX	Internetwork Packet Exchange
ISP	Internet service provider
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation

OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PDN	public data network
POP	point of presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
UDP	User Datagram Protocol
URL	uniform resource locator
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network
XNS	Xerox Networking System

Related publications

For more information about the Contivity Secure IP Services Gateway, refer to the following publications:

- Release notes provide the latest information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Configuring Basic Features for the Contivity Secure IP Services Gateway* introduces the product and provides information about initial setup and configuration.
- *Configuring Authentication and Certificates for the Contivity Secure IP Services Gateway* provides instructions for configuring authentication services and digital certificates.

- *Configuring Firewalls, Filters, NAT and QoS for the Contivity Secure IP Services Gateway* provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- *Configuring Advanced Features for the Contivity Secure IP Services Gateway* provides instructions for configuring the tunneling protocols IPsec, L2TP, PPTP, and L2F, as well as instructions for configuring PPP, frame relay, PPPoE, and advanced WAN settings.
- *Configuring Routing for the Contivity Secure IP Services Gateway* provides instructions for configuring RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *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
Gateway administration

This chapter introduces administrator settings, tools, system configuration, and file management. It also includes information about SNMP traps.

Administrator settings

The gateway supports multiple administrators. You can assign different rights to allow or prevent administrative users from managing or viewing gateway and user configuration information. You assign administrative privileges and rights on the Profiles > User > Edit screen. The gateway also supports a primary administrator.

The Manage Switch and Manage Users access right settings can be assigned one of the following privilege levels:

- None - This user does not have administrator rights to manage the gateway or manage users; the user cannot view or manage configuration or user settings.
- View - This user has administrator rights to view (monitor) gateway configuration or user rights settings; however, the user cannot manage (change) them. This is the lowest level of administrator rights.
- Manage - This user has administrator rights to view (monitor) and manage (configure) other gateway configuration or user rights settings. This is the highest level of administrative rights.
- Add Subgroups is a check box that lets you give the user the authority to add and delete subgroups under the given directory when the user only has View authority with Manage Switch access rights.

The Administrator Settings screen allows you to change the primary administrator user ID and password. It also controls the Administrator Idle Timeout Setting for all administrators, the default language, and serial port settings.

There can be only one primary administrator. The primary administrator user ID and password combination provides the user with this information access to all screens and control settings. The primary administrator user ID and password are also used to access the serial port and the recovery disk.

Note: The primary administrator user ID and password are only saved during a system shutdown. Therefore, once you set these parameters, you must implement an Admin > Shutdown to save the new settings. Doing a reset (using the Reset button on the back of the gateway) does not store the parameters.

Note: Do not lose or forget the password once the gateway has been configured. Losing or forgetting your password would require you to return the gateway to Nortel Networks for reconfiguration to default settings. All settings and backups would be lost. There is no way to access the system without the primary administrator password.

You can change the primary administrator user ID and password on the Admin > Administrator screen.

Tools

The gateway supports standard IP tools such as `ping`, `Traceroute`, and ARP `show` and `delete`. You can access these tools through the Admin > Tools screen.

The `ping` command generates an ICMP echo-request message, which is sent by any host to test node reachability across a network. The ICMP echo-reply message indicates that the node can be successfully reached.

The Traceroute tool is used for measuring a network round-trip delay. Messages are sent per hop and the wait occurs between each message. If the address is unreachable, it uses this formula to determine how long it takes for the Traceroute to time out.

```
maximum hops (30) x the wait timeout (5) x 3 seconds
```

The Address Resolution Protocol (ARP) dynamically discovers the low-level physical network hardware address that corresponds to the high-level IP address for a host. ARP is limited to physical network systems that support broadcast packets that can be heard by all hosts on the network.

System configuration

You can save the current or delete existing system configuration files through the Admin > Config screen. Additionally, you can select one of the previously named configurations and restore it as the current configuration.

File management

You can navigate through the gateway file system through the Admin > File System > File System Maintenance screen. It lists the devices (drives) and directories. This provides flexibility in viewing details of a file or directory, and it allows you to delete unnecessary files. For example, if you had problems performing an FTP transfer with a specific file, you could view the file details to learn its file size and when it was last modified for troubleshooting purposes. Additionally, you can toggle between hard drives when a backup drive is available.

SNMP

The SNMP screen (Admin > SNMP) allows you to do the following:

- Designate the remote SNMP management stations that are authorized to send SNMP Gets to the gateway.
- Enable specific MIBs.

Note: A Nortel Networks proprietary MIB is included on the Nortel Networks CD. Click on the CesTraps.mib file to load the MIB. See Appendix A, “MIB support,” for a description of the CesTraps.mib.

The SNMP counters measure packet attributes that are based on the outer IP header. In the tunneled environment there is also an inner IP header, but this IP header does not contribute to the SNMP MIB counters. For example, the outer packet header might be a good packet header and counted, but the inner packet header might be corrupted and would not contribute to the drop counter.

You can view the Health Check screen for the results of SNMP traps.

The SNMP Traps screen (Admin > SNMP Traps) allows you to configure the gateway to generate Simple Network Management Protocol (SNMP) Version 1 traps, based on MIB II. From the SNMP Traps screen, you can do the following:

- Designate the remote SNMP trap hosts that can receive traps from the gateway.
- Select the specific traps that you want the SNMP hosts to receive.
- Configure a trap to be sent only once.

To enable traps, you select one of the trap groups on the SNMP Traps screen: hardware, server, service, standard IETF, or attack. The traps displayed on the group screens—in particular the Hardware Trap Configuration and the Service Trap Configuration screens—reflect the hardware and software available on your gateway. For example, if you have a gateway with no WAN interface cards, the traps for WAN interfaces will not appear on the Hardware Trap Configuration screen.

Note: The results of many of the selections you make on the SNMP Traps screen are reported on the Health Check screen.

Most traps sent by the Contivity gateway to configured trap hosts are also displayed on the SNMP Traps screen. However, certain traps, including traps related to the status of branch office tunnels, are not displayed on this page due to space limitations. (For example, a physical interface status change would cause the sending of many traps reporting the failure of all the tunnels using this interface.) All traps—whether they appear on the SNMP Traps page—are sent to the SNMP management application specified as the trap destination.

Chapter 2
Status and logging

The System Status screens allow you to see from the Web interface which users are logged on, their traffic demands, and a summary of your gateway's hardware configuration, including available memory and disk space.

The status screens include:

- Sessions
- Reports
- System Status
- Health check
- Statistics
- Firewall
- Accounting

The gateway has several logs that provide different levels of information:

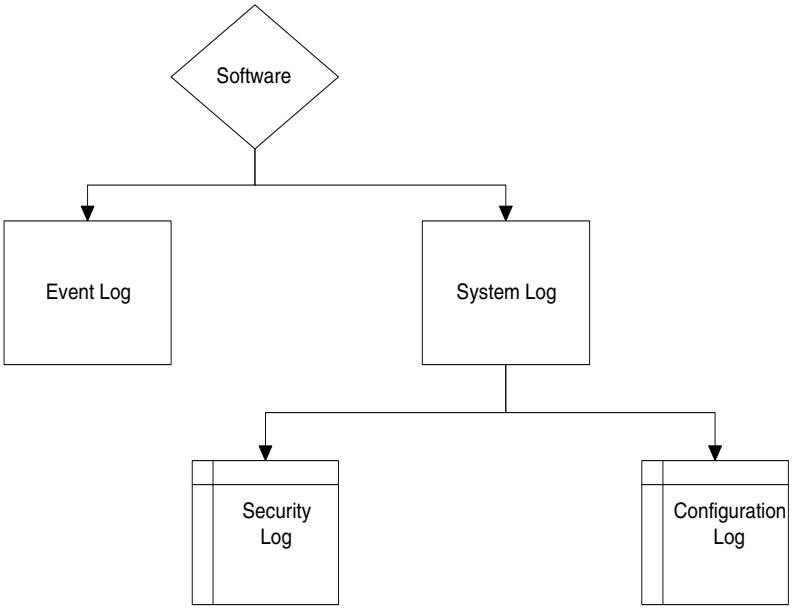
- Event log
- System log
- Security log
- Config log

The logs are stored in text files on disk and they indicate what happened, when, and to which user (IP address and user ID).

The event log captures real-time logging over a relatively short period of time (for example, the event log could wrap its 2000 possible entries in minutes). The system log captures data over a longer period of time, up to 61 days.

Most events are sent to the event log first. Significant events from the event log are sent to the system log. (Not all data that is saved by the system log comes from the event log.) The gateway filters from the system log security entries for the security log and configuration entries for the configuration log. Figure 1 shows a Nortel Networks logging scheme.

Figure 1 Nortel Networks logging scheme



The different log options allow you to write specific event levels to the log files and view them, including:

- Normal
- Urgent
- Detailed
- All

Sessions

You can monitor which users are tunneled into the gateway, when they logged in, and the number of bytes and packets they have transmitted or received. Additionally, you can see selected session details, and you can even log off users.

Once a session becomes connected, detailed information about the connection is available from the Status > Sessions screen. This screen lists all connected sessions, including administrative sessions. Click on the appropriate buttons beside each session to either log out the session or view detailed information about it. As well as statistics, this information contains what encryption was negotiated, the SOIs of the security associations and more.

Reports

The Reports feature allows you to generate comprehensive reports of users and related information. You generate reports in an on screen tabular format, and you can import them into a spreadsheet or database through the comma-delimited format.

At midnight (12:00 a.m.), the data collection task performs summary calculations and rewrites history files, along with other management and cleanup functions. You should leave the gateway running overnight to perform this task. The gateway must be running at midnight to generate a historical graph for the day.

The Status Reports screen allows you to view system and performance data in text or graphical format. You can generate current or historical graphs of valuable system data. The Reports feature provides a comprehensive display or down-loadable reports on user activity.

If you have multiple gateways throughout the world, you might want to use the Greenwich Mean Time (GMT) standard. This synchronizes the various log files so that the timestamps are directly comparable.

System

The System Status screen shows the gateway's up time, software and hardware configurations, and the current status of key devices. When there is a pending shutdown or an Internetwork Packet Exchange (IPX*) public network address change that requires a reboot, such events are listed at the top of this screen.

Health check

The Health Check screen provides an overall summary of the current state of the gateway's hardware and software components at a glance. It lists all aspects of unit operation, with the most critical information to check at the top of the page. By clicking on the link on the right side of the screen, you can go directly to the screen for configuration of that feature.

Statistics

The Statistics screen provides many subscreens with a wealth of general and diagnostic information about the system hardware, software, and connections. Much of the information is specifically designed for Nortel Networks Customer Support personnel to assist them in diagnosing problems. Some screens, however, for example, the LAN Counters, Interfaces, and WAN Status screens, might provide you with some traffic information. The Status > Statistics screen allows you to see text displays of system-level statistics that can help resolve lower-level problems with connections. These displays are similar to command-line output from the operating system.

In normal operation, and routine troubleshooting, many of these screens will never need to be examined. Some of the information, such as routing information, is also available through other screens, such as System > Routing.

Accounting

The accounting log provides information about user sessions. The log provides last and first names, user ID, tunnel type, session start and end dates, and the number of packets and bytes transferred. You can search the log according to most of these fields.

Accounting records

Accounting records are detailed logs that record the various activities performed by the gateway. The logs are directly available from the management interface and can be exported to other applications for additional processing. The Contivity Secure IP Services Gateway gathers and stores data about the current state of the gateway and the connections. The data is stored in files on the gateway's hard drive.

- Session Status: RADIUS Accounting–the gateway stores copies of RADIUS accounting records. These records, which can be retrieved via FTP or sent to a RADIUS server, contain information about each VPN session initiated to the gateway.
- System Data: Data Collection Task–The data collection task runs on the Contivity Secure IP Services Gateway and gathers data about the system's status. Each minute, data is captured by the task and written to a data file. The information captured by this task is used to create the graphs and reports available from the Status > Reports page.

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

The data collection system stores records in text-based files stored in the system/dclog subdirectory. The system stores the most recent 60 days of data. The system stores daily files, summary files, and summary history files. Ongoing administration tasks include monitoring the configuration files, backing up and restoring the gateway or the LDAP database, and upgrading images and clients.

Note: Accounting records are not sorted and are displayed in a random order.

RADIUS accounting

The Contivity Secure IP Services Gateway stores copies of RADIUS accounting records. These records are normally sent to a standard RADIUS Accounting server. To configure a RADIUS accounting server, use the Servers > RADIUS Acct screen.

You can view the information in these records on the Status > Accounting page. These are standard RADIUS accounting records. The gateway creates a file for each day and keeps the most recent 60 days of data, which are stored in the SYSTEM/ACCTLOG directory.

Note: 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.

Data collection task

The data collection task runs on the Contivity gateway and gathers data about the system's status. Each minute data is captured by the task and written to a data file. The gateway uses the information captured by this task to create the graphs and reports available from the Status > Reports screen. This information is stored in text-based files in the system/dclog directory of the gateway. The Contivity gateway creates the following types of files in the this directory:

- Daily files that contain interval records gathered every 60 seconds. These values are interval values and there is a file for each day (for example 20040622.DC).

- Summary file always has exactly five records that contain summary data in a file called summary.dc. These values are used to give historical graphs and reports about specific values.
- Summary history file contains records that represent cumulative daily data for the most recent 60 days in a file called summs.dc. Each day's summary is represented by four records. These records are for the current, total, average, and maximum values for the day.

A data collection record consists of 16 pairs of entries for each data collection object currently being collected. Each value pair consists of a Field ID and an integer value. The following is an sample data collection record:

0-930057960,1-3,2-3,3-0,4-0,5-0,6-0,7-0,8-0,9-0,10-56,11-76,12-1,13-11021,14-40,15-38,16-0

Table 1 lists the field IDs that are currently implemented.

Table 1 Field IDs for data collection records

Field identification	Collected field value	Description
0	TIMESTAMP	Seconds since Jan 1, 1970 - 00:00:00 Hours
1	TOTALSESSIONS	Summary of all sessions
2	ADMINSESSIONS	Number of Admin sessions
3	PPTPSESSIONS	Number of PPTP sessions
4	IPSECSESSIONS	Number of IPSEC sessions
5	L2FSESSIONS	Number of L2F sessions
6	L2TPSESSIONS	Number of L2TP sessions
7	IPADDRESSUSE	Number of IP Addresses in use
8	CPUUSE	Un-filtered CPU usage measurement {integer representing a percent between 0 and 100}
9	CPUSMOOTH	Filtered CPU usage measurement {integer representing a percent between 0 and 100}

Table 1 Field IDs for data collection records

Field identification	Collected field value	Description
10	MEMUSE	Filtered memory usage measurement {integer representing a percent between 0 and 100}
11	BOXPACKETSIN	Number of Inbound Packets
12	BOXPACKETSOUT	Number of Outbound Packets
13	BOXBYTESIN	Number of Inbound bytes
14	BOXBYTESOUT	Number of Outbound bytes
15	BOXDROPPEDPACKETS	Number of discarded packets
16	FAILEDAUTHATTEMPTS	Number of failed authentication attempts
17	LASTFIELDID (this field is never written to data record)	

Logs

The Contivity has several logs that provide different levels of information. The logs are stored in text files and indicate what happened, when the event occurred, and the IP address and user ID of the person causing the event.

Event log

The event log is a detailed recording of all events that take place on the system. These entries are not necessarily written to disk, as with the system log. The event log retains all system activity in-memory but only the significant entries are saved in the system log (on disk). The event log includes information about tunneling, security, backups, debugging, hardware, daemon processes, software drivers, and interface card driver events. It also records a successful connection from a Contivity VPN Client clone during configuration mode.

The event log maintains the most recent 2000 events in memory and is overwritten when it becomes full. Some of the events are written to the disk log files (the configuration log, security log, and system log). These log files are maintained on the hard drive for up to 60 days. They are available for review for any given day.

The following is the general format of event log entries:

- Date and time stamp
- CPU that issued the event (0=CPU 0, 1=CPU 1)
- Task or software module that issued the event
- Priority code assignment (number in brackets)
- Message

The priority code consists of two digits in brackets (for example, [12]). The first digit of the [*xx*] entry specifies where the message is stored:

- 0 - Message is displayed in the event log only (non-persistent event).
- 1 - Message is written to the system log directory.
- 3 - Message is written to the system log and sent to configured syslog server.

For event log and system log messages, the second digit indicates the priority:

- 1 - Low priority
- 2 - Medium priority
- 3 - High priority

For events sent to the syslog server, the second digit indicates the message type:

- 1 - Alert
- 2 - Critical
- 3 - Error
- 4 - Warning
- 5 - Notice
- 6 - Information
- 7 - Debug

Some examples of event severity codes are as follows:

- [01] - Event is displayed only in the event log; low priority
- [12] - Event is displayed in the system log; medium priority
- [31] - Event is sent to the syslog server; alert message
- [37] - Event is sent to the syslog server; debug message

The following sample event log is followed by descriptions of the line entries.

1 07/03/2003 22:46:11 0 Security [11] Session: IPSEC[jdoe] attempting login

2 07/03/2003 22:46:11 0 Security [01] Session: IPSEC[jdoe] has no active sessions

3 07/03/2003 22:46:11 0 Security [01] Session: IPSEC[jdoe] Jay Doe has no active accounts

4 07/03/2003 22:46:11 0 ISAKMP [02] Oakley Aggressive Mode proposal accepted from jdoe (134.177.58.151)

5 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 SHARED-SECRET authenticate attempt...

6 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 attempting authentication using LOCAL

7 07/03/2003 22:46:12 0 Security [11] Session: IPSEC[jdoe]:6454 authenticated using LOCAL

8 07/03/2003 22:46:12 0 Security [11] Session: IPSEC[jdoe]:6454 bound to group /Base/Pittsburgh/Jay Doe

9 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 using group filter permit all

10 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 IN FILTER 1 permit IP any any

11 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 OUT FILTER 1 permit IP any any

12 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 RESTRICTED FILTER 1 deny TCP any GT 1023 any EQ 80

13 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 RESTRICTED FILTER 1 deny TCP any GT 1023 any EQ 21

14 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 RESTRICTED FILTER 1 deny TCP any GT 1023 any EQ 20

15 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 RESTRICTED FILTER 1 deny UDP any any EQ 161

16 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 RESTRICTED FILTER 1 deny TCP any GT 1023 any EQ 23

17 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 RESTRICTED FILTER 1 deny TCP any GT 1023 any EQ 256

18 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 RESTRICTED FILTER 1 deny TCP any EQ 256 any GT 1023

19 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 RESTRICTED FILTER 1 deny TCP any EQ 257 any GT 1023

20 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 RESTRICTED FILTER 1 permit IP any any

21 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 OUT FILTER 1 permit IP 47.184.90.26 0.0.0.0 any

22 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 LOCAL IN FILTER 1 permit TCP any GT 1023 any EQ 80

23 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 LOCAL IN FILTER 1 permit UDP any any EQ 161

24 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 LOCAL IN FILTER 1 permit ICMP any any 8

25 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 LOCAL IN FILTER 1 permit ICMP any any 0

26 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 LOCAL IN FILTER 1 permit ICMP any any 3

27 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 LOCAL IN FILTER 1 permit UDP any EQ 68 any EQ 67

28 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 LOCAL IN FILTER 1 permit TCP any GT 1023 any EQ 17

29 07/03/2003 22:46:12 0 Security [01] Session: IPSEC[jdoe]:6454 LOCAL IN FILTER 1 permit TCP any GT 1023 any EQ 586

30 07/03/2003 22:46:12 0 Security [11] Session: IPSEC[jdoe]:6454 authorized

31 07/03/2003 22:46:12 0 Security [12] Session: IPSEC[jdoe]:6454 physical addresses: remote 134.177.58.151 local 47.184.90.27

32 07/03/2003 22:46:13 0 Security [12] Session: IPSEC[jdoe]:6454 assigned IP address 47.184.91.56, mask 255.255.254.0

33 07/03/2003 22:46:13 0 ISAKMP [02] ISAKMP SA established with jdoe (134.177.58.151)

34 07/03/2003 22:46:13 0 Security [12] Session: IPSEC[jdoe]:6454 physical addresses: remote 134.177.58.151 local 47.184.90.27

35 07/03/2003 22:46:14 0 Security [12] Session: IPSEC[jdoe]:6454 physical addresses: remote 134.177.58.151 local 47.184.90.27

36 07/03/2003 22:46:14 0 Outbound ESP from 47.184.90.27 to 134.177.58.151 SPI 0x001d7dbd [03] ESP encap session SPI 0xbd7d1d00 bound to cpu 1

37 07/03/2003 22:46:14 0 Inbound ESP from 134.177.58.151 to 47.184.90.27 SPI 0x0000c959 [03] ESP decap session SPI 0x59c90000 bound to cpu 1

38 07/03/2003 22:46:14 0 IPvfy.03d9aad4{Tun} [01] SetExpectedSrcAddress: 0x385bb82f, Bcast 0xff5bb82f

39 07/03/2003 22:46:14 0 IP Redirector [10] TunnelAddrReg(47.184.91.56 0x3c88fc4 65535)

40 07/03/2003 22:46:14 0 ISAKMP [03] Established IPsec SAs with jdoe (134.177.58.151):

41 07/03/2003 22:46:14 0 ISAKMP [03] ESP 3DES-CBC-HMAC-MD5 outbound SPI 0x1d7dbd

42 07/03/2003 22:46:14 0 ISAKMP [03] IPcomp LZS outbound CPI 0x3471

43 07/03/2003 22:46:14 0 ISAKMP [03] ESP 3DES-CBC-HMAC-MD5 inbound SPI 0xc959

44 07/03/2003 22:46:14 0 ISAKMP [03] IPcomp LZS inbound CPI 0x907b

45 07/03/2003 22:46:15 0 Address Pool [11] Dhcp: address bound to 47.184.91.66-47.184.91.66 -- renewal in 21600 seconds.

Lines 1-4 are a result of receiving the first IPsec Key Exchange (IKE) (UDP port 500) packet and are normal for a client login. The characters in brackets, for example, [jdoe], indicate the user name that is attempting login for these entries. The fourth line, the ISAKMP entry, indicates the public IP address from which the session is being initiated.

Lines 5-8 show that the user is attempting to log in with a shared secret (username and password) from the internal LDAP. The third line indicates that the authentication attempt was successful. The fourth line shows the group profile and user entry that was associated with the user. Authentication is now complete. The next section covers authorization (the privileges the newly authorized user has).

Line 9 shows the filters that were applied to the user. This line tells what filter name, permit all in this case, was assigned to the user in the group profile.

Lines 10-11 show no restrictions on IP traffic between the client and the internal networks.

Lines 12-20 show restricted filter definitions.

Line 21 allows any traffic from the management interface outbound.

Lines 22-29 show the LOCAL filter indicates what traffic is allowed from the client to the gateway itself. In order, the filters allow for HTTP management from the client; SNMP queries from the client; ICMP echo replies, ICMP echoes, ICMP destination unreachable, BootP client requests to a BootP server port, Quote-of-the-day messages, and the Password server. The BootP messages are used by the client to ask the Contivity for its DNS and WINS information. The Quote-of-the-day server is used to provide the banner messages, if any, for the IP Security (IPsec) client.

Line 30 shows authorizations are complete.

Line 31 indicates the tunnel endpoints. These are the address of the interface on the gateway that accepted the connection and the address of the computer that initiated the connection (most often the ISP assigned address of the PC).

Line 32 indicates the address and netmask that have been assigned to the client.

Lines 33-35 show phase I negotiations are complete and the ISKMP SA has been established. The tunnel endpoints are listed again.

Lines 36-37 indicate the IPsec Security Associations are established and the Security Parameter Indices (SPI) that have been assigned for the outbound (encapsulation) and inbound (decapsulation) sessions. (The CPU that the session was assigned to is also noted, which is only of importance to a 4x00 series unit, which has multiple processors.)

Lines 38-39 show the assigned address and associated netmask are registered with the gateway. (The line with the IPvfy message lists the addresses in hex and the octets in reverse order.)

Line 40-44 indicate that the IPSec SAs have been established, as well as the fact that compression has been negotiated.

Line 45 indicates that the gateway is assigning IP addresses to clients that it received from a Dynamic Host Configuration Protocol (DHCP) server. After handing an address to this client, it requests another address from the DHCP server to keep the requested number of addresses in its cache to hand out to clients.

System log

The system log contains all system events that are considered significant enough to be written to disk, including those displayed in the configuration and security logs. Events that would appear in the system log include:

- LDAP activity
- Configuration activity
- Server authentication and authorization requests

The following is the general format of the log entries:

- Time stamp
- Task that issued the event (tEvtLgMgr, tObjMgr, tHttpdTask)
- Number that indicates the CPU that issued the event (0=CPU 0, 1=CPU 1)
- Software module that issued the event
- Priority code assignment (number in brackets) (for a description of these codes, see "Event log" on page 32)
- Indicates that the packet matched the rule in the listed section
- Indicates the matching packet source, destination, protocol, and action configured for that rule

The following example shows a system log:

11:29:31 tEvtLgMgr 0 : CSFW [12] Rule[OVERRIDE 1]Firewall: [192.32.250.204:1024-10.0.18.12:2048, icmp], action: Allow

Security log

The Security log records all activity about system or user security. It lists all security events, both failures and successes. The events can include:

- Authentication and authorization
- Tunnel or administration requests
- Encryption, authentication, or compression
- Hours of access
- Number of session violations
- Communications with servers
- LDAP
- Remote Authentication Dial-In User Service (RADIUS)

Configuration log

The Configuration log records all configuration changes. For example, it tracks adding, modifying, or deleting configuration parameters:

- Group or user profiles
- LAN or wide area network (WAN) interfaces
- Filters
- System access hours
- Shutdown or startup policies
- File maintenance or backup policies

Chapter 3
Administrative tasks

This chapter describes administration tasks that help you operate the gateway. These tasks provide details on scheduling backups, upgrading the software image, saving configuration files, performing file maintenance, creating recovery diskettes, and system shutdown.

Shutdown

The Shutdown options allow you to shut down immediately, to wait until current users are logged off, or to wait until a designated time. A normal shutdown safely terminates connections so that no data is lost, compared with a spontaneous loss of power.

Additionally, you can select whether to power off or restart after shutdown, and also choose the configuration file to use upon restarting. To allow you to conduct an orderly shutdown, you can disable new logins, and you can disable logins after the shutdown to perform system maintenance.

Always use the System Shutdown screen to shut down the system rather than the Power or Reset buttons on the back of the gateway. This ensures the integrity of your file system.

Note: After performing a system shutdown, click on the Reload/Refresh button to see the latest gateway information.

Go to the Admin > Shutdown screen to turn off the gateway.

Recovery

The Recovery screen allows you to configure a recovery diskette for restoring the software image and file system to the hard drive of the gateway in the unlikely event that there is a hard disk crash. The recovery diskette is included with your gateway. You can also use this screen to create additional copies of the recovery diskette, as well as to reformat a diskette.

Note: The Contivity 1000, 1010, 1050, and 1100 do not have a floppy drive in the unit. The Contivity 600 also does not have a floppy drive, but the recovery image is stored in a PROM; you can invoke it by pressing a switch on the back of the unit.

