Version 4.80

Part No. 311642-G Rev 00
August 2003

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring Basic Features for the Contivity Secure IP Services Gateway

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

All rights reserved. August 2003.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and Contivity are trademarks of Nortel Networks.

Adobe, Acrobat, and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Macintosh is a trademark of Apple Computer, Inc.

AXENT is a trademark of AXENT Technologies, Inc.

Cisco and Cisco Systems are trademarks of Cisco Technology, Inc.

SafeNet is a trademark of SafeNet, Inc.

Linux is a trademark of Linus Torvalds.

Microsoft, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation.

Netscape and Netscape Communicator are trademarks of Netscape Communications Corporation.

intraNetWare, IPX, NetWare, and Novell are trademarks of Novell, Inc.

RSA and SecurID are trademarks of RSA Security Inc.

Java and JavaScript are trademarks of Sun Microsystems, Inc.

Ethernet is a trademark of Xerox Corporation.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface 13

Before you begin 13
Text conventions 13
Acronyms 15
Related publications 16
How to get help 18

Chapter 1
Overview 19

Network deployment alternatives 19
Virtual private networking 20
Licensing features 21
Command line interface 22
Federal Information Processing Standard (FIPS) 22

Chapter 2
Getting started 23

IP addressing 23
Using the IP Address Configuration utility 25
Configuring the serial interface 27
Changing the management IP address 31
Using boot modes 32
Managing through a Web browser 32
Preparing for configuration 33
Welcome screen 36
Setting up the Contivity 1010/1050/1100 39
Default configuration 39
Default configuration parameters 39

Branch office quick start utility 40
Enterprise environment 42
Service provider environment 43
Branch office quick start template 46
Connecting for Internet access 46
Compact flash disk 49

Chapter 3
Configuring the system 51

Configuring the system identity 51
Setting up LAN interfaces 53
Configuring circuitless IP 60
Setting up WAN interfaces 63
Configuring WAN interfaces 64
Configuring data rates on WAN interfaces 66
Configuring Network Time Protocol (NTP) 68
Using safe mode configuration 70
Using proxy ARP 73

Chapter 4
Configuring user tunnels 75

Configuring group characteristics 78
Setting up user tunnels 82

Chapter 5
Configuring branch office tunnels 91

Sample branch office configuration 95
Configuring a branch office 98
Sample branch office procedure 104

Chapter 6
Configuring control tunnels 105

Control tunnel types 106
Restricted mode 108
Nailed-up control tunnels 108

Creating control tunnels 110
Creating a user control tunnel from the serial interface 113

Chapter 7
Configuring networks, domains, and client policies 115

Configuring networks 115
Configuring domains 117
Client policy 118

Appendix A
Branch office quick start template 121

Glossary 123

Index 131

Figures

Figure 1 Typical PDN 20
Figure 2 VPN service models 21
Figure 3 Sample IP addressing scheme 24
Figure 4 Welcome screen 37
Figure 5 Default configuration 39
Figure 6 Branch office quick start 46
Figure 7 System Identity screen 52
Figure 8 LAN-to-Contivity connection 54
Figure 9 LAN Interfaces screen 57
Figure 10 CLIP network topology 61
Figure 11 Configure circuitless IP 62
Figure 12 Routing policy screen 63
Figure 13 Contivity-to-PDN configuration 64
Figure 14 WAN Interfaces screen 65
Figure 15 Data rates 66
Figure 16 Date and Time screen 68
Figure 17 Switch Settings screen 71
Figure 18 Forwarding screen 74
Figure 19 Tunnel connection configuration 75
Figure 20 Groups Edit screen 79
Figure 21 Services screen 84
Figure 22 Add Groups screen 85
Figure 23 Add User screen 87
Figure 24 User Management screen 89
Figure 25 Typical branch office environment 92
Figure 26 Branch-to-branch with a firewall and a router 93
Figure 27 Indirectly connected branch offices 94
Figure 28 Sample branch office configuration 96
Figure 29 Setting up a branch office configuration 97

Figure 30 Branch office screen 99
Figure 31 Connection configuration screen 101
Figure 32 Branch office control tunnel 106
Figure 33 Sample control tunnel environment 107
Figure 34 Edit Connectivity screen 110
Figure 35 Editing networks 116
Figure 36 Editing domains 118
Figure 37 Client policy screen 119

Tables

Table 1 Configuration options 23
Table 2 Sample IP addressing associations 24
Table 3 Web interface configuration options 33
Table 4 Configuration checklist 34
Table 5 Subnet assignments 43
Table 6 BOQS parameters 45

Preface

This guide introduces the Nortel Networks* Contivity* Secure IP Services Gateway. It also provides overview and basic configuration information to help you initially set up your Contivity Secure IP Services Gateway.

Before you begin

This guide is for network managers who are responsible for setting up and configuring the Contivity Secure IP Services Gateway. This guide assumes that you have experience with windowing systems or graphical user interfaces (GUIs) and familiarity with network management.

Text conventions

This guide uses the following text conventions:

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

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

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

Acronyms

This guide uses the following acronyms:

ACK	acknowledgement
CA	certificate authority
CHAP	Challenge Handshake Authentication protocol
CRL	certificate revocation list
DN	distinguished name
DNS	domain name system
EAC	Extranet Access Client
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
IP	Internet Protocol
IKE	IPsec Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet service provider
L2TP	Layer2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
LAN	local area network

MAC	media access control address
NAT	network address translation
NOC	network operations center
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSS	operations support systems
PAP	Password Authentication Protocol
PDN	public data networks
POP	point-of-presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RSVP	Resource Reservation Protocol
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

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 Authentication and Certificates for the Contivity Secure IP Services Gateway* provides instructions for configuring authentication services and digital certificates.

- *Configuring Firewalls and Filters for the Contivity Secure IP Services Gateway* provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- *Configuring Tunneling Protocols and Advanced WAN Settings for the Contivity Secure IP Services Gateway* provides instructions for configuring the tunneling protocols IPsec, L2TP, PPTP, and L2F, as well as instructions for configuring PPP, frame relay, PPPoE, and advanced WAN settings.
- *Configuring Routing for the Contivity Secure IP Services Gateway* provides instructions for configuring RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Reference for the Contivity Secure IP Services Gateway Command Line Interface* provides syntax, descriptions, and examples for the commands that you can use from the command line interface.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

You can purchase printed books and documentation sets from Vervante. To order printed documentation, go to Vervante at the www.vervante.com/nortel URL.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

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

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

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
Overview

This chapter introduces the Nortel Networks Contivity Secure IP Services Gateway. The Contivity Secure IP Services Gateway is a family of products that deliver security and IP services in a single integrated platform. With IP routing, Virtual Private Networking (VPN), stateful firewall, policy management and QoS services, a single Contivity device offers the IP services that normally require multiple purpose devices. Designed for enterprise networks, the Contivity leverages the cost advantages of the Internet while providing secure communications across the public IP infrastructure.

As a highly scalable device, the Contivity can address the security and IP services needs of the smallest branch site or largest headquarters environment. A Contivity can be installed as an IP access router, VPN gateway, or stateful packet firewall.

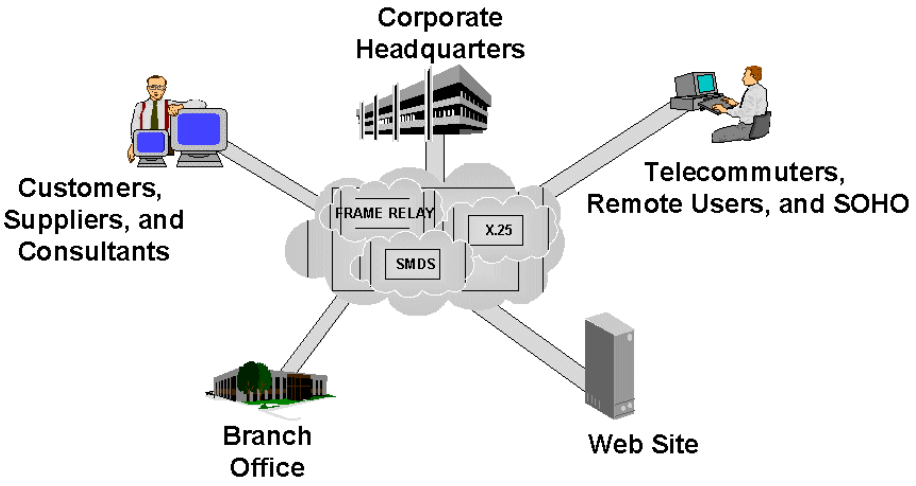
The Contivity Secure IP Services Gateway incorporates Nortel Networks Secure Routing Technology (SRT). SRT is a software framework that provides a security structure through all Contivity operational components, including IP routing, VPN, firewall, and policy services. This allows for management consistency and scalable performance even when running multiple IP services in the same device. SRT also provides dynamic routing (RIP/OSPF) over secure IPsec tunnels, uniform security policies across VPN, routing, and firewall services and a flexible software licensing scheme.

Network deployment alternatives

With its combination of secure, manageable, and scalable features, you can shift information technology resources from solving the current remote user access problems to other, more proactive administrative and management areas. And you can eliminate modem-management pool problems from your organization and shift them to your extranet provider.

Extranet access allows remote users to dial in to an Internet Service Provider (ISP) anywhere and reach corporate headquarters or branch offices. The extranet provides remote users access to corporate databases, mail servers, and file servers. Figure 1 shows a typical packet data network (PDN).

Figure 1 Typical PDN



The Contivity allows ISPs to take over the role of point-of-presence (POP) providers of modem access. It improves performance while lowering overhead, which translates to significant corporate savings.

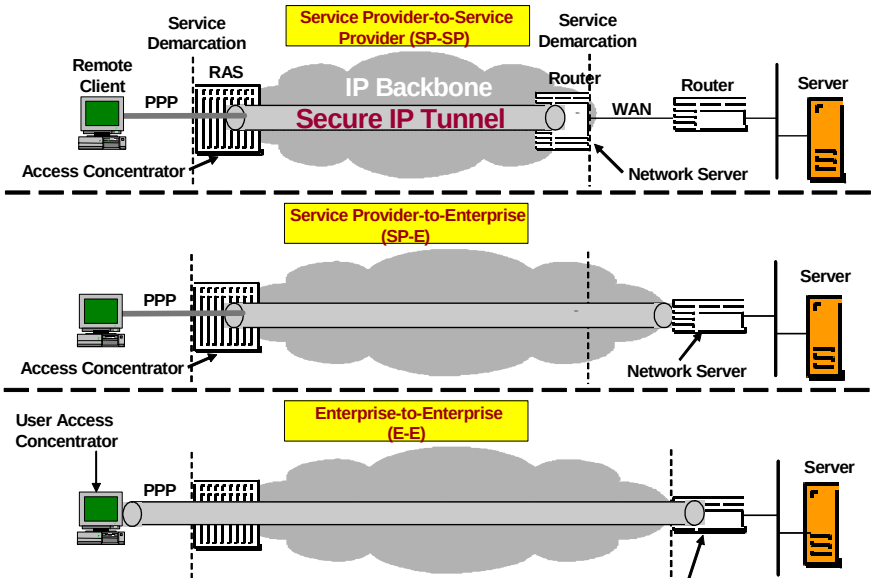
Virtual private networking

A VPN is a private data communication channel that uses a public IP network as the basic transport for connecting corporate data centers, remote offices, mobile employees, telecommuters, customers, suppliers, and business partners. Physically discontiguous networks are made to appear logically connected and contiguous.

A remote access VPN service requires the creation and operation of a secure tunnel between client software on a remote device, such as a PC, and host software on a VPN security gateway, such as a Contivity.

Figure 2 shows examples of VPN services.

Figure 2 VPN service models



The Contivity uses a combination of authorization, authentication, privacy, and access control for each user.

Licensing features

Licence keys can be obtained through Nortel Networks customer support. The Contivity Secure IP Services Gateway provides several license key options:

- Advanced Routing
- Contivity Stateful Firewall
- VPN Tunnels

The Advanced Routing License key must be installed to enable OSPF on the Contivity. (The Firewall License Key is required only when the redistribution capabilities of RIP and OSPF are necessary).

The Contivity Stateful Firewall License key must be installed to enable the Contivity Stateful firewall.

Tunnel keys are specific to the Contivity hardware model that you are using. Contivity switches are manufactured to allow either access to the maximum number of tunnels (VPN bundle) or support for 5 tunnels (Base Unit). This feature offers reduced cost for users who want fewer tunnels. The existing VPN bundle does not add a cost increase nor a need for a tunnel license key.



Note: It is only necessary to install a key once on each Contivity. To enter the license key, go to the Admin > Install screen. You must reboot the Contivity to gain access to the new tunnel limit.

Command line interface

The command line interface allows you to make configuration changes to the Contivity via Telnet. You can access the command line interface by initiating a Telnet session to the Contivity management IP address. For further information, see *Reference for Contivity Secure IP Services Command Line Interface*.

Federal Information Processing Standard (FIPS)

You must separately order, purchase, and implement a FIPS kit to be FIPS compliant. This kit contains detailed documentation concerning setting up, operating, and configuring the Contivity Secure IP Services Gateway to be FIPS compliant. The FIPS kit also includes tamper-resistant labels to be put on the hardware as instructed in the FIPS kit documentation.

Chapter 2
Getting started

This chapter describes methods for configuring and managing the Contivity Secure IP Services Gateway.

Full details on hardware installation, including adding local area network (LAN) or wide area network (WAN) cards, are in the *Getting Started* or installation guide that came with the Contivity. You should complete the hardware installation before starting this chapter.

Table 1 describes the choices you have when first configuring the required parameters. Either option allows you to set the management IP Address, subnet mask, and default Contivity (optional)

Table 1 Configuration options

Initial configuration method	Advantages and disadvantages
IP Address Configuration Utility (recommended)	Utility on the CD makes initial configuration easy
Serial Interface Configuration Menu (optional)	Must connect the serial interface cable

IP addressing

Figure 3 shows sample IP address assignments in a network using a Contivity. Refer to Table 2 to see the IP address associations.

Figure 3 Sample IP addressing scheme

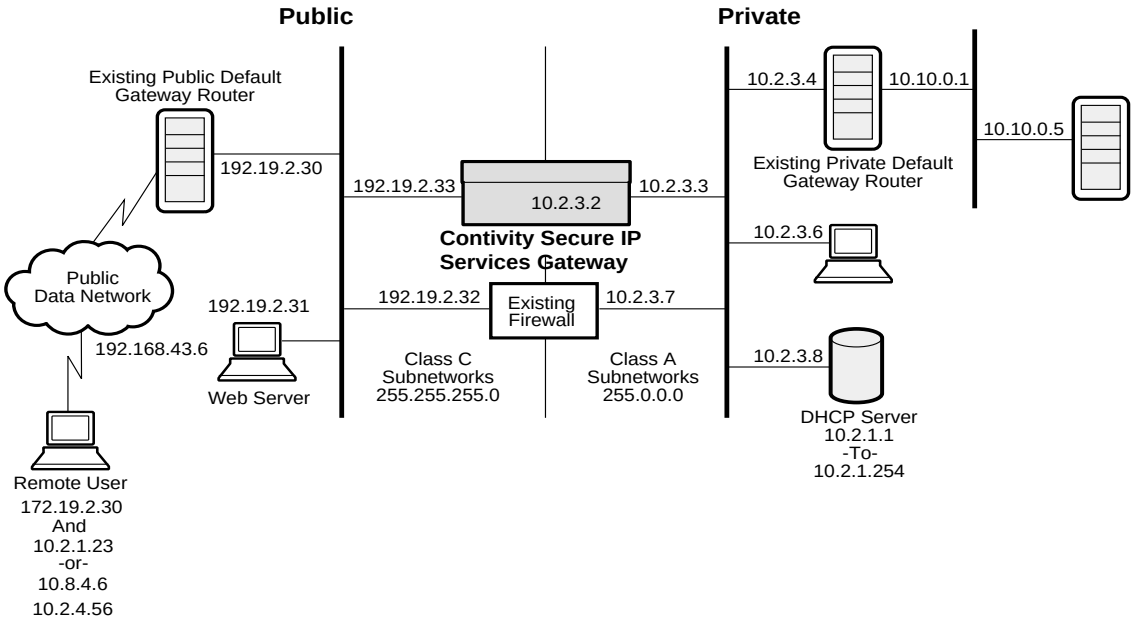


Table 2 Sample IP addressing associations

IP address	Description (when applicable, where configured)
192.168.43.6	Dial-up networking to ISP (Internet access, ISP assigned)
192.19.2.30	Public default Internet gateway router
192.19.2.33	Public LAN port IP address (remote user destination address)
192.19.2.32	Firewall public network address
10.2.3.2	Contivity management IP address: System→Identity
10.2.3.3	Contivity private LAN interface IP address: System→LAN Edit IP address
10.2.3.4	Private network default gateway router: System→Routing Add/Edit Default Route
10.2.3.6	Sample partners FTP server for inventory and price list
10.2.3.7	Firewall private network address
10.2.3.8	DHCP server IP address
10.2.1.1 to 10.2.1.254	Private Network Addresses Assigned to Remote Tunnel Sessions: DHCP pool: Servers→User IP Addr
172.19.2.30	ISP-assigned address

Table 2 Sample IP addressing associations (continued)

10.2.1.23	DHCP-assigned IP address for a remote user
10.8.4.6	Sample remote user static IP address: Profiles→Users Edit
10.2.4.56	Sample client-specified address: Profiles→Groups Edit IPsec/PPTP/ L2TP/L2F

The Contivity supports the Internetwork Packet Exchange (IPX) protocol. This allows the Contivity to transmit and receive IPX packets over PPTP.



Note: PPTP supports IPX traffic only for remote access connections. IPX is not supported in branch office tunnels.

The Contivity supports IPX by encapsulating IPX traffic within IP tunnels over PPTP. The private interfaces and public interfaces can carry IP and IPX traffic simultaneously. The IP addresses are not shown in the preceding illustration.

Using the IP Address Configuration utility

Nortel Networks provides a convenient utility to perform the initial configuration of the Contivity Secure IP Services Gateway. The program ExtNetIP.exe is included on the Contivity Secure IP Services Gateway CD. Copy the utility to your hard disk and execute it from there. The ExtNetIP.exe program launches the IP Address Configuration Utility, which allows you to assign a management IP address and subnet mask to the Contivity.

To use the IP Address Configuration Utility you must have the following:

- A PC running Windows 95, Windows 98, Windows NT, or Windows 2000 with a functioning TCP/IP stack. To test the function of your TCP/IP stack, send a ping command to any host.
- The PC must be running on the same subnet as the Contivity that is to be configured, and it must have an operational network connection.

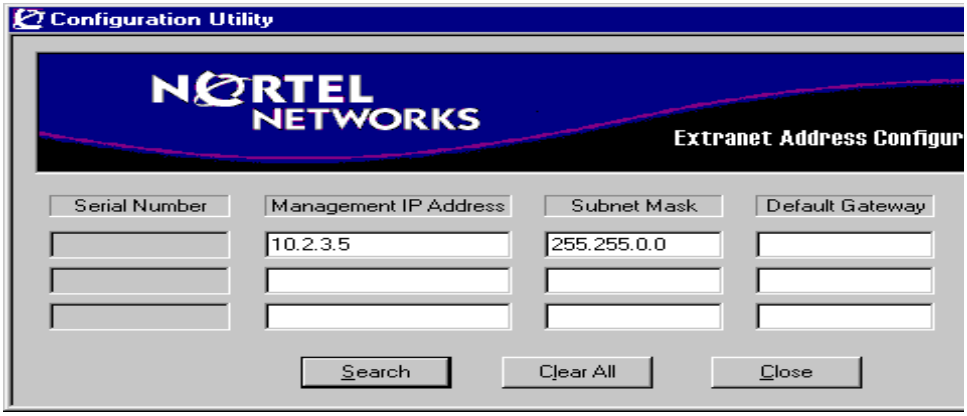
If your environment does not match these requirements, then you must use the serial interface configuration.

To run ExtNetIP.exe from the diskette:

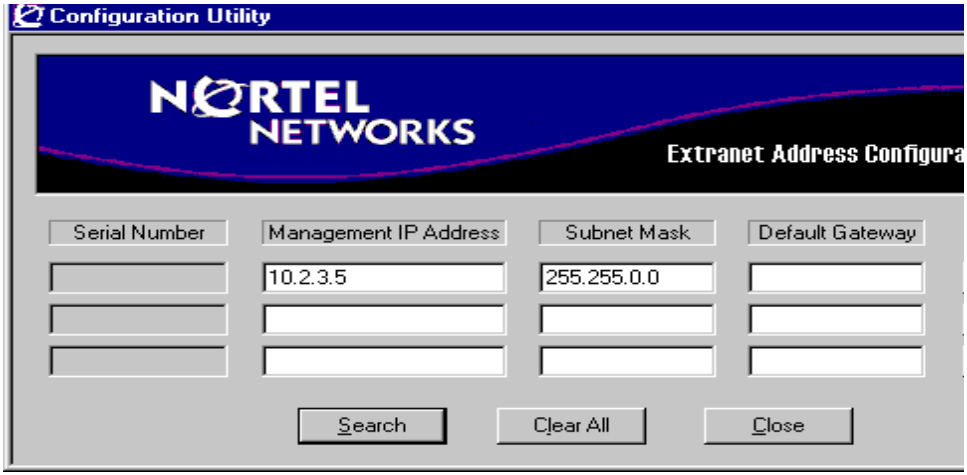
1 Insert the CD and locate ExtNetIP.exe in the tools folder and then double-click on the extnetip.exe icon.



The following screen appears while the program searches for a Contivity (and its serial numbers) that has not been configured with an IP address and subnet mask.



2 The program automatically enters the serial number for the first Contivity discovered into the table.



3 Assign a management IP address and subnet mask to the Contivity; the default Contivity address is optional and can be added later.

To add another Contivity to your network, click on Search to automatically add the Contivity serial numbers. To verify the any Contivity that has been discovered, refer to the serial number bar code on the rear of the Contivity.

4 Click Apply to configure the management IP address, subnet mask, and default gateway on the Contivity. The IP address Configuration Utility screen disappears.

Note: If you move the Contivity from one network to another, change the management IP address and Subnet Mask accordingly.

You can obtain help from the extNetIP.hlp file, which is the IP Address Configuration Utility Help file.

Configuring the serial interface

The Serial Interface allows you to give the Contivity a management IP address and subnet mask so that you can then use a Web browser for management. As an alternative to the Serial Interface configuration, you can use the Nortel Networks IP Address Configuration Utility, which Nortel Networks recommends for an initial configuration.

Your terminal emulator must use the following communications parameters:

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

The Serial Interface configuration procedure is typically only necessary in a system recovery situation.

1. Connect the serial cable (supplied with your Contivity) from the Contivity's serial port to a terminal or a communications port of a PC.
2. Power on the terminal or PC.
3. Using a terminal emulation program, such as HyperTerminal on the PC, click on Enter. The Welcome screen appears and you are prompted to supply a user name and password.

```
Welcome to the Contivity VPN Switch
Copyright 1999,2000,2001 Nortel Networks
Version: V03_50.44
Creation date: Dec. 7, 2000, 20:51:06
Date: 04/27/2001
Unit Serial Number: 17563

Please enter the administrator's user name: admin

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

   The factory default user name is *admin* and the default password is *setup*.

   Before moving the Contivity from one network to another, change the management IP address, subnet mask, and default Contivity. Otherwise, you will need to follow the Serial Interface configuration procedure to access your Contivity because it will not be accessible from a Web browser with an invalid address.

   Before proceeding, verify that you have selected a management IP address that can be routed on the subnet attached to the private interface of the Contivity and have this information available.

4 After the user name and password have been entered, the following 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):_
```

5 Enter **1** and click on **Enter** to enter the Interface menu:

```
Interface Menu

0) Slot 0, Port 1, Private LAN
   Management IP Address = 11.0.0.100
   Subnet Mask = 255.0.0.0
   Interface IP Address = 11.0.0.10 (Subnet Mask = 255.0.0.0)
   Speed/Duplex = AutoNegotiate

1) Slot 1, Port 1, Public LAN
   IP Address = 192.168.1.20
   Subnet Mask = 255.255.255.0
   Speed/Duplex = AutoNegotiate

R) Return to the Main Menu.

Please select a menu choice:_
```

6 Select **0** and click on **Enter** to enter the Slot 0, Port 1, Private LAN menu and add the management IP address.

The default settings appear, followed by the Configuration menu for the management IP address. The Old Management IP Address field is blank on a new Contivity.

```
Slot 0, Port 1, Private LAN
  Interface IP Address =
  Subnet Mask = 0.0.0.0
  Speed/Duplex = AutoNegotiate

  * Type 0.0.0.0 to delete.

Old Management IP Address =
New Management IP Address =
```

If you are prepared to assign a management IP address to the private interface, do so at this time at the New Interface IP Address prompt and click on Enter. If you do not wish to assign a private IP address at this point, simply click on Enter.

```
Old Interface IP Address =
New Interface IP Address =
```

7 The subnet mask menu will appear next. Enter the desired subnet mask and click on Enter.

```
Old Subnet Mask = 0.0.0.0
New Subnet Mask =
```

The Interface Configuration menu appears. Select the menu option desired and click on Enter.

8 Follow the screen prompts. The descriptions of the fields required to complete this procedure are in the “Startup configuration requirements” section at the beginning of this chapter.

9 After you complete the configuration, type E and click on Enter to save the settings and exit. You can then manage the Contivity from a Web browser.



Note: This administrator’s password is also the primary administrator’s password. This password guarantees access to the Contivity via the serial port or a Web browser. This administrator’s user ID (default=admin) and password (default=setup) combination is also called the *primary administrator*. This person always has access to all screens and controls, including the serial port and the recovery disk. There can be only one primary administrator.

Changing the management IP address

The management IP address must reside on a defined subnet. If there are no defined subnets, the management IP address can reside on any one that you create. You cannot change your management IP address to a subnet different from an already defined subnet.

To change the management IP address when an interface IP address is defined:

1. Select Option 1 Interfaces and then select 0.
2. Select Option 3 Default Private Route.
3. Select Option 1 Interfaces.
4. Go through the menu again and change the management IP address to the address that you want.

To reset the Contivity IP address values using the serial interface:

- Change the management IP address, subnet mask, or Contivity address to another set of values on the same logical network.
- Move the Contivity to a different logical or physical network.
- Completely reset the management IP addresses.
- Reset the Contivity so that it can be moved to a currently unknown logical network, which allows the network administrator to reuse the Address Configuration Utility to assign new addresses to the Contivity when it gets there. You might use this option if you do not know the addresses in advance.

To change IP addresses or move the Contivity to another network:

1. Log in to the serial interface.
2. Select Option 3 (Switch IP Address). Set the address to 0.0.0.0.
3. Select Option 1 (Management IP Address). Set the address to 0.0.0.0.
4. Choose E.
5. Wait at least 15 seconds. Serial interface data is only written to the hard disk at 15-second intervals.

Using boot modes

The Contivity can be booted in one of the two system modes: Safe mode or Normal mode. Each mode has its own software image, configuration files, and LDAP database.

A system booted in Safe mode is only allowed to accept secured management tunnel establishment. When the secured management tunnel is established, Telnet, HTTP, and FTP traffic is allowed to come into the Contivity; no other VPN traffic is allowed through the secured management tunnel or the Contivity.

In Normal mode, the system operates with the normal software and configuration and transports both VPN traffic and management traffic.

To save your configuration into the Save Mode boot directory:

1. Select B) System Boot options.
2. Select 2) System Reset options.
3. Select 1) Reset system to Normal Mode.
4. Select 2) Reset system to Safe Mode.

Managing through a Web browser

Upon completion of running the IP address configuration utility or using the serial interface configuration, launch a Web browser of your choice.

1. Enter the management IP address to invoke the Nortel Networks Login screen. For example, if the management IP address is 10.2.3.2, then the Uniform Resource Locator (URL) is http://10.2.3.2.
2. Select an option in the navigational menu and submenu, and then you are prompted for the login and password.
3. Enter the system default login and password in lowercase characters, as follows:

   Login: **`admin`**
   Password: **`setup`**

At this point, follow the Quick Start Configuration procedure or the Guided Configuration procedure. Refer to Table 3 on page 33 for help in determining which procedure to use.

Preparing for configuration

To properly prepare for configuration of the Contivity Secure IP Services Gateway, you should have the following items available:

- A plan to distribute IP addresses to clients when connections are requested; for example, via a DHCP server or an internal client address pool (with an address pool you need a range of IP addresses).
- An Authentication database: If you are not using internal authentication via the LDAP database, then make sure you have either the external LDAP or the RADIUS server's IP address and password or Shared Secret (password).
- An external accounting server, such as RADIUS, with its IP address and Shared Secret (password).
- Client dial-in: Prepare the clients for the type of tunneling protocol they need to use. The PPTP client application is available on the Nortel Networks CD for Windows 95, and it comes with Windows 98 and Windows NT. Nortel Networks also provides the IPsec client on the Nortel Networks CD.
- A complete network topology of the environment in which you are testing the Contivity, including the Contivity address, the default router address, and any other IP addresses that you think might be required.

Table 3 shows the alternatives when first configuring your Contivity. Begin with either the Quick Start or the Guided Configuration. After you are familiar with the Contivity's navigational menu and capabilities, select Manage Switch.

Table 3 Web interface configuration options

Configuration type	Results
Quick Start	Configure and test a basic PPTP configuration
Guided Config	Structured Contivity configuration and management
Manage Switch	Comprehensive Contivity configuration and management

Table 4 provides a place for you to record the information that you need to configure basic Contivity Secure IP Services Gateway parameters.

Table 4 Configuration checklist

Screen	Values required	Your Values
System > Identity	Management IP address	
System > Domain Identity	Host name Domain name	
System > DNS Service	Primary IP address Secondary IP address Tertiary IP address	
System > LAN	Private IP address Public IP address	
System > WAN (if using T1, V.35, or T3)	ISP provided information	
System > Date and Time	Manual entry of date and time or NTP configuration server broadcast or multicast IP address	
Services > Available	IPsec private address IPsec public address PPTP private address PPTP public address L2TP and L2F public address L2TP and L2F private address	
Services > Management	HTTP private address HTTP public address SNMP private address SNMP public address FTP private address FTP public address TELNET private address TELNET public address CRL retrieval private address CRL retrieval public address	
Routing > Static Routes Enabled/Disabled	Public Contivity IP address Private Contivity IP address	
Routing > OSPF Enabled/Disabled	Router ID AS boundary router (true or false)	

Table 4 Configuration checklist (continued)

Screen	Values required	Your Values
Routing > Rip Enabled/ Disabled	True or false	
Routing > Interfaces LAN IP Address	OSPF (enabled or disabled) RIP (enabled or disabled) VRRP (enabled or disabled)	
Servers > Radius Auth	Access (enabled or disabled Server-Supported Option (enabled or disabled) Radius Servers (enabled or disabled) Primary host name or IP addresses, public or private, Port, Shared secret/confirmed Alternate 1 host name or IP addresses, public or private, Port, Shared secret/confirmed Alternate 2 host name or IP addresses, public or private, Port, Shared secret/confirmed	
Servers > LDAP	Internal or external Base DN Master IP address, port or SSL Bind DN, Bind password, Confirmed Slave 1 IP address, port or SSL Bind DN, Bind password, Confirmed Slave 2 IP address, port or SSL Bind DN, Bind password, Confirmed	
Servers > User IP addr	Broadcast Any DHCP or DHCP servers: Primary IP address Secondary IP address Tertiary IP address Address pool: Pool name Start End Subnet mask	

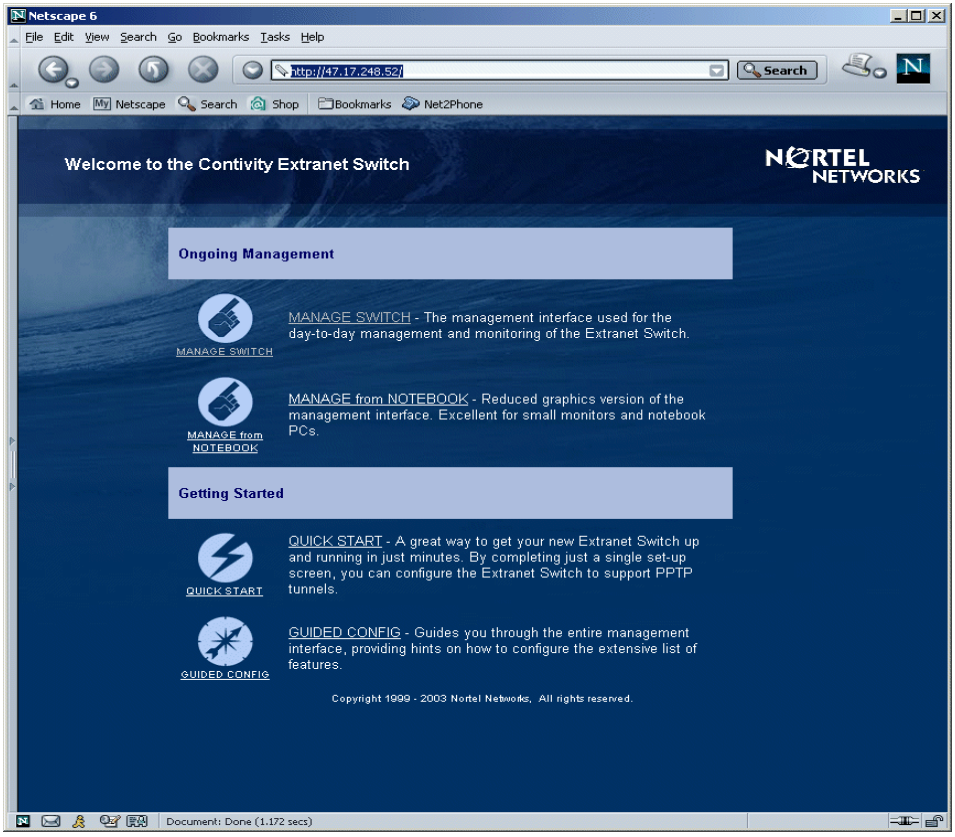
Table 4 Configuration checklist (continued)

Screen	Values required	Your Values
Admin > Key Installation	Advanced routing install key Contivity Stateful Firewall install key	
Admin > Auto Backup	Automatic Backup file servers IP address of FTP servers for backup: Host Path User ID Password	

Welcome screen

The Welcome screen (Figure 4) allows access to any of the configuration areas for the Contivity Secure IP Services Gateway.

Figure 4 Welcome screen



Before entering the configuration options, first register your Contivity to activate licenses, warranties, and services.

To start using your Contivity, choose from one of the following options:

- Click on Manage Switch to begin a configuration management session. This option allows access to all Configuration Management facilities. For your first configuration, follow the Quick Start or Guided Configuration.
- Click on Manage from Notebook to run the Contivity Secure IP Services Gateway Manager in notebook display mode.

- Click on Quick Start to begin the Quick Start Configuration. This option allows you to configure interfaces, set up PPTP tunnels for up to three users, and establish a connection to the Contivity. If you prepare for the configuration as recommended, the Quick Start can take as little as 15 minutes to complete.
- Click on Guided Config to begin the Guided Configuration. This option allows access to all Configuration Management facilities. The design and structure of the Guided Configuration, however, is such that you might want to follow the top-to-bottom layout provided. This approach walks you through the entire navigational menu from the Profiles to the Admin selections.

  Each functional area begins with a summary of the objectives of the area and then steps you through the area (for example, profiles), one subsection at a time. Context-sensitive help is available at each subsection to supplement the summary.

  Provided you have the information required to set up the Contivity, the Guided Configuration is estimated to take two to three hours to complete, depending on how extensive your configuration is.
- Click on Register Online to register the Contivity with Nortel Networks. It only takes a few minutes and it gives you access to the latest software and technical tips. Your Contivity requires Internet access from the private interface in order to register.

The Contivity's navigational menu options include the top-level configuration and monitoring areas of the Contivity. Each of these key areas has secondary levels, which appear once you click on an area; for example, when you click on System, the secondary level listings appear. The menu is structured to provide system configuration details, followed by profiles for groups and users. Then you can configure authentication servers, secure tunnels, administrative details, and monitor the status of the Contivity.

Setting up the Contivity 1010/1050/1100

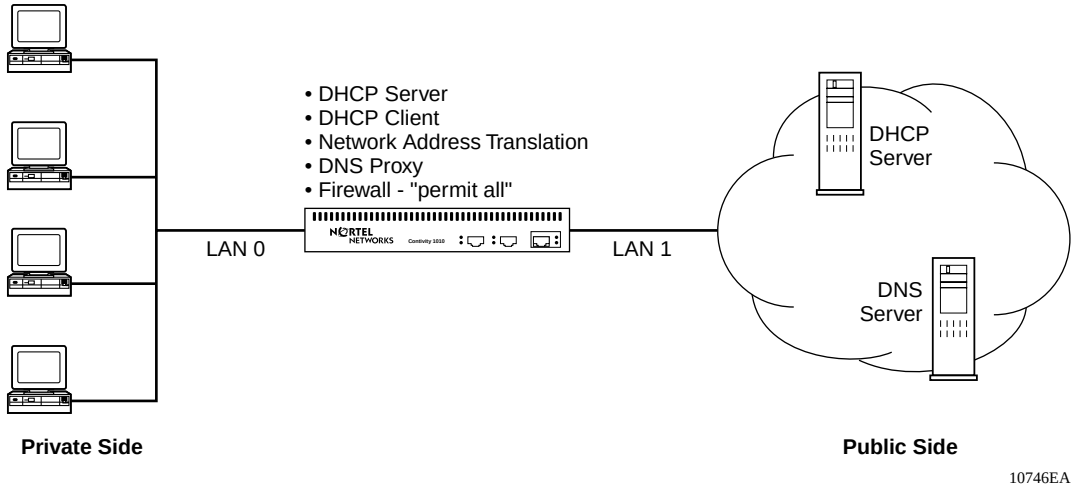
The Contivity 1010, 1050, and 1100 series of switches provides support for five (5) tunnels at introduction and 30 tunnels for licensing. The maximum tunnels include the sum of all branch office, client, and management tunnels combined. For example, if one management tunnel and two branch office tunnels are open, only two client tunnels can be connected initially (27 client tunnels with the 30 tunnel license). The license is for 25 additional tunnels. LDAP supports 150 entries.