Accessing the diskette drive

If the Contivity gateway has a front cover, you need to remove it to gain access to the diskette drive. Refer to the installation guide for details. Booting the gateway using the recovery diskette, utilities accomplish restoration of the gateway's hard disk, including:

- Hard disk reformatting
- FTP access to the hard disk
- Restoration of the previously backed-up software image and file system from a backup host to the hard disk
- Downloading a new factory default software image and file system from a file server to the hard disk

These utilities are accessed via Hypertext Transfer Protocol (HTTP) management of the gateway after it has been booted from the recovery diskette.

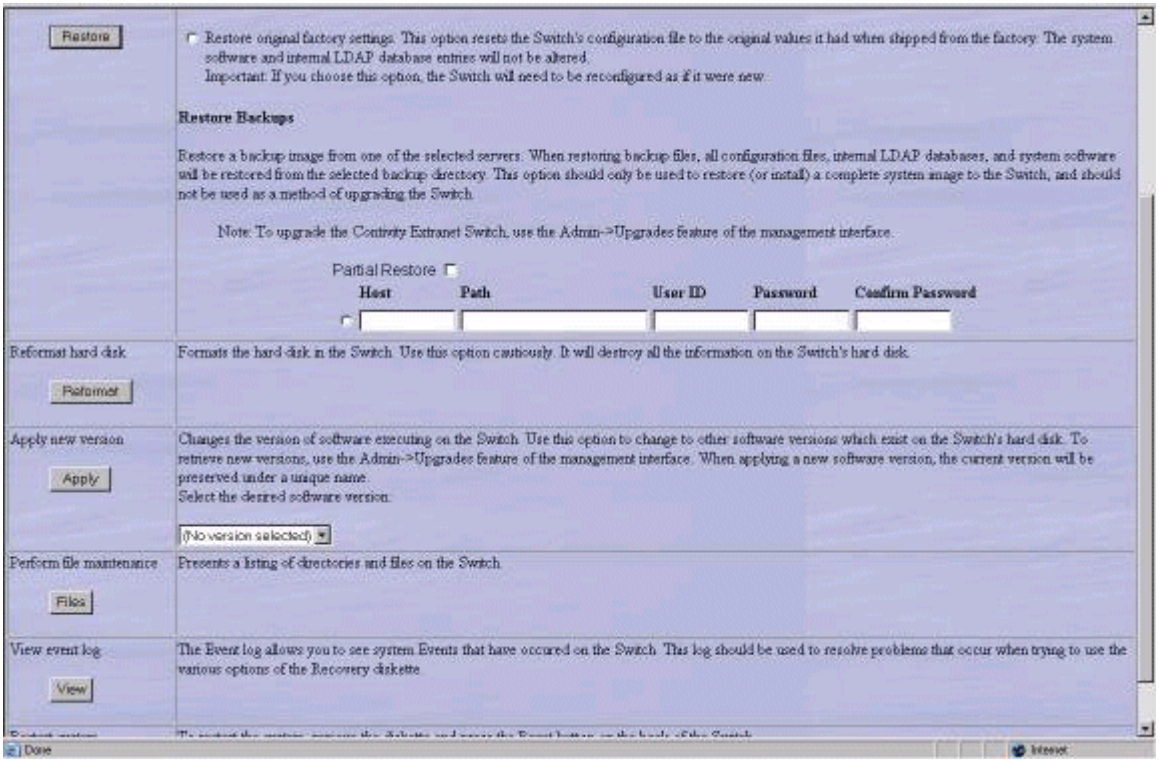
Using the recovery diskette

Remove the gateway's front cover. Insert the recovery diskette into the drive and press the Reset button on the back of the gateway. This supplies the gateway with a minimal configuration utility that allows you to view the gateway from a Web browser.

In the Web browser, enter the management IP address of your gateway. The Recovery Diskette screen shown in Figure 2 appears, which allows you to:

- Restore the factory default configuration or the backup configuration.
- Reformat the gateway's hard disk.
- Apply a new software version to the gateway.
- Perform file maintenance.
- View the Event log.
- Restart the system.

Figure 2 The Recovery Diskette screen



To use the recovery diskette:

1 Restore the configuration:

To restore the factory default configuration or the backup configuration, select the hard disk drive to which you want to restore the system files, either ide0 (drive 0) or ide1 (drive 1), and then do one of the following:

- Restore the factory configuration by selecting Restore Factory Configuration; then click on Restore to return the gateway to its original factory default configuration. This erases data contained in flash memory and also in the configuration file.

Warning: Selecting this option requires you to rebuild your entire configuration again from scratch.

An online message specifies the result of the Factory Configuration reset action.

- Or you can restore the gateway's previously backed-up configuration by clicking on Restore. If you previously chose to automatically backup the file systems, then the backup server host (or IP address) and path name, user ID, and password appear in the table.

  Check the Partial Backup checkbox if you want to restore the configuration files, log files or system files from a previous partial backup. The system restores the corresponding directory/files.

  Click on the radio button of the preferred backup server. The backed up file system, including software image and configuration files, from the latest backup copy residing on the designated server is restored onto the hard drive of your gateway.

  You can use the same backup server for multiple gateways. Each gateway creates a unique directory based on its serial number. The following example shows the host, path, and serial number (where the serial number [SN] is five digits):

  ```
  C:/software/backup/v101/SN01001
  ```

  The serial number is used to differentiate backup configurations from multiple gateways that are saved on the same backup server. The serial number uniquely identifies each gateway's backup data.

A blank row in the server backup field always appears to allow you to manually enter a backup server in case you did not configure automatic backup server locations.

Note: Because FTP servers are often different, there may be some information in your server documentation about setting paths that can help you with the upgrade procedure.

Alternatively, a new factory default software image and file system can be restored to the gateway's hard disk. Specify the name or address and path of the network file server onto which the software from the Nortel Networks CD has been installed.

Note: This restores the disk to an operable but "clean" condition (for example, configuration values are at factory defaults).

To view your gateway's serial number when the gateway is operational, choose Status > System from the Navigational menu. The Serial Number is also on the bar code label on the back of the gateway.

2 Click on Reformat Hard Disk if you must reformat the hard disk, for example if you:

— Have problems restoring your configuration that are not caused by the network or the file/backup server from which the file restoration is being retrieved

— Want to reconfigure the gateway from scratch

— Install a new disk

Caution: Selecting this option completely wipes out anything that was stored on the hard disk.

An online message indicates whether the reformatting of the hard disk was successful.

3 Click on the list to view the available software image and file systems that are stored on the hard disk and select the image version that you want to activate.

4. Click on Apply to apply the new version and reboot automatically. Changes are active. The gateway boots to that version until changed.
5. Click on Files to bring up the File Maintenance screen, which allows you to view the entire hard disk file system.
6. Click on View to display the Event Log beneath the Recovery Diskette screen. This is especially useful if a Restore operation fails.
7. Set the boot disk by clicking the list to select the hard disk drive from which you want to boot the gateway, either ide0 (drive 0) or ide1 (drive 1). Click on Set.
8. Click on Synchronize to immediately synchronize the primary and secondary disks. Thereafter, the disks automatically synchronize every hour. The gateway does not synchronize the software and configuration. Everything under the system directory is synchronized except for the core directory. Synchronization happens automatically, so you do not have to initiate it.
9. Upgrade the system boot software by clicking on the list to select a drive onto which you want to update the system boot software. Click on Upgrade to rewrite the boot software onto the hard disk. You would do this if the system boot sector were to become corrupted.
10. Restart the system by removing the diskette and pressing the Reset button on the back of the gateway. Then reposition your Web browser to the Management IP address, and choose Reload or Refresh from your browser menu to access the management page of the software running on the hard disk.

Note: This procedure cannot be used for the Contivity 1000 due to the lack of a floppy drive in the unit. The Contivity 600 also does not have a floppy drive, but the recovery image is stored in a PROM; you can invoke it by pressing a switch on the back of the unit.

Automatic backups

The gateway checks at regular intervals to see whether system file changes have been made. When there are changes, they are written to each of the backup servers. All of the system files are backed up the first time; thereafter, only the files that have changed are backed up.

Note: Any changes to backup parameters made while a backup is in process do not take effect until the currently running backup completes.

The gateway does not begin a backup for at least 5 minutes after rebooting. This time period is to allow all resources to start operating. This delay occurs even if you go into the Admin > Auto Backup screen and request that a backup be started immediately. The Automatic Backup screen allows you to configure regular intervals or specific times when your system files are saved to designated host backup file servers. You can designate up to three backup file servers.

You should configure Automatic Backups immediately so that you do not lose system or configuration information in case of problems. You configure the Automatic Backup servers from the Admin > Automatic Backup screen. The gateway does not begin a backup for at least 5 minutes after rebooting. This time period is to allow all resources to start operating. This delay occurs even if you go into the Admin > Auto Backup screen and request that a backup be started immediately; it is delayed until after the 5-minute period.

If you specify a path in the Admin > Autobackup screen and the directory does not exist on the FTP server, the automatic backup fails and “The host path does not exist” message is logged in the Event log. You must create a directory on the FTP server prior to running automatic backup.

Note: Automatic backup does not recognize a path beginning with the slash (/) character as it has in previous releases. The automatic backup path can only be given as relative to the home directory of the user ID used for the FTP transfer.

To enable automatic backup:

1 Click on the Enable button to enable the associated Host Backup File Server.

2. Enter the Backup File Server Host name or IP address.
3. Enter the Backup File Server Path, for example, Building3/Cntvty_backups.
4. Select the Specific Time option to execute the backup at a specific time. Enter the time at which you want the backup to occur.
5. Select the Interval option to execute the backup at certain intervals of time. Specify in hours the time period after which the system automatically backs up changed files to the backup file server. The minimum interval is 1 hour, and the maximum is 8064 (336 days); the default is 5 hours.
6. Enter the User ID that is required for FTP login to the backup file server.
7. Enter the Password that is required for FTP login to the backup file server.
8. Reenter the Password that is required for FTP login to the backup file server.
9. Click on the Backup button to execute a backup to each enabled server now. This action also synchronizes the hard disk drives when there is more than one in a device. Otherwise, the hard disks synchronize automatically every 60 minutes.

After entering the automatic backup file server information, click on the screen and press the keys Alt and Print Scrn (Screen) to save the screen image to a buffer. Next, paste the image into a file (for example, into Microsoft* Word) and keep it as a record of the backup file servers that you are using.

Upgrading the software

To upgrade the Contivity Secure IP Services Gateway, you download the latest Nortel Networks software using the File Transfer Protocol (FTP). Because FTP servers are often different, check your server documentation for information about setting paths that can help you with the upgrade procedure.

You can download the latest software from the Nortel Networks Web site, from your own FTP site if you previously downloaded the software from the Nortel Networks FTP site, or from the Nortel Networks software CD.

Some FTP servers do not use standard FTP port numbers so they cannot be used as download FTP servers for Nortel Networks software. For more information, contact Nortel Networks Customer support.

Note: You cannot upgrade the software through a branch office tunnel that is translating the management address with dynamic Network Address Translation (NAT).

If file retrieval fails, the Contivity gateway will retry the transfer. The WU-FTP server does not support this behavior and may cause the negotiation to fail. You should explore connectivity issues as the first possible level of failure.

Checking available disk space

Nortel Networks recommends that you keep a maximum of four software versions on the system disk. If four versions already exist on the Admin > Upgrade screen, you must delete one version before you download another version.

To remove a software version:

1. Go to the Admin > File System screen.
2. Select the Hard Drive (/ide0/).
3. Click on Display. You will see a list of the versions on the Contivity gateway.
4. Click on v0*x_xx.xx* and select Details. When the screen refreshes, you will see the directory that you just selected. Click on Delete Directory. A new screen appears verifying this is what you intended to do. If there was more then one image on the hard drive, follow the above process to delete all the older image upgrades that will not be used.

Before you upgrade your software, check to be sure that you have enough available disk space:

- From the GUI, if you go to Status > Statistics > File System, the last line lists the free space on the disk.

- From the CLI, if you type **show status statistics system file-system**, the last line lists the free space on the disk.

Note: Some restrictions apply if you have a Contivity 1010, 1050, or 1100. To export the configuration and LDIF files from the device, FTP the files to a server and view the file size. If the combined size of the LDIF and configuration files is less than 1MB, you can upgrade to the latest version. The Contivity 1010, 1050, and 1100 allow a maximum of two images on the flash disk. You must remove the second image (if present) prior to downloading an upgrade.

Creating a control tunnel to upgrade from a remote location

To upgrade the software on a Contivity gateway from a remote location, you must create a user control tunnel at the physical location of the gateway. User control tunnels provide secure access to a remote gateway so that you can manage it over a network.

The only way to create a user control tunnel is through the serial port on the gateway. To create a user control tunnel:

1. Connect the serial cable (supplied with the Contivity gateway) from the gateway's serial port to a terminal or to the communications port on a PC.
2. Turn on the PC or the terminal.
3. On the PC, start HyperTerminal* or another terminal emulation program and press Enter.

   The Welcome screen appears.

4. Enter the gateway administrator user name and then the password.

   The serial main menu appears.

5. Type **5** (`Create A User Control Tunnel (IPsec) Profile`).
6. Enter the user ID that you will use to log in remotely to the gateway.
7. Enter the password that you will use.
8. Enter the password again.

9 When you are prompted for an IP address, you can enter a static IP address that will be assigned to the user during the control tunnel connection. If an address pool is configured, you do not need to enter a static IP address.

Go to the next section, "Creating a recovery diskette" on page 51. You must create the diskette at the site of the gateway to be upgraded.

Creating a recovery diskette

Before you upgrade the gateway, create a recovery diskette. You need to perform this task on the gateway itself. To create a recovery diskette:

1 Insert a blank diskette into the floppy drive.

2 Navigate to Admin > Recovery and click on Create Diskette.

Note: If you have a diskless system, for example, a Contivity 1100, the recovery image is stored in flash memory.

Backing up system files

Before you upgrade, you should verify that a recent automatic backup was done.

1 If you are located at a remote site, connect to the gateway through a tunnel (branch office or user control).

2 On the Web GUI, choose Admin > Auto Backup and ensure that a recent automatic backup has been performed to an FTP server.

3 If a recent backup does not exist, create the backup on the Automatic Backup screen:

   a Enter an IP address or host name, path, interval, FTP user ID, and password.

   b Click on the Backup button to start the backup immediately.

This will save your entire hard drive, including the LDAP and configuration files.

Retrieving the new software

For Version 4.80 and later, the Contivity release image is available in a compressed .zip file so that each individual file does not download separately. The Contivity decompresses the image as it retrieves it. You must then apply the new image.

To use the compressed zip file:

1 Place the zip file (for example, V04_80.114.tar.gz) on the FTP server that you will be using for the upgrade.

```
D:\ftp>dir
Volume in drive D has no label.
Volume Serial Number is 9B29-6769
Directory of D:\ftp
06/18/2003  01:20p      <DIR>          .
06/18/2003  01:20p      <DIR>          ..
06/18/2003  06:53a          31,779,808 V04_80.069.tar.gz
```

Note: Do not attempt to create your own zip archive. Use the .tar.gz file distributed by Nortel Networks.

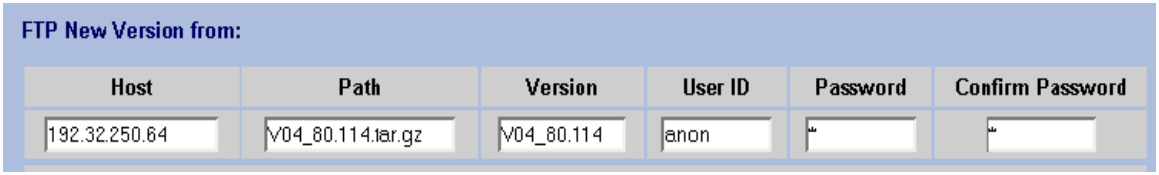
1 On the Web GUI, choose Admin > Upgrades.

2 Fill in the fields on the Upgrades screen as follows:

- Host: type the IP address or the name of the machine where the new software is located.
- Path: type the directory path location of the new software. The path value is the relative location of the .gz file from the FTP root in the directory. In the example below, the V04_80.069.tar.gz file is located at the root of the FTP directory.
- Version: type the exact name of the code that you are upgrading to (for example, V04_80.114).

  Figure 3 shows an example upgrade to V04_80.114 from server 192.32.250.64. The file V04_80.114.tar.gz must be located at the root of the FTP directory.

Figure 3 FTP menu example



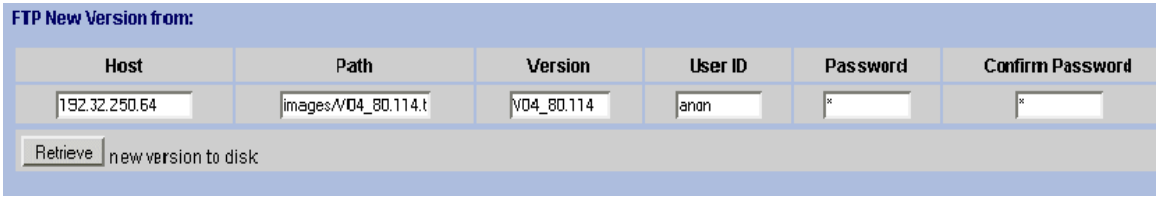
When you FTP to the FTP server from another PC, you see the location of the file.

```
D:\ftp>ftp 192.32.250.64
Connected to 192.32.250.64.
220 entrust-ca Microsoft FTP Service (Version 2.0).
User (192.32.250.64:(none)): anon
331 Password required for anon.
Password:
230 User anon logged in.
ftp> ls V04_80.069.tar.gz
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
V04_80.069.tar.gz
226 Transfer complete.
ftp: 19 bytes received in 0.62Seconds 0.03Kbytes/sec.
ftp>
```

If you want to locate the tar file in a subdirectory on the FTP server, you need to prepend the subdirectory to the path.

Figure 4 shows an example with the tar file located in the images directory under the FTP root.

Figure 4 FTP menu with subdirectory example

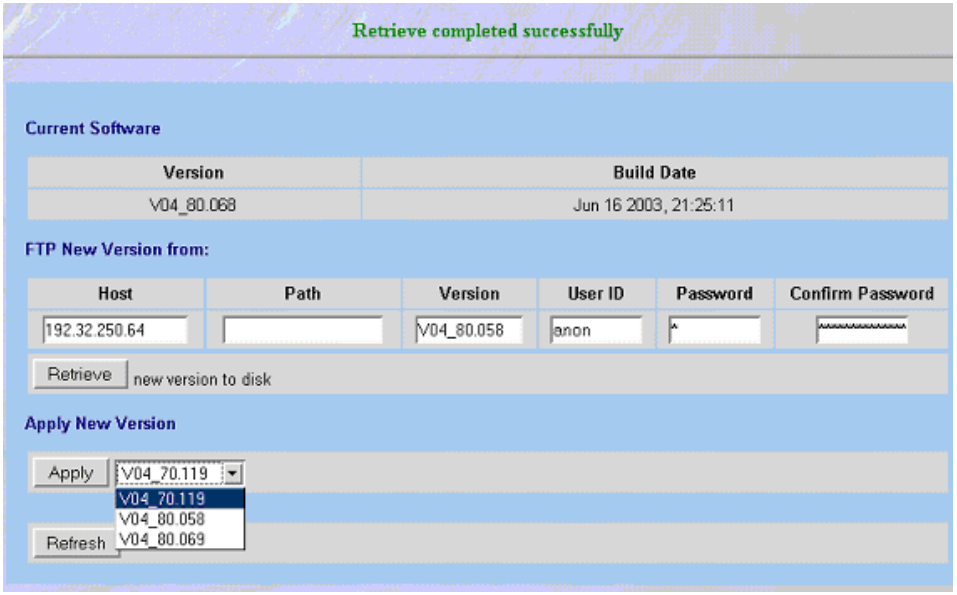


- User ID: type the login ID required to gain access to the FTP server where the new Contivity software is located.
- Password and Confirm Password: type the password (twice) that corresponds to the user ID that you just entered.

3 After filling in all the required fields, click on Retrieve. The New version retrieval window displays the progress of your download and indicates whether the retrieval was successful.

4 When the retrieval of the zipped image is complete, you can apply it as the new version.

Figure 5 New version retrieval



Before completing the upgrade

During the Apply process of upgrading to a new version of code, the gateway copies files from your current version of software to the new version before the gateway is rebooted. Because processes are still running, the copying of files can potentially cause file access problems.

To eliminate the possibility of file access problems after the upgrade, Nortel Networks recommends that you disable new logins, log off all active tunnels, and disable RADIUS accounting to prevent the gateway from processing pending updates.

To minimize the possibility of file access problems after the upgrade, Nortel Networks recommends that you perform the steps in this section.

1 Disable new logins.

   a Choose Admin > Shutdown and select the Disable new logins option (place a check mark in the box).

Caution: Make sure to follow the next step, or you will shut down the gateway.

   b Select a system shutdown type of None and click on OK.

2 Log off all active tunnel sessions.

   a Choose Status > Sessions.

   b Scroll to the bottom of the screen and click on both Log Off buttons to log off all non-administrative users and all branch office connections.

Note: These sessions would be logged off in any case during the Apply process

3 Disable RADIUS accounting.

   a Choose Servers > RADIUS ACCT and disable all of these options (remove the check marks from the check boxes):

      — Internal RADIUS Accounting
      — Interim RADIUS Accounting Record
      — Response Timeout for RADIUS Accounting Server
      — External RADIUS Accounting Server.

   b Click on OK.

Applying the software

After you start the apply process, avoid all queries on the gateway (for example, do not display the Health Check screen). Queries try to access files and so can cause problems during the upgrade process.

To apply the new software:

1 On the Web GUI, choose Admin > Upgrades.

2. From the Apply New Version list, select the software version that you just downloaded.
3. Click on Apply to start the upgrade process.

After you upgrade the software

After the gateway reboots itself with the upgraded software, follow these steps:

1. Wait 2 minutes after the reboot before you run queries to make sure that all startup processes have had time to read the files they need.
2. If you are managing the gateway remotely, connect to the gateway over a user control tunnel.
3. Clear the cache on your browser and close all browser windows.
4. Restart your browser, log on to the gateway, and navigate to Status > System. Verify that the new software version has been applied by checking the Software Version field.
5. To restore the internal LDAP database and the latest configuration file:
   a. Enable the FTP service on the Services > Available screen.
   b. Go to the system/config and system/slapd/ldif directories to replace the backed-up configuration and LDAP files.
   c. Click on the Restore link on the Admin > Configurations screen, select the correct file from the Boot Configuration list, and click on OK.
   d. Go to the Servers > LDAP screen, click on the Stop Server button, select the correct file from the Restore from File list, and click on Restore Now.
   e. When the restore is complete, restart the server from this screen.
6. If you upgraded the software to Version 4.*xx* from Version 2.*xx* or Version 3.*xx*, follow these steps to re-index the LDAP database.
   a. Choose Servers > LDAP and stop the internal LDAP database by clicking on the Stop Server button under the Internal Server Control heading.
   b. Under Backup/Restore Internal LDAP Database, enter a name in the Backup to File field and click on Backup Now to back up your internal LDAP database to a file.

c When the backup is complete, choose Servers > LDAP and stop the internal LDAP server by clicking on Stop Server under Internal Server Control.

d Under Backup/Restore Internal LDAP Database, select the backup file that you just created from the Restore from File list and click on Restore Now.

This procedure will re-index the LDAP database.

7 Reenable RADIUS accounting if you disabled it.

8 Go to Admin > Shutdown and deselect the Disable new logins options (remove the check marks from the check boxes).

Caution: Make sure to follow the next step, or you will shut down the gateway.

9 Select a system shutdown type of None and click on OK.

You have successfully upgraded your switch.

Chapter 4
Troubleshooting

This chapter introduces the concepts and practices of advanced network configuration and troubleshooting for the Contivity Secure IP Services Gateway. Its purpose is two-fold: to provide configuration details for you to consult when setting up or modifying your extranet, and to serve as a resource when diagnosing client and network problems.

Typically, there are three types of problems to address when managing an extranet:

- Connectivity
- Performance
- General

As a network administrator, your primary concern is maintaining connectivity. For extranet access, this means maintaining the secure connections between your remote users and the private intranet serviced by the gateway. Performance is another area of concern. Paying attention to performance can help you address issues before they become problems.

Connectivity problems occur when the remote user cannot establish a connection with areas of their private corporate network. There are several points of failure to consider when diagnosing connectivity problems. Problems can range from something as simple as a modem configuration error on the client workstation to a complex HDLC protocol error on the T1 WAN interface.

Troubleshooting remote access problems typically starts at the client end when the remote user cannot establish a connection, loses a connection, or has difficulty browsing the network or printing. When connectivity problems occur and the source of the problem is unknown, it is usually best to generally follow the OSI network architecture layers. Therefore, start diagnosing the physical environment, the modem, and cables before moving up to the network and application layers (for example, pinging a host and Web browsing).

As with connectivity, there are many places in the extranet network where network performance can be affected. By regularly checking your network statistics, logs, and health check information, and by informing users of good network practices, you can often avoid problems and enhance the productivity of your extranet.

General problems are categorized here as problems other than those related to connectivity or network performance. For the latest release-specific problems, check the release notes.

Troubleshooting tools

For the Contivity administrator, a robust troubleshooting “toolbox” is filled with both standard and special tools for diagnosing network problems. Standard tools like Telnet, PING, Trace Route (tracert.exe), sniffers, and analyzers are a basic necessity. To this collection, some special tools are added to the Contivity Secure IP Services Gateway manager and remote client applications. These special tools include client- and gateway-based tools.

Client-based tools

IPsec Contivity VPN Client Monitor provides network statistics on device, connection, and network errors that are helpful for monitoring traffic flow and assessing IPsec connection performance. Statistic counters are updated once a second. For more information on the IPsec Contivity VPN Client Monitor, refer to the Contivity VPN Client online Help.

Microsoft Point-to-Point Tunneling Protocol (PPTP) Dial-Up Networking Monitor provides network statistics on device, connection, and network protocols that are helpful for monitoring traffic flow and assessing PPTP connection performance. For more information on the PPTP Dial-Up Networking Monitor, refer to the PPTP help or your Microsoft PPTP client documentation.

System-based tools

The Manager Status > Health Check screen provides a detailed picture of how the gateway is performing. View colored status indicators to evaluate individual component status, and click on associated hyperlinks to jump to manager screens for corrective action.

The Manager Status > Statistics screen **a**llows you to delve into the inner workings of the gateway where you can view detailed system and network statistics.

The Manager Status > Security, Config, System, and Event Log screens allow you to view various logs recording system and network events that help you trace problems and determine their origins.

Other tools

Table 2 lists the tools that are helpful for diagnosing connectivity problems from Windows* 95, Windows 98, and Windows NT* workstations.

Table 2 Troubleshooting tools

Windows 95/Windows 98	Windows NT	Use for...
Winipcfg command	Ipconfig command	Obtaining IP address, DNS, WINS information
Netstats command	Netstats command	Viewing statistics from Microsoft TCP/IP stack
Ping and tracert commands	Ping and tracert commands	Testing connectivity, name resolution, route tracing
Dial-Up Monitor status	Dial-Up Monitor status	Viewing modem settings, throughput and errors

Solving connectivity problems

This section lists many of the common connectivity problems that can occur and the recommended solutions. Problems, and some typical client user responses that can help with diagnosis, are categorized as follows:

Modem and dial-up problems

“I cannot browse the Web or check my e-mail over my dial-up connection.”

“I cannot ping my ISP site.”

Extranet connection problems

“I can browse the Web over my dial-up connection, but I cannot log in to my network over the extranet connection.”

Problems with name resolution using DNS services

“I logged in to my corporate network, but I get messages saying the host is unknown.”

"I can ping the host using its IP address, but not using its host name."

Network browsing problems

"I cannot browse the corporate network."

"I cannot print."

"I cannot access the Internet over my extranet connection."

Diagnosing client connectivity problems

A connection can fail at varying points in an extranet. If remote users have a problem accessing their corporate network, and the source of the problem is unknown, Nortel Networks recommends that they follow these steps to first determine whether the problem is with their modem, Point-to-Point Protocol (PPP) dial-up, or with the extranet connection:

1. Confirm that the remote user's modem is attached and working properly by having them run a terminal emulation program at their remote workstation, such as, Hyperterminal*, and issuing the AT command. The response should be AT OK if the modem is operating correctly.
2. Verify that the remote user has a PPP dial-up connection over the internet. To do this, before they try to establish an extranet access or PPTP connection, have them try Web browsing www.nortelnetworks.com or another Web site that they commonly access. If the remote user can access the Web site, their PPP dial-up connection is working properly. Refer to the section "Common client connectivity problems" to further troubleshoot the connection problem. If the remote user still cannot verify that their dial-up connection is working properly, continue with step 3.
3. Ask the remote user to check that their modem type and settings are configured properly. To do this, they need to right-click on the Dial-Up Networking connection icon (the icon they click on to dial their connection) on their desktop to view its properties. Verify that these settings are correct for their modem configuration.
4. If the remote user is connected, but unable to access any resources or servers, have them check their system's connection information by going to the Start menu, selecting Run, and typing winipcfg in the text box (or `ipconfig` if

using Windows NT). Ask them to view the statistics for their PPP adapter and confirm that the entries match those provided by their Internet service provider (ISP).

5 If the remote user is still unable to view resources or servers over their PPP dial-up connection, contact their ISP to see if they have logged any connection attempts from the user, and for additional troubleshooting assistance.

Common client connectivity problems

Extranet connection problems

If the client is successfully connecting to their ISP, but is having problems accessing their intranet over their PPTP or IPsec Contivity VPN Client connection, have them check the following areas to further troubleshoot their connection problem.

The following messages and their associated cause and action statements are directed to the IPsec Contivity VPN Client user at the remote workstation. This information is also available in the Contivity VPN Client online Help.

Remote host not responding

Cause: This indicates that the gateway never responded to the IPsec connection attempt or that User Datagram Protocol (UDP) port 500 is blocked.

Action: Verify that the gateway is accessible by pinging the host name or IP address that you filled into the destination field. To `ping` a host called extranet.corp.com, for example, open an MS-DOS command prompt and type `ping extranet.corp.com`. If you receive a reply message, it indicates that the gateway is accessible but it is not responding. If you received a message that says Request Timed Out from the `ping` command, it means that the gateway is inaccessible. You may be able to further diagnose the problem using the MS-DOS Trace Route command (`tracert.exe`) on Windows systems.

The gateway only allows a certain number of PING packets from another Internet host before requiring a tunnel connection to be established.

Maximum number of sessions reached

Cause: This indicates that the maximum number of users for the account you are using are currently logged in.

Action: If you are the only user with access to your account, it is possible to get this error if you restarted an IPsec connection immediately after losing the dial-up connection to your ISP. This is because the gateway takes up to one minute to determine that your connection has been dropped and log you off from your account. Simply wait a minute and retry your connection.

Login not allowed at this time

Cause: This indicates that your account has been limited to specific hours of access and you are trying to connect outside of the allowed time.

Action: Contact your network administrator if you are unsure of your specific hours of access.

Authentication failed

Cause: The IPsec user name is incorrect or the password is invalid for the user name entered.

Action: Verify that the user name you entered is correct and retype the password before trying the connection again.

No proposal chosen

Cause: The gateway you are connecting to is not configured to handle the authentication method configured under the current connection profile.

Action: Verify that you are using the correct IPsec parameters, such as a choice of ESP-3DES with SHA1. Make sure it matches what the client (for example an International client) is capable of doing.

Other IPsec errors

Cause: Typically other error messages indicate an error in configuration on the gateway that must be corrected by the network administrator.

Action: Contact your Network Administrator with the specific error message.

Extranet connection lost

If the PPTP or IPsec Contivity VPN Client connection was initially established and then fails, one of two error messages appear: “The physical connection has been lost” or “The secure extranet connection has been lost.”

The physical connection has been lost

Cause: The PPP connection to your ISP was disconnected.

Action: Re-establish the PPP dial-up connection to your ISP before you re-establish the extranet connection to the remote network.

The secure extranet connection has been lost

Cause: For IPsec only, the gateway that you are connected to has either logged your connection off or the gateway is no longer responding.

Action: Re-establish the extranet connection by clicking the Connect button. If this works, the connection was probably lost due to the Idle Timeout configured on the gateway. If no data is transferred through the extranet connection for a long period of time, normally 15 minutes or more, the gateway automatically disconnects the connection.

If you were unable to successfully re-establish the extranet connection, the dial-up connection may be preventing data from traveling between the Contivity VPN Client and the gateway. Hang up the dial-up connection and reconnect before you try to re-establish a connection to the gateway. If you are still unable to connect to the gateway, open an MS-DOS Command Prompt and try pinging the gateway using the host name or address that you specified in the Destination field. If you receive a Destination Unreachable error message there is a routing problem at the ISP. If you receive a Request Timed Out error message, the gateway is probably not available, and you should contact your network administrator.

Auto disconnect closes the dial-up connection during data transfer activity

Cause: In Windows 95 only, The Microsoft Auto Disconnect feature does not recognize data activity unless it passes through Internet Explorer. Microsoft has documented this as a known problem in Windows 95.

Action: At the remote workstation, disable the Auto Disconnect feature if you are not using Internet Explorer to access data on the remote network. To do this, open the Control Panel and choose the icon labeled Internet. Select the Connection property sheet and deselect the "Disconnect if idle for" box.

Problems with name resolution using DNS services

When the client can ping a host using an IP address, but not with its host name, or receives messages that the host name cannot be resolved, DNS misconfiguration is usually the problem.

Cause: A DNS server may not be configured for PPTP or IPsec connections on the gateway.

Action: Validate that the Contivity VPN Client has been configured with a DNS entry. For Windows NT 4.0, open a command prompt and enter `ipconfig/all`. Verify that a DNS server entry is listed. For Windows 95, from the Start menu on the task bar, select Run and enter `winipcfg`. Select Nortel Networks Extranet Switch Extranet Access Adapter from the list of adapters and click on More Info. Record the information displayed under the DNS Server entry and verify it with the network administrator.

Cause: The hostname being resolved has both a public and a private IP address. This is commonly referred to as a split-horizon DNS.

Action: Open a command prompt and ping the host you are trying to reach with a fully qualified host name (for example, www.nortelnetworks.com). If you receive a response, verify that the IP address returned on the first line (for example, www.nortelnetworks.com [207.87.31.127]) is an IP address from the remote corporate network. If it is not, notify your network administrator that the internal hostname should be modified so that it is not the same as the external hostname.

Cause: The retail release of Windows 95 contained a bug that prevented use of more than one DNS server. This problem was fixed in OS Release 2.

Action: If you are using a release earlier than OS Release 2 of Windows 95, a patch is available from Microsoft to upgrade the winsock.dll. This patch is downloadable from www.microsoft.com.

Network browsing problems

Cannot browse the network (with NetBEUI)

Cause: For both PPTP and IPsec, the gateway does not currently support the NetBEUI protocol.

Action: To be able to browse resources on a remote domain through a connection to a gateway, it is necessary to remove the NetBEUI protocol and have a WINS server configured. By removing NetBEUI, the Microsoft Client uses NetBIOS over TCP/IP to browse network resources. This applies to both the PPTP dial-up client provided by Microsoft and the Contivity VPN Client provided by Nortel Networks.

Cannot access Web servers on the Internet after establishing an Contivity VPN Client connection

Cause: For both PPTP and IPsec, this condition occurs as a result of having all network traffic passed through the corporate network. Typically, firewalls and other security measures on the corporate network limit your access to the Internet.

Action: The gateway administrator can set up a default route on the gateway to forward traffic to the Internet. If this default route is not configured, you need to disconnect the extranet connection to Web browse the Internet through your ISP connection.

Alternatively, if you are using a proxy-based firewall, you must set your Web browser to use the firewall to proxy for HTTP traffic when your tunnel connection is in use.

Cannot access network shares after establishing an extranet access connection

Cause: A Windows Internet Name Service (WINS) server may not be configured for PPTP or IPsec connections on the gateway.

Action: Validate that the Contivity VPN Client has been configured with a WINS server. Follow the steps outlined above under "Problems with name resolution using DNS services" to run `ipconfig` at a command prompt on Windows NT 4.0 or to run `winipcfg` on Windows 95. Verify that a primary WINS server is listed under the section for the adapter named IPsecShm on Windows NT 4.0, and on Windows 95 verify that a primary WINS server is listed in `winipcfg` for the Contivity VPN Client adapter. If there is no primary WINS server listed, notify the network administrator that the gateway may not be properly configured.

Cause: Your system may be set up for a different domain other than the one on the remote network.

Action: Skip the initial domain login when Windows 95 starts and choose Log on to the Remote Domain under the Options menu of the Contivity VPN Client dialog box. You are then prompted to log in to the domain of the remote network after the extranet connection is made. This is the recommended method for users with docking station configurations.

Alternatively, on NT 4.0, Windows 98, and Windows 95, change your workstation to be a member of a workgroup instead of a domain:

1. From the Start menu, select Settings > Control Panel. In the Control Panel, double-click on the icon labeled Network. The Network Control Panel applet opens.
2. Select the Identification tab. In Windows 95, the entries on the Identification tab can be modified directly; on NT 4.0 it is necessary to click the Change button to change the entries.
3. Change to use a Workgroup and verify that the computer name does not match the entry on the remote network. The name for the workgroup is not important; you can enter anything.
4. Click on OK to save the changes and reboot the machine.
5. When accessing a resource on the remote domain, if you are prompted for a user name and password, you need to have a domain name precede your user

ID. For example, if your user ID is JSmith and you are accessing a machine on the remote domain named CORP, you would enter your user name as CORP\JSmith.

Diagnosing WAN link problems

WAN link problems can occur between the gateway and the public data network (PDN) at three levels:

1. T1/V.35 interface
2. HDLC framing
3. PPP layer

If a connectivity problem occurs with the WAN link, there are two approaches you can use to diagnose and correct the problem.

- Start from the bottom to verify that physical connectivity exists, then make sure that the HDLC link is up, and finally examine the PPP status to see if it is passing IP packets back and forth.
- Start from the top down to go in the opposite direction, looking at PPP first and working down to the physical connection. An important point to remember when taking this approach is that at the higher protocol layers, there are more options to misconfigure, but changing them is easier and generally involves less effort.

A key point to remember when diagnosing WAN link problems is that the T1 service provider should usually be involved in the troubleshooting effort. This is not only because they can help diagnose the problem, but also because an ISP can bring down a link if it detects errors on the line. You should notify the ISP administrator if you are planning on working on the link.

Check the T1/V.35 interface

To diagnose a problem at the WAN physical layer, use the following steps to verify that the T1/V.35 interface to the public data network (PDN) is operating correctly, and that the T1 line is properly connected:

1. Have your ISP run a loopback test from their end to the CSU/DSU to verify that the external line is working correctly.

2. Check the connections between the gateway and the CSU/DSU. The V.35 cable should be a straight-through cable and firmly seated. Also the CSU/DSU should be configured to use internal clocking, and NRZ encoding with CCITT CRC for the checksum.
3. Make sure that all the control signals are asserted (CTS, DCD, DSR, RTS, and DTR). You can check these signals on the gateway from the Manager WAN Statistics screen. If any of these signals are incorrect, you can try disabling or enabling the link from the Manager WAN Interfaces screen, or unplugging and plugging in the link. If these steps do not resolve the problem, try switching ports on the same card, switching cables, or switching to a new card, if available.
4. If the previous steps fail to resolve the problem, and you still suspect a problem with the physical connection, try rebooting the gateway to reinitialize the WAN interface.

Check the HDLC framing

Assuming that the T1/V.35 interface is operating correctly, use the following steps to determine whether the HDLC layer is up and running properly, and to provide information for Nortel Networks Customer Support for further diagnosis:

1. Check to make sure that there are no input or output errors reported on the Manager WAN statistics screen. Also look to see if the input and output counters are incrementing at all. If the input/output counters are not incrementing, or are incrementing by huge amounts, then there are probably framing or timing errors on the link. Also, a large percentage of input errors may indicate a problem with the FCS (Frame Check Sequence) calculation.
2. Examine the Manager Statistics event log with debugging enabled. Any WAN-related log messages probably indicate some sort of error.
3. Report any of the preceding errors and messages to Nortel Networks Customer Support for assistance in diagnosing the HDLC framing problem.

Check the PPP layer

If the WAN link appears to be passing frames back and forth, yet IP packets are not flowing, the problem may be with how PPP is configured.

To examine the state of the PPP connection, and to provide information for Nortel Networks Customer Support for further diagnosis:

1. Check to see whether the state of the PPP connection is changing at all by periodically clicking on the Refresh button while viewing the WAN statistics screen. If the state is always Down, PPP might not know that the link is up. If the state toggles between Dead and LCP Negotiating, PPP is trying to come up but cannot. This is probably due to a problem with the underlying layers, although it could also be a bad configuration of the LCP options.
2. If the connection fails during authentication, then try disabling the PPP Authentication settings. A problem during Network Negotiating is usually due to misconfigured IPCP options.
3. Verify that all the authentication settings match the ISP-recommended router configuration.
4. If the PPP layer still does not come up, enable the interface debugger to generate large amounts of packet traces in the event log. Report this information to Nortel Networks Customer Support for further diagnosis.

Hardware encryption accelerator connectivity

If the hardware encryption accelerator fails, all sessions are automatically moved over to be handled by the software.

Solving performance problems

This section describes ways for improving the performance of the remote workstation connection to the corporate network through a gateway. It also includes Microsoft networking and client setup and operation tips.

Eliminating modem errors

Modem hardware errors can impact performance when connecting to your corporate network over a dial-up connection. If modem hardware errors are occurring, try the following techniques to correct these errors and improve performance:

- Adjust the modem speed –I f the speed of the modem is set too high it can cause hardware overruns. Reset the modem speed to match the real speed of the modem.
- Disable hardware compression – The data passed through the extranet connection is encrypted, and encrypted data is typically not compressible. Depending on the algorithm the modem is using to compress the encrypted (non-compressible) data, the data may expand in size and overrun the modem's buffers.

Performance tips for configuring Microsoft networking

For Microsoft networking to work as designed over the extranet, each of the following components, if configured, must be working together:

- DHCP Server assigns IP addresses to clients.
- WINS Server provides a translation of the NetBIOS domain name to the IP address.
- DNS Server provides a translation of the IP Host name to the IP address.
- Master Browser is an elected host that maintains lists of all NetBIOS resources.
- Domain Controller maintains a list of all clients in the NetBIOS domain and manages administrative requests such as logins.
- Contivity Secure IP Services Gateway terminates tunnels and routes Microsoft networking requests.

The following questions and answers are particularly directed toward the WINS server and browsing issues that can help you verify whether you have correctly set up these components.

What needs to be configured on the gateway for network browsing?

In the group profiles, set the values of the DNS server and the WINS server. Remember that these are inherited values, so that if all subgroups of a given group use the same servers, it is sufficient to configure them in the parent group.

If these servers are not on a directly reachable subnet from the gateway, or accessible through a default gateway, a static route must be configured on the gateway in order to reach them.

What should be configured on the PPTP or IPsec client?

The client should have the protocols for NetBIOS and TCP/IP configured. NetBEUI should not normally be configured.

A Windows 95 or Windows 98 client should be configured to be in the correct workgroup for the NT domains it is trying to reach. For example, if there are domains named Engineering and Admin, and the client is to use the Engineering domain, then it must be configured that way in its own configuration.

For PPTP only, you must also select the option Log onto Network under My Computer > Dial Up Networking > Connection_Name properties.

The client system's NetBIOS name must be unique in the private network to which the client is connecting. Do not use the same name as your office desktop machine or something like "my computer." Uniqueness is required.

What is the preferred way to access neighbors on the network?

Microsoft recommends against browsing the Network Neighborhood when tunneling. Another way to access a network resource is through the `run` command. For example, to access shared folders on the machine HotDog, choose Start > Run and type in \\HotDog. If you experience delays using Network Neighborhood, you may want to try this method instead.

Why should WINS settings be different for extranet access?

WINS servers cache a correspondence between IP addresses and NetBIOS names. These cached values are only invalidated by a timer and not by network activity. Therefore, a WINS server that is used heavily by clients should have its expiration timeouts set low.

In a static environment, where names and addresses correspond forever, this is not an issue. But in the extranet environment, clients are assigned new IP addresses whenever they form a tunnel. Therefore, the correspondence is transitory.

Microsoft default values for the timeouts are enormous (for example, 3 weeks). These need to be reduced for an extranet environment.

What WINS settings are recommended?

The WINS settings are available on the WINS server through the Start menu > Programs > Administrator Tools. Nortel Networks is currently experimenting successfully with the following values for a WINS server:

- Server Configuration
- Renewal Interval: 41 minutes
- Extinction Interval: 41 minutes
- Extinction Timeout: 24 hours
- Verify Interval: 576 hours

The renewal interval governs how often a client must reregister its name with the WINS server. It begins trying at one-half of the renewal interval. The extinction interval governs how long it is between the time a client name is released until it becomes extinct. These intervals are the most important to control when using dynamic addresses.

There is a trade-off in setting these intervals. If they are set too small there is too much additional client registration network activity. If they are set too large, transient client entries do not time out soon enough. If you also have secondary WINS servers, the renewal interval should be the same on the secondary servers as on the primary server.

For additional information on setting interval values for a WINS configuration, refer to the Microsoft Knowledge Base article “Min. and Max. Interval Values for WINS Configuration” available at http://support.microsoft.com/support. A WINS server that has a heavy CPU load or network load will not perform well. To help performance:

- Do not run other intensive tasks on the WINS server.
- In the WINS configuration, disable detailed logging.
- If you have primary and secondary WINS servers, try to assign them for a balanced load.

Hosts that never change IP addresses can be given static entries in the WINS database. For example, you could configure the address of the Primary Domain Controller as static. To do this, you also have to have a statically reserved DHCP address for the primary domain controller.

What can you try on the WINS server when it is not working?

You can request that the WINS server clean up its database. You can do this by going into the Mappings menu item and selecting Initiate Scavenging.

If the database becomes very large, it can be compacted using the jetpack.exe program in \winnt\system32. Please consult the WINS Help before doing this because the server must be shut down.

In the WINS mappings entry, enter a `show database` command. Note the entry for -__MSBROWSE__. This is the machine that is actually the elected master browser, and it changes frequently. If this entry is pointing to an invalid machine, this can cause problems.

Can I control which machine is the master browser?

When you start a computer running Windows NT Workstation or Windows NT Server, the browser service looks in the registry for the configuration parameter MaintainServerList to determine whether a computer will become a browser. This parameter is under:

```
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\
Parameters
```

For Windows 95, this parameter is under:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VNETSUP\
MaintainServerList
```

MaintainServerList parameter values are:

- No–This computer will never participate as a browser.
- Yes–This computer will become a browser.
- Auto–This computer, referred to as a potential browser, may or may not become a browser, depending on the number of currently active browsers.

The registry parameter IsDomainMasterBrowser impacts which servers become master browsers and backup browsers. The registry path for this parameter is:

```
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\
Parameters.
```

Setting the IsDomainMasterBrowser parameter entry to True or Yes makes the computer a preferred master browser. Whenever a preferred master browser starts, it forces a browser election.

When the browser service is started on the preferred master browser computer, the browser service forces an election. Preferred master browsers are given priority in elections, which means that if no other condition prevents it, the preferred master browser always wins the election. This gives an administrator the ability to configure a specific computer as the master browser.

To specify a computer as the preferred master browser, set the parameter for IsDomainMasterBrowser to True or Yes in the following registry path:

```
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\
Parameters
```

Unless the computer is configured as the preferred master browser, the parameter entry is always False or No. There is no user interface for making these changes; you must modify the registry.

Why are subnet masks important?

If a client does not have a WINS server or is unable to contact it, it must broadcast a query to try to locate a host. Unfortunately, Windows 95, Windows 98, and Windows NT clients do not always use the correct broadcast address when tunneling.

The following example helps explain this problem. Suppose that you are using a private net 10 address space. Assume further that you have a client with IP address 10.1.2.3 and subnet mask 255.255.0.0. This means that the net 10 space is being used like a class B address space, which is perfectly legal. The correct broadcast for this client is 10.1.255.255. However, Microsoft clients may broadcast to 10.255.255.255, using the natural class A for net 10, in spite of their configuration.

If all hosts that the client is trying to reach lie on the same physical segment, this probably will work. This is because every host on the physical network receives the all subnets broadcast and probably responds, if appropriate.

All hosts on the segment receive the broadcast to 10.255.255.255, even if they are on different subnets (10.1.x.x. and 10.2.x.x). However, in a routed environment the situation changes. In this case, a broadcast from 10.1.2.3 to 10.255.255.255 is not forwarded to the other 10.2 subnet.

In the extranet environment you should make the remote client appear as much as possible to be on the local LAN. If the extranet host is assigned address 10.1.2.3, it should behave as if it is on the 10.1 LAN.

When 10.1.2.3 broadcasts to find a network neighbor, it (incorrectly) sends to 10.255.255.255. Normal routing functionality would not forward such a packet. The gateway finds the best match among its physical interfaces (10.1 in this case) and modifies the broadcast to be correct for that interface (10.1.255.255 here).

In this example, if the gateway's 10.1 interface had been configured with any subnet mask other than 255.255.0.0, the broadcast would not have been converted as desired.

What should I do about subnets?

Every private interface on the gateway should be configured to have the same subnet mask as all of the clients residing on that subnet.

Why is there a delay in discovering the Network Neighborhood (with tunnels)?

NetBIOS treats the modem interface as if it is two different interfaces: the original modem and the tunnel. It designates the original modem as the primary interface. (You can observe this by typing `route print` in a DOS command shell.) If you tunnel over a LAN instead of a modem, the LAN adapter is designated as the primary interface.

When first instructed to seek the Network Neighborhood, NetBIOS always tries the primary interface first. This is always the wrong choice because NetBIOS always tries to send using the IP address assigned by the ISP (or possibly the address of another adapter) instead of the address assigned to the tunnel by the gateway.

The outcome is somewhat different for IPsec and PPTP. For IPsec, the client recognizes this incorrect behavior and refuses to even send the packets. You can see a counter of the number of invalid packets of this type on the client under the status Invalid IP address.

With PPTP, the client does send the packets, but they are rejected at the gateway as invalid tunneled packets because the source address does not match the gateway-assigned address. If you inspect the event log, there are messages of the form Bad source address in tunnel and the session/details counter for source address drops increases.

After about 10 to 15 seconds, NetBIOS gives up on the primary interface, gateways to the correct tunnel interface, and starts to browse the Network Neighborhood.

Why can't I browse another client in a different tunnel?

Cause: If you are not using a WINS server, this is not possible because network browsing requires broadcasts from one tunnel to another.

Action: Use a WINS server to browse another client in a different tunnel. When the clients tunnel in, they should register with the WINS server. Be sure that the client you want to browse has the Log onto Network setting enabled under My Computer > Dial Up Networking > Connection_Name properties.

Where can I get more information on troubleshooting dial-up connections?

The Microsoft Knowledge Base article “Dial-Up Networking 1.2 Dun12.doc” file, available from http://support.microsoft.com/support, contains help for resolving common dial-up problems.

Depending on the service provider, a point of presence (POP) may not support LCP options. If your connection constantly gets declined after the modems synchronize, and you know your password is correct, try disabling this option. The Microsoft Knowledge Base "Service Pack 2 May Cause Loss of Connectivity in Remote Access" article contains more details.

Where can I get more information on configuring PPTP on my client?

There are many articles in the Microsoft Knowledge Base on configuring PPTP for Windows NT, Windows 98, and Windows 95. Refer to the section "Additional information" for a partial list. In addition, Microsoft has the following white papers available at http://support.microsoft.com/support that contain helpful information:

- Microsoft Windows 95/Windows NT White Paper, "Installing, Configuring, and Using PPTP with Microsoft Clients and Servers"
- Microsoft Windows NT Server White Paper, "Understanding PPTP"

You must create a connection definition for your initial Internet link via your service provider. A separate connection definition is needed for creating the PPTP tunnel. A common configuration problem experienced during initial PPTP setup is the failure to select the PPTP VPN adapter (instead of the modem) on the PPTP connection definition in Dialup Networking.

What DNS and WINS servers should I set for the dial-up connection?

There should be no need to set these servers statically on your dial-up client because information is dynamically downloaded from the gateway for PPTP, IPsec, and Layer 2 Forwarding (L2F) tunnels at connect time.

Why does DNS resolve hosts to different addresses when a tunnel connection is active?

Cause: When a tunnel connection is activated, additional DNS servers are downloaded from the extranet device (for example, the gateway) to your client. In the case of Microsoft Windows 95, Windows 98, and Windows NT operating systems, the new DNS servers are added to the list of DNS servers that were

assigned by your ISP. This applies to PPTP as well as IPsec tunnels. In general, the DNS servers downloaded by the extranet device provide host-name-to-address translation for hosts within a private network while the ISP-based DNS servers can be expected to translate public host names.

For Windows 95/98 and Windows NT, when a host name must be translated to an IP address (for example to browse the Web or get e-mail), all DNS servers are queried in a shotgun style. The first server to respond with an IP address wins. This can produce some interesting behavior if a host name resolves to one address on the private network and another on the public Internet. For example, host mail.mycompany.com could Internally resolve to 10.0.0.282 and externally to 146.113.64.231.

Action: To avoid problems when using a mixture of internal and external DNS services, it is essential to avoid using names that can resolve to different addresses. In the preceding example, host 10.0.0.282 should probably be renamed pop.mycompany.com. Then users can be informed to use the hostname pop.mycompany.com to retrieve electronic mail, whether in the office or connected via a tunnel link.The original retail release of Windows 95 requires the Winsock DNS Update (wsockupd) to properly function with multiple DNS servers.

My downloaded DNS servers for my tunnel connection do not work

Cause: The Microsoft Windows 95/98 and Windows NT operating systems attempt to ping new DNS servers before adding them to the current list of servers.

Action: As a quick test, try to ping (with the tunnel connection active) the DNS servers that the extranet device is downloading at tunnel startup. If you cannot ping the servers, a basic connectivity problem using the tunnel connection exists.

To view the current list of DNS servers at any time use the MS-DOS command `ipconfig/all` on Windows NT or `winipcfg` on Windows 95 or Windows 98.

Why, after disconnecting a PPTP tunnel, do I get an immediate error reconnecting?

Cause: After you disconnect a PPTP tunnel, then immediately try to reconnect, the PPTP client indicates that the connection is busy or otherwise unavailable. On Windows 95 this is caused by the PPTP control channel socket being improperly shut down by the client.

Action: You can wait for the socket to time out, but it is often more expedient to reboot. On Windows NT a similar problem can be encountered, but caused by a TCP checksum error generated by the Microsoft IP stack. The only current resolution for the Windows NT error condition is to reboot.

Additional information

Below is a list of some of the Microsoft Knowledge Base topics you can browse for information related to dial-up and tunnel configuration. To view these topics, go to http://support.microsoft.com/support. Use the Search Support Online feature to search on the title you want:

- Troubleshooting Internet Service Provider Login Problems
- Service Pack 2 May Cause Loss of Connectivity in Remote Access
- Troubleshooting Modem Problems Under Windows NT 4.0
- Dial-Up Networking 1.2 Dun12.doc File (Windows 95 PPTP Troubleshooting)
- How to Troubleshoot TCP/IP Connectivity with Windows NT
- Remote Access Service (RAS) Error Code List for Windows NT 4.0
- RAS Error 720 When Dialing Out
- Troubleshooting PPTP Connectivity Issues in Windows NT 4.0
- PPTP Registry Entries
- Connecting to Network Resources from Multihomed Computer
- How to Force 128-bit Data Encryption for RAS
- Login Validation Fails Using Domain Name Server

Solving general problems

This section contains general recommendations and explains some common problems that can occur with common Web browsers, the Nortel Networks Contivity VPN Client Manager, and the gateway.

Web browser problems and the Contivity VPN Client Manager

If you have a problem browsing the Nortel Networks Contivity VPN Client Manager, start by checking the following recommendations to ensure that you are using the correct Web browser version and settings. For additional troubleshooting, check the described Web browser problems and solutions, error messages, and tips described later in this section.

Nortel Networks Contivity VPN Client Manager uses Java* and HTML features. For the management interface to function properly, verify that your Web browser meets the following minimum requirements:

- Platforms supported include Windows 95, Windows 98, Windows NT, or Macintosh*.
- Display setting of 256 colors or greater.
- Browser versions supported include Microsoft Internet Explorer, Version 4.0 or later and Netscape Communicator*,Version 4.0 or later. Not using a recent version of Internet Explorer causes the upper-left corners of the management screens to remain gray rather than displaying the navigational menu and the current menu selection, respectively.
- For ActiveX Scripts, Java, and JavaScript*, you must Enable both ActiveX and Java programs in Internet Explorer, and enable both Java and JavaScript in Netscape Communicator for proper Contivity Web management screens. These options are enabled by default on both Web browsers.

Enabling Web browser options

To make sure these options are enabled in Internet Explorer, from the Internet Explorer menu bar, choose View > Options > Security and choose:

- Run ActiveX scripts–If this option is disabled, navigational titles are not updated, and the Logoff and Help buttons do not work.
- Enable Java programs–If this option is disabled, navigational menus do not appear.

To make sure these options are enabled in Netscape*, from the Netscape menu bar, choose Edit > Preferences > Advanced, and choose:

- Enable Java – If this option is disabled, navigational menus do not appear.
- Enable JavaScript – If this option is disabled, navigational titles are not updated, and the Logoff and Help buttons do not work.

Long delays when Web browsing

Cause: HTTP. Sometimes while using the HTTP Web interface you can experience long delays (greater than five minutes).

Action: Wait until the requested screen is fully delivered before clicking on a new screen request.

Improving performance with Internet Explorer 4.0

Nortel Networks recommends that you create a DNS server entry for your management IP address. This alleviates a noticeable delay in loading the initial Main menu and navigational screens.

Clearing your Web browser cache when upgrading

To avoid problems when upgrading software revision levels (for example, moving from Version 01_01.16 or V01_05_01.28 to V01_00.33), Nortel Networks recommends that you clear your browser cache and exit the browser and all associated windows (such as mail and news readers). Refer to the following section for browser cache clearing instructions.

Clearing cache

A browser caches pages to improve performance when the same page is requested again. The gateway's HTTP server allows the browsers to cache the Java class files, and all image files, but not to cache the body pages that contain the dynamically generated information. Both Internet Explorer and Netscape allow you to clear the browser cache which causes all pages to be re-requested the next time they are required. To manually clear the browser cache in Internet Explorer V4.x, select View > Internet Options, and click on Delete Files. To manually clear the browser cache in Netscape V4.x, go to Edit > Preferences > Advanced > Cache and select Clear disk and memory cache.

Web browser error messages

No data in post message

Cause: This message often appears on the main body page if you use the browser's back arrow to revisit a previously displayed page. The browser displays this message when it knows you are revisiting a dynamically generated page.

Action: To see the page, you must use the left navigational area to select it.

Internal error message

Cause: The HTTP server was unable to allocate memory. This indicates that the gateway is very low on memory.

Action: Terminate any unnecessary tasks to free up memory. It may be necessary to reboot the gateway. If this condition recurs, there may be a serious problem. Contact Nortel Networks Customer Support.

Document not found message

Cause: This message is returned when the HTTP server cannot find the requested page on the gateway. This could happen because the Java navigation index file is out of synch with the rest of the system. A corrupted or incorrectly cached index file could also cause this problem.

Action: Clear your browser cache or restart your browser to correct this problem.

New administrator login ignored

Cause: Internet Explorer saves your user ID and password in its cache and automatically resends those values on subsequent login attempts. Therefore, when prompted after an idle timeout, the user ID and password value you enter are ignored, and Internet Explorer sends the original user ID and password. For example, if you log in as administrator with password abc123De, and you subsequently log out. If you log in again, this time as DottieDoe with password FGh45678, in spite of the different login and password, Internet Explorer sends Administrator with passwordabc123De.

Action: When you log off the gateway, close out of the Web browser completely (shut down the browser). This clears the cache and the next time that you log in you are starting fresh.

Excess resource consumption using Internet Explorer

Cause: Internet Explorer has a known problem with excessive memory consumption using Java applets. Over time, this problem can cause serious overall system performance degradation.

Action: If you notice that your system's performance seems to slow down for no reason, close and restart Internet Explorer. This releases unused memory and should improve system performance. Go to http://premium.microsoft.com/support/kb/articles/q173/1/45.asp for details.

Internet Explorer 4.0 multiple help windows

Cause: In Internet Explorer 4.0, if you select context-sensitive help and do not close the help window after viewing, you might end up with multiple help windows open.

Action: Close help windows after viewing them.

Distorted background images

Cause: In Netscape versions prior to 4.0 where you configure your Windows 95, Windows 98, or Windows NT system for 8-bit color (256 colors or less), images might appear distorted in the navigational area.

Action: To avoid this situation, increase the color display setting to 256 or greater. You should check with your video card manufacturer's documentation to confirm that your video card supports 256 colors or greater.

Reporting a problem with a Web browser

When reporting a problem with a browser to Nortel Networks, include the following information:

- Workstation operating system and version
- Browser vendor and version (major and minor version)
- Cache setting (size in Netscape, percent of drive for Internet Explorer)
- Verify document setting (every time or once per session)

System problems

Excessive active sessions logged

Cause: The number of active sessions can reach more than 4 billion. This is an erroneous number that results from a negative number of sessions.

Action: Restart the system.

Power failure

Cause: The power supplies can become unseated during shipping. When this problem occurs, you might not be able to start the gateway, or a warning might be posted to the Status > Health Check screen indicating a potential problem.

Action: If necessary, remove the front bezel as described in the installation guide, then push the bottom of the power supply in to reseat it.

Cannot convert from an internal address pool to an external DHCP server

Cause: You cannot convert IP address distribution from an internal address pool to an external DHCP server while sessions are active.

Action: Go to the Admin > Shutdown screen, and select Disable Logins after Restart. After everyone has logged off the gateway, then you can convert from an internal address pool to an external DHCP server.

Group and user profile settings not saved

Cause: When you use the Save Current Configurations option on the Admin > Configs screen, it saves only the operational parameters in the configuration file, such as interface IP addresses and subnet masks, backup host IP addresses, DNS names.

Action: To completely back up the gateway configuration, you must also back up the LDAP database, which contains the group and user profiles, filters, and backup file names.

1. Go to the Servers > LDAP screen and click on Stop Server.
2. Enter a file name in the Backup/Restore LDAP Database field. The name should conform to the MS-DOS naming conventions and append the filename with LDF (for example, ldapone.ldf). The restore process can take anywhere from five minutes for a very small LDAP database to several hours for a very large database.
3. You can view the progress of the restoration from the Admin > Health Check screen.

Restart fails after using recovery and reformatting the hard disk

Cause: When you are using the recovery disk and reformatting the hard disk, sometimes the system will not restart.

Action: Power-cycle the system using the green power button on the back of the gateway.

Solving routing problems

The following sections describe routing problems.

Client address redistribution problems

The number of current Utunnel host users may display more than the configured maximum.

Cause: This is not an error and is the running state of the system. For example, if you configured a maximum of 200 and have 150 logins, the screen will display the maximum as 200 and the current as 150. If you then modify the maximum to 100, the screen will display the maximum as 100 and the current as 150. As users log out, the current number will eventually be no greater than the maximum.

Action: No action.

Client address redistribution is enabled and the client is logged in, but the client is not communicating with the private network.

Cause: Client address redistribution is not enabled.

Action: Have the client log in again. Client address redistribution only takes effect if the client logs in when it is enabled.

1. Check the Routing > Policy screen to be sure Utunnel routes are enabled.
2. Check to be sure that OSPF and Routing Information Protocol (RIP) are properly set up.
3. Check to be sure you have the correct address ranges if you configured summarization.
4. Be sure you have an Advanced Routing license if you are using OSPF for client address redistribution.

Solving firewall problems

An error occurred while parsing the policy

Description: The policy that you are attempting to view or edit cannot be opened because it does not conform to the required format. This may be caused by an error in the LDAP database or a problem with the connection to the gateway.

Action:

1. Close the Contivity Stateful Firewall Manager.
2. Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
3. Be sure that the connection to the gateway is established.
4. Be sure that the LDAP server containing the policy is properly configured and is active.
5. Restart the browser and navigate to the System > Firewall screen.
6. Reload the Contivity Stateful Firewall Manager.

An error occurred while communicating with the gateway

Description: The Contivity Stateful Firewall Manager encountered an error while retrieving the data from the gateway. This may have been caused by a network error or the gateway may have stopped responding.

Action:

1. Close the Contivity Stateful Firewall Manager.
2. Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
3. Be sure that the connection to the gateway is established.
4. Restart the browser and navigate to the System > Firewall screen.
5. Reload the Contivity Stateful Firewall Manager.

Authorization failed. Please try again.

Description: This error occurs when the wrong authentication credentials are entered. The user is re-prompted for credentials until they are either correct or the user clicks on Cancel.

Action: No action required.

Unable to communicate with the gateway

Description: The Contivity Stateful Firewall Manager cannot establish a connection to the gateway. This may have been caused by a network error, or the gateway may not be responding to requests.

Action:

1. Close the Contivity Stateful Firewall Manager.
2. Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
3. Be sure that the connection to the gateway is established.
4. Restart the browser and navigate to the System > Firewall screen.
5. Reload the Contivity Stateful Firewall Manager.

The contents of the database may have changed

Description: This error occurred because the LDAP database has changed in such a way that the current data in the Contivity Stateful Firewall Manager might not be valid. This error is encountered when the following events occur:

- Internal LDAP server has been shut down and restarted.
- External LDAP server in use is switched to the internal LDAP server.
- Internal LDAP server in use is switched to an external LDAP server.
- External LDAP server's port or IP address changes.

Action:

To ensure that the most current data is loaded:

1. Close the current policy, if opened. Saving is not permitted until this error is remedied.
2. From the policy selection screen, select All from the Refresh menu.

System files were not loaded properly

Description: This error occurred because the files necessary to load the Contivity Stateful Firewall Manager were either not downloaded from the gateway properly or were not initialized properly.

Action:

If this error is encountered:

1. Close the Contivity Stateful Firewall Manager.
2. Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
3. Restart the browser and navigate to the System > Firewall screen.
4. Reload the Contivity Stateful Firewall Manager.

If the error continues to occur or if the Contivity Stateful Firewall Manager is being accessed through a user tunnel:

1. Open the Java Plug-in Properties.
2. On Windows systems, navigate to Start > Settings > Control Panel > Java Plug-in. For all other systems, refer to the Java Plug-in documentation.
3. Be sure that the check box for Cache JARs in Memory is deselected.
4. Click on Apply and close the Java Plug-in Properties window.
5. Close the Contivity Stateful Firewall Manager.
6. Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
7. Restart the browser and navigate to the System > Firewall screen.
8. Reload the Contivity Stateful Firewall Manager.

Chapter 5
Using packet capture (PCAP)

Packet capture (PCAP) enables network administrators and customer support personnel to remotely troubleshoot Contivity gateway and network problems. Packet capture is especially useful for troubleshooting a gateway such as the Contivity 1010/1050/1100, which is typically located in a small office where no technical expertise may be available.

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, you can capture packets traversing the Contivity gateway and write them to disk in a format that can be read with common packet analyzer tools.

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.

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 (physical interfaces, tunnels, and the gateway as a whole).
- Capture inbound or outbound traffic, or both.
- Limit the traffic to be captured by using filters.
- Automatically start and stop packet capture with triggers.

Note: The Contivity gateway does not provide tools for opening and viewing captured data. You must off load the PCAP files to view them.

Security features

Packet capture on the Contivity gateway provides the following features to enhance security:

- 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.
- When you save a capture buffer to a file on disk, the file is encrypted. You must enter the capture password to decrypt PCAP files.
- To open a capture file, you can use a tool called **`openpcap`** that is shipped with Contivity software. The tool is built for both 128-bit and 56-bit versions and 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.

Packets are 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 or sent on the wire

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 (all types)
  - 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 Network General 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 when you save tunnel captures to the disk. When you convert these files to file formats that do not support raw IP encapsulation (including Sniffer), L2 encapsulation is required.

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 another tunnel session that matches the capture criteria begins. Tunnel capture criteria include the following:

- Tunnel type: user tunnel, branch office, ABOT initiator, or ABOT responder
- Tunnel protocol: IPsec, L2TP, PPTP, or L2F
- IP address of the remote 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. 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 a different tunnel.

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 96).

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 or as a start or stop trigger. You configure capture filters, start triggers, and stop triggers independently.

Capture filters

To troubleshoot a specific type of problem and to limit the amount of data stored in the capture buffer, you can configure a predefined interface filter.

Non-IP frames will not match any filter. 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.

To apply a filter to a capture object, you must first stop the capture object if it is running.

Triggers

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

- 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. The packet capture object, however, is not fully stopped. Start trigger can still restart the capture.

A trigger works only for the direction that the capture is configured for. For example, if you enable packet 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.

You can use triggers with filters. Like filters, triggers never match non-IP frames. The packets that triggered the capture object to start or stop are also captured if they match capture filters.

You can use a start trigger with a stop trigger to capture specific transaction-oriented traffic. If you set both a start and a stop trigger, the start trigger can reenable saving traffic to a capture buffer. A start trigger and a stop trigger can both be activated on the same packet. In this case, only one packet is captured.

Saving captured data

By default, packet capture stops copying data to the capture buffer when the buffer becomes full. You can configure a capture object to overwrite the data in the buffer with new data by executing the **wrapping** command.

The command **capture save** is used to save captured network traffic from the capture buffer in memory to a file on the gateway disk. Packet capture must be stopped before you can save the buffer to a file. (See "Starting, stopping, and saving capture objects" on page 106.)

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, the gateway will not allow you to allocate more memory for a new capture buffer 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

Running packet capture can affect Contivity gateway performance. For this reason, packets are saved in the capture buffer and only written to disk when you stop the capture object and save the packets to a file.

Only one capture object can be running at one time for a specific source (interface or tunnel). Multiple capture objects can exist for the same source, but only one object is allowed to start. Capture objects for 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 the least amount of data needed for troubleshooting: for example, only inbound or outbound traffic, only the first *n* bytes of the packet.
- Configure a capture object for promiscuous mode only when necessary. (Promiscuous mode will affect gateway performance.)
- Configure filters and triggers to capture only relevant traffic, in particular if you need to run the global IP object (see "Filters and triggers" on page 96).
- When you no longer need a capture object or capture files, delete them to free up memory or disk space.
- Do not run capture objects for physical interfaces or tunnels at the same time that you run the global IP capture object (some packets will be captured more than once).

Enabling packet capture on a Contivity gateway

A serial connection is required to enable packet capture; you cannot enable packet capture via a Telnet session.

To prepare to run packet capture on the gateway:

1. If necessary, boot the gateway with a software version that has the PCAP feature.
2. 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
3. Connect the serial cable (supplied with the gateway) from the gateway's serial port to the terminal or to the communications port on the PC.
4. 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) 1999-2004 Nortel Networks, Inc.

Version:               V04_90.185
Creation date:      May 27, 2004, 20:51:06
Date:               05/27/2004
Unit Serial Number: 317563

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

5. 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
```

6 Access the command line interface by typing the letter "L" (uppercase or lowercase) at the prompt.

The User EXEC prompt appears:

```
CES>
```

7 Enter Privileged EXEC mode.

```
CES>enable
Password:*****
```

8 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: ********
```

9 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#
```

After you enable packet capture, it remains enabled until you explicitly disable it with the **`no capture enable`** command or until you reboot the gateway. You can now configure and start packet capture objects.

Configuring and running packet capture objects

This section provides instructions for creating, configuring, starting, and stopping capture objects, as well as instructions for saving captured traffic to a file on disk. For the complete syntax of the packet capture commands shown in this section, see the *Reference for the Contivity Secure IP Services Gateway Command Line Interface*.

Creating a capture object

To create a capture object, you use the **`capture add`** command. (For information about the types of object that you can create, see "Capture types" on page 94.)

1 To view the types of capture object that you can configure, enter this command at the Privileged EXEC prompt.

```
CES# capture add <object_name> ?
```

For example, enter the following command:

```
CES# capture add test1 ?
 bri              Bri interface capture
 dial             Dial interface capture
 FastEthernet     Fast Ethernet interface capture
 GigabitEthernet  Gigabit Ethernet interface capture
 global           Global RAW IP capture
 serial           Serial interface capture
 tunnel           Tunnel capture
```

2 Create a capture object by specifying an object name and type.

In the following example, you create a capture object called test_ethernet1 that captures traffic on Ethernet interface 1/2.

```
CES# capture add test_ethernet1 FastEthernet 1/2
CES#
```

In the following example, you create a capture object called test_tunnel that captures tunnel traffic.

```
CES# capture add test_tunnel tunnel
CES#
```

Configuring a capture object

After you create a capture object, you can configure it to capture a subset of the traffic that travels over the physical interface, tunnel, or the Contivity gateway as a whole. For example, you can configure a capture object as follows:

- Capture inbound or outbound traffic or both.
- Capture a non-default number of octets from each packet.
- Apply an interface filter to the object.
- Configure start and stop triggers for the object.
- Specify whether the capture stops when the buffer is full or whether new data should overwrite the existing data.

To configure a capture object:

1 Navigate to Capture Configuration mode by entering the **`capture`** command with the object name.

```
CES#capture ether0
CES(capture-ethernet)#
```

The resulting prompt shows the type of capture object (physical interface, tunnel, or global IP).

2 Display all parameters that you can configure for that type of capture object.

```
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-ethernet)#
```

3 Edit one or more parameters as required.

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

For the syntax of any command, see the *Reference for the Contivity Secure IP Services Gateway Command Line Interface*.

Tunnel capture parameters

Capture objects for tunnels have several unique parameters. The following example creates a tunnel object called "bot1," navigates to Capture Configuration mode, and displays the commands for tunnel objects. The commands in **bold** are the commands that are available only for tunnel objects.

Note: For more information about tunnel capture objects, see "Tunnel captures" on page 95.

```
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 address
  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)#
```

For the syntax of any command, see the *Reference for the Contivity Secure IP Services Gateway Command Line Interface*.

Global IP parameters

The parameters that you can configure for the global IP capture object are the same as the parameters available for physical interface objects. The following example creates a global capture object called “rawip,” navigates to Capture Configuration mode, and displays the commands for the global capture object.

Note: For more information about global IP capture objects, see “Global IP captures” on page 96.

```
CES#capture add rawip global
CES#capture rawip
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-global)#
```

Starting, stopping, and saving capture objects

The following example shows how to start a capture object called “test_ether1,” stop it, save the buffer to a file (called “test_ether1.cap”), and finally, clear the capture buffer. All the commands must be executed at Privileged EXEC mode.

```
CES#capture test_ether1 start
CES#capture test_ether1 stop
CES#capture test_ether1 save test_ether1.cap
Saving capture test_ether1 to file /ide0/test_ether1.cap please
wait . . .
220 frames written successfully
CES#clear capture test_ether1
CES#
```

Using the show capture command to display capture status

Use the **show capture** command to display a list of capture objects and to display the configuration and status of a specific capture object.

In the following example, the **show capture** command is executed with no object name 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
CES#
```

The following 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:                              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#
```

Sample packet capture configurations

This section provides sample configurations with the commands that you would use to create them.

Interface capture object using a filter and direction

In the following example, you configure a capture object called “test-filter-in” on Fast Ethernet interface 0/1. This object captures inbound FTP traffic only.

Note: The filter used in this example is a predefined Contivity filter. If you need a filter that is not provided with Contivity software, you must create the filter before you configure the capture object.

To create and use this capture object, you execute commands like the ones illustrated in this example. These commands do the following:

1. Create a capture object called “test-filter-in” on Fast Ethernet interface 0/1.
2. Enter Capture Configuration mode for the object.
3. Set the direction for the capture to inbound.
4. Set the filter to capture FTP traffic only.
5. Exit Capture Configuration mode.
6. Start the capture.

```
CES#capture add test-filter-in FastEthernet 0/1
CES#capture test-filter-in
CES(capture-ethernet)##direction inbound
CES(capture-ethernet)#filter "permit FTP"
CES(capture-ethernet)#exit
CES#capture test-filter-in start
CES#
```

To view the status of the running capture object, as well as its configuration, use the **show capture** command. (In this example, 20 frames have been captured in the buffer.)

```
CES#show capture test-filter-in
Capture state:                          RUNNING
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:                        20
Capture buffer utilization:             0%
Capturing direction:                    INBOUND
Capture buffer wrapping:                DISABLED
Capture buffer wrapped:                 FALSE
Capture filter applied:                 permit FTP
Capturing non-ip frames:                DISABLED
Capture filter discards:                329
CES#
```

To stop the capture and save the buffer contents to a file called “test3.cap,” enter the following commands:

```
CES#capture test-filter-in stop
CES#capture test-filter-in save test3.cap
Saving capture test-filter-in to file /ide0/test3.cap please wait .
. .
20 frames written successfully
CES#
```

Interface capture object using triggers

In the following example, you configure a capture object called “test-trigger” on Fast Ethernet interface 0/1. This object uses FTP traffic as the start trigger and Telnet traffic as the stop trigger.

Note: The filters used in this example are predefined Contivity filters. If you need a filter that is not provided with Contivity software, you must create the filter before you configure the capture object.

To create and use this capture object, you execute commands like the ones illustrated in this example. These commands do the following:

1. Create a capture object called “test-trigger” on Fast Ethernet interface 0/1.
2. Enter Capture Configuration mode for the object.
3. Set the start trigger to “permit FTP.”
4. Set the stop trigger to “permit Telnet.”
5. Exit Capture Configuration mode.
6. Start the capture.

```
CES#capture add test-trigger fastethernet 0/1
CES#capture test-trigger
CES(capture-ethernet)#trigger start "permit FTP"
CES(capture-ethernet)#trigger stop "permit Telnet"
CES(capture-ethernet)#exit
CES#capture test-trigger start
CES#
```

To view the status of the running capture object, as well as its configuration, use the **`show capture`** command. In this example, you can see that:

- The “captured frames” field indicates that the capture has been triggered by the receipt of FTP traffic.
- The “start trigger discards” field shows the number of packets that were discarded before the start trigger was activated by the receipt of FTP traffic.

```
CES#show capture test-trigger
Capture state:                          RUNNING
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:                        107
Capture buffer utilization:             0%
Capturing direction:                    BIDIRECTIONAL
Capture buffer wrapping:                DISABLED
Capture buffer wrapped:                 FALSE
Start trigger applied:                  permit FTP
Start trigger discards:                 362
Stop trigger applied:                   permit Telnet
CES#
```

After Telnet traffic has activated the stop trigger, the **show capture** command would resemble the following example. The "Capture state" field now shows that the capture has been stopped by the stop trigger.

```
CES#show capture test-trigger
Capture state:                              STOPPED by stop
trigger
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:                            188
Capture buffer utilization:                 1%
Capturing direction:                        BIDIRECTIONAL
Capture buffer wrapping:                    DISABLED
Capture buffer wrapped:                     FALSE
Start trigger applied:                      permit FTP
Start trigger discards:                     362
Stop trigger applied:                       permit Telnet
CES#
```

To stop the capture object and save the buffer contents to a file called "test4.cap," enter the following commands:

```
CES#capture test-trigger stop
CES#capture test-trigger save test4.cap
Saving capture test-trigger to file /ide0/test4.cap please wait . .
.
220 frames written successfully
CES#
```

Tunnel capture object using a remote IP address

In the following example, you configure a capture object called "test-remote-IP" that captures traffic arriving over a tunnel with the specified remote IP address.

To create and use this capture object, you execute commands like the ones illustrated in this example. These commands do the following:

1. Create a capture object called "test-remote-ip."
2. Enter Capture Configuration mode for the capture object.
3. Set the remote IP address to 192.168.100.1.

4 Exit Capture Configuration mode.

5 Start the capture.

```
CES#capture add test-remote-ip tunnel
CES#capture test-remote-ip
CES(capture-tunnel)#remoteip 192.168.100.1
CES(capture-tunnel)#exit
CES#capture test-remote-ip start
CES#
```

To stop the capture and save the buffer contents to a file called “test6.cap,” enter the following commands:

```
CES#capture test-remote-ip stop
CES#capture test-remote-ip save test6.cap
Saving capture test-trigger to file /ide0/test6.cap please wait . .
.
10 frames written successfully
CES#
```

Viewing a packet capture output file on a PC

After you save a capture buffer to a file on the gateway disk, download the file to a workstation and analyze the contents offline using one of many available tools. The Contivity gateway does not provide utilities to view and analyze packet capture data; however, the Contivity software CD provides a utility called **openpcap** that you use to open and decrypt PCAP files on a PC or workstation.

- 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 **editcap** 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 the Ethereal window.

Saving, downloading, and viewing PCAP files

To save and download a PCAP file and view it using the Contivity **openpcap** 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 you entered when you enabled packet capture (see "Enabling packet capture on a Contivity gateway" on page 100).

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 115.

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

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. To view a Contivity PCAP file with Sniffer Pro:

1. Install Ethereal software (see "Installing Ethereal software" on page 112).
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 113.
3. Open a new DOS window and change directory to the c:\Program Files\Ethereal directory to access the **editcap** command.
4. Execute the **editcap** command so that Sniffer Pro can view the capture. If the capture was done on an Ethernet interface or on a tunnel, type the extension **.enc**; if the capture was on done on WAN interface, type the extension **.syc**. Following are sample commands.