Default configuration

The Contivity 1010, 1050, and 1100 series use a unique default configuration to simplify setup in the small office or home office environment.

Figure 5 show a typical default configuration.

Figure 5 Default configuration



Default configuration parameters

By default, the Contivity 1010, 1050, and 1100 are configured with the following parameters:

- The DHCP server is configured on the switch's private interface, with a default range of 192.168.1.3/24 to 192.168.1.255/24. By default, 192.168.1.1 and 192.168.1.2 are assigned to the branch office switch's private and management interfaces, respectively. The DHCP server provides its own address for the DNS server and default Contivity.
- The DHCP client is configured on the switch's public interface to retrieve its IP address from the ISP's DHCP server. Other parameters retrieved from the DHCP server should include the default Contivity and the DNS server.
- DNS proxy is configured to forward DNS requests to an external DNS server. The address of the DNS server is obtained during startup from the ISP's DHCP.
- Network Address Translation (NAT) translates the private IP address space (determined by default configuration of the DHCP server) into one public address assigned to the public interface by your ISP.
- Port NAT maps multiple IP addresses in the private space to a single public IP address. The default configuration only supports initiating IP sessions from the private side of the switch, which reduces security risks.
- The Contivity Interface Filter is set as the default firewall.
- The firewall setting PermitAll is the default for both the public and private interfaces. This default is different from the DenyAll default setting for other Contivity VPN switches.

Branch office quick start utility

The branch office quick start utility (BOQS) simplifies deployment of Contivity in the branch office environment. BOQS converts the Contivity 1010, 1050, or 1100 device from an Internet access gateway into a secure access gateway by provisioning a VPN connection to a central office or optionally, to a network operation center (NOC). BOQS allows a NOC or central office management to access the Contivity 1010, 1050, or 1100 so that network administrators can further configure the these units without going to the remote site.

Network administrators and service providers can use the branch office quick start for provisioning IP-based VPN services on a large scale. It provides VPN services using Contivity 1010, 1050, or 1100 devices as branch office VPN switches and other Contivity VPN switches as central office switches.

In addition to connectivity, the central office switch must be able to accept newly created secure connections from the Contivity 1010, 1050, or 1100. Therefore, the BOQS must be used with the knowledge and approval of a network administrator. It can only be initiated after IP addressing has been planned and the central office switch has been configured. Then you can send the provisioning parameters to the remote branch office locations.

The Contivity 1010, 1050, and 1100 must be connected to a public network and have access to the Internet before local users can use BOQS. The unique default configuration allows easy deployment of Contivity 1010, 1050, and 1100 switches in DHCP configurations (where a DHCP server is used on the public network). However, if you use static IP addressing or PPPoE on the public side, the Contivity 1010, 1050, or 1100 must be configured manually before local users can use BOQS.

All users on the private network must renew their IP addresses. For further information, see your Microsoft documentation. When the branch office tunnels are established, public access to the Internet is replaced with access to the central office.



Note: The BOQS will remain accessible after the information is entered. The network administrator must change the admin account (**username**/**password**) to restrict access.

After the VPN services are provisioned, branch office networks are logically connected to a central office network or to a NOC network. Branch office end users can rerun BOQS multiple times to restore the initial VPN configuration or to fix data errors.

BOQS supports two network topologies:

- Enterprise topology where the network operations center is located within the central office.
- Service Provider topology where the network operations center is independent entity from central office

Enterprise environment

Enterprises rely on the Internet for a wide range of business operations. Locating a Contivity VPN Switch at the central office and Contivity 1010/1050/1100 series of switches at the branch office locations provides a secure solution. Before you deploy the Contivity 1010, 1050, or 1100 switches at the local sites, you must configure configure routing and tunnels on the switch at the central office.

For routing, you must do the following:

- Enable global RIP service.
- Enable RIP on private interface.
- Disallow importing default routes in the group where responder tunnels are created.
- From the CLI, use the following command:

```
router rip
network a.b.c.d m.m.m.m
exit
```

For tunnels, you must do the following:

- Create one responder tunnel for each branch office Contivity 1010/1050/1100 device.
- Set the Connection Type to Responder.
- Be sure that the Control Tunnel option is NOT selected.
- Determine the connection name for the tunnel. Nortel Networks recommends that the name be the same as the initiator ID, but it could be the same as the central office tunnel name.
- Set the state to Enabled.
- Set the Local Filter to permit all.
- Set IPSEC Authentication to Text Pre-Shared Key.
- Set the Initiator ID to the same name as the central office tunnel name.
- Set the Text Pre-Shared Key to the same name as central office tunnel password.
- Set Dynamic Routing to enabled.
- Set RIP to enabled.

After the central office setup and the BOQS are complete, the Contivity 1010, 1050, or 1100 is directly accessible from the central office. This means that there is just one hop between the central office and the branch office. RIP propagates routes to this subnet across the tunnel created by BOQS.

You must have at least two more IP addresses than IP workstations on the Contivity 1010, 1050, or 1100 private network. The first address from the subnet is assigned to the private interface of the branch office switch and the second address becomes the management IP address of the switch. Each branch office must be in its own subnet.

Table 5 shows how offices with approximately 50 workstations can each have subnets assigned.

Table 5 Subnet assignments

Private Network IP address	Private Network IP Mask	Contivity 1010/ 1050/1100 Private Interface Address	Contivity 1010/1050/ 1100 Management Interface Address	BO Workstations Addresses (assigned by DHCP Server)
200.1.1.0	255.255.255.192	200.1.1.1	200.1.1.2	From 200.1.1.3 to 200.1.1.62
200.1.1.64	255.255.255.192	200.1.1.65	200.1.1.66	From 200.1.1.67 to 200.1.1.126
200.1.1.128	255.255.255.192	200.1.1.129	200.1.1.130	From 200.1.1.131 to 200.1.1.190

Service provider environment

Service providers generally have an isolated NOC from which all devices are managed. The addressing scheme could be different from a central office and require a separate designated tunnel to configure the Contivity 1010/1050/1100 series of switches.

Every Contivity 1010, 1050, and 1100 must have a distinct IP address that is visible from the NOC subnet. A NOC can assign any address reachable from a NOC network to a Contivity 1010, 1050, or 1100. BOQS configures NAT on the NOC tunnel to translate the address specified in the “Branch office switch manage NAT IP address” and “management address from branch office private subnet.” If the field is empty, the NOC must use an actual management address to access the Contivity 1010, 1050, or 1100.

Because the NOC tunnel uses static routing, all Contivity 1010, 1050, and 1100 devices must be configured with a static route to the NOC private network. The NOC private address and NOC private mask fields are where a BOQS user enters this information. This information is the same for all Contivity 1010, 1050, and 1100 devices.

You must provision the NOC switch to accept control tunnel connections from the branch office. Because static routing is used in control tunnels, you do not have to enable routing protocols on the NOC switch. Use the following guidelines:

- All responder tunnels should be created in one group or in subgroups of one group for easy management. Connection Name of the tunnel should correspond to NOC tunnel name and created in an enabled state with local filter set to Permit All.
- Text Pre-Shared Key should be selected as the IPSEC authentication method, Initiator ID set to the value of Control Tunnel Name, and Text Pre-Shared Key should be equal to Control Tunnel password.
- Select Static routing. Accessible local networks should be added. All networks from which the Contivity 1010, 1050, or 1100 will be managed must be on that list.
- NAT Local option should NOT be used.
- Accessible Remote Networks should contain one address subnet (mask equal to 255.255.255.255) with Contivity 1010, 1050, or 1100 Management IP. Contivity 1010, 1050, or 1100 Management IP is either explicitly provided in the field “Branch office switch manage NAT IP address” or if this field is left empty, it is the second address from the subnet specified in the Branch Office Private IP Address and Mask fields.

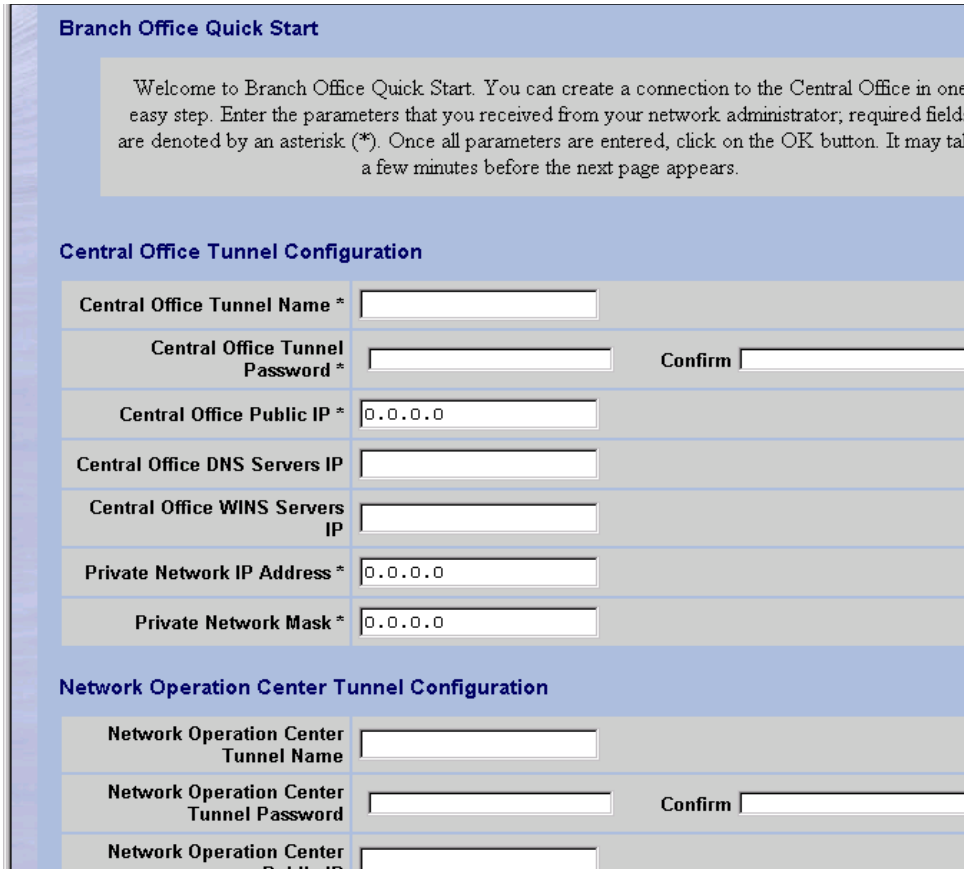
Table 6 contains the BOQS parameters.

Table 6 BOQS parameters

Central office tunnel configuration	
Central office tunnel name	Name of the branch office tunnel on the central office switch.
Central office tunnel password	Password for the branch office tunnel.
Central office public IP address	Public address of the central office switch (same for all branch offices).
Central office DNS server IP address	IP address of the DNS server in the central office. The DHCP server configured on private interface distributes this address to the branch office. You can configure multiple addresses, but you must separate them with commas. This field is optional and can be left empty.
Central office WINS sever IP address	IP address of WINS server in the central office. The DHCP server configured on private interface distributes this address to the branch office workstations. You can configure multiple addresses, but you must separate them with commas. This field is optional and can be left empty.
Private network IP address	Subnet address of the branch office network..
Private network mask	Subnet mask of the branch office network.
Network Operation Center tunnel configuration	
Network operation center tunnel name	Name of the branch office tunnel configured on NOC switch (same as initiator id on the NOC switch).
Network operation center tunnel password	Text pre-shared key used in branch office tunnel.
Network operations center public IP address	Public address of NOC switch (same for all branch offices).
Network operations center private network IP address	IP Address part of subnet address in which NOC is located (private subnet of NOC switch).
Network operations center private net mask	IP mask of subnet address in which NOC is located (private subnet of NOC switch).
Branch office switch management IP address	Address used by NOC to manage switch. Must be unique for each Contivity 1010/1050/1100 and reachable from the NOC. If left empty, can be managed with the second address of the subnet configured in branch office private network IP address/ IP mask field

Figure 6 shows the branch office quick start screen.

Figure 6 Branch office quick start



Branch office quick start template

The branch office quick start template provides a list of values that the local Contivity 1010, 1050 or 1100 users will need to enter on the BOQS screen. See Appendix A, "Branch office quick start template," for a copy of the template. You can enter the appropriate values in the right-hand column and then fax, send, or email the template to the local user along with any other information that they may need, such as who to contact for further information or questions.

Connecting for Internet access

This section provides information on how to set up the Contivity 1010/1050/1100 series of switches for basic Internet access through a cable or DSL modem.

To set up the Contivity 1010, 1050, or 1100:

1. Plug the power cord into an AC power outlet, plug the external power supply into the port on the back labeled DC Input, and then turn on the power switch.
2. Connect the cable or DSL modem to the LAN 1 (**public**) port located on the front panel using a standard Ethernet cable (not included with the Contivity unit).
   - To connect more than one PC or other devices to the Contivity 1050 or 1100, use standard Ethernet cables to connect to the LAN 0 (**private)** ports labeled A-D located on the front panel. To connect the Contivity 1050 or 1100 directly to the PC, use a standard Ethernet cable.
   - To connect more than one PC to the Contivity 1010, connect an Ethernet switch or hub to the LAN 0 port and then connect the PCs. To connect the Contivity 1010 directly to the PC, use the cable that ships with it.
3. Because the Contivity 1010/1050/1100 has the DHCP server enabled by default on the LAN 0 port, the PC should be set up to accept IP addresses that the DHCP server will assign the LAN 0 ports. For Microsoft* Windows* operating systems:
   a. Go to the Control Panel and click on the network connections icon.
   b. Select TCP/IP protocol, click on the Properties button, and then select the “Obtain an IP address automatically” option.
   c. Reboot your PC to obtain the new IP address (range 192.168.1.3 to 192.168.1.254).

   For other operating systems, see the user documentation for those systems.
4. Determine the type of addressing to use:

   By default, the LAN 1 port acts as a DHCP client, which receives an IP address from the public side. Launch a Web browser application to verify connectivity to the Internet.

   If you use Point to Point Protocol over Ethernet (PPPoE), you must use the Web-based management utility for advanced configuration options to enable it:

   a. Open the Web browser and type http://192.168.1.2. Click on Manage Switch and enter **admin** and **setup** as the username and password.

b Go to the System > LAN screen, select Cancel Acquision, select PPPoE from the Select Protocol list, and click on Apply. The Add PPPoE Interface screen appears.

c For Administrative State, click on Enable

d For Interface Filter, select permit all.

e Click on OK.

f Go to an external Web site to verify Internet access.

Alternatively, you can use the following CLI commands to configure PPPoE client (with username – abc and password xyz):

```
interface fastethernet 1/1
ip address type static # is it needed
pppoe ppp username abc password xyz
pppoe enable
exit
```

If you use static IP addressing, you must use the Web-based management utility for advanced configuration options to enable it:

a Open the Web browser and type http://192.168.1.2. Click on Manage Switch and enter **admin** and **setup** as the username and password.

b Go to the System > LAN screen, select Cancel Acquision, and then select IP from the Select Protocol list and click on Apply. The Add IP Address screen appears.

c Select the Static option

d For Interface Filter, select permit all.

e Enter the IP address and the subnet mask.

f Click on OK.

g Go to an external Web site to verify Internet access.

Alternatively, you can use the following CLI commands to configure the static address (for example, 47.17.2.23/24) and default Contivity (for example, 47.17.2.1):

```
interface fastethernet 1/1
ip address type static
ip address 47.17.2.33 255.255.255.0
ip route 0.0.0.0 0.0.0.0 47.17.2.1 enabled
exit
```

Compact flash disk

The Contivity 1010, 1050, and 1100 use a compact flash disk instead of a traditional hard disk that provides 32 MB of flash disk storage. Because of the limited storage capacity, the following functionality is not provided:

- Safe mode
- Java runtime plug-in
- Graphs
- Japanese strings
- Context-sensitive help

The help files are located on the CD and on the Nortel Networks documentation Web site. When you click on the Help menu from the UI, you can enter the location of the help files on a server.

File compression is used extensively on the Contivity 1010, 1050, and 1100. Compressed files will retain their original names and all existing directory operations that the software performs will continue to work. The following functionality is compressed:

- VXworks image
- All Web pages
- All scripts
- Numerous text files

Two software images can be stored on the flash disk at the same time. Operational changes for the compact flash disk are:

- The config file is saved every minute and the past three versions are kept. The config file is only written when the configuration changes.
- The on-disk system log (syslog) is not be supported. However, you can configure an external syslog server.
- No accounting information is stored on the compact flash disk. However, an external RADIUS accounting server is supported.
- The data collection log (DCLOG) is not supported, which means that the graphing capabilities of the UI are also not supported.

- The core is not saved on the compact flash disk. It is sent to an FTP server. Configuration parameters for the FTP server are stored in flash. The core file is placed on the server. To set up the FTP coredump, got to the FTP Coredump section of the Admin > Admintstrator screen, click on the Enabled checkbox and enter the appropriate FTP server information. Because many switches may be configured to coredump to the same location, the core files will have a more descriptive name: core*_date_24-hour-time_management_ip*.mem. For example, a core file generated by 10.0.8.186 on Oct.12th, 2001, at 4:46:06 PM will be named core_20011012_164606_10.0.8.186.mem.

Chapter 3
Configuring the system

This chapter describes how to configure various system-level features.