   Ethernet interface capture:

   ```
   editcap -F ngsniffer d:\pcap\ether.cap ether1.enc
   ```

   IPsec tunnel capture:

   ```
   editcap -T ether -F ngsniffer d:\pcap\ipsec.cap ipsec.enc
   ```

   Global IP capture:

   ```
   editcap -T ether -F ngsniffer d:\pcap\rawip.cap rawip.enc
   ```

   T1 frame relay capture:

   ```
   editcap -F ngsniffer d:\pcap\fr.cap frelay.syc
   ```

5. From Sniffer Pro, open the **.enc** file or the **.syc** file to view the 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, set the Protocol Forcing option in Sniffer Pro to view the correct Layer 3 information.

   a. Click on Tools > Options > Protocol Forcing.

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

   c. Click on OK and then open the file.

Deleting capture objects and disabling packet capture

When you no longer need a capture object, delete it to free up memory. You can also disable packet capture globally to remove all configured capture objects and free the memory used to store them.

Note: If you disable packet capture globally, you will need to use the serial port to reenable it again (see "Enabling packet capture on a Contivity gateway" on page 100).

Any capture data that you saved in a file using the **capture save** command remains stored on the disk until you explicitly delete the file.

To delete a packet capture object:

1 Display all configured capture objects on the gateway to locate the object or objects that you want to delete.

```
CES#show capture
Name           Type      Size    Buffer use Count State
test-fast      ETHERNET  1048576     0%     10    STOPPED
test-filter-in ETHERNET  1048576     0%     20    STOPPED
test-raw-ip    GLOBAL    1048576     0%     33    STOPPED
test-remote-ip TUNNEL    1048576     0%     9     STOPPED
test-trigger   ETHERNET  1048576     1%     188   STOPPED by stop
trigger
test-user      TUNNEL     1048576    0%     56    STOPPED
CES#
```

2 Execute the **no capture** command for the specific object.

For example, the following command deletes the capture object "test-trigger."

```
CES# no capture test-trigger
CES#
```

To disable packet capture globally and delete all configured capture objects, execute the **no capture enable** command:

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

Appendix A
MIB support

The Contivity Secure IP Services Gateway supports the management information base (MIB) for use with network management protocols in TCP/IP-based Internets and TCP/IPX-based networks. The gateway supports SNMP Gets only. It does not support SNMP Sets.

Nortel Networks also provides proprietary MIBs for the gateway's SNMP trap support. The MIBs, cestraps.mib and newoak.mib, are available on the Contivity Secure IP Services Gateway distribution CD in the Doc directory.

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

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

SNMP RFC support

This section discusses the SNMP-related RFCs that the Contivity Secure IP Services Gateway supports.

Novell IPX MIB

The gateway supports the IPX MIB that is distributed by Novell, Inc.

Novell RIP-SAP MIB

The gateway supports the IPX RIP-SAP MIB that is distributed by Novell, Inc.

RFC 1850 -- OSPF Version 2 Management Information Base

The gateway supports RFC 1850, *OSPF Version 2 Management Information Base*. As stated in the introduction to the RFC, the RFC "defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing the Open Shortest Path First Routing Protocol."

RFC 1724 -- RIP Version 2 MIB Extension

The gateway supports RFC 1724, *RIP Version 2 MIB Extension*. As stated in the introduction to the RFC, the RFC "defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines the objects for managing RIP Version 2."

RFC 1213 -- Network Management of TCP/IP-Based Internets MIB

The gateway supports RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB II*. This RFC provides the architecture and system for managing TCP/IP-based internets. With the exception of the EGP Group (Section 6.10) and the Transmission Group (Section 6.11), the gateway provides full support for the RFC.

RFC 2667 -- IP Tunnel MIB

The gateway supports RFC 2667, *IP Tunnel MIB*. As stated in the introduction to the RFC, it "describes a Management Information Base (MIB) used for managing tunnels of any type over IPv4 networks, including GRE [16,17], IP-in-IP [18], Minimal Encapsulation [19], L2TP [20], PPTP [21], L2F [25], UDP (e.g., [26]), ATMP [22], and IPv6-in-IPv4 [27] tunnels."

RFC 2787 -- VRRP MIB

The gateway supports RFC 2787, “Definitions of Managed Objects for the Virtual Router Redundancy Protocol.” As stated in the introduction, RFC 2787 “defines an extension to the Management Information Base (MIB) for use with SNMP-based network management. In particular, it defines objects for configuring, monitoring, and controlling routers that employ the Virtual Router Redundancy Protocol (VRRP).”

RFC 2737 -- Entity MIB

This MIB contains five tables, we have partially implemented two of these tables.

```
*entPhysicalTable
entLogicalTable
entLPMappingTable
*entAliasMappingTable
entPhysicalContainsTable
```

The entPhysicalTable provides a listing of the hardware elements that are present in the system. For example each slot is listed, and if there is a card in the slot, then the card and any ports on the card. The exception to this is the hardware accelerator which does not appear in the table). The listing shows element relationships via the columns entPhysicalContainedIn and entPhysicalParentRelPos. The only columns that have been implemented are:

```
entPhysicalIndex
entPhysicalDescr (although the value is not strictly what the MIB
specifies)
entPhysicalContainedIn
entPhysicalClass
entPhysicalParentRelPos
entPhysicalName
entPhysicalIsFRU
```

All other columns will return an appropriate default value for the object.

The entAliasMappingTable provides a mapping from entPhysicalIndex to ifTable.ifIndex. Hence by walking this table, a management station can deterring the ifIndex associated with a physical port.

RFC 1573 -- IanaIfType MIB

This MIB contains the enumerations for rfc2233 ifTable.ifType. These enumerations describe the various types of interfaces that ifTable can support.

RFC 2233 -- If MIB

This MIB is the latest evolution of rfc1213 Interfaces group, plus several new objects.

RFC 2571-- Snmp-Framework MIB

This MIB provides textual conventions and object definitions used in the SNMP agent architecture.

RFC2790 -- Host Resources MIB

The Host Resources MIB defines a uniform set of objects for the managing host computers. Host computers are independent of the operating system, network services, or any software application.The Host Resources MIB defines objects that are common across many computer system architectures.

The Contivity Secure IP Services Gateway does not support the following groups/ objects:

- hrSystem Group
  - hrSystemInitialLoadDevice
  - hrSystemInitialLoadParameters
  - hrSystemNumUsers
  - hrSystemProcesses
  - hrSystemMaxProcesses
- hrStorage Group

  hrStorageAllocationFailures
- hrDevice Group
  - hrDevice Table

hrDeviceErrors

— hrNetworkTable
— hrPrinterTable
— hrDiskStorageTable

hrDiskStorageCapacity

— hrPartitionTable

hrPartitionSize

— hrFSTable

hrFSLastFullBackupDate

hrFSLastPartialBackupDate

- hrSWRun Group

  hrSWRun

- hrSWRunPerf Group

  hrSWRunPerf

- hrSWRunTable
  — hrSWRunIndex
  — hrSWRunName
  — hrSWRunType
  — hrSWRunStatus
  — hrSWRunPriority
- hrSWRunPerfTable
  — hrSWRunPerfCPU

RFC2495 -- DS1 MIB

These objects are used when you use a DS1/E1/DS2/E2 interface. At present, this applies to the ifType variable in the Internet-standard MIB ds1 (18).

This MIB provides an alternative reporting method for monitoring line status on a T1 line. ANSI reporting is still supported, but the reporting method is either ANSI or DS1 MIB.

RFC2863 Interface MIB (64 bit counters support)

The support for the following entries has been added in the interface table: ifHCInOctets, ifHCInUcastPkts, ifHCOutOctets and ifHCOutUcastPkts. These counters already existed and were extended from Counter32 to Counter64.

CES MIB

This MIB contains CES proprietary MIB data. For instance the “ping MIB” is contained in this file. The ping MIB, via an SNMP GET REQUEST, causes the CES to ping another device and get statistics based on the results of the ping. For instance sending a PDU specifying pingAverageTime.192.32.250.248.4.4076, sends four pings, of 4076 bytes, to address 192.32.250.248. (It actually sends five because one ping is sent by itself so that if the device being pinged is the other end of a Branch Office tunnel, it ensures that the tunnel is brought up before trying to send pings through the tunnel. This ping is not counted in the statistics.) The object returns the values of:

```
-2 Invalid parameter(indices).
-1 No reply.
0 Less than 16ms average time.
>0 The average time.
```

The objects and their parameters(indices) are:

```
pingAverageTime - returns the average ping time for the set of
specified pings.
pingPercentLoss - returns the percentage of loss.
```

The first index is the IP address to ping. The second index is the number of pings, if this is not specified or is an invalid value it defaults to 3. The third index is the size of the ping request. If it is not specified or is an invalid value then it defaults to 1024.

CES MIB has been expanded to provide trap acknowledgement.

cestraps.mib -- Nortel Networks proprietary MIB

This section lists the contents of the cestraps.mib, the Nortel Networks MIB for the Contivity Secure IP Services Gateway.

```
-- Trap #5005 ---------------------------------
-- Each Trap contains the Trap OID as well as the following OIDs:
--     SeverityLevel
--     System Name
--     System Date
--     System Time
--     System Uptime
--
       NEWOAKTRAP DEFINITIONS ::= BEGIN

       IMPORTS
           enterprises                FROM RFC1155-SMI
           DisplayString              FROM RFC1213-MIB
           OBJECT-TYPE                FROM RFC-1212
           TRAP-TYPE                  FROM RFC-1215;

    -- This MIB module uses the extended OBJECT-TYPE macro as
    -- defined in [9], and the TRAP-TYPE macro as defined in [10].

    contivity         OBJECT IDENTIFIER ::= { enterprises 2505 }


    ContivitySnmpTraps OBJECT-TYPE
        SYNTAX  DisplayString
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
        "Nortel Networks Inc's Enterprise trap."
    ::= {contivity 1}

-- Trap #5006 ---------------------------------
antiSpoofingStatus OBJECT-TYPE
SYNTAX DisplayString
ACCESS read-only
STATUS mandatory
DESCRIPTION "Status of Anti Spoofing Feature.
Possible Values:
Disabled: Anti-Spoofing is Disabled;
Warning: Anti-Spoofing : Packets Dropped;
Alert: Anti-Spoofing state not known!;
The values have the following meaning:
-- The first means the feature is disabled
```

```
-- The second means packets were dropped due to a detected spoofed
address
-- The third should never happen, but means the status has been set
to a bogus value.
"
::= {serviceCESTrapInfo 6}
antiSpoofingStatusTrap TRAP-TYPE
ENTERPRISE serviceCESTrapInfo
VARIABLES {
severityLevel, antiSpoofingStatus, systemName,systemDate,
systemTime, systemUpTime
}
DESCRIPTION "Status of Anti Spoofing Feature"
::= 5006
```

newoak.mib

This section provides the contents of the newoak.mib, which defines the “newoak” enterprise ID, the “contivity” object identifier, and the sysObjectIDs for each Contivity model.

```
--  This MIB module uses the extended OBJECT-TYPE macro as
        --  defined in [9], and the TRAP-TYPE macro as defined in
[10].

        newoak    OBJECT IDENTIFIER ::= { enterprises 2505 }

-- The following MODULE-IDENTITY definition can be commented out if
the MIB parser
-- you are using has trouble parsing it. If you do comment it out,
then uncomment
-- the following object identifier definition.
--    contivity OBJECT IDENTIFIER ::= {newoak 1}
--
     contivity  MODULE-IDENTITY
          LAST-UPDATED "0004252130Z"  -- April 25, 2000 7:30pm EST
          ORGANIZATION "Nortel Networks,Inc."
          CONTACT-INFO
            "support@nortelnetworks.com
            Postal: Nortel Networks,Inc.
                    80 Central St.
                    Boxboro, MA 01719
            Tel:    +1 978 264 7100
            E-Mail: support@nortelnetworks.com"

          DESCRIPTION
              "This MIB defines the sysObjectIDs for different
               variations ofthe Convitiy Extranet Switch."
          ::= { newoak 1 }
-- IDENTIFIER ::= {newoak 1}
     contivityExtranetSwitch2000 OBJECT IDENTIFIER ::= {newoak 2}
     contivityExtranetSwitch1000 OBJECT IDENTIFIER ::= {newoak 3}
     contivityExtranetSwitch4500 OBJECT IDENTIFIER ::= {newoak 4}
     contivityExtranetSwitch15XX OBJECT IDENTIFIER ::= {newoak 5}
     contivityExtranetSwitch2500 OBJECT IDENTIFIER ::= {newoak 6}
     contivityExtranetSwitch2600 OBJECT IDENTIFIER ::= {newoak 7}
     contivityExtranetSwitch1600 OBJECT IDENTIFIER ::= {newoak 8}
     contivityExtranetSwitch4600 OBJECT IDENTIFIER ::= {newoak 9}

      END
```

Hardware-related traps

```
hardwareTrapInfo OBJECT IDENTIFIER
    ::= {ContivitySnmpTraps 1}

-- Trap #1001
hardDisk1Status OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS mandatory
    DESCRIPTION "Hard Disk Number 1 Status."
    ::= {hardwareTrapInfo 1}

-- Trap #1002
hardDisk0Status OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Hard Disk Number 0 Status."
    ::= {hardwareTrapInfo 2}

-- Trap #1003
memoryUsage OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Memory Usage Status."
    ::= {hardwareTrapInfo 3}

-- Trap #1004
LANcardStatus OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of any LAN cards on the system."
    ::= {hardwareTrapInfo 4}

-- Trap #1005
CPUtwoStatus OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of second CPU."
    ::= {hardwareTrapInfo 5}

-- Trap #1006
fanOneStatus OBJECT-TYPE
    SYNTAX  DisplayString
```

```
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of the first CPU fan."
    ::= {hardwareTrapInfo 6}

-- Trap #1007
fanTwoStatus OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of the second CPU fan."
    ::= {hardwareTrapInfo 7}

-- Trap #1008
chassisFanStatus OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of the Chassis fan."
    ::= {hardwareTrapInfo 8}

-- Trap #1009
fiveVoltsPositive OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of +5 Volt power."
    ::= {hardwareTrapInfo 9}

-- Trap #10010
fiveVoltsMinus OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of -5 Volt power."
    ::= {hardwareTrapInfo 10}

-- Trap #10011
threeVoltsPositive OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of +3 Volt power."
    ::= {hardwareTrapInfo 11}

-- Trap #10012
twoDotFiveVA OBJECT-TYPE
    SYNTAX  DisplayString
```

```
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of 2.5VA power."
    ::= {hardwareTrapInfo 12}

-- Trap #10013
twoDotFiveVB OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of 2.5VB power."
    ::= {hardwareTrapInfo 13}

-- Trap #10014
twelveVoltsPositive OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of +12 Volt power."
    ::= {hardwareTrapInfo 14}

-- Trap #10015
twelveVoltsMinus OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of -12 Volt power."
    ::= {hardwareTrapInfo 15}

-- Trap #10016
normalTemperature OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of normal temperature reading."
    ::= {hardwareTrapInfo 16}

-- Trap #10017
criticalTemperature OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of critical temperature reading."
    ::= {hardwareTrapInfo 17}

-- Trap #10018
chassisIntrusion OBJECT-TYPE
    SYNTAX  DisplayString
```

```
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "The chassis intrusion sensor indicates that
                 the unit has been opened."
    ::= {hardwareTrapInfo 18}

-- Trap #10019
dualPowerSupply OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of the redundant power supplies."
    ::= {hardwareTrapInfo 19}

-- Trap #10020
t1WANStatus OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of T1 WAN card(s)."
    ::= {hardwareTrapInfo 20}

-- Trap #10021
t3WANStatus OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of T3 WAN card(s)."
    ::= {hardwareTrapInfo 21}
```

Server-related traps

```
serverTrapInfo OBJECT IDENTIFIER
    ::= {ContivitySnmpTraps 2}

-- Trap #3001
radiusAcctServer OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of External Radius Accounting Server."
    ::= {serverTrapInfo 1}

-- Trap #3002
backupServer OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of External Disk Backup Server."
    ::= {serverTrapInfo 2}

-- Trap #3003
diskRedundency OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of Local Disk Redundancy."
    ::= {serverTrapInfo 3}

-- Trap #3004
IntLDAPServer OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of Internal LDAP Server."
    ::= {serverTrapInfo 4}

-- Trap #3005
LoadBalancingServer OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of Load Balancing Server."
    ::= {serverTrapInfo 5}

-- Trap #3006
DNSServer OBJECT-TYPE
    SYNTAX  DisplayString
```

```
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION "Status of DNS Server."
        ::= {serverTrapInfo 6}

    -- Trap #3007
    SNMPServer OBJECT-TYPE
        SYNTAX  DisplayString
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION "Status of SNMP Server."
        ::= {serverTrapInfo 7}

    -- Trap #3008
    IPAddressPool OBJECT-TYPE
        SYNTAX  DisplayString
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION "Status of the IP address pool."
        ::= {serverTrapInfo 8}

    -- Trap #3009
    ExtLDAPServer OBJECT-TYPE
        SYNTAX  DisplayString
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION "Status of External LDAP Server."
        ::= {serverTrapInfo 9}

    -- Trap #30010
    radiusAuthServer OBJECT-TYPE
        SYNTAX  DisplayString
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION "Status of Radius Authentication Server."
        ::= {serverTrapInfo 10}

-- Trap #30011
      certificateServer OBJECT-TYPE
          SYNTAX  DisplayString
          ACCESS  read-only
          STATUS  mandatory
          DESCRIPTION "Status of Certificates Validity."
          ::= {serverCESTrapInfo 11}
```

Software-related traps

```
softwareTrapInfo OBJECT IDENTIFIER
    ::= {ContivitySnmpTraps 3}

-- Trap #5001
NetBuffers OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Network buffer usage."
    ::= {softwareTrapInfo 1}

-- Trap #5002
fireWall OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Status of internal firewall."
    ::= {softwareTrapInfo 2}
```

Login-related traps

```
loginTrapInfo OBJECT IDENTIFIER
    ::= {ContivitySnmpTraps 4}

    -- Trap #101
    failedLogin OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Failed Login Attempt."
    ::= {loginTrapInfo 1}
```

Intrusion-related traps

```
intrusionTrapInfo OBJECT IDENTIFIER
  ::= {ContivitySnmpTraps 5}

-- Trap #201
securityIntrusion OBJECT-TYPE
  SYNTAX  DisplayString
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "Login Security Intrusion."
  ::= {intrusionTrapInfo 1}
```

System-related traps

```
-- Trap #401
powerUpTrap OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Power Up."
    ::= {ContivitySnmpTraps 6}

-- Trap #601
periodicHeartbeat OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "Periodic Heartbeat."
    ::= {ContivitySnmpTraps 12}
```

Information passed with every trap

```
SeverityLevel OBJECT-TYPE
    SYNTAX INTEGER
    {
    fatal(1),
    major(2),
    minor(3),
    informational(4),
    insignificant(5),
    reversal(6)
    }
        ACCESS read-only
        STATUS mandatory
        DESCRIPTION "Severity of specific trap."
        ::= {ContivitySnmpTraps 7}
systemName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "System Name."
    ::= {ContivitySnmpTraps 8}

systemDate OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "System Date."
    ::= {ContivitySnmpTraps 9}

systemTime OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "System Time."
    ::= {ContivitySnmpTraps 10}

systemUpTime OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "System Up Time."
    ::= {ContivitySnmpTraps 11}
```

Table 3 provides trap categories and explanations.

Table 3 Trap categories

Hardware	
1.3.6.1.4.1.2505.1.1.0.1001	hardDisk1StatusTrap
1.3.6.1.4.1.2505.1.1.0.1002	hardDisk0StatusTrap
1.3.6.1.4.1.2505.1.1.0.1003	memoryUsageTrap
1.3.6.1.4.1.2505.1.1.0.1004	lanCardStatusTrap
1.3.6.1.4.1.2505.1.1.0.1005	cpuTwoStatusTrap
1.3.6.1.4.1.2505.1.1.0.1006	fanOneStatusTrap
1.3.6.1.4.1.2505.1.1.0.1007	fanTwoStatusTrap
1.3.6.1.4.1.2505.1.1.0.1008	chassisFanStatusTrap
1.3.6.1.4.1.2505.1.1.0.1009	fiveVoltsPosStatusTrap
1.3.6.1.4.1.2505.1.1.0.10010	fiveVoltsMinusTrap
1.3.6.1.4.1.2505.1.1.0.10011	threeVoltsPositiveTrap
1.3.6.1.4.1.2505.1.1.0.10012	twoDotFiveVATrap
1.3.6.1.4.1.2505.1.1.0.10013	twoDotFiveVBTrap
1.3.6.1.4.1.2505.1.1.0.10014	twelveVoltsPositveTrap
1.3.6.1.4.1.2505.1.1.0.10015	twelveVoltsMinsTrap
1.3.6.1.4.1.2505.1.1.0.10016	normalTemperatureTrap
1.3.6.1.4.1.2505.1.1.0.10017	criticalTemperatureTrap
1.3.6.1.4.1.2505.1.1.0.10018	chassisIntrusionTrap
1.3.6.1.4.1.2505.1.1.0.10019	dualPowerSupplyTrap
1.3.6.1.4.1.2505.1.1.0.10020	t1WANStatusTrap
1.3.6.1.4.1.2505.1.1.0.10021	t3WANStatusTrap
1.3.6.1.4.1.2505.1.1.0.10022	hwAccelTrap
Server	
1.3.6.1.4.1.2505.1.2.0.3001	radiusAcctServerTrap
1.3.6.1.4.1.2505.1.2.0.3002	backupServerTrap
1.3.6.1.4.1.2505.1.2.0.3003	diskRedundencyTrap
1.3.6.1.4.1.2505.1.2.0.3004	intLDAPServerTrap
1.3.6.1.4.1.2505.1.2.0.3005	loadBalancingServerTrap
1.3.6.1.4.1.2505.1.2.0.3006	dnsServerTrap

Table 3 Trap categories (continued)

Server	
1.3.6.1.4.1.2505.1.2.0.3007	snmpServerTrap
1.3.6.1.4.1.2505.1.2.0.3008	ipAddressPoolTrap
1.3.6.1.4.1.2505.1.2.0.3009	extLDAPServerTrap
1.3.6.1.4.1.2505.1.2.0.30010	radiusAuthServerTrap
1.3.6.1.4.1.2505.1.2.0.30011	certificateServerTrap
Software	
1.3.6.1.4.1.2505.1.3.0.5001	netBuffersTrap
1.3.6.1.4.1.2505.1.3.0.5002	FireWallTrap
1.3.6.1.4.1.2505.1.3.0.5003	FipsStatusTrap
Failed Login	
1.3.6.1.4.1.2505.1.4.0.101	FailedLoginTrap
Intrusion	
1.3.6.1.4.1.2505.1.5.0.201	SecurityIntrusionTrap
Presence	
1.3.6.1.4.1.2505.1.0.401	PowerUpTrapEntry
1.3.6.1.4.1.2505.1.0.601	PeriodicHeartbeatTrap

Table 4 provides descriptions for the Contivity gateway traps.

Table 4 Contivity traps MIB descriptions

Standard / Proprietary OID	OID	Name	Description
Proprietary	1.3.6.1.4.1.2505.1.1.0.1001	hardDisk1StatusTrap	Hard Disk Number 1 Status.
Proprietary	1.3.6.1.4.1.2505.1.1.0.1002	hardDisk0StatusTrap	Hard Disk Number 0 Status.
Proprietary	1.3.6.1.4.1.2505.1.1.0.1003	memoryUsageTrap	Memory Usage Status.
Proprietary	1.3.6.1.4.1.2505.1.1.0.1004	fanCardStatusTrap	Status of any LAN cards on the system.
Proprietary	1.3.6.1.4.1.2505.1.1.0.1005	cpuTwoStatusTrap	Status of second CPU.
Proprietary	1.3.6.1.4.1.2505.1.1.0.1006	fanOneStatusTrap	Status of the first CPU fan.
Proprietary	1.3.6.1.4.1.2505.1.1.0.1007	fanTwoStatusTrap	Status of the second CPU fan.
Proprietary	1.3.6.1.4.1.2505.1.1.0.1008	chassisFanStatusTrap	Status of the chassis fan.

Table 4 Contivity traps MIB descriptions

Proprietary	1.3.6.1.4.1.2505.1.1.0.1009	fiveVoltsPosStatusTrap	Status of the +5 Volt power.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10010	fiveVoltsMinusTrap	Status of -5 Volt power.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10011	threeVoltsPositiveTrap	Status of +3 Volt power.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10012	twoDotFiveVATrap	Status of 2.5VA power.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10013	twoDotFiveVBTrap	Status of 2.5VB power.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10014	twelveVoltsPositveTrap	Status of +12 Volt power.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10015	twelveVoltsMinsTrap	Status of -12 Volt power.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10016	normalTemperatureTrap	Status of the normal temperature reading.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10017	criticalTemperatureTrap	Status of the critical temperature reading.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10018	chassisIntrusionTrap	The chassis intrusion sensor indicates that the unit has been physically opened.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10019	dualPowerSupplyTrap	Status of the redundant power supplies.

Table 4 Contivity traps MIB descriptions

Proprietary	1.3.6.1.4.1.2505.1.1.0.10020	t1WANStatusTrap	Status of T1 WAN card(s); Possible values for Wanic: Alert: Invalid Device X. Warning: Device WanicX disabled. Alert: Device WanicX down. Warning: Device WanicX not initialized. Warning: Device WanicX PPP negotiating. Alert: Device WanicX PPP down. Alert: Device WanicX FR no support. Alert: Device WanicX Unknown DL. Possible values for T1: Alert: Invalid Device X. Warning: Device LMCDTEX disabled. Alert: Device LMCDTEX down. Warning: Device LMCDTEX not initialized. Possible values for CSU/DSU: Alert: Invalid Device X. Warning: Device LMCCDX disabled. Alert: Device LMCCDX down. Warning: Device LMCCDX not initialized.
Proprietary	1.3.6.1.4.1.2505.1.1.0.10021	3WANStatusTrap	Status of T3 WAN card Possible Values: Alert: Invalid Index X. Warning: Device HSSIX disabled. Alert: Device HSSIX down. Warning: Device HSSIX not initialized. Alert: Device HSSIX PPP down. Warning: Device HSSIX PP initializing.

Table 4 Contivity traps MIB descriptions

Proprietary	1.3.6.1.4.1.2505.1.1.0.10022	hwAccelTrap	Status of hardware accelerator card. Possible Values: Invalid hardware accelerator unit %d. Unknown hardware accelerator unit %d. Healthy: Bulk Accelerator in slot %d: Unit %d Status 1 - ATTACHED. Warning: Bulk Accelerator in slot %d: Unit %d Status 2 - DISABLED. Healthy: Bulk Accelerator in slot %d: Unit %d Status 3 - ACTIVE. Warning: Bulk Accelerator in slot %d: Unit %d Status 4 - RECOVERING. Warning: Bulk Accelerator in slot %d: Unit %d Status 5 - SHUTDOWN. Alert: Bulk Accelerator in slot %d: Unit %d Status 6 - FAILED.
Proprietary	1.3.6.1.4.1.2505.1.2.0.3001	radiusAcctServerTrap	Status of External Radius Accounting Server.
Proprietary	1.3.6.1.4.1.2505.1.2.0.3002	backupServerTrap	Status of External Disk Backup Server.
Proprietary	1.3.6.1.4.1.2505.1.2.0.3003	diskRedundencyTrap	Status of Local Disk Redundancy.
Proprietary	1.3.6.1.4.1.2505.1.2.0.3004	intLDAPServerTrap	Status of Internal LDAP Server.
Proprietary	1.3.6.1.4.1.2505.1.2.0.3005	loadBalancingServerTrap	Status of Load Balancing Server.
Proprietary	1.3.6.1.4.1.2505.1.2.0.3006	dnsServerTrap	Status of DNS Server.
Proprietary	1.3.6.1.4.1.2505.1.2.0.3007	snmpServerTrap	Status of SNMP Server.
Proprietary	1.3.6.1.4.1.2505.1.2.0.3008	ipAddressPoolTrap	Status of the IP address pool.
Proprietary	1.3.6.1.4.1.2505.1.2.0.3009	extLDAPServerTrap	Status of External LDAP Server.
Proprietary	1.3.6.1.4.1.2505.1.2.0.30010	radiusAuthServerTrap	Status of Radius Authentication Server.

Table 4 Contivity traps MIB descriptions

Proprietary	1.3.6.1.4.1.2505.1.2.0.30011	certificateServerTrap	Status of Certificates Validity Possible Values: Healthy: Certificates Validity: Operational. Alert: Certificates Validity: All certificates are going to expire/ expired. Warning: Certificates Validity: One more certificate is invalid. Disabled: Certificates Validity: No certificate defined.
Proprietary	1.3.6.1.4.1.2505.1.2.0.30012	extLDAPAuthServerTrap	Status of External LDAP Authentication Server. Possible Values: Warning: External LDAP Authentication Server: Server is down (indicates at least one server is not reachable and at least one server is reachable). Alert: External LDAP Authentication Server: Server is down (indicates all servers are not reachable).
Proprietary	1.3.6.1.4.1.2505.1.2.0.30013	cmpServerTrap	Status of CMP Server. Possible Values: One/more Certificate Requests error: there is at least one request error. One/more Certificate Requests processing: there is at least one request in processing. No Certificate Requests submitted: there is no request sent.
Proprietary	1.3.6.1.4.1.2505.1.3.0.5001	netBuffersTrap	Network buffer usage.
Proprietary	1.3.6.1.4.1.2505.1.3.0.5002	fireWallTrap	Status of internal firewall.
Proprietary	1.3.6.1.4.1.2505.1.3.0.5003	fipsStatusTrap	Status of FIPS.
Proprietary	1.3.6.1.4.1.2505.1.4.0.101	failedLoginTrap	Failed Login Attempt.
Proprietary	1.3.6.1.4.1.2505.1.5.0.201	securityIntrusionTrap	Login Security Intrusion.
Proprietary	1.3.6.1.4.1.2505.1.0.401	powerUpTrapEntry	Power Up.
Proprietary	1.3.6.1.4.1.2505.1.0.601	periodicHeartbeatTrap	Periodic Heartbeat.

Table 4 Contivity traps MIB descriptions

Standard	1.3.6.1.2.1.11.0.0	coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is re initializing itself and that its configuration may have been altered.
Standard	1.3.6.1.2.1.11.0.2	linkDown	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration. Varbind list: ifIndex -- ifIndex of the interface. ifAdminStatus -- ifAdminStatus of the interface. ifOperStatus -- ifOperStatus of the interface. ifDescr -- ifDescr of the interface. ifType -- ifType, this provides discrimination of interfaces that are tunnels. ifReasonForStatus-ces -- reason for the change in status. ifPhysLocation-ces -- this is the slot number. ifPhysRelPos-ces -- the port number on the board defined in interfacePhysLocation. ifIpAddr-ces -- IP address assigned to the phys port or the local IP address of a tunnel. fName-ces -- Name of the tunnel or physical interface. ifTunnelRemoteIpAddr-ces -- for non-tunnel interfaces it is zero. sysObjectID -- sysObjectID of the unit. sysName -- sysName of the unit.

Table 4 Contivity traps MIB descriptions

Standard	1.3.6.1.2.1.11.0.3	linkUp	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up. Varbind list: ifIndex -- ifIndex of the interface ifAdminStatus -- ifAdminStatus of the interface. ifOperStatus -- ifOperStatus of the interface. ifDescr -- ifDescr of the interface. ifType -- ifType, this provides discrimination of interfaces that are tunnels. ifReasonForStatus-ces -- reason for the change in status. ifPhysLocation-ces -- this is the slot number. ifPhysRelPos-ces -- the port number on the board defined in interfacePhysLocation. ifIpAddr-ces -- IP address assigned to the physical port or the local IP address of a tunnel. ifName-ces -- Name of the tunnel or physical interface. ifTunnelRemoteIpAddr-ces -- for non-tunnel interfaces it is zero. sysObjectID -- sysObjectID of the unit. sysName -- sysName of the unit.

Table 4 Contivity traps MIB descriptions

Standard	1.3.6.1.2.1.11.0.5	authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. The snmpEnableAuthenTraps object indicates whether this trap will be generated. snmpAuthenOperation-ces identifies the operation (GetRequest, GetNextRequest,...) was being attempted. snmpAuthenIpAddress-ces identifies the source IP address of the operation. snmpAuthenCommString-ces identifies the community string that was used in the operation.
Proprietary	1.3.6.1.4.1.2505.1.14.3.0.1	firewallRuleTriggeredTrap	An event sent at the user's request to signal that a rule has been matched. firewallPolicyType-ces -- Policy type. firewallRuleType-ces -- Type of rule that triggered this event. firewallRuleNumber-ces -- Number of the rule that triggered this event. ifIndex -- ifIndex is the index into the ifTable for port that received the packet. ifName-ces -- The name of the interface, same as ifName. firewallSrcAddr-ces -- Source IP address of the packet. firewallSrcPort-ces -- Source port address of the packet. firewallDestAddr-ces -- Destination IP address of the packet. firewallDestPort-ces -- Destination port of the packet. firewallProtocolID-ces -- The value of the protocol field in the IP header. firewallRuleAction-ces -- Action defined for the triggered rule.

Appendix B
Using serial PPP

The Serial Point-to-Point Protocol (PPP) feature allows you to manage the gateway from a remote location using PPP and the serial interface. If the gateway were to become unreachable over the Internet, you could still dial up and manage it through the serial interface menu.

With this feature, the serial interface becomes much like a private WAN interface. You can manage through it or even tunnel through it. You can enable Serial PPP support on the gateway using the Web interface (System > Settings). When configuring Serial PPP, you can set the gateway to Auto Detect, or you can specify that either PPP or the Serial Menu are the options available through the serial port.

Serial PPP authentication is performed by the Password Authentication Protocol (PAP), which uses a standard user ID and a password that is sent in the clear. When authenticated, the serial interface acts like a private WAN interface.

Establishing a serial PPP connection

To enable Serial PPP:

1. Set up a Dial-Up Networking connection.
2. Set up the modem.
3. Set up the gateway.
4. Dial into the gateway using the Primary Administrator's user name and password.

Setting up a Dial-Up Networking connection

To establish a Serial PPP connection using a Microsoft Dial-Up Networking connection from the client system:

1. Double-click on My Computer.
2. Double-click on the Microsoft Dial-Up Networking icon.
3. Set the COM port baud rate on the client system to be compatible with the gateway's baud rate. The rates should be the same to establish a connection. Possible rates are:
   - 9600 (default)
   - 19200
   - 38400
   - 56000
4. Go to Server Types, and under Type of Dial-Up Server, select PPP: Internet, Windows NT Server, Windows 95. Make sure that none of the Advanced options are set.
5. Go to Allowed network protocols, and select TCP/IP.
6. Go to TCP/IP Settings, and specify your IP address. This is the Management IP address that the gateway uses to communicate with the client that is dialing in through the modem.
7. Click Server Assigned name server addresses.
8. Unclick IP header compression.
9. Click Use default gateway on remote network.
10. Do not configure Scripting and Multilink.
11. Click Configure the client modem, and use the following settings:
    - 8 data bits
    - 1 stop bit
    - No parity
    - Hardware flow control

    Do not choose Log On to Network if the selection appears.

Setting up the modem

The following procedure assumes you are using a 3Com/US Robotics 56K x2 modem. It describes how to set up a modem to communicate with the gateway using a dial-up networking connection. Table 5 lists the DIP switch settings.

Table 5 DIP switch configuration

Parameter	Setting
Data Terminal Ready	On
Verbal Result Codes	On
Suppress Result Codes	On
Echo Offline Commands	Off
Auto Answer (must be set)	On
Carrier Detect Normal	On
Load NVRAM Defaults	On
Dumb Mode	Off

Setting up the gateway

To set up the gateway's parameters through the Web interface (System > Settings):

1 Go to the System > System Settings screen and select one of the following modes of operation under the Serial Port option:

- Serial Menu (default)--leaves the gateway's serial interface in the traditional serial menu mode. In this mode, no serial PPP is supported. When connecting a program such as Hyper Terminal to the interface, the standard serial interface menu appears. In Auto Detect Mode, if you are using a terminal emulator, such as Hyper Terminal, you must press Enter several times to get the logon and password prompt. Also, you can ignore the modem initialization string (which might not be in use) that is displayed on the Hyper Terminal screen.
- PPP--you can set up the gateway to use the Point-to-Point Protocol (PPP) over the serial port. This feature allows you to manage the gateway from a remote location using PPP and the serial interface. If the gateway were to become unreachable over the Internet, you could still dial up and manage

it through the serial interface menu. This feature allows you to access all of the management services (HTTP, Telnet, FTP, SNMP) through the Web interface. Once a session is established through PPP, the serial interface acts as a private WAN interface with an internal IP address (0.0.1.35).

- Auto detect--automatically detects whether the connected device is using PPP or serial menu mode at startup. The gateway cannot determine the device's baud rate, nor can it determine a change from PPP to serial menu mode, except upon startup. Auto Detect checks the mode each time the gateway is restarted. When performing its Auto Detect check, the gateway sends out AT command set characters to configure a modem if one is attached.

  When the gateway is in Auto Detect mode, and if a terminal session is connected and the terminal baud rate is the same as the gateway's, the terminal displays the AT command sets on the screen. Simply press Enter several times until a serial menu session starts. You should use the Auto Detect Mode rather than PPP Mode. Using PPP mode could leave the gateway in a state such that you could never manage it from the serial interface menu directly. If this happened, you would still have to manage the gateway through a PPP application (such as Dial-Up Networking). Directly connecting a serial cable and running Hyper Terminal would not work because the interface would only recognize PPP.

2 Select one of the following Baud Rates to match the baud rate of your terminal. After you select the baud rate, you must click the Reset button to change the port to the selected baud rate. This option is necessary for PPP if a modem initialization string specifies a fixed baud rate.

- 57600
- 38400
- 19200
- 9600 (default)

3 Enter the modem initialization string. Refer to the manufacturer's documentation to learn the vendor-specific character initialization string. Preconfiguring the modem and using the gateway's default initialization string (ATZ) provides the best results.

A sample 3Com/US Robotics 56K modem initialization string that instructs the external modem to connect at 19,200 Kb/s is ATZAT&B1AT&N10.

4 Click the Reset button to reset the port to the selected baud rate and apply any other modem changes.

Dialing in to the gateway

Use the standard dial-up networking procedure to connect to the gateway. After connecting, you can then manage the gateway using either Telnet (for the command line interface) or the browser-based GUI. Use the gateway's management IP address for the Telnet session or the browser's destination URL.

Troubleshooting Serial PPP

When the serial port is set up for PPP only, you can still do in-band Web management.

Cause:

I have a modem connected, but I cannot get a PPP connection.

Actions:

- Verify that the modem supports the gateway's selected baud rate. Most connection problems occur because the modem is not operating at the same baud rate as the gateway. For example, a 3Com/US Robotics 56 Kb/s modem's default baud rate when attempting to establish a connection to the gateway is 38400, but the gateway's default baud rate is 9600.
- Verify that the gateway is set up for PPP over the serial port. You can verify this by checking the settings in the Web interface (System > Settings).
- Verify that you clicked Reset from the Web interface when making changes to the screen (System > System Settings). This guarantees the serial port resets and initializes the modem. This is especially true with a modem connected to a gateway that was restarted.
- Check the event log for failures.
- Make sure you have the correct dial-up networking settings. Refer to the section, "Setting up a Dial-Up Networking connection."
- Make sure you have the remote modem set to auto answer and that it is in smart mode so that it can respond to the AT command set.
- Verify that the auto detection did not fail, and that the gateway is in serial menu mode.

Cause:

You were dialed in and managing the gateway remotely using PPP and you changed the baud rate and applied it, but now you cannot manage the gateway.

Action:

To manage the gateway, disconnect the dial-up connection and attempt to reestablish it. This gives the modem a chance to renegotiate the baud rate with the gateway.

Cause:

You are set up to use PPP but want to use the serial port for the serial menu.

Action:

Choose the serial port mode Serial Menu. Press OK using the Web management interface (System > System Settings) and restart the gateway. A serial cable must be installed in place of the modem in order to use the Serial Menu. Remember to power off the gateway when plugging in and unplugging the serial port connection; otherwise, you might damage system components.

Cause:

You are set up to use the Serial Menu but want to use the port for PPP.

Action:

You can change the serial port settings (System > System Settings) or the Serial Menu itself. For these changes to take effect, restart the gateway. For the best results, connect the modem while the gateway is turned off.

Cause:

You are using a dial-up serial PPP connection and you encounter repeated CRC errors.

Action:

Make sure that the modem that is connected to the gateway has hardware flow control enabled.

PPP option settings

These settings describe the gateway's behavior when negotiating serial PPP.

For IP:

- IP Address negotiation is enabled.
- The gateway needs the peer's IP address to make a connection.
- The peer should not suggest an IP address for the gateway. The gateway uses its management IP address.
- The gateway rejects VJ compression.
- The gateway rejects VJ connection ID compression.

For LCP:

- The gateway does not initiate a connection.
- The gateway accepts magic number negotiation.
- The gateway rejects address control field compression.
- The gateway rejects protocol field compression.
- The gateway does not allow asynchronous character map to be negotiated.
- The gateway accepts Maximum Receive Unit (MRU) requests.

For authentication:

- The gateway does not authenticate itself to a peer with PAP upon request.
- The gateway requires that peers perform PAP authentication using the administrator's login and password.
- The gateway does not authenticate itself to a peer with the Challenge Handshake Authentication Protocol (CHAP) upon request.
- The gateway does not require that the peer authenticate itself with CHAP.

Appendix C
System messages

System forwarding (syslog) enables you to forward information from your gateway's system log to different host machines using the system logging daemon (syslogd).

This appendix provides a listing of possible syslog messages that the Contivity Secure IP Services Gateway might write to a remote system. Each message is followed by a description and the recommended corrective action, if any.

Certificate messages

Error removing CA certificate file: xxx

Description: The gateway can be manufactured with a trusted certificate authority (CA) certificate for use by SSL. The temporary manufacturing file containing the certificate is removed the first time you boot the gateway. This error message indicates that the gateway is unable to remove the temporary certificate file. The error might be caused by a general problem with the local file system.

Action: Manually delete all files in the /system/cert/ca directory.

Installed new CA certificate from file: *xxx*

Description: The gateway can be manufactured with trusted CA certificates for use by SSL. This informational message indicates a trusted SSL CA certificate was installed when the gateway was manufactured.

Action: No action required.

tCert: Shutdown complete

Description: This informational message indicates that the task responsible for certificate maintenance has shut down. This is usually part of the normal system shutdown.

Action: No action required.

tCert: task creation failed

Description: The task responsible for X.509 certificate maintenance on the gateway failed to start properly. This most likely indicates severe resource exhaustion on the gateway.

Action: Reboot the gateway. If the reboot does not fix the problem, contact Nortel Networks Technical Support.

tCert: X.509 certificates disabled in flash memory

Description: This is an informational message that indicates the use of X.509 certificates by the gateway has been totally disabled.

Action: No action required.

Warning: System CA certificates may have been tampered with, please reinstall!

Description: The gateway performs a periodic integrity check of the SSL-related X.509 certificates that are stored on the gateway's local file system. This message signals a failure during the integrity check. This indicates that one or more of the SSL-related certificates might have been tampered with, or that a certificate has been corrupted.

Action:

1 Delete, then reinstall any SSL-related certificates. It is not necessary to delete and reinstall the tunnel-related certificates since they are stored in the LDAP database and not on the local file system.

2 Manually verify the tunnel-related certificate fingerprints. You should perform this procedure any time you suspect tampering.

ISAKMP messages

ISAKMP [13] No proposal chosen in message from *xxx* (a.b.c.d)

In many cases, a Session:IPsec message precedes the ISAKMP message. If the Session:IPsec message indicates an error, then the Session message describes the cause and required action. If there is no Session:IPsec error message, refer to the following list of causes and solutions for explanations.

Description: The encryption types proposed by branch office *xxx* do not match the encryption types configured locally.

Action: Check the encryption types on both sides to make sure they match. If necessary, reconfigure the encryption on one system.

Description: The requested authentication method (for example, RSA* Digital Signature) is not enabled.

Action: Enable all required authentication types. Make sure the unneeded types are disabled.

Description: One side of the connection is configured to support dynamic routing while the other side is configured for static routing, where branch office is *xxx*.

Action: Configure both sides to use the same routing type.

Description: Both sides are configured to support static routing. However, the local and remote network definitions of the two sides do not match, where branch office is *xxx*.

Action: Configure both sides to have matching local and remote network definitions.

Description: The Perfect Forward Secrecy (PFS) setting of the two sides do not match. Branch office *xxx* does not have PFS enabled, while PFS is required by the local settings.

Action: Make sure the PFS settings on both sides match. Either enable PFS on the remote side, or disable PFS locally.

ISAKMP [13] Error notification (No proposal chosen) received from *xxx* (a.b.c.d)

Description: The proposal made by the local gateway has been rejected by a Contivity VPN Client. This usually indicates that the client is using an international version (56-bit) while the gateway has stronger encryption enabled.

Action: The encryption methods used by the client and the gateway must match. Either provide the user with a Contivity VPN Client version that supports the stronger encryption method used by the gateway, or enable 56-bit encryption on the gateway.

Description: The proposal made by the local gateway has been rejected by a remote branch office gateway, or by an IPsec implementation from another vendor.

Action: Check with the administrator of the remote system to determine the cause of the problem. If the remote system is another gateway, the cause is noted in that system's log.

ISAKMP [13] Authentication failure in message from *xxx* (a.b.c.d)

In many cases, a Session:IPsec message precedes the ISAKMP message. If the Session:IPsec message indicates an error, the Session message describes the cause and required action. If there is no Session:IPsec error message, refer to the following list of causes and solutions for explanations.

Description: No encryption types are enabled for the account in question.

Action: Enable the desired encryption types.

Description: The requested authentication method (for example, RSA Digital Signature) is not enabled.

Action: Enable all required authentication types. Make sure the unneeded types are disabled.

ISAKMP [13] Error notification (Authentication failure) received from *xxx* (a.b.c.d)

Description: A Contivity VPN Client attempted to connect, but the user supplied the wrong password.

Action: Make sure that the user and the gateway have the same password.

Description: A remote branch office gateway rejected your gateway's attempt to authenticate.

Action: Contact the administrator of the remote system. If the remote system is a Contivity Secure IP Services Gateway, the cause is noted in that system log.

No response from client - logging out

Description: Your gateway has lost network connectivity with the remote side.

Action: Verify the network connectivity between your gateway and the remote side.

Description: A remote branch office using pre-shared key authentication is using a key that is different from what is configured on the local gateway. Because the two sides are using a different encryption key, your gateway cannot decrypt the encrypted messages from the other side, and therefore drops the messages.

Action: Make sure that both systems are using the same pre-shared key.

ISAKMP [13] *xxx* (a.b.c.d) has exceeded idle timeout - logging out

Description: The remote system has been idle (meaning that no traffic has been sent) for the amount of time configured in the Idle Timeout parameter (Profiles > Groups > Connectivity).

Action: If the Idle Timeout value is too low, increase it. To disable idle timeouts entirely, set the Idle Timeout value to 00:00:00.

ISAKMP [13] Invalid ID information in message from *xxx* (a.b.c.d)

Description: One side of the connection is configured to support dynamic routing while the other side is configured for static routing. Branch office is *xxx*.

Action: Configure both sides to use the same routing type.

Description: Both sides are configured to support static routing, however the local and remote network definitions of the two sides do not match. Branch office is *xxx*.

Action: Configure both sides to have matching local and remote network definitions.

ISAKMP [13] Error notification (Invalid ID information) received from *xxx* (a.b.c.d)

Description: One side of the connection is configured to support dynamic routing while the other side is configured for static routing. Branch office is *xxx*.

Action: Configure both sides to use the same routing type.

Description: Both sides are configured to support static routing. However, the local and remote network definitions of the two sides do not match. Branch office is *xxx*.

Action: Configure both sides to have matching local and remote network definitions.

Branch office messages

Couldn't install route for *remxxx@xxx*

Description: The gateway was unable to install the route for the remote network (indicated by *remxxx@xxx).* This might result when the route collides with an existing static route.

Action: Remove the existing static route or change the route for the remote network to be a subset or superset of the static route.

SSL messages

Checking chain: invalid parent cert, *xxx*

Description: The given certificate in the chain is not valid. This might indicate that the certificate installed at the external LDAP server has expired or is invalid in some other way.

Action: Verify that the certificate is valid or use a certificate that you know is valid.

Checking chain: invalid child cert, *xxx*

Description: The given certificate in the chain is not valid. This might indicate that the certificate installed at the external LDAP server has expired or is invalid in some other way.

Action: Verify that the certificate is valid or use a certificate that you know is valid.

Child cert *[xxx]* not valid signature by *[xxx]* - *xxx*

Description: The given certificate in the chain is not properly signed. This error can indicate that the certificate was incorrectly installed at the external LDAP server.

Action: Reinstall the certificate at the external LDAP server.

Invalid root cert, *xxx*

Description: One of the root certificates passed to the gateway during SSL negotiations was invalid.

Action: Configure the remote side to pass a valid chain of certificates to the gateway.

No matching trusted CA certs

Description: None of the certificates in the chain are trusted CA certificates. This message can result if the CA certificate has not been installed or has not been marked as trusted on the gateway.

Action: Make sure the CA certificate has been installed and that the certificate is marked as trusted on your gateway.

Database messages

Configuration file: *xxx* does not exist

Description: The slapd.cnf file does not exist on the disk, therefore the internal LDAP server could not start. This error can occur if the gateway disk has been modified.

Action: Reinstall the gateway software.

Failed to start

Description: The internal LDAP server did not start. This can be can caused by a missing configuration file.

Action: Reinstall the gateway software.

Index file for attribute *xxx* from file *xxx* could not be created

Description: The given attribute index file for the internal LDAP server could not be created. This might indicate that the gateway disk is full or that the database index files are corrupt.

Action: Restore the gateway software from an FTP backup or reimport the database from the LDIF file.

LDIF file: *xxx* could not back up

Description: The internal LDAP server database could not be backed up to the specified LDIF file. This can result if the name of the LDIF file is not in 8.3 format.

Action: Make sure the backup file has an 8.3 file name.

LDIF file: could not restore *xxx*

Description: The internal LDAP server database could not be restored from the specified LDIF file. This might indicate that the LDIF file does not exist.

Action: Choose an LDIF file that currently resides on the gateway disk.

Security messages

Account: *xxx[xxx]* uid *xxx* not found in account

Description: A UID of the remote entity was not found in the account used to initiate a branch office connection (the UID entry in the message is a UID for PPTP or Layer 2 Tunneling Protocol (L2TP), and a remote gateway address for IPsec). This error can result if the credentials given by the remote side of the branch office connection do not match the local configuration.

Action: Make sure the Remote Identity information of the IPsec Authentication Certificates section (Profiles > Branch Office > Edit Connection) is configured properly.

AuthServer: ldap inconsistent; no server type in entry *xxx*

Description: An LDAP entry for an authentication server does not contain a server type. This can indicate that the LDAP server is not accessible.

Action: Start the LDAP server, or change the external LDAP server configuration to make it accessible.

CaAuthServer: failed remove - *xxx*

Description: An LDAP entry for a CA authentication server was not fully created and then could not be removed. This can result if the LDAP server is not accessible.

Action: Start the LDAP server, or change the external LDAP server configuration to make it accessible.

CaAuthServerCollection: authenticate *xxx* cert *[xxx]* invalid signature by *[xxx]* - *xxx*

Description: The certificate passed in with the authentication request does not have a valid signature, based on the CA certificate configured on the gateway. This can indicate either an incorrect certificate at the remote side (either a client or branch office), or an incorrect CA certificate was installed on the gateway.

Action: Make sure that both sides have the correct certificates installed.

CaAuthServerCollection: authenticate *xxx[xxx]*:*xxx* bad certificate - *xxx*

Description: The certificate passed in with the authentication request is not a valid X.509 certificate. This error can result if the certificate configured either at the client or the other side of the Branch Office is incorrect.

Action: Install the correct certificates.

Conn backlog reached, possible SYN attack

Description: The number of connections on a socket is reaching or has completely reached the maximum number of queued connections.

Action: The device could possibly be under a syn attack and you should notify your IS department.

Security: store new system IP address *xxx* failed - *xxx*

Description: The system IP address could not be stored in the gateway configuration LDAP entry. Possible cause: the LDAP server is not accessible.

Action: Start the LDAP server or change the external LDAP server configuration to make it accessible.

Security: store new system name *xxx* failed - *xxx*

Description: The system name could not be stored in the gateway configuration LDAP entry. This might indicate that the LDAP server is not accessible.

Action: Start the LDAP server, or change the external LDAP server configuration to make it accessible.

Security: store new system subnet mask *xxx* failed - *xxx*

Description: The system subnet mask could not be stored in the gateway configuration LDAP entry. This might indicate that the LDAP server is not accessible.

Action: Start the LDAP server, or change the external LDAP server configuration to make it accessible.

Entry is referenced *[xxx]* - *xxx*

Description: The LDAP entry is being referenced by another LDAP entry (for example, a filter set being referenced by a User Group or Branch Office Connection).

Action: Remove all references to the LDAP entry in question, then delete the entry.

Error copying entry *[xxx]* to *[xxx]* - *xxx*

Description: An error occurred while copying an LDAP entry.

Action: Delete the new copy that caused the error and retry the rename operation.

Error copying subentries of *[xxx]* to *[xxx]* - *xxx*

Description: An error occurred while copying a set of LDAP entries. This can be caused by an unreachable LDAP server.

Action: Start the LDAP server, or change the external LDAP server configuration to make it accessible.

Error copying tree *[xxx]* to *[xxx]* - *xxx*

Description: An error occurred while copying a tree of LDAP entries. This might indicate that the LDAP server is not accessible.

Action: Start the LDAP server, or change the external LDAP server configuration to make it accessible.