Configuring the system identity

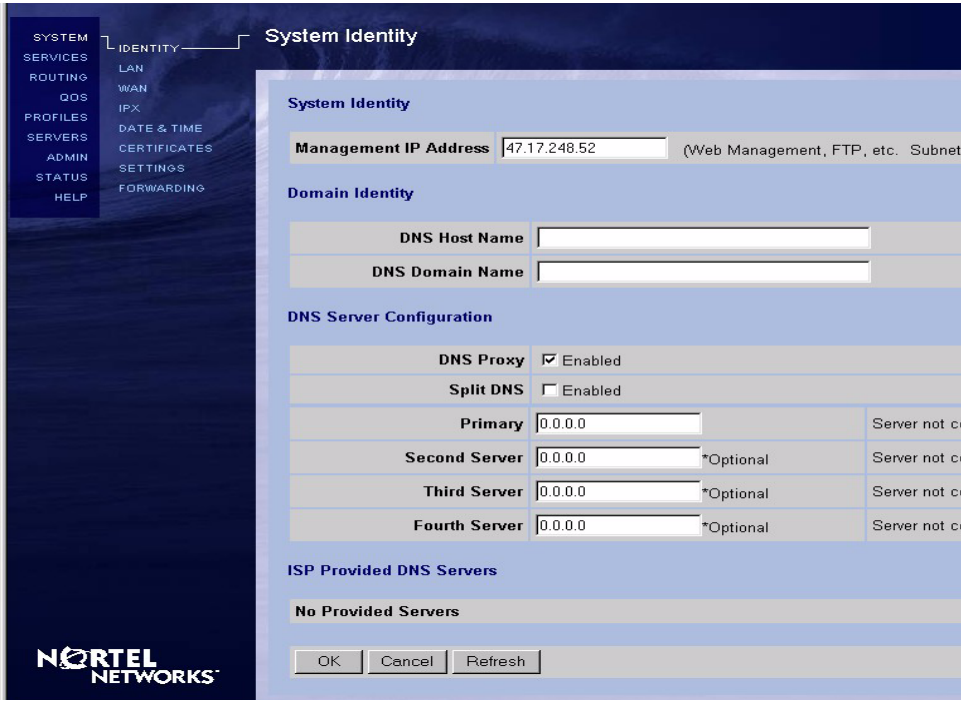
Each Contivity Secure IP Services Gateway is uniquely identified by the system's address and domain name system (DNS) name. The DNS name can be used instead of the IP address to identify the Contivity and launch its management interface through a Web browser.

The System Identity screen allows you to optionally change your Contivity Management IP address, and provide the DNS Host Name and Domain Name. Additionally, you can assign up to three DNS addresses to resolve IP address name resolution requests. You can also reset the Contivity Management IP address values using the serial interface.

To configure the System Identity:

1. Enter a Management IP Address for the system. You need this address to contact all system services, such as HTTP, FTP, and SNMP. To be accessible, the Management IP Address must map to the same network as one of the private interfaces. For example, if you are planning on assigning IP address 10.2.3.3 with the subnet mask 255.255.0.0 to the private physical interface, the Management IP Address must reside in the 10.2.x.x network.

Figure 7 System Identity screen



If you configure the Contivity on one network and plan to move it to another network, change the Management IP address and private LAN interface addresses before moving the Contivity. Then, communicate with the Contivity using the new Management IP address from your browser's URL address field.

2 Under Domain Identity, enter the DNS Host Name to identify the system. This should be the same name that is used by the DNS server to identify the management address of the Contivity that is located on your private network. You can enter up to 64 characters maximum.

3 Enter the Name of the Internet Domain into which this system is being placed. This must be the same Internet Domain as the System Name in the Domain Name System (DNS) server. A domain is a part of the Internet naming hierarchy that refers to general groupings of networks that are based on organization-type or geography. For example, mycompany.com is the domain name for a commercial (.com) enterprise.

4 Under DNS Server Address, enter the address of the DNS server that is located on your private network. The DNS server translates textual host names

into IP addresses. For example, DNS can translate the fully-qualified host name www.mycompany.com to its IP address192.19.2.33. The Primary DNS server is the first one addressed for servicing name resolution requests that are needed by the system; if the Primary DNS server is unavailable, service is requested of the Secondary DNS server. This is the DNS entry that management tools use to resolve names in configurations. Always use the IP address for setting a DNS server host instead of a domain name.



Note: If no DNS servers are specified, management requests that are using names rather than network addresses fails.

5 Enter an address for the Secondary Domain Name System (DNS) server. If the Primary DNS server is unavailable, service is requested of the Secondary DNS server (if present).

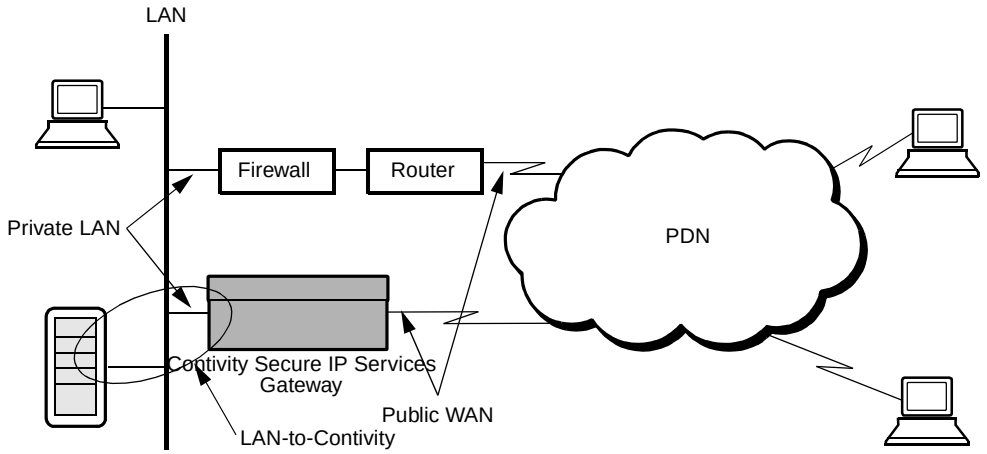
6 Enter an address for the Tertiary Domain Name System (DNS) server. If the Primary and Secondary DNS servers are unavailable, service is requested of the Tertiary DNS server (if present).

Setting up LAN interfaces

The LAN interface that is available on the system board is configured to be private by default. Connect its interface to your corporate LAN. Additional interfaces that are inserted into the expansion slots are public by default.

The private LAN interface and the management IP address must be on the same network, and the public LAN interface should be on a different network, both physically and logically. If your Contivity has a single network interface and you want to position the Contivity behind the firewall and router, then you should set the Contivity's interface type to private. Figure 8 shows a connection from a LAN to a Contivity.

Figure 8 LAN-to-Contivity connection



A host can send only enough packets to a public interface to establish a tunnel connection. If the tunnel is not established before a preset maximum number-of-packets-allowed counter is reached, then the packets from that host are discarded.

Public indicates that this interface is attached to a public data network like the Internet. The Contivity rejects nontunneled protocols and only accepts tunneled protocols like IPsec, PPTP, L2TP, L2F, and diagnostic ping on a public interface. A host can send only enough packets to a public interface to establish a tunnel connection. If the tunnel is not established before a preset maximum number-of-packets-allowed counter is reached, then the packets from that host are discarded.

When the public interface is configured to act as a DHCP client, the DHCP client needs to correspond to an external DHCP server to acquire the IP address, subnet mask and default route parameters. You can set a cost value to give preferential routing when two or more public DHCP clients are configured. In this situation, DSL and cable modem are the preferred choice for connections to the internet.

Private indicates that an interface is attached to the private network and it can accept nontunneled networking protocols such as TCP/IP, FTP, and HTTP. The Private interface also accepts tunneled protocols (for example, IPsec, PPTP, L2TP, L2F) that can be used for secure management access to the Contivity.



Note: The private LAN interface and the management IP address should be on the same network, and the public LAN interface should be on a different network, both physically and logically.

If you have one network only and want to position the Contivity behind the firewall and router, then you should use a private LAN interface only (do not use a public LAN interface).

From the System > LAN screen, you can:

- Click on Configure to modify the interface characteristics.
- Click on Statistics to view the Link Statistics.
- From the Select Protocol list, select the tunneling protocol to use: IP is the standard Internet Protocol. and Point to Point Protocol over Ethernet (PPPoE) allows PPP to run over Ethernet.



Note: You cannot use dynamic routing on PPPoE interfaces. DHCP is configured by default on the Contivity 1010, 1050, and 1100 so you must first first select Cancel Acquision and then select PPPoE from the Select Protocol menu. You can use PPPoE on only one interface at a time. IPX is not supported.

This screen also provides the following information about the LAN interfaces:

- IP Address shows the current IP address that is assigned to the interface.
- Subnet Mask defines which bits of the IP address represent the network the device is on and which bits represent the host's ID on the network. The device uses the Subnet Mask to determine which IP addresses are directly reachable on the network and which must be routed through a Contivity. A sample IP address is 10.2.3.3 with a subnet mask of 255.255.0.0. This indicates that all hosts with addresses 10.2.*n.n* are directly reachable.

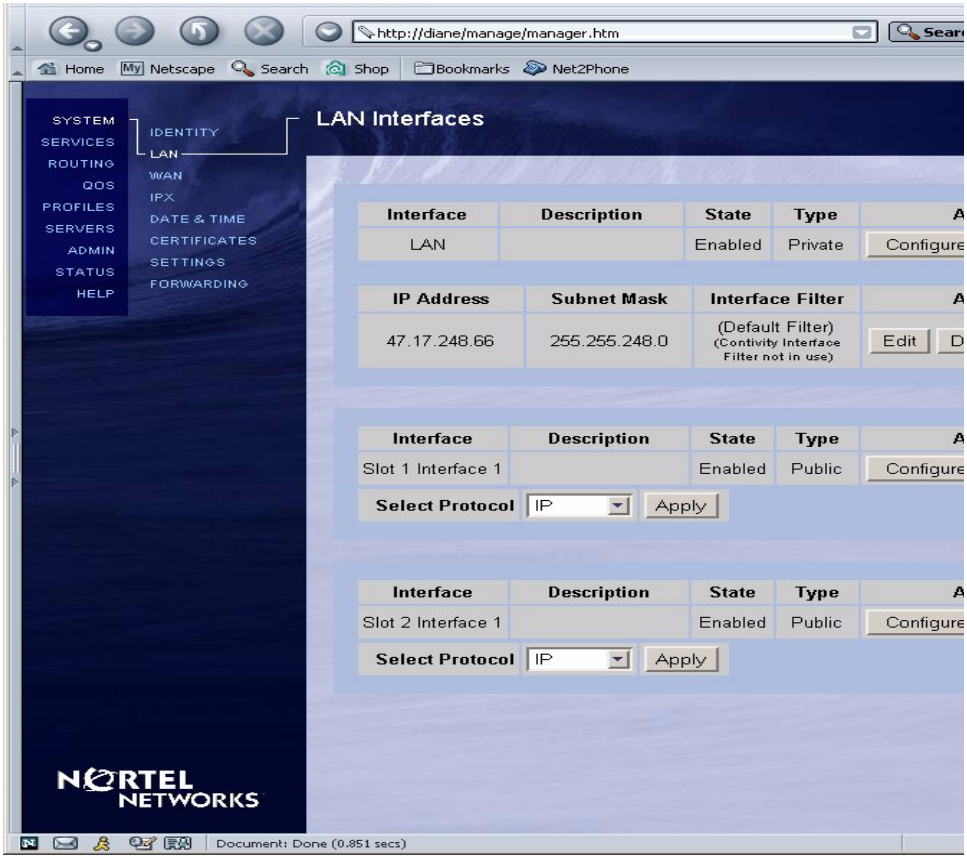
- Interface Filter shows whether the Contivity Stateful Firewall is in use on this LAN interface (this reflects the selection on the Services > Firewall screen). This entry also shows the interface filter that is currently being used by the Contivity Firewall. This is the interface filter that is selected on the System > LAN Interfaces > Edit IP Address screen. If no interface filter has been selected, the default of Deny All is used. The Deny All and the Deny All (default filter) have the same effect. The Deny All (default filter means that there is no filter selected so the default behavior applies, which is to deny all packets.



Note: The management screen can take up to 3 minutes to return if Ethernet parameters are changed when the link is not active on the Ethernet port.

The Configure button on the System > LAN Configure screen allows you to provide optional information for the LAN interfaces.

Figure 9 LAN Interfaces screen



This information then appears on the System > LAN screen. Additional fields appear on the Edit LAN Interface screen for optional network cards. LAN represents the physical port interface to which you assign an IP address. Slot *n* Interface *n* represents an optional LAN card in expansion Slot *n* using Interface *n*.

1 Under the Configuration section, use the Speed/Duplex field to automatically or manually configure the LAN interface's port speed and mode.

Note: You can also use the Interface selection on the Contivity's Serial Port menu to set auto negotiation.

2 Select Auto-Negotiate to specify that the Contivity automatically set the port speed and mode to match the best service provided by the connected station,

up to 100 Mbps in full-duplex mode. Auto-Negotiate is the default selection, and complies with the IEEE 802.3u auto negotiating standard.

3 Select one of the following selections to manually set the LAN interface's port speed and mode to match the speed and mode used by the connected station.

- 100Mbs/Full duplex
- 100Mbs/Half duplex
- 10Mbs/Full duplex
- 10Mbs/Half duplex



Note: You might not be able to connect to the remote system if the system is not using auto negotiation or if it uses an incompatible form of auto negotiation. If this occurs, manually set your Contivity's speed and mode settings to match those used by the remote system.

4 You can provide an optional description for the LAN interface. The description appears on the LAN Interfaces screen.

5 MAC Pause (Ethernet packet flow control) enables the Contivity to automatically adjust and control the flow of incoming and/or outgoing packets from any standard speed LAN device. Check to enable MAC Pause (Frame-based flow control) on the selected interface port. When enabled, specify the appropriate Pause parameters to be set in the hardware. Specify a value for MAC Pause Ticks. Select a value from the Free Receive FIFO Threshold list. The default is 0.

6 The State field appears on the screen for an optional LAN card in expansion Slot *n* using Interface *n*. Click to enable or disable the card.

7 The Interface Type field appears on the screen for an optional LAN card in expansion Slot *n* using Interface *n*. Click to specify whether the interface is public or private.

The Add IP address screen (System > LAN Add) allows to you assign an IP address and subnet mask to the interface. Use the Edit IP Address screen (System > LAN Edit) to modify the information.

To obtain an IP address:

1 Check the Static button to assign a static, unchanging IP address.

The IP address consists of 32 bits, which are written as four octets (8-bit bytes) in dotted-decimal format; for example 192.168.34.21.

The subnet mask defines how many bits of the IP address represent the network the device is on and how many bits represent the host's ID on the network.

The device uses the Subnet Mask to determine which IP addresses are directly reachable on the network and which must be routed through a Contivity. A sample IP address is 10.2.3.3 with a subnet mask of 255.255.0.0. This indicates that all hosts with addresses 10.2.*n.n* are directly reachable.

2. Check the DHCP button to have the IP address assigned by a DHCP server.
3. Enter a cost. The default is 10.
4. Interface filter shows whether or not the Contivity Firewall is in use (this reflects the selection on the Services > Firewall screen).
5. This entry also shows the interface filter that is currently being used by the Contivity Firewall. Select from a list of all interface filters that have been set up on the Contivity (on the Profiles > Filters screen), and to select a different filter for the Contivity Firewall.



Note: If you change the interface filter setting, a message informs you that you must restart your Contivity before the new interface filter is used. If the Contivity Firewall is not enabled, the new selection has no effect.

6. Use the New Interface Filter link to go to the Profiles > Filters screen and create a new filter. The default Interface Filter setting is Deny All.

You can copy an existing tunnel filter for use as an interface filter or vice versa. However, when you copy a filter, the operation does not copy any components (such as a rule, port, protocol, or address) that have the same name as an existing component in the destination filter set. You should use unique names for the device in all filter rules.

Configuring circuitless IP

Circuitless IP (CLIP) allows you to define virtual addresses as termination points, such as TCP connections, for branch office and client tunnels. It also allows virtual addresses for routing protocols. The Contivity CLIP implementation allows you to build tunnel and ICMP filters for the public side, private side, or both.

A CLIP interface allows:

- Internal address mapping to reach external ports and services
- Increased flexibility for VPN tunnel termination
- Efficient operation of VPN load balancing with an Alteon switch
- Device connectivity independent of physical interfaces

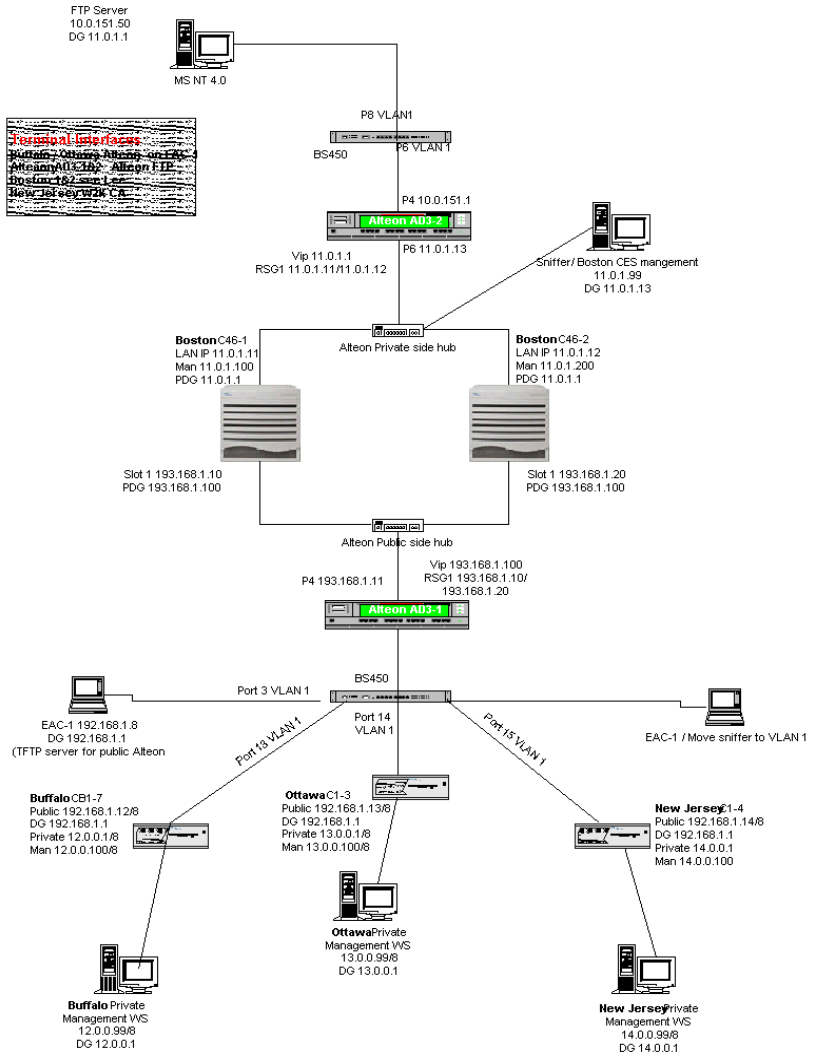
All current tunnelling protocols are supported, including: IPsec, L2TP and PPTP. Tunnel terminations are allowed based on tunnel types. Peer-to-peer, ABOT, and client tunnel types are supported. You can use CLIP addresses for load balancing with an Alteon switch where the same CLIP address is used by multiple Contivity gateways behind the Alteon switch.

For client or remote branch office tunnels, the Contivity servers (load balancers) appear as one device. The Contivity servers are configured with a common CLIP, although each has its unique interface IP address. The CLIP address is also unique within each Contivity.

For Contivity servers supporting the branch offices, you should use the asynchronous branch office tunnel. You should also configure the Contivity servers as responders and the remote clients as initiators.

In Figure 10 the private Alteon WebOS switch is configured to direct returning data back to the client through the same Contivity as the ingress traversal. This is achieved through the Alteon's VPN load balancing function. The Alteon WebOS supports up to 255 port connections. However, the network topology supports only eight Contivity load balancers as basic configuration.

Figure 10 CLIP network topology

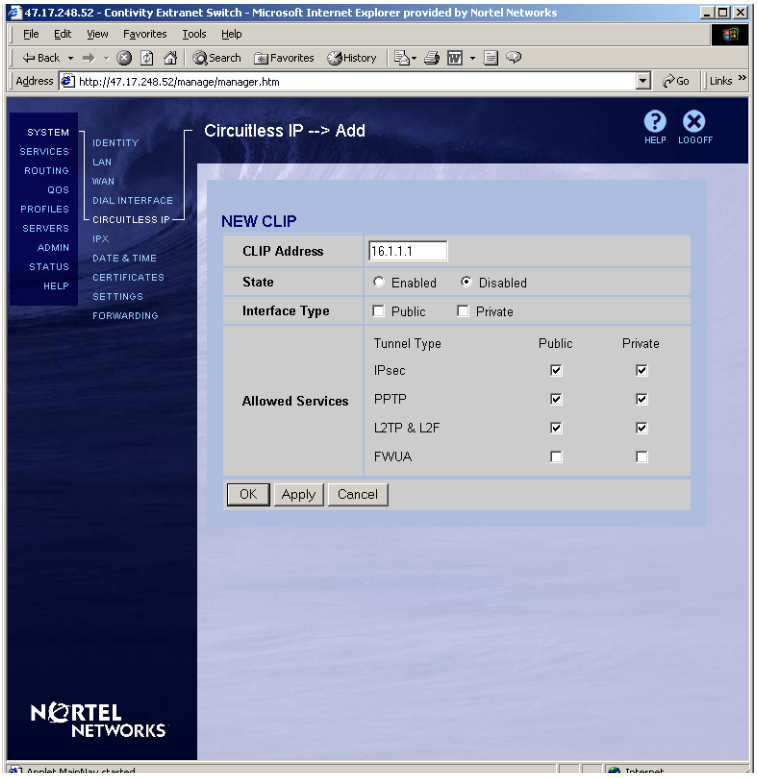


As part of the network management support, you can obtain real-time statistical information from the statistics button on the CLIP management page. The statistics include circuitless IP address information as well as connected session information.

To configure CLIP:

1 Go to System > Circuitless IP and under Configured Circuitless IP, click on the Add button.

Figure 11 Configure circuitless IP



2 Enter the circuitless IP address and select either Public or Private as the interface type. You can configure up to six CLIP addresses.

3 For the Allowed Services, select either Public or Private for each tunnel type.

4 Click on Apply and OK.

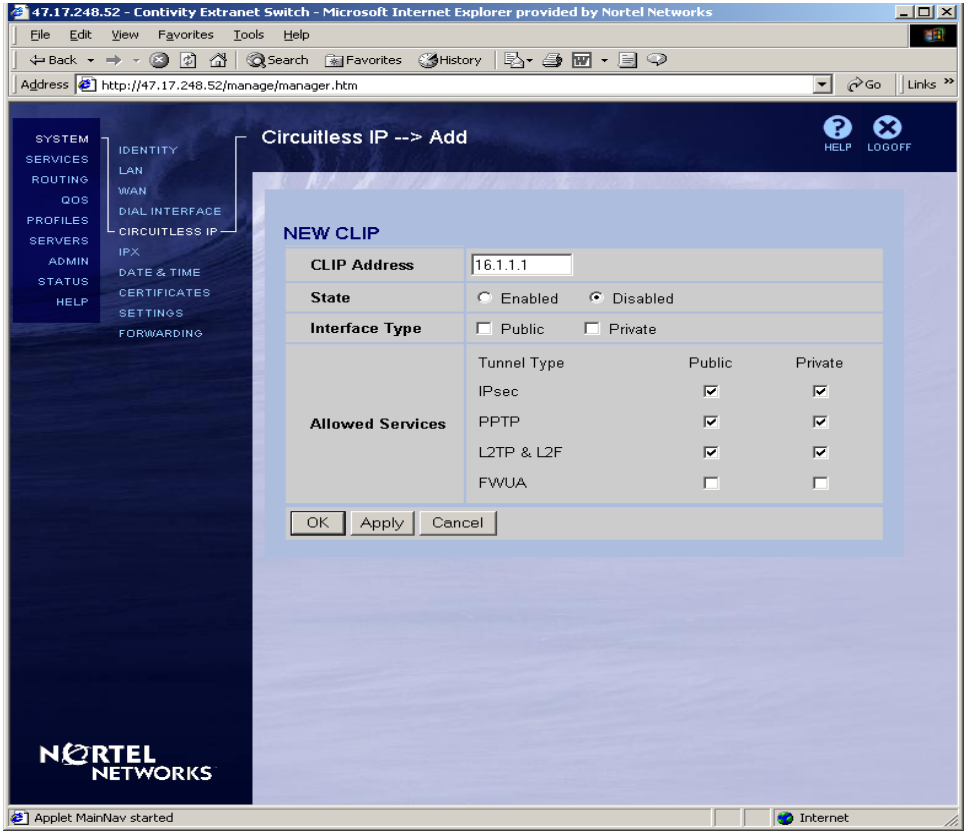
5 When you have the correct configuration, check the Enabled box and click on OK.

6 Click on the Allowed Services button to view the status of the allowed services. The Refresh button allows you to view any changes.

To enable CLIP redistribution through dynamic routing protocols:

1 Go to the Routing > Policy screen.

Figure 12 Routing policy screen



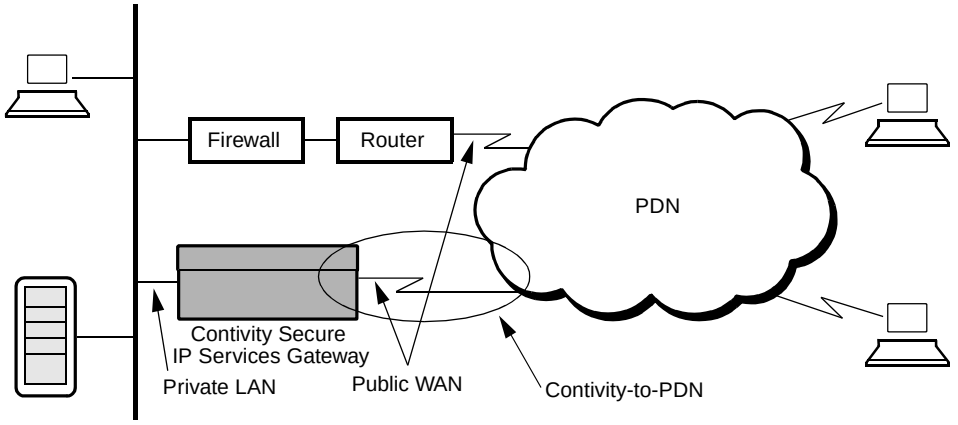
2 Select CLIP as the route source for the protocol.

3 Click on OK.

Setting up WAN interfaces

You assign WAN interface connections between the Contivity and the PDN. Figure 13 shows the connection attributes that you must configure. These attributes assign WAN interface connections between the Contivity and the ISP.

Figure 13 Contivity-to-PDN configuration

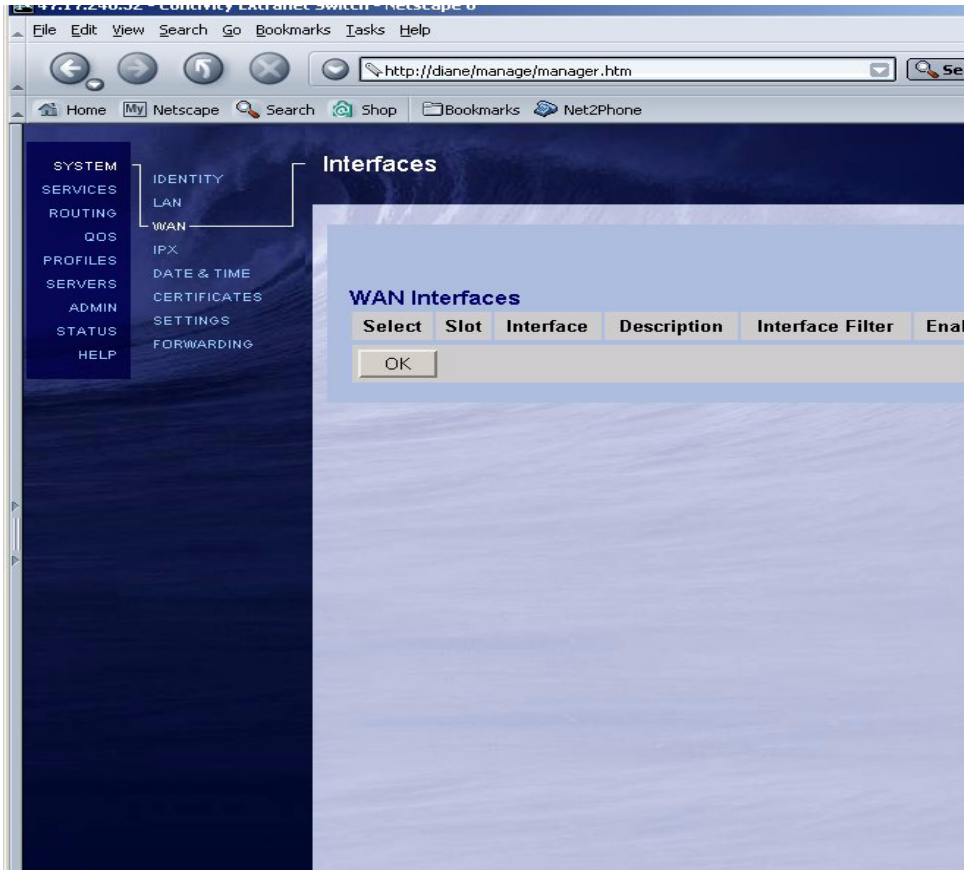


The System > WAN Configure screen allows you to configure WAN devices with local and remote IP addresses and PPP-related settings. When you click on the PPP Authentication or Advanced Settings configuration buttons, the associated configuration screen appears. You also use this screen to specify the interface filter that is used for the option Contivity Firewall on this interface. The addresses are used by the IP Control Protocol (IPCP), which communicates IP addresses to peer connections over PPP. Many of these values are provided by your Internet (ISP).

Configuring WAN interfaces

The WAN interfaces screen (System > WAN) shows the WAN interfaces currently installed in the Contivity, the slot in which the cards reside, an interface description (if one has been provided), and the current state. It also indicates whether the Contivity Firewall is active and the interface filter that is in use. From this screen, you can move to another screen to configure or disable a WAN card, or view statistics.

Figure 14 WAN Interfaces screen



Note: To change the IP address of a WAN link, you must disable the interface, change the address and re-enable the interface. This automatically disables static routes for the interface. If you change the IP address back to the original address, you must manually re-enable static routes.

To configure WAN interfaces:

1 Click on Configure to configure a new IP address for the associated device, or add or modify PPP advanced and authentication settings. The Configure WAN Interfaces screen appears.

2 Click on Enable/Disable to toggle between Enable (on) and Disable (off).

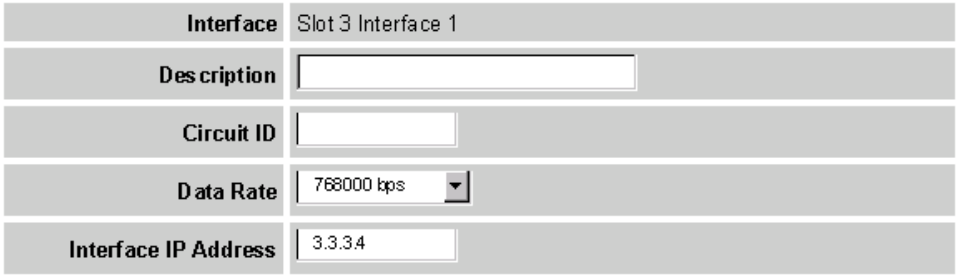
3 Click on Statistics to view statistics for the interface.

Configuring data rates on WAN interfaces

The Configure WAN Interfaces screen allows you to configure the line speed. Select one of the speeds in the Data Rate pull-down menu.

Figure 15 shows the data rates.

Figure 15 Data rates



The pull-down contains all the permitted data rates. For a CSU/DSU, the data rate is calculated based on the T1 fraction.

To use the Serial UI:

1 From the Main menu, select Option 1 for Interfaces.

2 Select a port.

3 For setting the data rate, choose a number between 1 and 24.

The following shows the output:

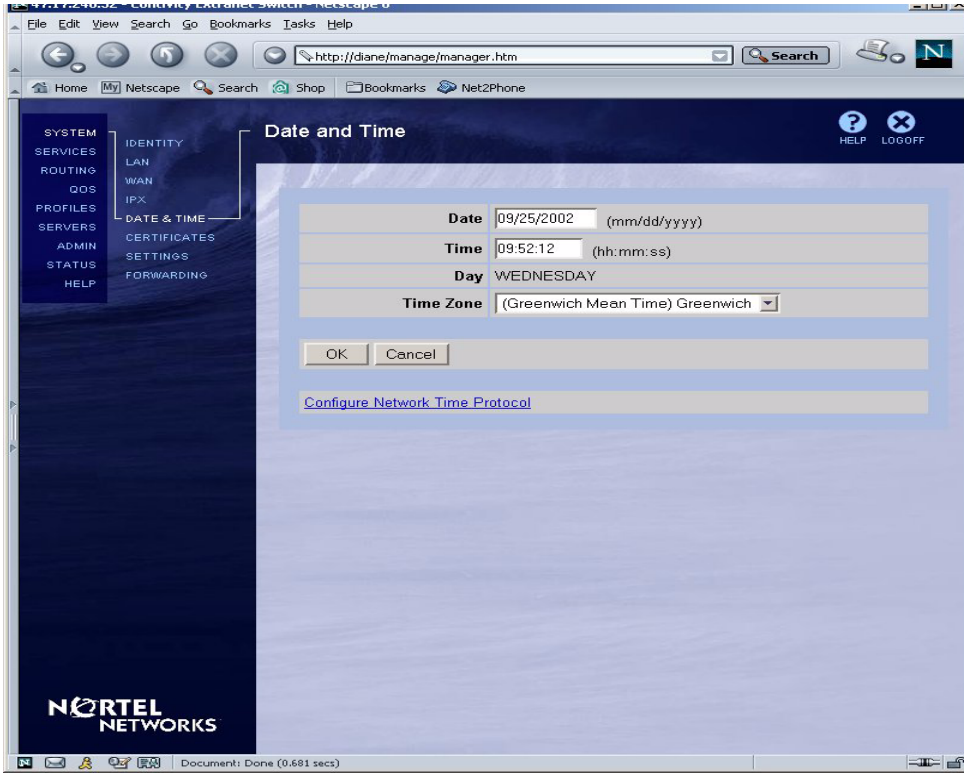
```
Main Menu:  System is currently in NORMAL mode.
1) Interfaces
     2) Administrator
     3) Default Private Route Menu
     4) Default Public Route Menu
     5) Create A User Control Tunnel(IPsec) Profile
     6) Restricted Management Mode       FALSE
     7) Allow HTTP Management            TRUE
     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): 1
- Interface Menu
0) Slot 0, Port 1, Private LAN
        Management IP Address = 120.77.0.58, ( Subnet Mask =
255.255.0.0)
        Interface IP Address = 120.77.0.8
        Subnet Mask = 255.255.0.0
        Speed/Duplex = AutoNegotiate
1) Slot 1, Port 1, Public LAN
        IP Address = 198.89.10.14
        Subnet Mask = 255.255.255.0
        Speed/Duplex = AutoNegotiate
2) Slot 3, Port 1, Private LAN
        IP Address = 130.78.0.2
        Subnet Mask = 255.255.0.0
        Speed/Duplex = AutoNegotiate
3) Slot 4, Port 1, Public WAN
        IP Address =
        Subnet Mask = 255.255.255.255
        Data Rate = 1536000 bps   R) Return to the Main Menu
Please select a menu choice: 3
   3) Slot 4, Port 1, Public WAN
        IP Address =
        Subnet Mask = 255.255.255.255
        Data Rate = 1536000 bps
*  Just type <CR> to skip.
        Old IP Address =
        New IP Address* = 2.2.2.2
Current Data Rate = 1536000bps (24 x 64kbps)
        Choose a multiple (1..24) of 64kbps, or <CR> to skip.
```

Configuring Network Time Protocol (NTP)

NTP synchronizes the clocks of various devices across networks. It also automatically adjusts the time of network devices so that they are synchronized within milliseconds. The Contivity receives NTP updates from an NTP time server and continuously synchronizes its clock to universal standard time. The Contivity supports up to eight NTP (unicast) servers and broadcast, multicast servers.

The System > Date and Time > Network Time Protocol screen allows you to set up NTP on the Contivity. NTP synchronizes the clocks of various devices across networks.

Figure 16 Date and Time screen



It also automatically adjusts the time of network devices so that they are synchronized within milliseconds. The Contivity receives NTP updates from an NTP time server and continuously synchronizes its clock to universal standard time. The Contivity supports up to eight NTP (unicast) servers and broadcast, multicast servers.

To configure NTP:

1. Click on the Enable check box.
2. If you want the Contivity to listen for and respond to broadcast messages, check the Synchronize time with NTP Broadcast Server box. If you want the Contivity to listen for and respond to multicast messages, check the Synchronize time with NTP Multicast Server box. The IP multicast address is 224.0.1.1 for NTP. NTP listens for both broadcast and multicast messages at the group address of the global network. To avoid disruption in multicast mode, both the client and servers should use authentication and the same trusted key and key identifier.
3. Under Servers, click on the Add button to add a server:
   a. IP address of the NTP (unicast) server.
   b. Under Interface, for security, you can specify either a private or public interface. The private interface is the management IP address. When adding a public interface, you can choose from a list of public interfaces. If you are using the Contivity Firewall, you need to configure an interface filter to add NTP.
   c. Enter the Key ID. This specifies the Key ID for Message Digest (MD5) authentication. In authentication mode, each packet transmitted has a 32-bit Key ID and a 64/128-bit cryptographic checksum using MD5 algorithms. With MD5, the receiving peer recomputes the checksum and compares it with the one in the packet. They must share at least one MD5 key (trusted key) and must associate the shared key with the same Key ID.
   d. Enable Bursting to send a burst of eight packets at each poll interval.
   e. Select the NTP version number (1, 2, 3, or 4) used on the NTP server. The default is 3.
   f. Click OK.

4. Under Trusted Keys, click on the Add button to add an area key ID. The Contivity displays the Add/Edit Trusted Key screen. Enter the key ID, the password and the password confirmation.
5. Click on the Return to the Date and Time page link to return to the previous page.