Error deleting entry *[xxx]* - *xxx*

Description: An error occurred while deleting an LDAP entry. This might indicate that the LDAP server is not accessible.

Action: Start the LDAP server, or change the external LDAP server configuration to make it accessible.

Error deleting tree *[xxx]* - *xxx*

Description: An error occurred while deleting a tree of LDAP entries. This might indicate that the LDAP server is not accessible.

Action: Start the LDAP server, or change the external LDAP server configuration to make it accessible.

LocalAuthServer: failed remove - *xxx*

Description: An LDAP entry for an LDAP authentication server was not fully created and then could not be removed. This might indicate that the LDAP server is not accessible.

Action: Start the LDAP server, or change the external LDAP server configuration to make it accessible.

SchemaCls: Database schema not available

Description: The external LDAP server does not support a schema entry so it is not possible to update its schema over the network. This error can occur if the external LDAP server does not support the cn=schema entry.

Action: Update the external LDAP server schema manually, then reconnect to it.

xxx xxx being referenced by *xxx*

Description: The LDAP entry is being referenced by another LDAP entry (for example, a filter set being referenced by a User Group or Branch Office Connection).

Action: Remove all references to the LDAP entry in question, then delete the entry.

Session: *xxx* uid invalid - authentication failed

Description: The given IPsec hashed UID was not found in the LDAP database. This can be caused if the UID typed in at the client was invalid or the account no longer exists.

Action: Make sure the correct UID was typed at the client and make sure the account is valid.

Session: *xxx[xxx]* invalid uid - authentication failed

Description: The given group UID was not found in the LDAP database, or the UID was found under a group account and this was not a group login. This error might result if the UID was mistyped at the client or the account no longer exists.

Action: Make sure the correct UID was typed at the client and make sure the account is valid.

Session: *xxx[xxx]* session rejected - system is initializing

Description: The gateway had to reject the incoming request since it is still initializing.

Action: Wait a short time to make sure that the gateway has initialized, then try again.

Session: *xxx[xxx]* session rejected - system is shutting down

Description: The gateway rejected the incoming request since it is shutting down.

Action: Wait for the gateway to restart, then try again.

Session: *xxx[xxx]:xxx xxx* auth method not allowed

Description: The authentication method of the incoming request is not allowed in the group that the session is bound to. The session is bound to a group by one of the following:

- The group that the user's account is in (in LDAP)
- The RADIUS default group
- The RADIUS class attribute
- The CA authentication server's default group

Action: Enable the authentication method for the bound group.

Session: *xxx[xxx]:xxx* - authentication failed using all authservers

Description: The incoming request could not be authenticated by any configured authentication servers (LDAP, RADIUS, or CA).

Action: Provide the correct credentials. (For example, create a new user account.)

Session: *xxx[xxx]:xxx* AddLink failed *[xxx]* current links *xxx*

Description: The multilink session could not be created. This can be caused by any of the following:

- New logins are disabled.
- The max sessions on the gateway has been reached.
- There is not enough heap on the gateway.

- The call admission priority slot is full.
- The call admission priority slot is outside of access hours.
- The max links configured for the group has been reached.

Action: Verify the correct settings for each of the possible causes.

Session: *xxx[xxx]:xxx* IP address assignment failed

Description: An address could not be assigned to the session. This can result if the static address for the session is in use or if the address pool is exhausted.

Action: Expand the number of addresses in the pool, or change the static address on the account.

Session: *xxx[xxx]:xxx* L2TP host *[xxx]* account misconfigured

Description: The L2TP Access Concentrator on the Branch Office Connection does not exist or does not have a LAC or gateway UID.

Action: Recreate the L2TP Access Concentrator entry and make sure this entry is linked to the Branch Office Connection.

Session: *xxx[xxx]:xxx* account has max links *(xxx)*

Description: The maximum number of multilink sessions has been reached.

Action: Increase the maximum number of allowed PPP links on the Profiles > Groups > Edit > Connectivity screen.

Session: *xxx[xxx]:xxx* account has max sessions *(xxx)*

Description: The maximum number of sessions for the given account has been reached.

Action: Increase the number of logins on the Profiles > Groups > Edit > Connectivity screen.

Session: *xxx[xxx]:xxx* account is disabled

Description: The account is not currently enabled. This error can occur if the Branch Office Connection request is a different tunnel type than the local gateway.

Action: Make sure that both sides are configured to support the same tunnel type.

Session: *xxx[xxx]:xxx* account not allowed now

Description: The session request is outside the permitted hours of access.

Action: Change the Access Hours setting assigned to the group on the Profiles > Groups > Edit > Connectivity screen.

Session: *xxx[xxx]:xxx* authentication failed using *xxx*

Description: The credentials for the session could not be validated by any of the authentication servers.

Action:

1. Make sure you are using the correct credentials.
2. Expand the capability of the RADIUS authentication server to handle the authentication method.
3. Add a new account with the given credentials.

Session: *xxx[xxx]:xxx* client assigned address *[xxx]* already in use

Description: The address given by the tunnel client is currently is use. This might indicate that the address is either being used in a static or dynamic route, or that the address is assigned to an active tunnel.

Action: Configure the client to use a different address.

Session: *xxx[xxx]:xxx* connect Qos level *xxx* full

Description: The gateway does not have any more slots for the session's call admission priority. This can indicate that the configured Call Admission Priority for the group that the request is assigned to is too low.

Action: Increase the Call Admission Priority on the Profiles > Groups > Edit > Connectivity screen.

Session: *xxx[xxx]:xxx* invalid password - master admin authentication failed

Description: The primary administrator password was invalid. This can result from using the wrong password or from making a mistake while typing the password.

Action: Make sure you are using the correct password, and make sure you typed it correctly.

Session: *xxx[xxx]:xxx* login rejected - new logins disabled

Description: New logins are currently disabled. This can result if the gateway was shut down with one of the following settings enabled on the Admin > Shutdown screen:

- The **Disable new logins** checkbox is selected, or
- The **Disable logins after restart** checkbox is selected.

Action: Enable new logins by deselecting the disable login settings on the Admin > Shutdown screen and then restart the gateway.

Session: *xxx[xxx]:xxx* no memory free: *xxx* threshold: *xxx*

Description: There is not enough heap memory available to establish the session. This can result if the gateway has consumed a large amount of memory while processing management requests.

Action: Increase the amount of physical memory on the gateway, or wait until the management requests are complete.

Session: *xxx[xxx]:xxx* only one session/static address allowed

Description: An address can be used by only one session. This error occurs if the gateway receives a second login to an account that has a static address configured.

Action: Change the account to use dynamic addresses from either a static address pool or DHCP.

Session: *xxx[xxx]:xxx* pool address *[xxx]* already in use

Description: The returned static pool address is currently is use. This error can occur if another tunnel is using this address via a static address configuration or another address pool. The error also occurs if a static host route using this address has been added.

Action: No action is necessary. The gateway attempts to allocate a different address.

Session: *xxx[xxx]:xxx* session directed to use server *xxx*

Description: This is an informational message indicating that load balancing is enabled and the session is being redirected to another gateway. This occurs when the gateway is either more heavily CPU-loaded or session-loaded than the other gateway.

Action: No action is necessary.

Session: *xxx[xxx]:xxx* static address *[xxx]* already in use

Description: The static address assigned to the account is in use by another tunnel or via a static host route.

Action: Change the static address.

Session: *xxx[xxx]:xxx* system has max sessions *(xxx)*

Description: The gateway has reached its maximum number of sessions. This occurs when the gateway reaches the maximum number of tunnels that can be configured.

Action: Use load balancing with another gateway (if you are using IPsec clients), or upgrade the gateway to the next higher model.

RADIUS accounting messages

RADIUS: Cannot send accounting request to <*server-name*>, possibly due to DNS translation failure

Description: This message indicates a connection failure. While sending a request, an error occurred due to a socket creation problem. This usually indicates a DNS resolution problem.

Action: Verify the following:

- DNS host name is correct.
- DNS server is configured properly.
- DNS server is available.

RADIUS: no reply from server <*server-name*>(<*port number*>)

Description: This message indicates a connection failure. The connection timed out while waiting for a response.

Action: Verify the following:

- RADIUS server's IP address and port number are correct.
- RADIUS server is available.
- Shared secret is correct.

RADIUS: <*server-name*> server timed out

Description: This message indicates a connection failure. The connection timed out while waiting for a response.

Action: Verify the following:

- RADIUS server's IP address and port number are correct.

- RADIUS server is available.
- Shared secret is correct.

RADIUS: network socket failure with <*server-name*>, recvfrom error: <*error*>

Description: This message indicates a connection failure. An error occurred while receiving the response.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

RADIUS: <*server-name*> server failed

Description: This message indicates a connection failure. An error occurred while receiving the response.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Indicated packet length too large

Description: This message indicates that an invalid response was received. The length of the response packet is not equal to the number of bytes received.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

RADIUS: failure sending <*user-name*> accounting record to <*server-name*>

Description: This message indicates that an invalid response was received. The length of the response packet is not equal to the number of bytes received.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Non-matching ID in server response

Description: This message indicates that an invalid response was received. The Transaction ID in the response packet is not the expected value.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Unsupported response type (<*number*>) received from server

Description: This message indicates that an invalid response was received. The response packet type is not one of the expected types: Access-Accept, Access-Reject, or Access-Challenge.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Received bad attribute type from server

Description: This message indicates that an invalid response was received. The RADIUS Attribute value is incorrect.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Response OK

Description: This message indicates that a valid response was received.

Action: No action necessary.

RADIUS: <*user-name*> accounting record sent to <*server-name*> OK

Description: This message indicates that a valid response was received.

Action: No action necessary.

RADIUS authentication messages

RADIUS: Cannot send request to <*server-name*>, possibly due to DNS translation failure

Description: This message indicates a connection failure. While sending a request, an error occurred due to a socket creation problem. This usually indicates a DNS resolution problem.

Action: Verify the following:

- DNS host name is correct.
- DNS server is configured properly.
- DNS server is available.

Login failure due to: Server network connection failure

Description: This message is received by the Contivity VPN Client, and indicates a connection failure. While sending a request, an error occurred due to a socket creation problem. This usually indicates a DNS resolution problem.

Action: Verify the following:

- DNS host name is correct.
- DNS server is configured properly.
- DNS server is available.

RADIUS: no reply from RADIUS server <*server-name*>(<*port number*>)

Description: This message indicates a connection failure. The connection timed out while waiting for a response.

Action: Verify the following:

- RADIUS server's IP address and port number are correct.
- RADIUS server is available.
- Shared secret is correct.

RADIUS: <*server-name*> server timed out authenticating <*user-name*>

Description: This message indicates a connection failure. The connection timed out while waiting for a response.

Action: Verify the following:

- RADIUS server's IP address and port number are correct.
- RADIUS server is available.
- Shared secret is correct.

RADIUS: network socket failure with <*server-name*>, recvfrom error: <*error*>

Description: This message indicates a connection failure. An error occurred while receiving the response.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

RADIUS: <*server-name*> server error while authenticating <*user-name*>

Description: This message indicates a connection failure. An error occurred while receiving the response.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Indicated packet length too large

Description: This message indicates that an invalid response was received. The length of the response packet is not equal to the number of bytes received.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

RADIUS: <*server-name*> sent invalid response packet for <*user-name*>

Description: This message indicates that an invalid response was received. The length of the response packet is not equal to the number of bytes received.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Non-matching id in server response

Description: This message indicates that an invalid response was received. The Transaction ID in the response packet is not the expected value.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Unsupported response type (<*number*>) received from server

Description: This message indicates that an invalid response was received. The response packet type is not one of the expected types: Access-Accept, Access-Reject, or Access-Challenge.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Received bad attribute type from server

Description: This message indicates that an invalid response was received. The RADIUS Attribute value is incorrect.

Action: Retry authentication attempt and verify that RADIUS server packets are properly formed.

Invalid reply digest from server, possible shared secret mismatch

Description: This message indicates that an invalid response was received. The computed authenticator does not match the value in the packet.

Action: Verify that the shared secrets match.

RADIUS: <*server-name*> sent packet with invalid response authenticator for <*user-name*>

Description: This message indicates that an invalid response was received. The computed authenticator does not match the value in the packet.

Action: Verify that the shared secrets match.

RADIUS server returned access challenge

Description: This message indicates that a valid access-challenge response was received.

Action: No action required.

RADIUS: <*server-name*> sent challenge for <*user-name*>

A valid access-challenge response was received.

Action: No action required.

RADIUS access challenge received

Description: This message is received by the Contivity VPN Client. A valid access-challenge response was received.

Action: No action required.

RADIUS server rejected access

Description: This message indicates that a valid access-reject response was received.

Action: No action required.

RADIUS: <*user-name*> access DENIED by server <*server-name*>

Description: This message indicates that a valid access-reject response was received.

Action: No action required.

Response OK

Description: This message indicates that a valid access-accept response was received.

Action: No action required.

RADIUS: <*user-name*> access OK by server <*server-name*>

Description: This message indicates that a valid access-accept response was received.

Action: No action required.

Routing messages

Unable to create *xxx* for OSPF

Description: The gateway could not create the necessary components to initialize OSPF. This could happen if the gateway runs out of free memory.

Action: Disable and enable OSPF globally in Routing > OSPF screen. If this does not work, disable OSPF, boot the gateway and enable OSPF in Routing > OSPF screen.

OSPF Disabled

Description: The administrator disabled OSPF from the Routing > OSPF screen.

Action: No action required.

Closing OSPF-RTM connection

Description: OSPF closed the RTM connection, which occurs if the administrator disables OSPF from Routing > OSPF screen.

Action: No action required.

Ospf_Global.State changed from ENABLED to DISABLED by user 'admin' @ *x.x.x.x*

Description: The administrator disabled OSPF from the Routing > OSPF screen.

Action: No action required.

Opened OSPF-RTM connection

Description: The administrator enabled OSPF from the Routing > OSPF screen and successfully registered with RTM.

Action: No action required.

OSPF Enabled

Description: The administrator enabled OSPF from the Routing > OSPF screen.

Action: No action required.

Ospf_Global.State changed from DISABLED to Enabled by user 'admin' @ *x.x.x.x*

Description: The administrator disabled OSPF from the Routing > OSPF screen.

Action: No action required.

Can not accept x.x.x.x as router id

Description: OSPF can not accept the given router ID in the Routing > OSPF screen.

Action: You must change router ID in the Routing > OSPF screen. Invalid router IDs are 127.0.0.1 and 0.0.0.0.

LoadOspfAreas Failed

Description: OSPF failed to load all areas of information from the config file. This could happen if the config file is damaged.

Action: Delete all OSPF areas, re-create them from the Routing > OSPF screen, and reboot the gateway.

LoadOspfIntf Failed

Description: OSPF failed to load information for all interfaces from the config file. This could happen if the config file is damaged.

Action: Delete all OSPF interfaces, re-create them from the Routing > Interface screen, and reboot the gateway.

VR *xxx*: Starting *xxx* as Master for *xxx*

Description: Logged when VRRP is starting as a master for an address. The parameters are:

- The VRID of this VR
- The reason for starting, either because it was enabled or the interface went up
- The IP address

Action: No action required.

VR *xxx*: Starting *xxx* as Backup for *xxx*

Description: Logged when starting as a backup for an address. The parameters are:

- The VRID of this VR
- The reason for starting, either because it was enabled or the interface went up
- The IP address

Action: No action required.

VR *xxx*: Starting *xxx* as master delayed Backup for *xxx*

Description: Logged when master delay mode is in effect. The parameters are:

- The VRID of this VR
- The reason for starting, either because it was enabled or the interface came up
- The IP address

Action: No action required.

VR *xxx*: Shutting down *xxx* on *xxx*

Description: Logged when VRRP is stopping. The parameters are:

- The VRID of this VR
- The reason for stopping, either because it was disabled or the circuit went down
- The IP address

Action: No action required.

Unable to get configuration for VR *xxx*

Description: This is an error event. It is logged when VRRP is enabled but the common configuration parameters are missing. These are the items set under the Routing > VRRP screen. The parameter is the IP address that is missing information.

Action: No action required.

RIP *xxx*: RIP Enabled

Description: Logged when RIP is globally enabled.

Action: No action required.

RIP *xxx*: RIP Disabled

Description: Logged when RIP is globally disabled.

Action: No action required.

RIP *xxx*: Can't alloc main node

Description: Logged when there is not enough memory to allocate RIP parameters.

Action: No action required.

RIP *xxx*: Circuit *xxx* created

Description: Logged when the RIP circuit was created. The parameter stands for circuit ID.

Action: No action required.

RIP *xxx*: Circuit *xxx* deleted

Description: Logged when the RIP circuit was deleted. The parameter stands for circuit ID.

Action: No action required.

RIP *xxx*: Unable to register with UDP

Description: Logged when you cannot register with UDP protocol.

Action: No action required.

RIP *xxx*: setsockopt RIP socket *xxx* SO_RCVBUF *xxx* failed

Description: Logged when RIP receive buffers are not large enough. This can happen when a large numbers of RIP neighbors send their RIP updates simultaneously. The first parameter is the socket number and the second parameter is the maximum receive buffer size.

Action: No action required.

RIP *xxx*: bind RIP socket *xxx* failed

Description: Logged when RIP failed to bind the socket.

Action: No action required.

RIP *xxx*: Unable to spawn Dispatcher task *xxx* for RIP

Description: Logged when RIP failed to spawn the main task responsible for receiving RIP packets. The parameter stands for the name of the task.

Action: No action required.

RIP *xxx*: Unable to spawn timer task *xxx* for RIP

Description: Logged when RIP failed to spawn the timer task. The parameter stands for the name of the task.

Action: No action required.

RIP *xxx*: cid xxx mismatched auth password from *xxx*

Description: Logged when RIP authentication failed while receiving RIP packets. The first parameter is the circuit ID on which it was receiving RIP packets and the second parameter is the IP address from which it received RIP packets.

Action: No action required.

Hardware messages

The gateway software provides informational messages when cards are removed and replaced. When you exchange two cards with each other, the gateway considers this two simultaneous replacements.

Interface [*nnn*] not present, deleting from config

Description: This indicates that the configuration file contains an interface [*nnn*] entry, but there is no card in the slot. The interface [*nnn*] entry is deleted from the configuration.

Action: No action required.

Interface [*nnn*] replaced, resetting config

Description: This indicates the card type specified in the configuration file does not match the card type currently in the slot. The configuration information is reset to defaults then initialized with the current hardware.

Action: No action required.

Interface [*nnn*] replaced, deleting from config

Description: This indicates the card type specified in the configuration file does not match the card currently in the slot. The interface is deleted from the configuration. This applies when the replaced card has more ports than the current card.

Action: No action required.

HWAccel [*nnn*] not present, deleting from config

Description: This indicates the configuration file contains a HWAccel [*nnn*] entry, but there is no hardware accelerator in the slot. The HWAccel [*nnn*] entry is deleted from the configuration.

Action: No action required.

Appendix D
Configuring for interoperability

This chapter explains the requirements and procedures for setting up different vendor hardware or software to interoperate with the Contivity Secure IP Services Gateway. These instructions enable you to establish encrypted tunnels to and from the gateway with the noted vendors. These requirements and procedures are subject to change based on hardware and software changes by the vendors.

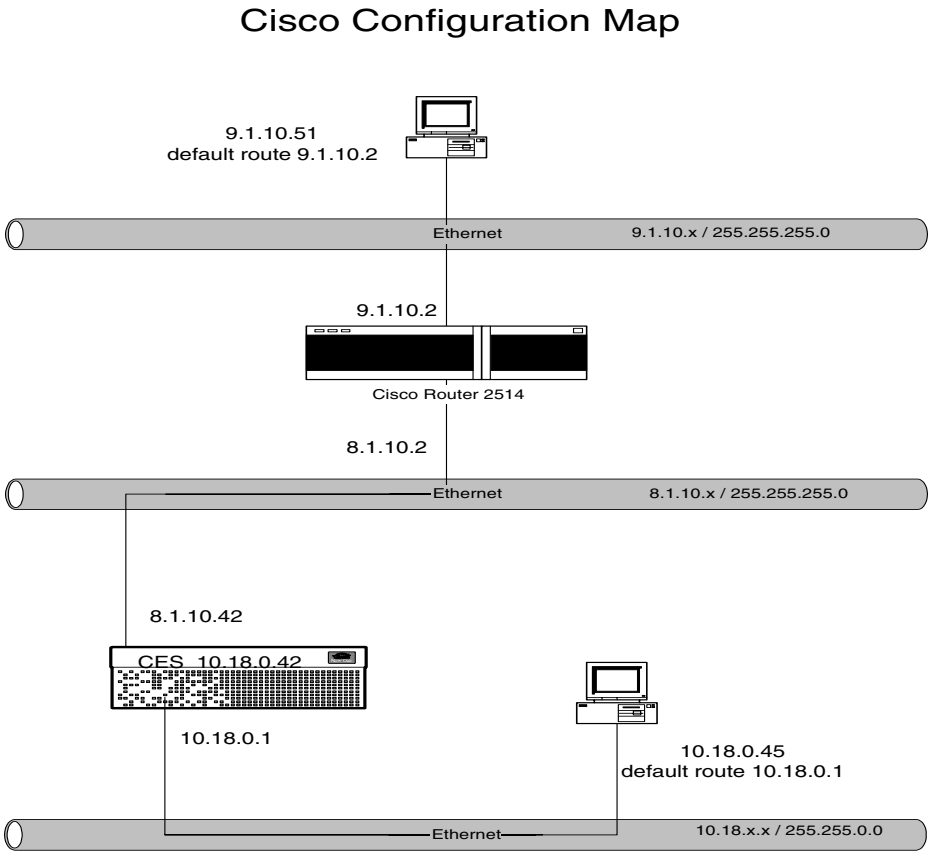
Procedures are available for the following products:

- Cisco* 2514 router, Version 11.3
- SafeNet, Inc. (IRE), SafeNet*/Soft-PK Security Policy Database Editor, Version 1.0
- Third-party clients
- Internetwork Packet Exchange (IPX)

Configuring the Cisco 2514 router, Version 11.3

To set up the gateway to establish encrypted tunnel connections with the Cisco 2514 router, as shown in Figure 6, you should configure the Cisco 2514 with the Show Configuration command.

Figure 6 Contivity gateway and Cisco 2514 network topology



The following is a `show config` command:

```
Cisco2514# show config
Using 1088 out of 32762 bytes
version 11.3
no service password-encryption
hostname Cisco2514
enable secret 5 $1$aSJB$Xz/o4I4IqCY.FT2RH372/1
enable password password
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 3000
crypto isakmp key test address 8.1.10.42
!
crypto ipsec transform-set esp1 esp-des esp-md5-hmac
!
crypto map bay 11 ipsec-isakmp
 set peer 8.1.10.42
 set session-key lifetime seconds 3000
 set transform-set esp1
 match address 132
!
!
interface Ethernet0
 ip address 9.1.10.2 255.255.255.0
 no mop enabled
!
interface Ethernet1
 ip address 8.1.10.2 255.255.255.0
 no mop enabled
 crypto map bay
!
interface Serial0
 no ip address
 no ip mroute-cache
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
ip classless
ip route 10.18.0.45 255.255.255.255 8.1.10.42
access-list 132 permit ip host 9.1.10.51 host 10.18.0.45
access-list 132 permit ip host 10.18.0.45 host 9.1.10.51
dialer-list 1 protocol ip permit
```

```
dialer-list 1 protocol ipx permit
snmp-server community public RO
line con 0
line aux 0
line vty 0 4
password terminal
login
end
```

Configuring the gateway for Cisco interoperability

To configure the gateway for Cisco interoperability, go to the Profiles > Networks screen and click on Edit.

Create any local accessible networks that you want available.

1. Enter the IP address for the new subnet; for example, 10.18.0.45.
2. Enter the subnet mask for the new network.
3. Click on Add. The Networks Edit screen appears and shows the newly created subnet in the Current Subnets list for the named network.
4. Add each local subnet for which you want tunneled connections coming to or going from the gateway to a Network profile.
5. Verify that your settings are synchronized with the Cisco router on the Profiles > Branch Office: Edit GROUP screen.

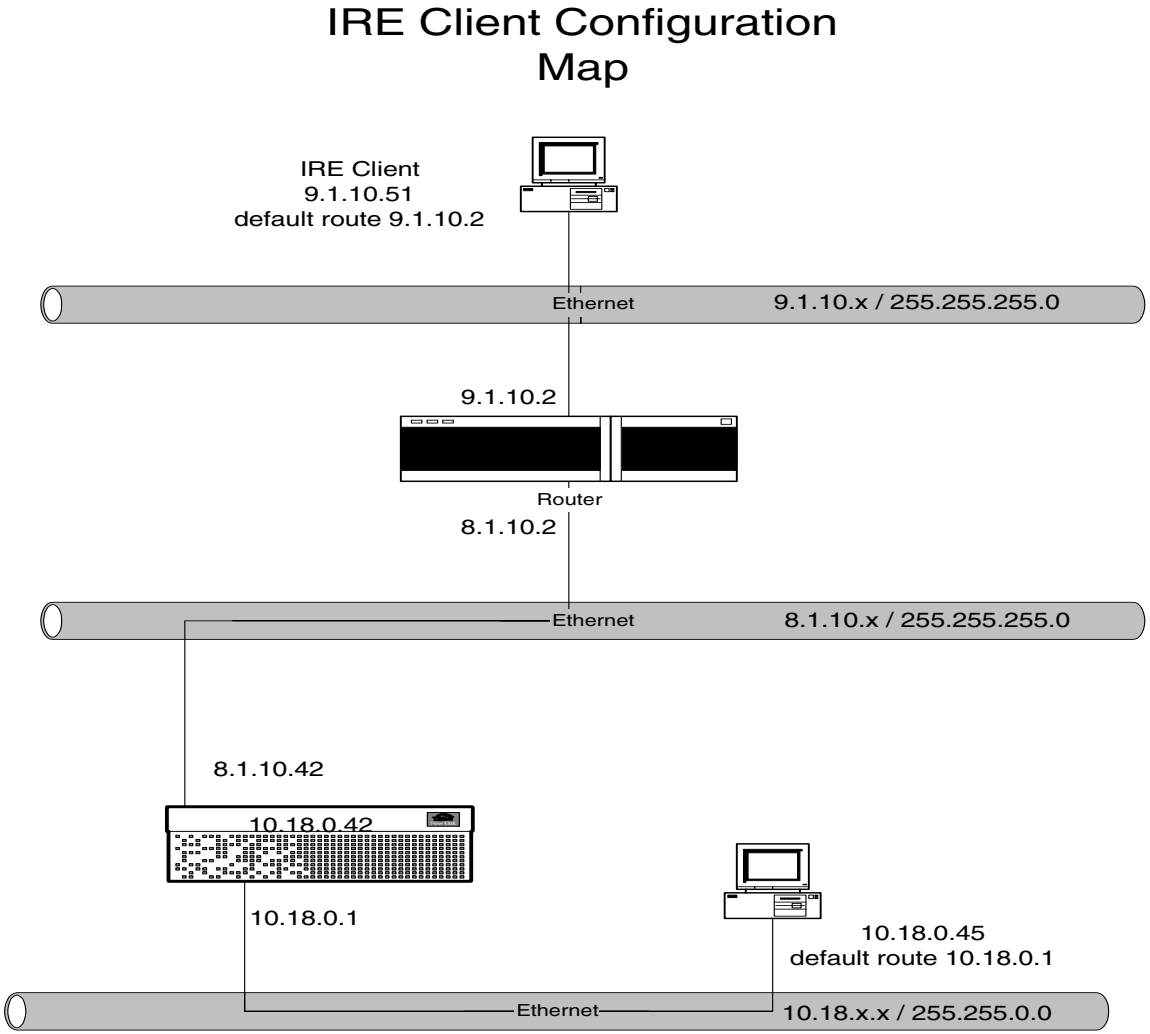
   For Cisco, turn off Vendor ID and Perfect Forward Secrecy (PFS). Go to the Profiles > Groups > IPsec: Configure screen.

6. Create and configure the IPsec branch office connection on the gateway, using the network profile you just created for the local accessible network.
7. On the Profiles > Branch Office screen, you must enable IPsec Authentication: Text Pre-Shared Key.

Configuring the SafeNet/Soft-PK Security Policy Database Editor, Version 1.0s

To set up the gateway to establish encrypted tunnel connections with the IRE Soft-PK Security Policy Client as illustrated in Figure 7, you should configure the screens as described on following pages.

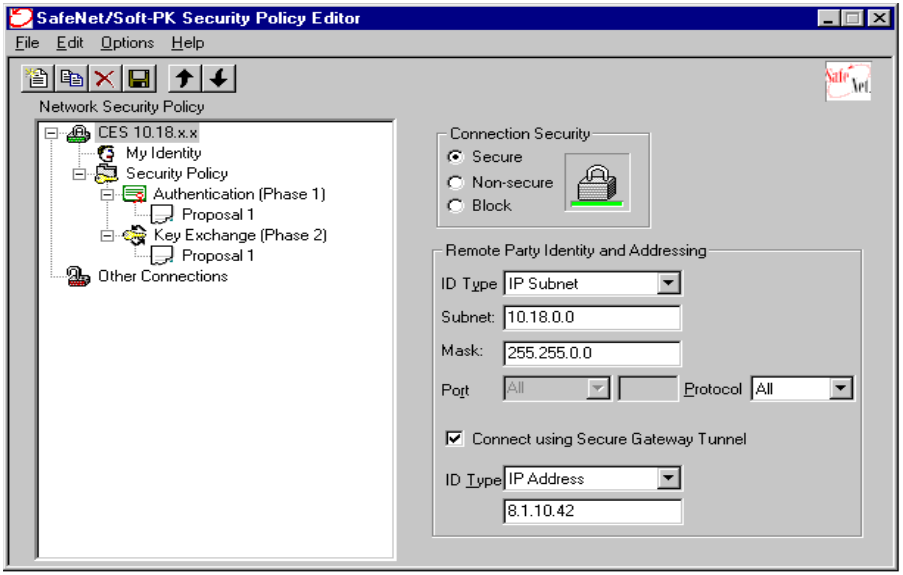
Figure 7 Contivity gateway and IRE SafeNet network topology



Connecting to IRE SafeNET/Soft-PK Security Policy Client

To set up the gateway to establish encrypted tunnel connections with the IRE SafeNet/Soft-PK Security Policy Client, follow these instructions:

1 Open the SafeNet/Soft-PK Security Policy Client, and click on File: New. The following screen configures the network so that any packets going to the 10.18.0.0 subnet goes through the gateway's 8.1.10.42 interface to establish a tunnel.



2 Click on the switch: CES 10.18.x.x.

3 Click on Connection Security: Secure.

4 Under Remote Party Identity and Addressing, select the following:

- ID Type: IP Subnet
- Subnet: 10.18.0.0.
- Mask: 255.255.0.0
- Protocol: All

5 Under Connect using Secure Gateway Tunnel, select the following:

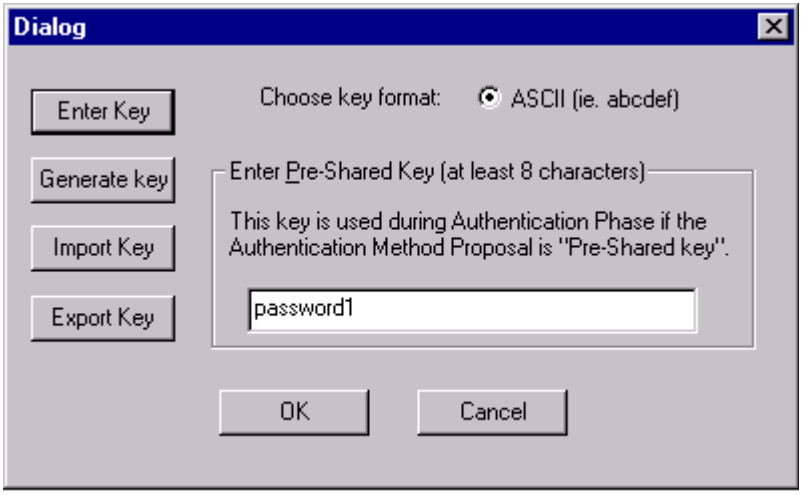
- ID Type: IP Address
- 8.1.10.42

The SafeNet/Soft PX Security Policy Editor dialog box opens.

6 Click on My Identity to configure the SafeNet client, and select the following:

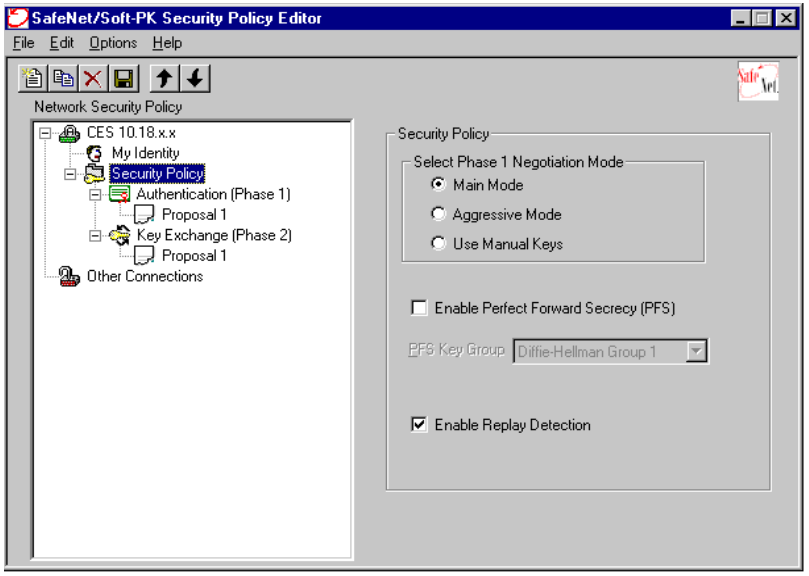
- Select Certificate: None
- ID Type: IP Address
- Port: All

7 Click on Pre-Shared Key. The Pre-Shared Key dialog box appears.



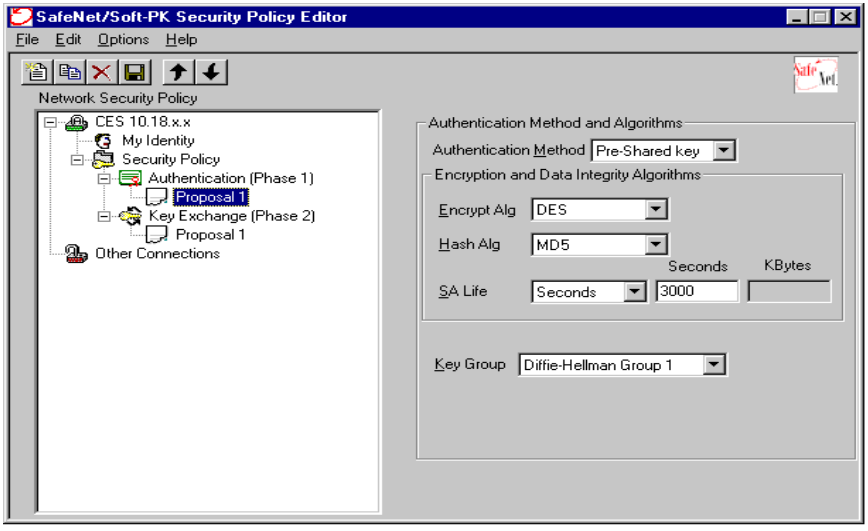
8 In the Pre-Shared Key dialog box, click on Enter Key, then enter the pre-shared key.

9 Click on OK. The SafeNet/Soft-PK Security Policy Editor dialog box appears.



10 Click on Security Policy: Select Phase 1 Negotiation Mode: Main Mode.

11 Click on Enable Replay Detection.



12 On the Authentication (Phase 1), Proposal 1, Authentication screen, enable the following:

- Authentication Method: Pre-Shared key
- Encrypt Alg: DES
- Hash Alg: MD5
- SA Life: Seconds and 3000 (Seconds)
- Key Group: Diffie-Hellman Group 1

13 On the Key Exchange (Phase 2), Proposal 1 screen, enable the following:

- Encapsulation Protocol (ESP)
- Encrypt Alg: DES
- Hash Alg: MD5
- Encapsulation: Tunnel
- SA Life: Seconds and 3000 (Seconds)

Configuring the gateway for IRE interoperability

To configure the gateway for IRE interoperability, go to the Profiles > Networks screen and click on Edit.

Create the network object used for local accessible networks:

1. In the Networks Edit screen, enter the IP address for the new subnet; for example, 10.18.0.45.
2. Enter the subnet mask for the new network: 255.255.0.0.
3. Click on Add. The Networks Edit screen reappears and shows the newly created subnet in the Current Subnets list for the named network.
4. Add each local subnet for which you want tunneled connections coming to or going from the gateway to a network profile.
5. Verify that your settings are synchronized with the SafeNet client (Profiles > Branch Office: Edit GROUP).
6. Create and configure the IPsec Branch Office connection on the gateway, using the network profile you just created for the local accessible network. On the Profiles > Branch Office screen, you must enable the IPsec Authentication: Text Pre-Shared Key option.
7. For some vendors, you want to turn off Vendor ID and/or Perfect Forward Secrecy (PFS). Go to the Profiles > Groups > IPsec: Configure screen to do this.

Third-party client installation

The gateway supports third-party IPsec clients and includes support for the following:

- Authentication using either pre-shared authentication (using IKE Aggressive mode) or digital signature certificate authentication (using IKE Main mode) into a gateway remote access user's IPsec account for third-party IPsec clients.

- Client address assignment to be used within the IPsec tunnel formed as a result of the Quick Mode negotiation. The client's external IP address or a pre-arranged internal IP address can be used as the address that is negotiated during the IKE Quick Mode exchange.
- Split tunneling with third-party IPsec clients, such that if split tunneling is enabled on the gateway, then the subnet that the client specifies as the gateway's identity within the tunnel during IKE Quick Mode must be listed as one of the split tunnel networks for the Quick Mode proposal to be accepted. If split tunneling is not enabled on the gateway, then the gateway identity that the client specifies for Quick Mode can be any value that the client chooses.

Depending on the third-party client that you are using, you need to configure either a branch office tunnel or a user tunnel. For example, the gateway has been configured and tested with the LINUX* FreeS/WAN client. If you are using the FreeS/WAN LINUX client, you must configure your user and the gateway as a branch office tunnel. If you are using another client that supports IPsec Aggressive mode, you can configure your gateway as a user tunnel.

Considerations for using third-party clients

There are several considerations regarding the use of third-party clients with Contivity:

- Client Dynamic Addressing -- Many third-party clients now support the Aggressive mode method of establishing a security association. The advantage of Aggressive mode for remote user access is that, unlike Main mode, the VPN server does not authenticate the security association based on prior knowledge of the IP address of the user. Therefore, the remote user can be dynamically assigned an address by their ISP.
- Client Address Advertisement -- When connecting to the Contivity VPN client, the gateway assigns the client-side inner address of the IPsec tunnel from the enterprise address space. This is the address that devices on the private network send data to in response to requests from the client. The gateway captures packets destined for those addresses and sends them through the public interface encapsulated within IPsec, addressed to the ISP-assigned outer address of the client.

In the case of third-party clients, the gateway does not have a mechanism to assign the inner address of the client. The inner address of the client tunnel is normally set the same as the ISP-assigned outer address. Servers in the enterprise need to find a route back to these clients. You must configure the gateway as the default gateway on the network. The gateway can then forward tunneled traffic to served clients and forward other traffic to the Internet or other default gateways. This option is not always desirable because of the impact on the customer network infrastructure.

- Authentication -- Various authentication services supported with the Contivity VPN Client are not supported with third-party clients. RADIUS, RSA SecurID*, AXENT*, and other RADIUS-based services will not work with the gateway, even if the third-party client has the support available. LDAP with pre-shared key and unmanaged certificates are the only authentication services supported by the gateway with third-party clients.
- Client Customization -- This capability allows a service provider to customize the look of the client with their branding. In addition, it allows the service provider to preconfigure the service profiles (gateway destination and authentication options) and lock down the client configuration for the end-user so that they cannot modify or change these attributes.
- Load Balancing -- Traditional load balancers do not often work with the IPsec protocol because of the security features on individual packets and separate key management and data channels. The gateway has built-in load balancing features for IPsec client terminations that allow two gateways to load balance and failover connections. This feature works with third-party clients.
- QoS -- The Contivity VPN Client is subject to manager-defined QoS policies. Connection slots can be reserved for different classes of user, and they can be assigned differing forwarding priorities for their traffic. The gateway preserves Diff-Serv markings for dial tunnels, copying the Diff-Serv Code Point from the inside packet to the tunnel header.
- Advanced attribute definition from the server -- On a group-by-group basis, you can load the client with its tunneled IP address and subnet mask, a Microsoft domain name, both WINS and DNS servers, a message of the day and the Contivity banner. The network manager can also determine access days and hours, crypto strength, how often the client will re-key, and whether the client can store a password for the group. It can initiate a password-protected screen saver if the user leaves the PC, and can log off idle connections. You can filter traffic in the tunnel based on IP address and/or port

number and can configure to close the tunnel if certain network applications are run. You can set the tunnel to automatically start when predefined applications or destinations are accessed, and close when these application are completed. These features are not available with third-party clients.

- Address Assignment -- Client-tunneled IP addresses can be assigned via a DHCP server, on a per-group basis from a named pool, via RADIUS attribute, or statically. The client receives the inner IP address from the enterprise address space. Third-party remote access clients get their inner address assigned the same as the outer, which is normally what the ISP assigns, and is not part of the enterprise address space.
- Split Tunneling -- On a group-by-group basis, a service provider can determine which IP addresses will go into the tunnel and which will use the local adapter (for general Internet access, or local printing/server usage). With third-party clients, you should enable split tunneling. If disabled, the client must be put into a group configured to allow undefined networks.
- Advanced Security features -- The Contivity VPN Client tunnel only accepts packets originating from the machine on which it is loaded. If attempts are made to route packets through a Contivity VPN Client, the tunnel is closed. When non-split tunneling is enabled, only packets that have passed through the VPN (have been correctly decrypted, and authenticated) will be accepted; other packets are dropped. If any attempt is made to change the station address of the client, the tunnel is automatically closed. Third-party clients do not necessarily have this security.
- Tight integration with MS-DUN and IPASS -- This allows one-click access that dials and authorizes the ISP connection and then creates the VPN connection automatically. This makes it significantly easier for the end user. Third-party clients typically do not have this ease-of-use feature.
- High end PKI integration -- The gateway integrates software from the leading certificate vendors, for a high-end managed PKI implementation. Managed PKI features like automated enrollment and automatic renewal are critical for large-scale rollouts. Other clients have loose or no integration for managed PKI and rely on the features of a browser or simple cut-and-paste methods. This is not available with third-party clients when used with the gateway, even if the client has the support built in.

Configuring the gateway as a branch office tunnel

To configure the gateway as a branch office tunnel:

1. Go to the Profiles > Branch Office screen and click on the Define Branch Office Connection button. The Branch Office > Define Connection screen appears.
2. Specify the addresses of the public interfaces of the two gateways forming the connection.
   a. For the local endpoint address, select the address of the local gateway from the drop down list.
   b. For the remote endpoint address, enter the address of the remote gateway that will form the opposite end of the branch office connection.
3. Set the tunnel type to IPsec.
4. Depending on what your third-party clients support, you can use either pre-shared key or digital certificate authentication. Click to enable the user name and password to authenticate user identity. The user name is the user's IP address and the password can be any password. Match the pre-shared secret with the client shared secret.
5. Click on RSA Digital Signature to enable certificate authentication if your third-party client supports RSA Digital Signature authentication. You must then select a default server certificate from the drop down list. You configure servers from the System > Certificates screen.
6. Go the Profiles > Branch Office screen and click on the Edit button, scroll down to the IPsec section and click on the Configure button. The Branch Office screen appears.
7. Select the encryption type supported by your third-party client.
8. Select Enable or Disable for the VendorID.
9. Set Perfect Forward Secrecy (PFS) to match the client side.
10. In the Rekey Time-out section, enter the amount of time to which you want to limit the lifetime of a single key used to encrypt data. The default is 08:00:00 (8 hours).
11. In the Rekey Data Count section, you can choose to set a rekey data count depending on how much data you expect to transmit through the tunnel with a single key. The default is 0 KB; a setting of 0 disables this count.

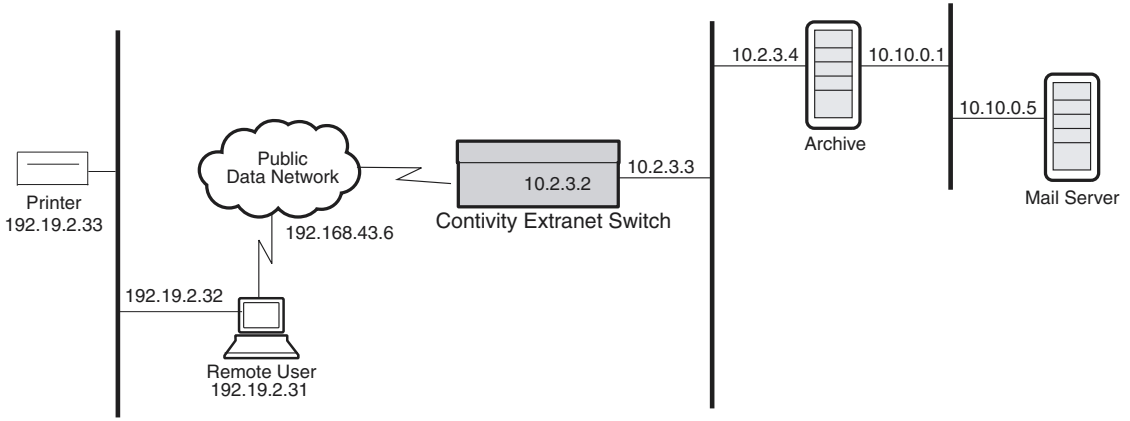
Configuring the gateway as a user tunnel

If you have third-party client software that supports Aggressive mode IPsec, you can configure the gateway as a user tunnel. You must use either the LDAP database or the certificate authentication. The gateway supports both pre-shared key and RSA digital signature authentication methods and you must specify at least one of these methods.

Nortel Networks recommends enabling split tunnels for all groups that support third-party clients. If split tunneling is disabled, third-party clients can only connect if the group is configured to allow undefined networks. This means that the client can establish IPsec security associations for all networks. If you do not enable split tunneling, you must enable the Allow undefined networks option.

Figure 8 shows a network with a split tunneling environment.

Figure 8 Split tunneling example



To configure the gateway as a user tunnel:

1. Go the Profiles > Groups screen and click on the Add button. Enter a group name of up to 64 characters (spaces are permitted); for example, Research and Development.
2. Click on the Edit button next to the name of the new group, scroll down to the IPsec section, and click on the Configure button. The IPsec Edit screen appears.

3. Set Split tunneling to Enabled if you want your gateway to have control over the networks that the third-party client can access. If split tunneling is disabled and Allow undefined networks for non-Contivity VPN Clients is enabled, the clients can connect to all internal networks. If you select both Split Tunneling and Allow undefined networks for non-Contivity VPN Clients, the gateway uses the split tunneling feature and ignores the Allow undefined networks selection.
4. Under Client Selection, select Non-Contivity VPN Clients (LINUX) or Both Contivity and Non-Contivity VPN Clients from the drop-down list.
5. Third-party clients can use either pre-shared key or digital certificate authentication. Click on the check box to enable the user name and password to authenticate user identity. If you are using Main mode, the user name is the user's IP address and the password can be any password.

   Click on RSA Digital Signature to enable certificate authentication if your client supports this. You must then select a default server certificate from the drop down list. You configure servers from the System > Certificates screen.
6. Selections in the Encryption fields are dependent on the type of encryption that your third-party client supports.
7. Click on the check box to enable Perfect Forward Secrecy (PFS). PFS ensures that if one key is compromised, subsequent keys are not compromised.
8. In the Forced Logoff edit box, specify a time after which all active users are automatically logged off. The default is 0, which means the option is turned off. The possible range is 00:00:01 to 23:59:59.
9. Click on the check box to enable compression for IPsec tunneling.
10. In the Rekey Time-out section, enter the time to which you want to limit the lifetime of a single key used to encrypt data. The default is 08:00:00 (8 hours).
11. In the Rekey Data Count section, you can choose to set a rekey data count depending on how much data you expect to transmit through the tunnel with a single key. The default is 0 KB; a setting of 0 disables this count.
12. Select Enable or Disable, depending on whether you want to allow IPsec Data Protection.

Configuring IPX

The Internetwork Packet Exchange (IPX) protocol is the Novell* adaptation of the Xerox Networking System (XNS) protocol. IPX has the following characteristics:

- It is a connectionless datagram delivery protocol. A datagram is a unit of data that contains all of the addressing information required for it to be delivered to its destination.
- It does not guarantee the delivery of packets. Higher-level protocols assume the responsibility for reliability.

The gateway supports IPX by encapsulating IPX traffic within PPTP client connections. Note that the gateway's IPX support is not available for the IPsec tunneling protocol.

IPX is the network-layer routing protocol used in the Novell NetWare* environment. The primary tasks of IPX are addressing, routing, and switching information packets from one location to another on a network. In a LAN-based client the network interface card (NIC) provides network node addressing; in a tunneled environment, the gateway provides the network node addressing.

Network addresses form the basis of the IPX internetwork addressing scheme for sending packets between network segments. Every network segment of an internetwork is assigned a unique network address by which routers forward packets to their final destination network. On the gateway, all public interfaces are treated as a single network segment with a unique network address. A network address in the NetWare environment consists of eight hexadecimal characters. In the following example, 0x indicates that this is a hexadecimal number, and *n* is any hexadecimal character.

`0xnnnnnnnn`

Socket numbers are the basis for an IPX *intranode address* (the address of an individual entity within a node). They allow a process (for example, IPX Routing Information Protocol [RIP] and Service Access Points [SAP]) to distinguish itself to IPX. To be able to communicate on the network, the process must request a socket number. Any packets IPX receives addressed to that socket are then passed on to the process within the node.

The gateway uses IPX RIP and SAP to dynamically learn and advertise IPX routes and services. The gateway assigns IPX addresses to tunneled clients; remote users cannot configure the IPX tunnel address for their systems.

The gateway does not forward IPX packets from a private nontunneled LAN to another private nontunneled LAN, nor does it propagate routing or server tables from a private nontunneled LAN to another private nontunneled LAN.

IPX client

On the PPTP client (for example, Microsoft Dial-Up Networking), you must enable the dial-up networking IPX option. Enabling the IPX option allows you to tunnel using IPX, IP, or IPX and IP according to the dial-up networking selections.

Windows 95 and Windows 98

When running Windows 95 or Windows 98, load the intraNetWare* client, which is available from the Novell Web site:

`http://www.novell.com`

Note: The NetWare client for Windows 95 and Windows 98 does not function properly; therefore, you must use the Novell intraNetWare client when using IPX with PPTP.

Windows NT

The NetWare client is already on Windows NT systems. You can use that or the Novell intraNetWare client, which you can access from the Novell Web site at http://www.novell.com.

IPX group configuration

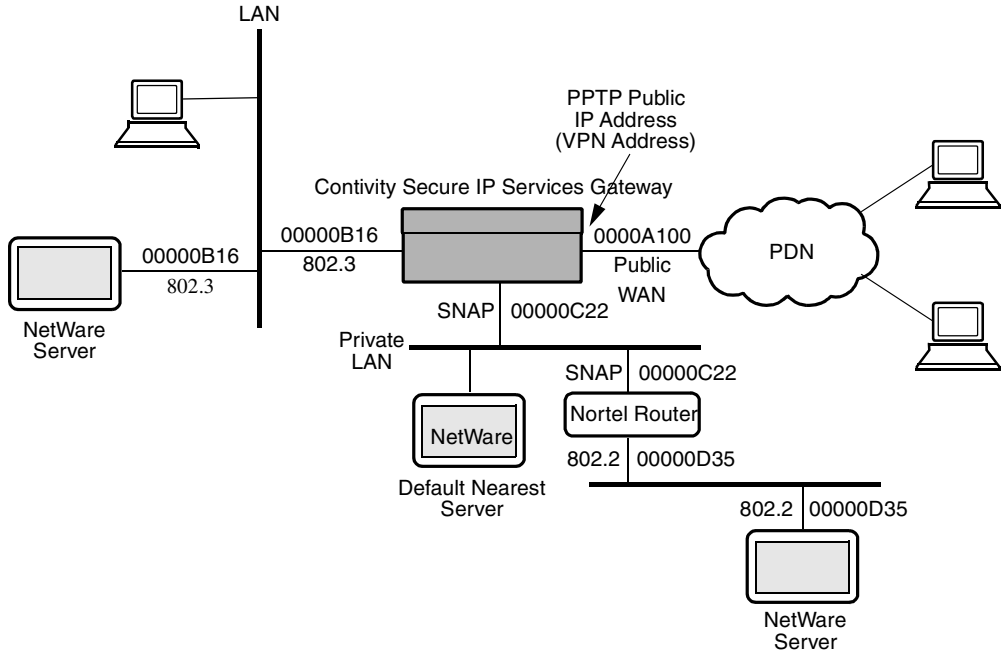
IPX is disabled on a per-group basis by default. Therefore, you must enable IPX for group users to access IPX. Enable IPX for group users from the Profiles > Groups > Edit > Connectivity screen.

Sample IPX VPN gateway topology

Regardless of the number of IPX public interfaces that are configured on the gateway, they all use the same IPX network address. You must enable the private interfaces that you want to use for IPX traffic, and for each private interface you must configure the IPX network address and IPX frame type. The IPX network address that you configure must match the IPX network address for that LAN, and the IPX frame type must match the IPX frame type for that LAN. In the following figure, the public interface IPX network address that the gateway provides is 0000A100.

In Figure 9, the private interface network address to the NetWare server is 00000B16 and the Frame Type is 802.3; similarly, the private interface network address to the Nortel Networks Router is 00000C22 and the Frame Type is SNAP.

Figure 9 IPX topology



Note: The Private LAN can also carry IP and IPX traffic simultaneously. The IP addresses are not shown in this figure.

Index

N

P

R

S

T

U

V

W