Using safe mode configuration

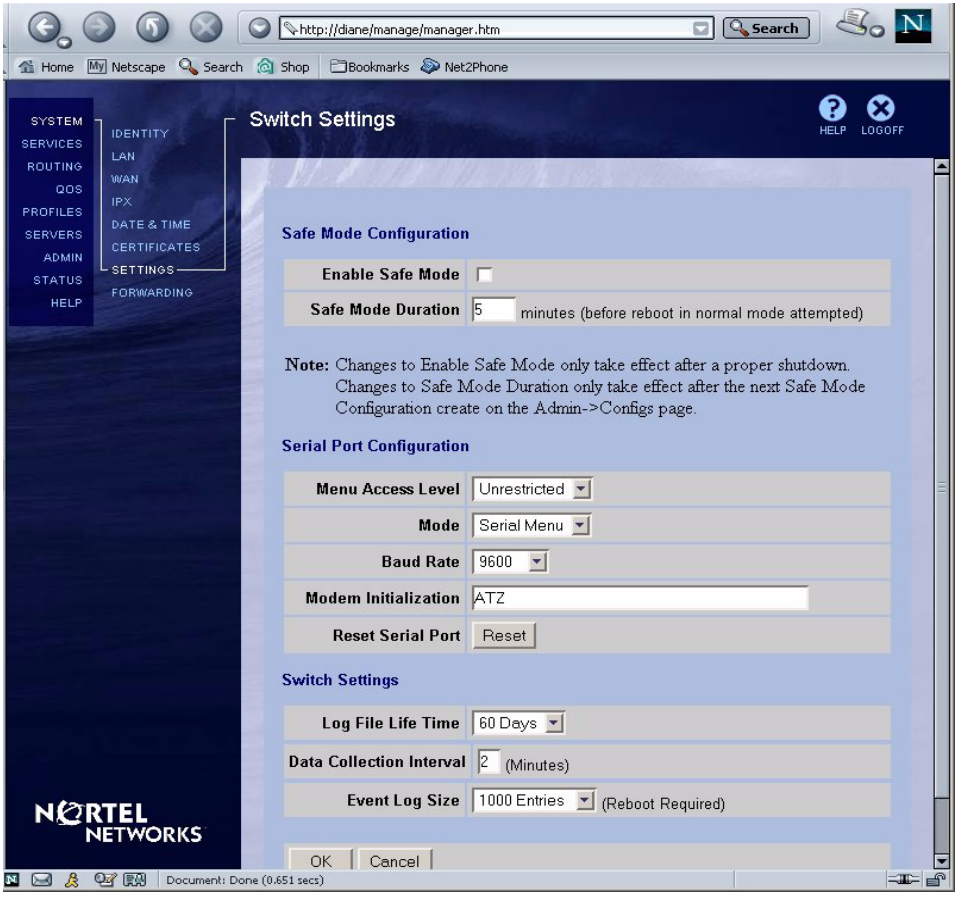
The Contivity can be booted in one of the two system modes: safe mode or normal mode. Each mode has its own software image, configuration files, and LDAP database.

A system booted in Safe mode is only allowed to accept secured management tunnel establishment. When the secured management tunnel is established, Telnet, HTTP, and FTP traffic is allowed to come into the Contivity; no other VPN traffic is allowed through the secured management tunnel or the Contivity. In Normal mode, the system operates with the normal software and configuration and transports both VPN traffic and management traffic.

To configure safe mode:

1. Go to the System > Settings screen.

Figure 17 Switch Settings screen



2 Click on the Enable check box to enable and disable Safe Mode.

3 Type in the number of minutes to determine how the long the system operates in Safe Mode before attempting to reboot in Normal Mode.

4 Under the Serial Port Configuration section, you configure the serial port. The parameters that you must set to allow the Contivity to communicate via the serial port. Whenever you change from either serial menu mode to PPP mode, or vice versa, you must restart the Contivity for the change to take effect.

   a The Menu Access Level setting determines which commands are available in a serial console port menu.

   - Unrestricted - All commands are available to the user (default).

- Restricted 1 - System Reset commands plus the commands to change interface IP address and mask.
- Restricted 2 - Only Reset commands are available.

b Select one of the following Modes of operation:

- Serial Menu (default). In this mode, a standard menu interface is presented. You can use an application such as Hyper Terminal, when directly connected to the Contivity, to access the menu interface. The Contivity uses the COM port for a serial menu terminal session. The Contivity's serial port baud rate is 9600 by default. When you change the serial interface baud rate, you must press the Reset button.
- PPP allows you to set up the Contivity to use the Point-to-Point Protocol (PPP) over the serial port. This feature allows you to manage the Contivity from a remote location using PPP and the serial interface. If the Contivity were to become unreachable over the Internet, you could still dial up and manage it through the serial interface menu.
- Auto Detect allows you to access all of the management services (HTTP, Telnet, FTP, SNMP) through the Web interface. When a session is established through PPP, the serial interface acts as a private WAN interface with an internal IP address.
- Auto Detect automatically detects whether the Contivity is using PPP or serial menu mode at startup. It cannot determine the Contivity'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 Contivity is restarted. When performing its Auto Detect check, the Contivity sends out AT command set characters to configure a modem if one is attached. When the Contivity is in Auto Detect mode, and if a terminal session is connected and the terminal baud rate is the same as the Contivity's, the terminal displays the AT command sets on the screen. Simply press Enter more than five times before a serial menu session is started.

c Select one of the following Baud Rates to match the baud rate of your terminal:

- 57600
- 38400
- 19200
- 9600 (default)

d Enter the modem initialization string. Refer to the manufacturer's documentation to learn the vendor-specific character initialization string.

If you pre-configure the modem and use the Contivity's default initialization string (ATZ) it will provide the best results.

e When you select the baud rate, you must click the Reset button to change the port to the new baud rate.

5 The Log File Configuration sets the life time of the log files. The default log file life time is 60 days. Select a value for the log file life time from the list.

6 The data collection interval specifies how the long the system should wait before collecting new system data for logging. Enter the time in minutes.

Using proxy ARP

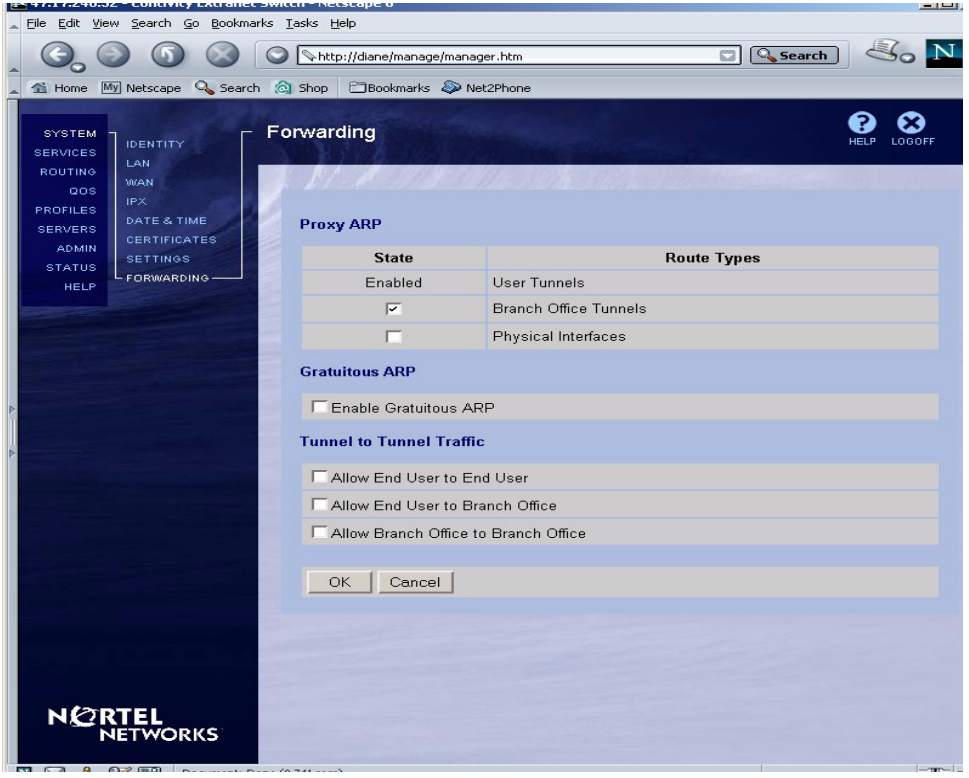
You can configure the Contivity to respond to ARP requests on any of its physical interfaces. The Contivity responds to the following types of routes:

- User tunnels are routes created for user tunnels. This entry is enabled by default and cannot be changed.
- Branch office tunnels are routes available through branch office connections. This option is disabled by default.
- Physical interfaces are routes available through physical interfaces. This option is disabled by default.

To configure proxy ARP:

1 Go to the System > Forwarding screen.

Figure 18 Forwarding screen



2 Click the appropriate check boxes to enable the different types of tunnel-to-tunnel traffic. All of these options are disabled by default for security reasons.

3 Click on Enable Gratuitous ARP to enable it.

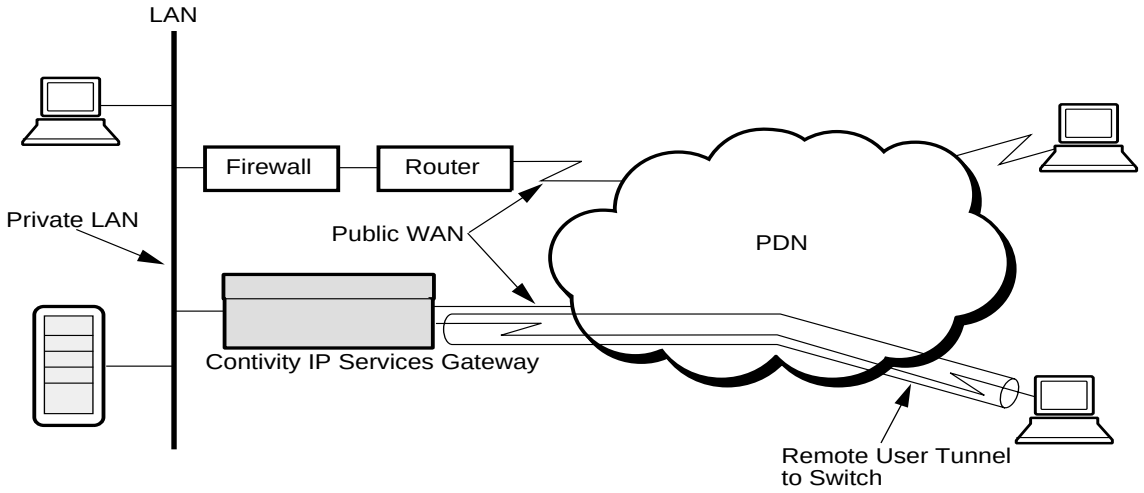
4 Under Tunnel to Tunnel Traffic, select from:

- Allow End User to End User to allow a remote user who is tunneled into the corporate Contivity to access other remote users that are also tunneled into the Contivity.
- Allow End User to Branch Office to allow a remote user who is tunneled into the corporate Contivity to access the resources of branch offices that are connected to the Contivity.
- Allow Branch Office to Branch Office to allow users who are on one branch office connected to your Contivity to access resources on other branch offices that are connected to your Contivity.

Chapter 4
Configuring user tunnels

The Contivity uses the Internet and tunneling protocols to create secure extranets. The following sections describe configuring the tunnel portion of the Contivity. The configuration process includes setting up the authentication table and specific tunnel parameters, such as IPsec encryption, L2TP access concentrators, and L2F network access servers. Figure 19 shows a typical network illustration with the Contivity connected to the PDN (public data network) and to a remote user through a tunnel.

Figure 19 Tunnel connection configuration



The connection attributes that you configure in the Contivity enable the remote user to create a tunnel into the Contivity. However, you are not configuring the connection from the remote user to the Internet Service Provider (ISP) at this point. The actual connection to the Contivity is a tunnel that is started from the remote user's PC through its dial-up connection. That connection is to the Internet (typically using an ISP), through the Internet, and ends at the Contivity on the private, corporate network.

The Contivity associates all remote users with a group, which dictates the attributes that are assigned to a remote user session. A group can even consist of a single user, thereby creating a personal extranet.

The Contivity organizes groups in a hierarchical manner. At the top of the hierarchy is the base group. The base group \Base contains the default characteristics that each new group inherits. You add additional groups to the hierarchy as children of the base group.

The Contivity takes precautions against unauthorized users potentially hacking tunneled information when the Contivity is operating in Split Tunnel mode. The primary precaution is to drop packets that do not have the IP address that is assigned to the tunnel connection as its source address. For example, you establish a PPP dial-up connection to the Internet with an IP address of 192.168.21.3. When you start the tunneled connection to a Contivity, you are assigned a tunnel IP address of 192.192.192.192. Now, any packets that attempt to pass through the tunnel connection with a source IP address of 192.168.21.3 (or any address other than 192.192.192.192) are dropped. Furthermore, you can enable filters on the Contivity to limit the protocol types that can pass through a tunneled connection. To completely eliminate security risks, do not use the Split Tunneling feature.



Note: PPP multilink is not supported with branch office tunnels. It is only supported with end user tunnels.

Password aging does not work for administrator accounts. Also, the following are client-specific password management symptoms:

- If you are using the IPsec client, you are warned three times that there will be an impending password expiration. You should change the password immediately. IPsec clients using versions earlier than 1.5.2 do not receive a password expiration warning.

- If you are using the PPTP client with the Connection Manager, the Connection Manager generates an impending password expiration warning.
- Other clients (L2TP and L2F) and PPTP client users who are not using the Connection Manager have no warning and no longer can log on. You must contact your system administrator if this happens. In this case, the Contivity is unable to notify the client because it has no actual control over the client. With PPTP, use the Connection Manager to establish a connection. With L2TP or L2F, set the Password Maximum Age to zero (never expires).

For example, \Base is the base group, Research and Development and Finance are child groups of the base group, and they are parent groups to groups below them.

Groups are collections of users with the same access attributes and rights. If all users have identical characteristics, then only one group is necessary. You create multiple groups when you need different attributes. A Lightweight Directory Access Protocol (LDAP) database stores users, groups, and their attributes. You can store this database internally (on the Contivity's hard disk) or externally (on a network host running LDAP server software).

The Contivity authenticates each user that tries to connect to the Contivity by checking the user ID and password against a database. The Contivity supports both LDAP and Remote Access Dial-In User Session (RADIUS) databases for authentication. When using LDAP for authentication, the user is always assigned to a group since LDAP also contains the user, group, and attribute information.

When authenticating a Point-to-Point Tunneling Protocol (PPTP) client against a RADIUS database, the group for a user requesting a session can be returned from the RADIUS server as a RADIUS class attribute.

When authenticating an IPsec client, the remote user is by default assigned to the group ID. If the group ID and group password are correct, the Contivity passes the user ID and password (or token card) to the RADIUS server for authentication.

You define a set of group attributes and give it a name. This group name is known as the Relative Distinguished Name and it is added to the LDAP database name when performing the database lookup.

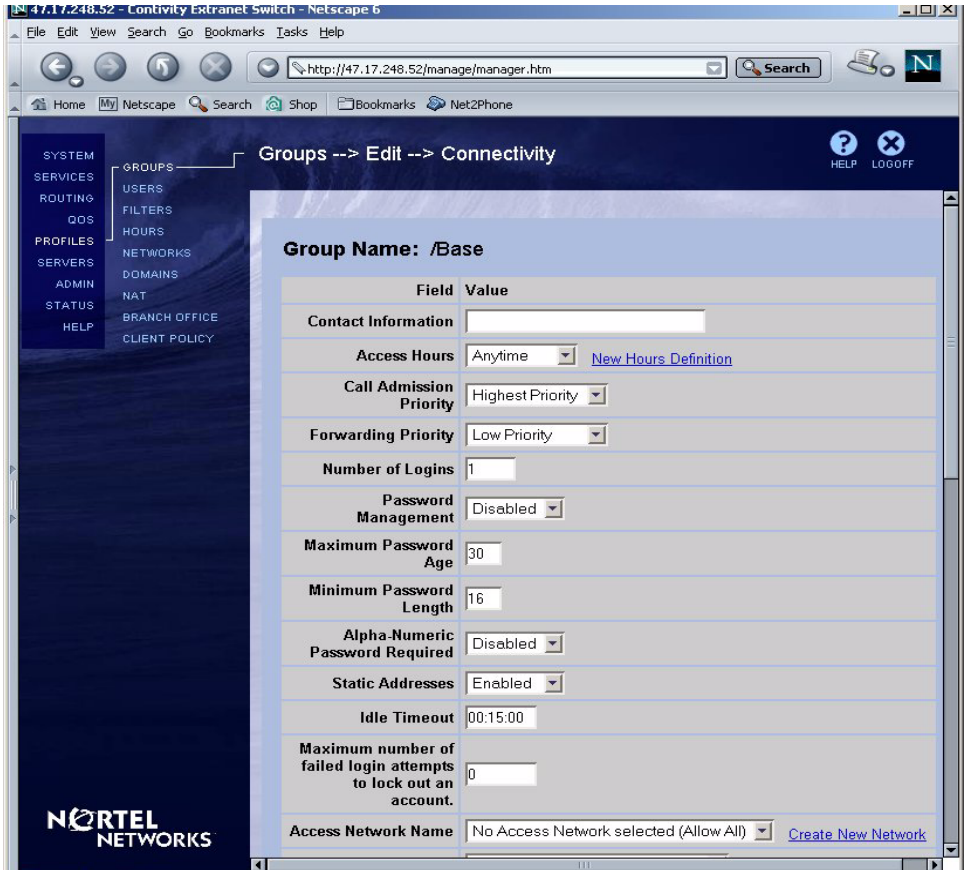
Note: The group name Certificates is not allowed as a valid group name when created under the /Base directory. If you change the name to Certificate, the group is created properly. If you create the group Certificates in a /Base subdirectory, it is created properly.

Configuring group characteristics

In addition to assigning users to groups and providing authentication access, you can configure other group characteristics:

1. Go to the Profiles > Groups screen and click on the Edit button next to the group that you want to configure.
2. Under the Connectivity section, click on the Configure button to change the any of the group characteristics.

Figure 20 Groups Edit screen



3 Enter the name of someone who serves as the point of contact. This is typically the administrator.

4 Specify the time ranges during which access is allowed for users in a group. These time ranges are are also configured from the Profiles > Hours screen.

5 Specify the call admission priority priority level (from low to highest) that you want to permit for the group. Each level is assigned a percentage of the total number of calls allowed access to the Contivity. If there is a particularly high number of users logged in, new users could be denied call access, based on their call admission priority, until existing callers disconnect.

6 Specify the forwarding priority level (from low to highest) that you want to provide to sessions for users in this group. Forwarding priority assures a certain level of latency and bandwidth allocation. For example, a group with

the highest forwarding priority has the highest possible bandwidth service and the lowest level of latency. Conversely, if there is a particularly high level of traffic on the line, packets for a low-priority group might be delayed or dropped. Since a low-priority group has the least amount of bandwidth and the highest level of latency, some of its packets would wait until the higher-priority-level packets have been forwarded or they would be dropped.

7 For number of logins, enter the maximum number of simultaneous logins IPsec clients in the group are allowed. The Contivity does not enforce the maximum number of logins across tunnel types. If you set the number of simultaneous logins to 1, a client can still get another tunnel type connection if the client is configured to use multiple tunnel types. To limit the number of connections a client can have, configure the user for a single tunnel type.

8 Select Enabled to enable the password management facilities:

- Maximum password age is the time after which the login password expires. The Maximum Password Age range is from 0 (no password expiration) to 180 days (6 months). Default is 30 days. Users receive a warning that the password will expire each time they log in for two days prior to the expiration date. They also receive three warnings before access is denied. (If your clients are using a Microsoft Dial-up Networking connection instead of the Nortel Networks Connection Manager, then they are not be notified of a password expiration or be given the opportunity to change the password prior to expiration. You should not use this feature unless you also plan to distribute the Connection Manager.
- Minimum password length can be from 3 to 16 alphanumeric characters. If you set the minimum length to eight characters, then the remote user must use at least eight characters as the login password. Default is 16 characters.
- Alpha-numeric passwords forces remote users to log in with a combination of alphabetic (A to Z) and numeric (1 to 9) characters. Nortel Networks does not recommend using all alphabetic characters because this makes it easier for hackers to decode. The default is Disabled.

9 Enter the amount of time a connection can be idle (no data has been transmitted or received through the connection for the specified amount of time). When the idle timeout expires, the session is terminated. This option helps prevent allocation of resources on the Contivity for sessions that are no longer active. The default Idle Timeout is 00:15:00 minutes; the range is 00:00:00 to 23:59:59. The maximum number of days is 29. A setting of

00:00:00 specifies no Idle Timeout. All sessions check their configuration at startup time. Therefore, if you change the time of the idle timeout during a session, the change only affects new sessions and not any existing ones.

10 For Access Network Name, specify a source IP address that restricts user access. Users may tunnel into the Contivity only if they are tunneling from a source IP network defined by the access network. If they tunnel from a network outside the defined access network, the tunnel is refused. Access Network Names must be previously defined on the Profiles > Networks screen to appear in the list. Use the link to create an access network if one does not exist.

11 Packet filters control the type of access allowed for users in a group, based on various parameters, including Protocol ID, Direction, IP addresses, Source, Port, and TCP Connection establishment. Go to the Profiles > Filters screen to create tunnel filters.

12 Select Enable to enable IPX support for the group.

13 Enter the Maximum Number of PPP Links that you want the Contivity to support. The range is 1 to 5; default is 1. The Multilink PPP (MP) implementation allows tunneling multilink connections to the Contivity when the tunneling is being done by the ISP.

14 RSVP allows you to signal the network for required bandwidth. The client must be configured appropriately for RSVP to work. Also, only the controlled load-service is supported. This option is disabled by default.

15 The Token Bucket Depth influences packet flow delays within the Contivity and participating routers in the Internet. The largest amount of data the Contivity holds in its queue determines latency. New packets arriving are delayed by a time that is proportional to the amount of traffic that is ahead of them in the queue, which is no greater than the Token Bucket Depth. When the queue exceeds the Token Bucket Depth, incoming packets are dropped. To guarantee reduced latency, the Bucket Depths should be small. Typically, you should not change this setting. Default is 3000 bytes.

16 The Token Bucket Rate is the highest long-term average data rate (in Kbps) required over time for the connection. It informs the Contivity and participating routers in the Internet how much bandwidth to reserve for the RSVP session. Typically, you should not change this setting. Default is 28 Kbps.

17 Click on the drop-down menu to select the Address Pools used by remote users to access this Contivity. The drop-down list shows all pools that have

been defined on the Contivity. (Address pools are defined on the Servers > User IP Addr screen). Select the New Address Pool link to define a new pool. Refer to "Remote User IP Address Pool" for details. This option is set to Default Pool by default.

18 Click on the Configure button in the User Bandwidth Policy section to modify bandwidth characteristics for this group. Click on the Use Inherited button to apply the settings of the parent group to this group.

19 Click on the Configure button in the User Bandwidth Policy section to modify bandwidth characteristics for this group. Click on the Use Inherited button to apply the settings of the parent group to this group.

a Select a Committed Rate from the list of available bandwidth rates. If the desired bandwidth rate is not listed, click on Define new bandwidth rate to create a new one.

b Select an Excess Rate from the list.

c Choose an Excess Action for traffic handling, either Drop or Mark.

A group inherits attributes from its parent group. For example, if the Research and Development group attributes include All Access Hours and Allow Static Addresses but deny Client-Supplied addresses, PPTP and IPsec tunneling, then the New Products (child) group would inherit these attributes.

Setting up user tunnels

To implement user tunnels, you must configure the following:

- Allowed tunnel access to the Contivity
- Tunneling protocol settings
- A user group
- Add users to the group
- A means, such as DHCP or pool, for assigning IP addresses to the client to allow user access

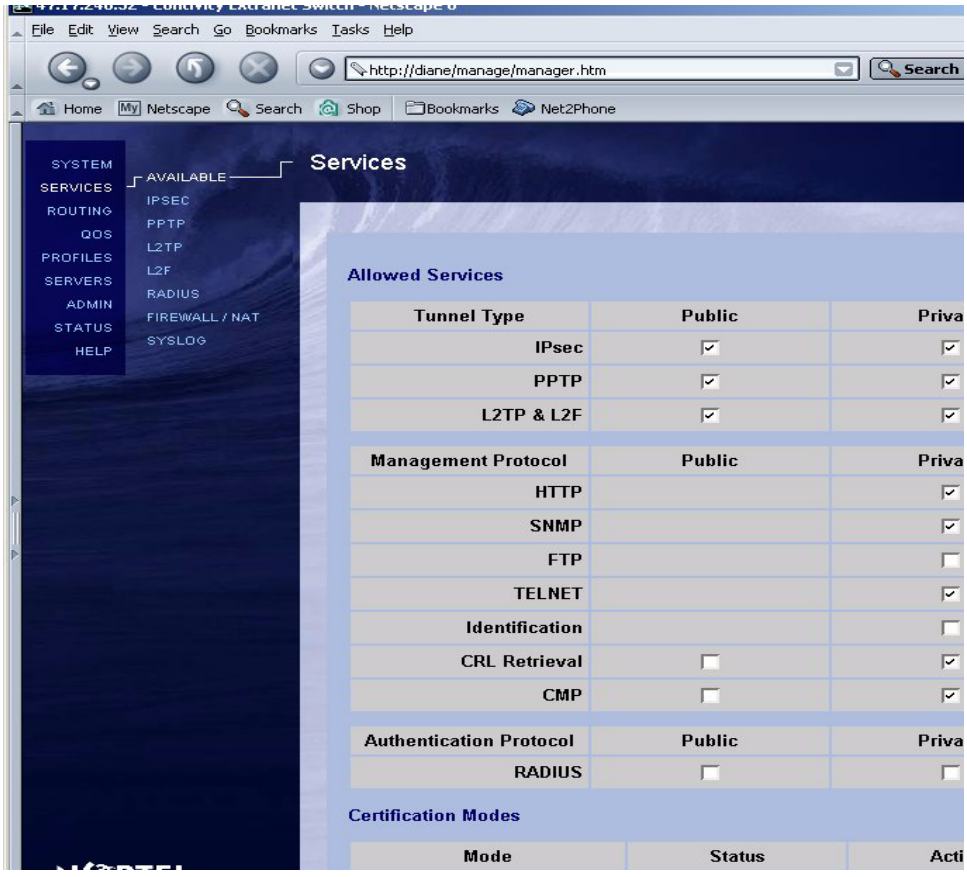
All tunneling protocols are enabled on the public and private networks by default. Since data in tunnels is encrypted, the default setting guarantees that all interactions with the Contivity are private. To prevent tunnel connections of a particular type (for all users, including administrators), you can simply disable the tunnel type.

For example, if you want to use IPsec as your only public tunneling protocol, then disable the Public selection for PPTP, L2TP, and L2F. By leaving IPsec, PPTP, L2TP, and L2F enabled on the private side, you can establish tunneled connections to the Contivity using any of the tunnel types from within your corporation.

To configure tunnel access to the Contivity:

1 Choose Services > Available.

Figure 21 Services screen



2 Select the tunnel type.

3 Select the Management Protocol for the Contivity's private interface.

4 Use the RADIUS check boxes to permit RADIUS requests on the public and private interfaces of the Contivity. If you enable RADIUS traffic, you must also enable RADIUS on the Services > RADIUS screen.

Configuring the Contivity tunneling protocol settings is dependent on the tunnel type.

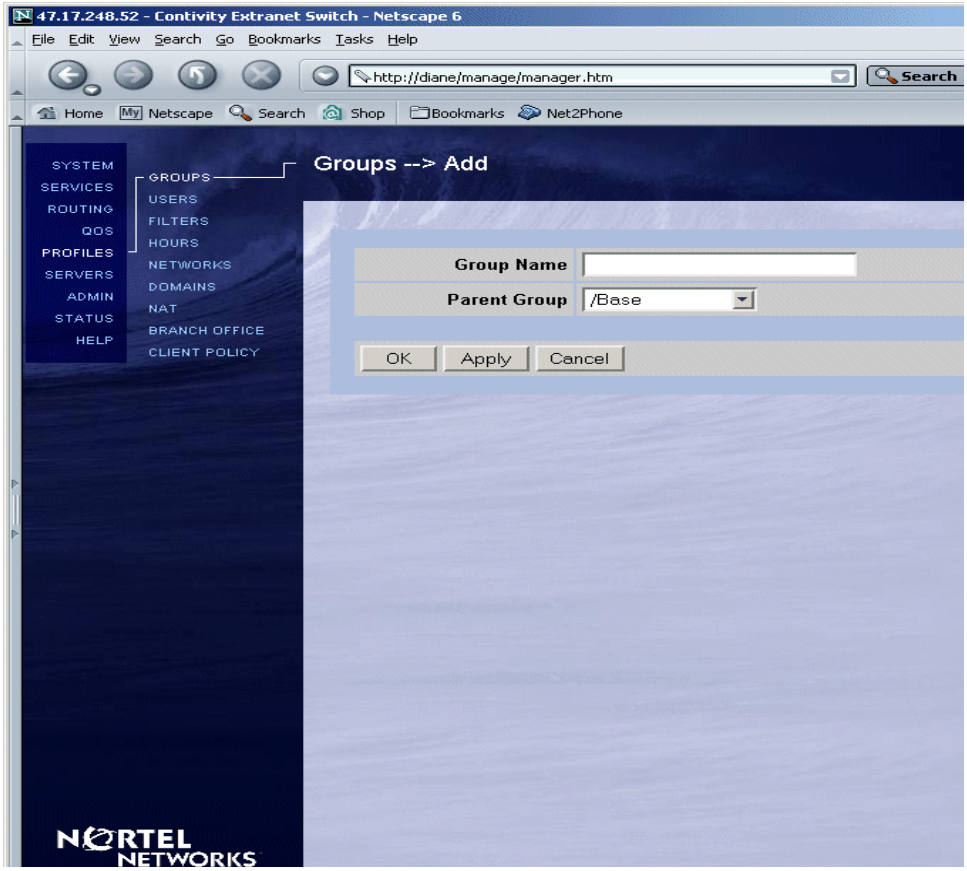
- For IPsec, choose Services > IPsec and select the required authentication, encryption, and authentication order.
- For PPTP, choose Services > PPTP and select the required authentication and authentication order.

- For L2TP, choose Services > L2TP and select the required authentication and authentication order and configure required L2TP access concentrators.
- For L2F, choose Services > L2F and select the required authentication and authentication order, and configure required network access servers.

To add a user group:

1 Go to Profiles > Groups and click on the Add button.

Figure 22 Add Groups screen



2 Enter a group name of up to 64 characters (spaces are permitted).

For example, you could use Research and Development. The new group is a child of the selected parent group. Therefore, the new group initially inherits the parent group's network access attributes, including authentication, tunnel types, filtering, and priorities. When created, these inherited options can be overwritten for the new group.

3 Click on Apply and OK to add the group name.

To add a user profile in a group:

1 Select a group to which you want to add users from among those in the Group list. If you need to add a new group, select Profiles > Groups.

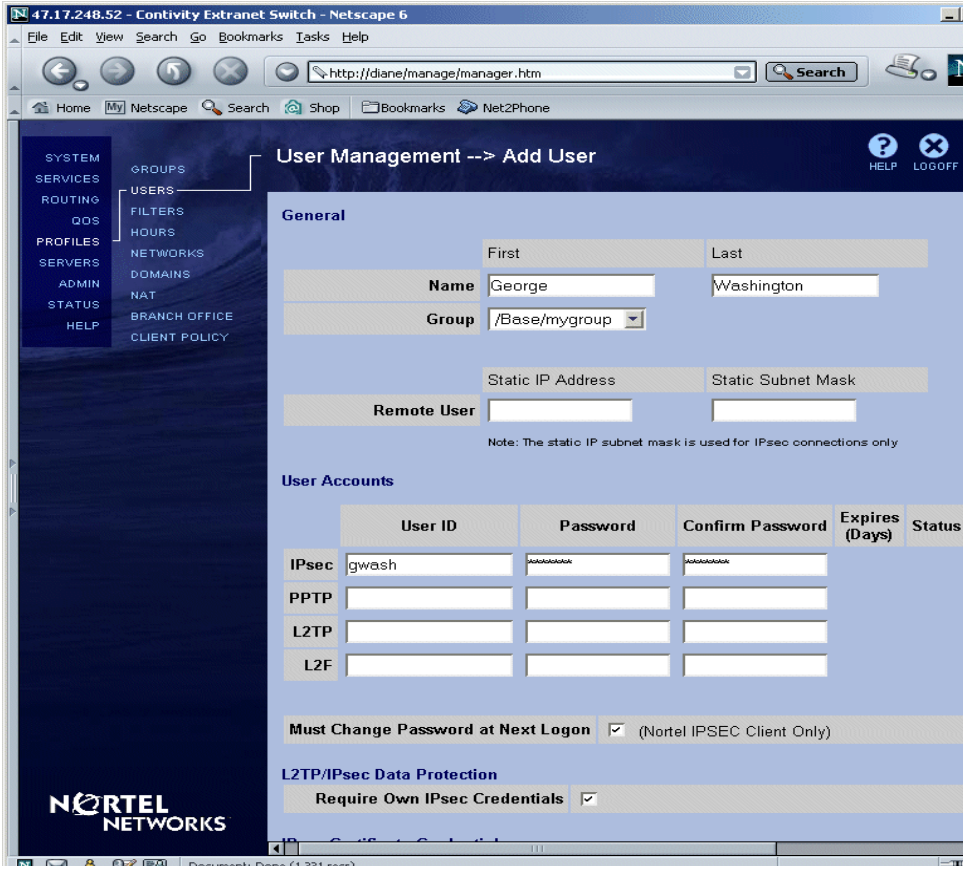
2 After selecting a group, you must click on Display to view the group members. This allows you to quickly change from viewing one group to another. The last names and first names of the selected group's users appear, sorted by last name.

3 Click on Add to add a user to the group; the Add User screen appears.



Note: To configure firewall user authentication, see *Configuring Authentication and Certificates for the Contivity Secure IP Services Gateway.*

Figure 23 Add User screen



This screen allows you to add a user profile. Only options that are enabled for the specified group appear on this screen. Also, only options that the administrator who is currently viewing the screen has rights to appear. A user profile includes:

- User IDs
- Passwords for the various tunneling protocols
- Assignment of administrative rights

- An IP address that is always associated with the remote user

Note: You can assign a user to two different groups, but only if the user has two different user IDs. You cannot enter the same user ID in two different groups. A user account can have up to four user IDs, depending on the group configuration, the account. If you are creating an enterprise user ID standard, you should try to avoid schemes that might potentially create conflicts as your company grows. For example, you should not use the user's full first name and last initial.

4 Enter the first and last name of the user whose profile you want to add. This is the regular name associated with a person (for example, Mario Smith). This user can have different IDs and passwords for each tunnel type. You can move the user to a another group by selecting a different group name.

Note: The GUI ignores leading and trailing spaces, but these must be specified if you then use CLI to edit the user name.

5 Enter a remote user static IP address to use in place of a pool (client-specified or DHCP) server-assigned IP address. This IP address is associated with the Static IP Address option in the Groups > Connectivity option (it is only used if the group allows it). If an IP address that is entered here is used instead of a DHCP server-assigned IP address, then only one login is allowed.

6 Enter the subnet mask. Assigning the correct subnet mask to a remote IPsec client is important when using split tunneling. When you enable split tunneling, packets destined to a host in the Split Tunnel Network list are directed into the tunnel by the IPsec client. All other traffic goes through a standard LAN or dial-up interface. This occurs on the client by adding the routes listed on the Split Tunnel Network list to the route table of the Microsoft TCP/IP stack and pointing those routes to the tunnel adapter interface. A route is also added to the route table based on the subnet mask assigned to the tunnel adapter. The IPsec Subnet Mask field allows you to specifically assign a subnet mask to a remote IPsec client that obtains an IP

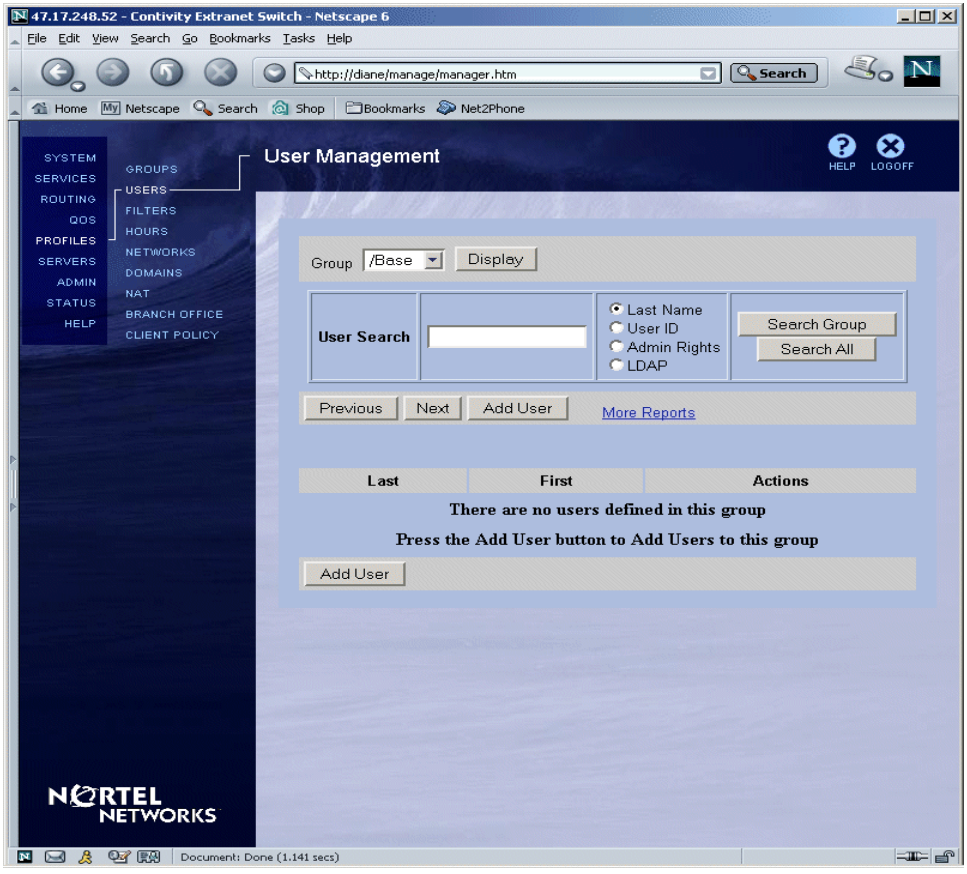
address either from the IP address pool, DHCP, RADIUS, or a static user configuration.

Note: If a host route for the destination address of the Contivity exists in the TCP/IP route table prior to launching the Contivity VPN Client, the route is deleted when the tunnel is closed.

To search within a selected group and then configure a user's account:

1 Go to Profiles > Users > User Management.

Figure 24 User Management screen



2. Select a group from which you want to search for a particular user from the Group drop-down list box (at the top of the screen), and click on Display. The search is limited to the available groups.
3. Enter the appropriate text to search for in the input box.
4. Select one of the following as the preferred search method, then click on Search.
   - Last Name searches for a last name. You must enter the entire last name.
   - UID searches for a user ID.
   - Admin Rights searches for anyone who has View or Manage administrator privileges.
   - LDAP search allows you to enter any LDAP database attribute that is part of the person, organizational Person, or inetOrgPerson object database (for example, cn=common name or sn=surname) to generate the associated user's profile. Refer to your LDAP vendor's documentation for complete details.

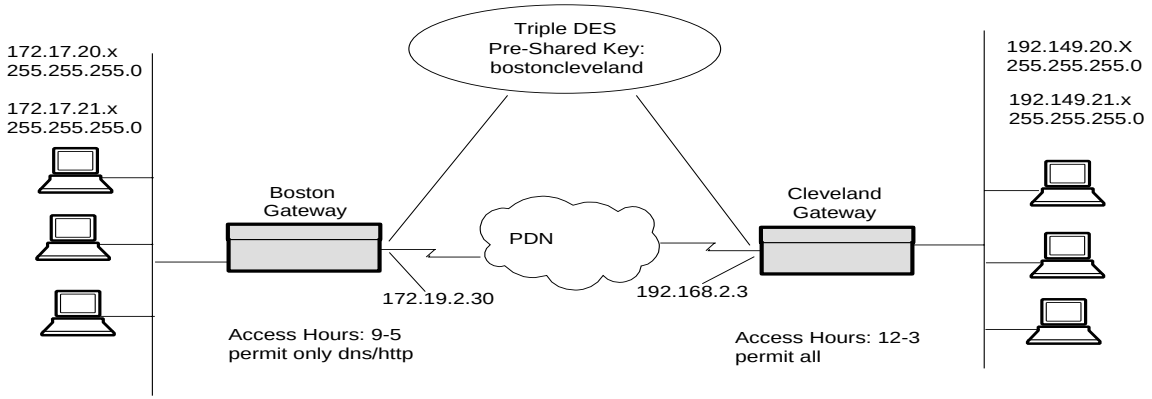
Chapter 5
Configuring branch office tunnels

The branch office feature allows you to configure a secure tunnel connection between two private networks. Typically, one private network is behind a locally configured Contivity while the other is behind a remote Contivity. Branch office configuration allows you to configure the accessible subnetworks behind each Contivity. The configuration also contains the information that is necessary to set up the connection, such as the Contivity's IP addresses, encryption types, and authentication methods. You can apply local policy restrictions, such as access hours, filter sets, and call admission priorities, to limit connectivity into local subnetworks.

The Contivity Secure IP Services supports symmetric, or peer-to-peer branch office tunnels with fixed endpoints, and asymmetric branch office tunnels. An asymmetric branch office tunnel is a branch office tunnel where one of the endpoints does not have a fixed IP address. Such situations exist in the small branch office or SOHO environments where the Contivity Secure IP Services Gateway's public interface is behind a DSL or cable modem. The DSL or cable modem services typically do not guarantee a static IP address. Branch office tunnels in these situations are asymmetric because only one side of the tunnel can initiate a connection.

Figure 25 shows a typical branch office environment.

Figure 25 Typical branch office environment



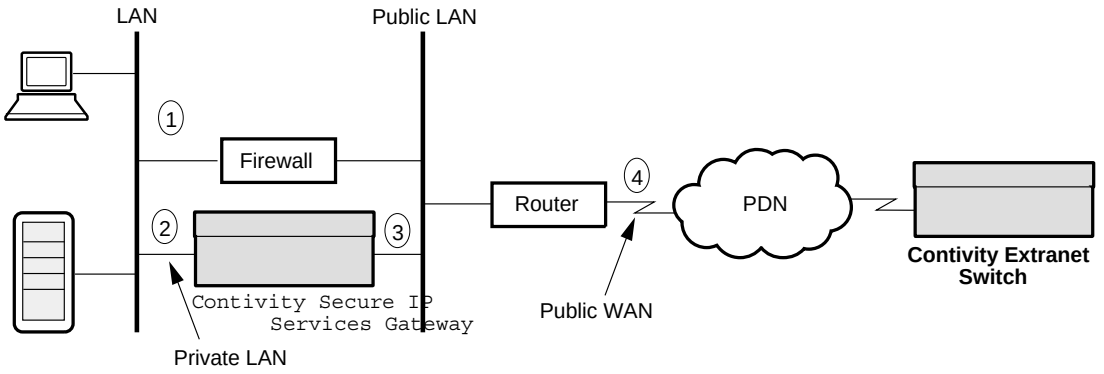
The section "Sample branch office configuration" provides sample branch office configurations for two locations, Boston and Cleveland. The initial configurations show connections established with pre-shared keys.

In a mixed environment, you might want to tunnel connections to certain networks, and have all other traffic go to the Internet. You must configure the default Contivity with a static route to the Contivity for accessible networks (refer to Profiles > Branch Office > Edit Branch Office Connection). The default private LAN router (the firewall) must redirect packets intended for remote branch office subnets.

In this case, as with any branch-to-branch configuration, you must configure each branch Contivity with the same encryption settings and pre-shared key (password). Of course, the accessible local and remote subnetwork addresses and subnet masks would be inverted in each Contivity's configuration.

Figure 26 shows a branch-to-branch configuration with a firewall and a router.

Figure 26 Branch-to-branch with a firewall and a router



In the branch-to-branch illustration, the following interactions take place with a Contivity Secure IP Services Gateway:

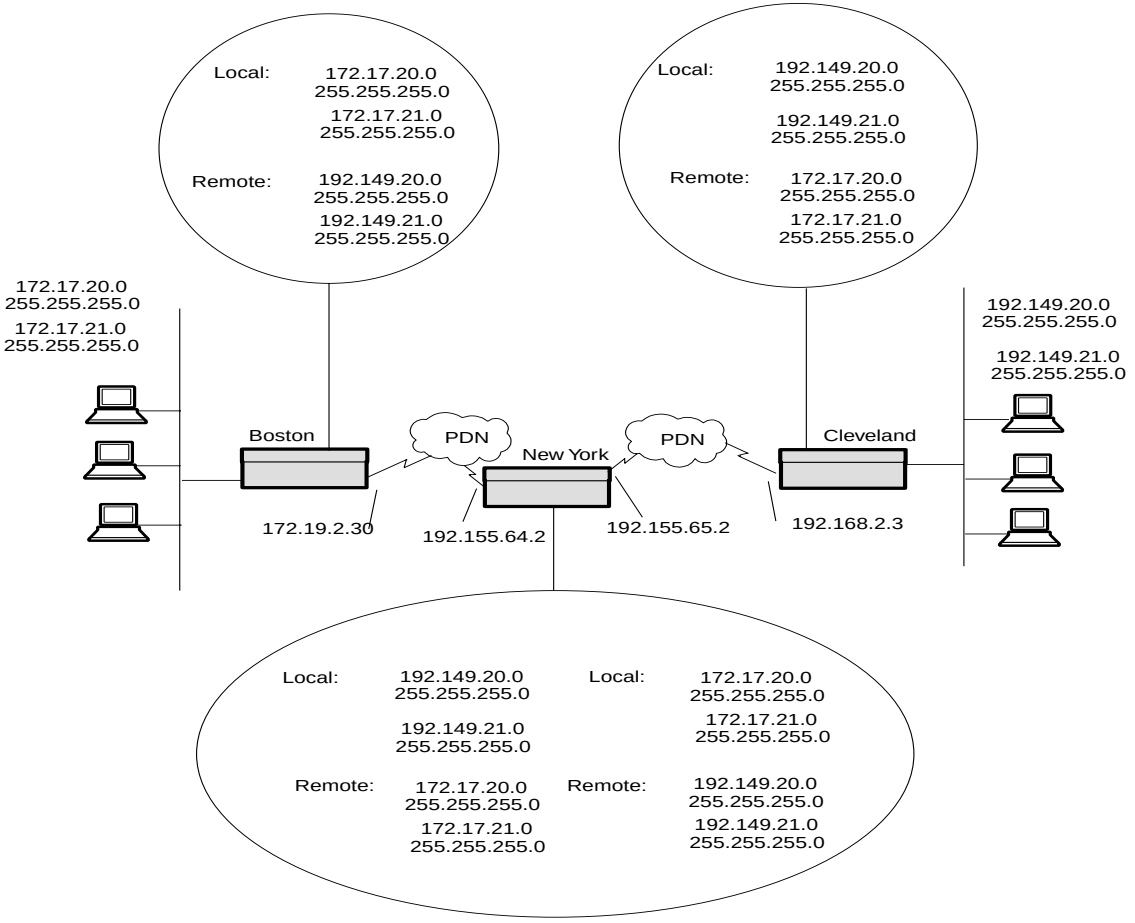
1. The PC sends packets to the default route (the firewall).
2. The firewall redirects the packets to the local Contivity branch office connection.
3. The encapsulated data goes onto the public LAN.
4. The default public LAN route directs the encapsulated data to the remote Contivity branch office connection.

For a Contivity that has a WAN link, actions 3 and 4 collapse together, and the encapsulated data is directed to the remote server.

In a three-Contivity topology, the two indirectly connected Contivity gateways can create tunnels at will as long as each Contivity properly includes all of the local and remote subnetworks and subnetwork masks as accessible networks. Figure 27 shows the relationship between three Contivity gateways and the local and remote networks that must be configured for each link to allow indirectly connected branch offices to bring up tunnels at will. The New York Contivity in the middle has two branch office connections configured.

All connections must have identical encryption settings. However, only adjacent connections are required to share keys. For example in the following figure, the Boston ↔ New York connection shares keys and the New York ↔ Cleveland connection shares keys. Boston and Cleveland are not required to share keys.

Figure 27 Indirectly connected branch offices



In branch offices, you might have two or more branches that use the same LAN addressing scheme. Nonetheless, users still have to communicate with one another across the branches.

Note: PPP multilink is not supported with branch office tunnels. It is only supported with end user tunnels.

NAT allows branch office connections to eliminate problems with overlapping addresses on both sides of the connection, and it allows you to hide the LAN addresses. To set up branch offices with NAT, see *Configuring Firewalls, Filters, and NAT for the Contivity Secure IP Services Gateway.*

Sample branch office configuration

This section describes an example of the procedure used to create a branch office VPN connection between two Contivity gateways. In this example, the local Contivity is at the enterprise headquarters in Boston and the remote Contivity is at a sales office in Cleveland.

When you set up a branch office connection, you must perform the configuration procedure twice, once for each of the two Contivity gateways that make up the connection. The branch office settings for the two Contivity gateways mirror each other. For example, the local address setting that you configure on the Boston Contivity would be considered the remote address setting when you configure the Cleveland Contivity.

Figure 28 shows the configuration information and the addresses that are used in this example. It lists the procedure for setting up a branch office connection and the management Web pages that are used during the configuration process. Figure 29 also shows where the information from the figure is entered on the management Web pages.

Figure 28 Sample branch office configuration

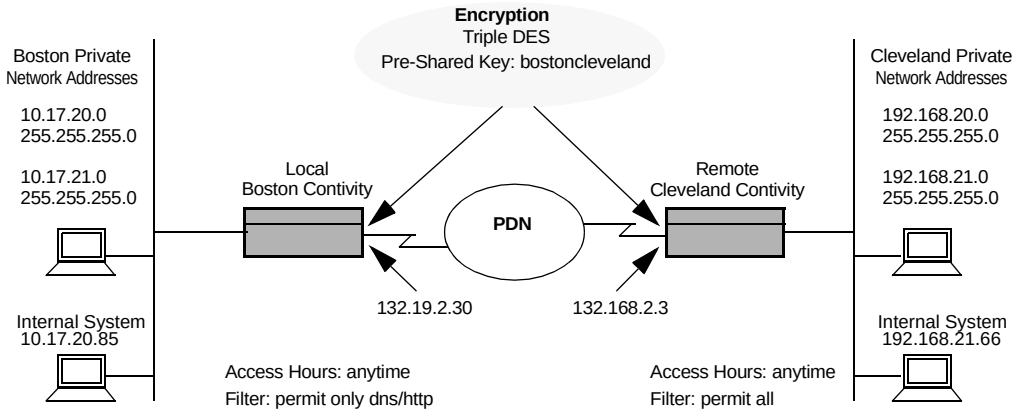
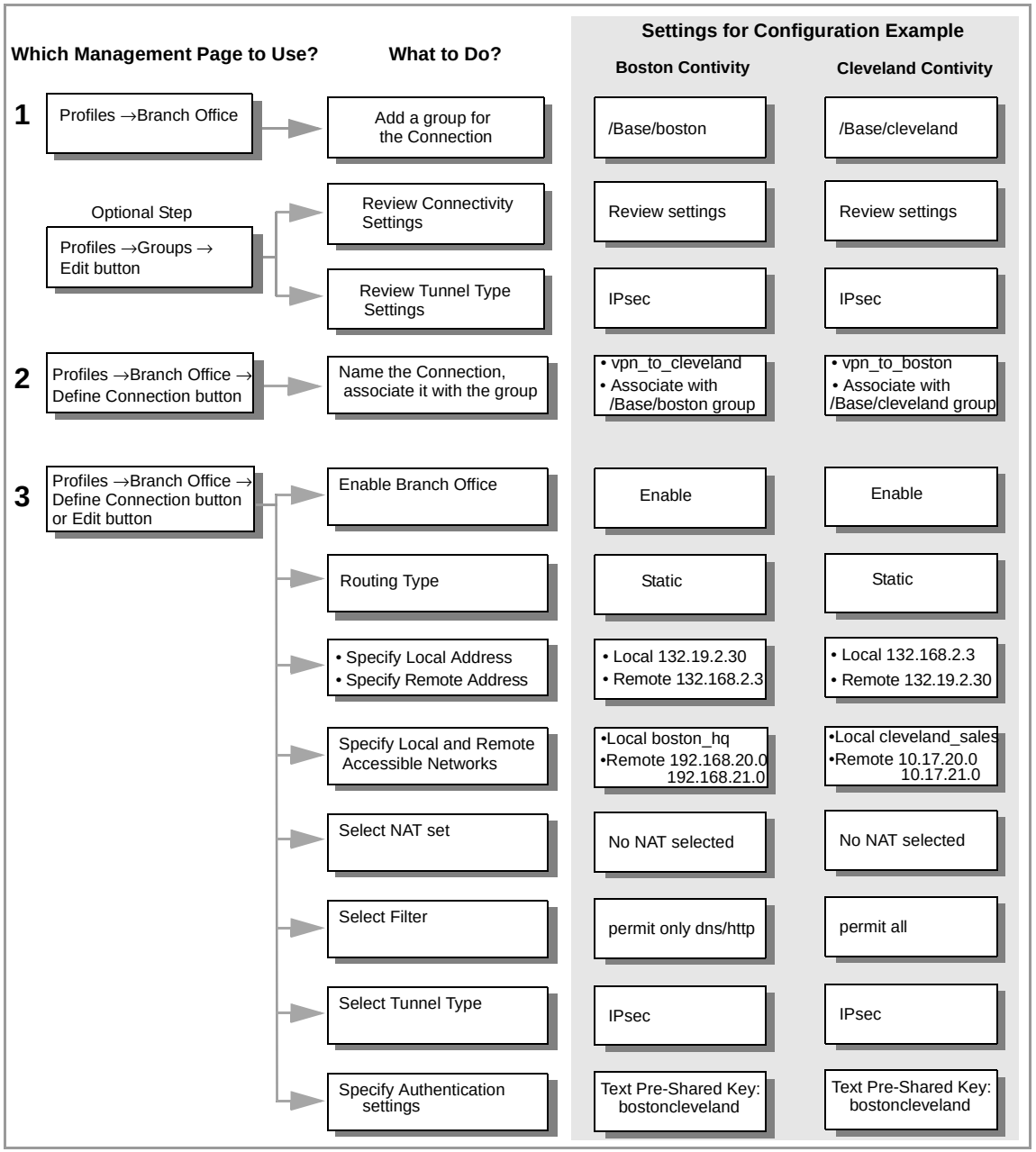


Figure 29 Setting up a branch office configuration



As the administrator of a branch office connection, you can manage the level of access that you give to users of the connection. You specify when the connection is used, what operations can be done through the connection, and which systems on the private networks can be accessed.

Before configuring a branch office connection, check that the following management Web pages are set up in accordance with your management policies and the planned usage for the connection. You use the settings on these pages when you configure the branch office connection.

- The System > Forwarding page must allow branch office-to-branch office traffic.
- The Profiles > Networks page must list the Contivity's private networks. In the sample configuration, the local Contivity's internal network name is boston_hq and the subnets are 10.17.20.0 and 10.17.21.0. The remote systems behind the remote Contivity can reach systems in these networks.

  The remote Contivity's internal network name is cleveland_sales and the subnets are 10.17.20.0 and 10.17.21.0. The remote systems behind the local Contivity can reach systems in these networks.
- The Profiles > Hours page must have the Hours of Access setting that you want to use. The example uses the setting of Anytime.
- The Profiles > Filters page must have the filters that you want to use for the branch office connection. For the example, the local Contivity uses a filter of permit only dns/http, and the remote Contivity uses permit all.

Configuring a branch office

To create a new branch office connection, give it a name and associate it with a group. You can choose an existing group or create a new one. The branch office connection then uses that group's attributes, such as password management and encryption. You set the group's attributes on the Profiles > Groups screen.

The branch office connection then inherits the attributes of that group. You can associate multiple branch offices with the same group, thereby saving setup time and increasing management efficiency. For example, you might plan on creating several VPN connections from various remote sales offices into your enterprise headquarters. In this case, you create all of the connections in the same group so they all have the same attributes, such as hours of access, encryption method, and password management.

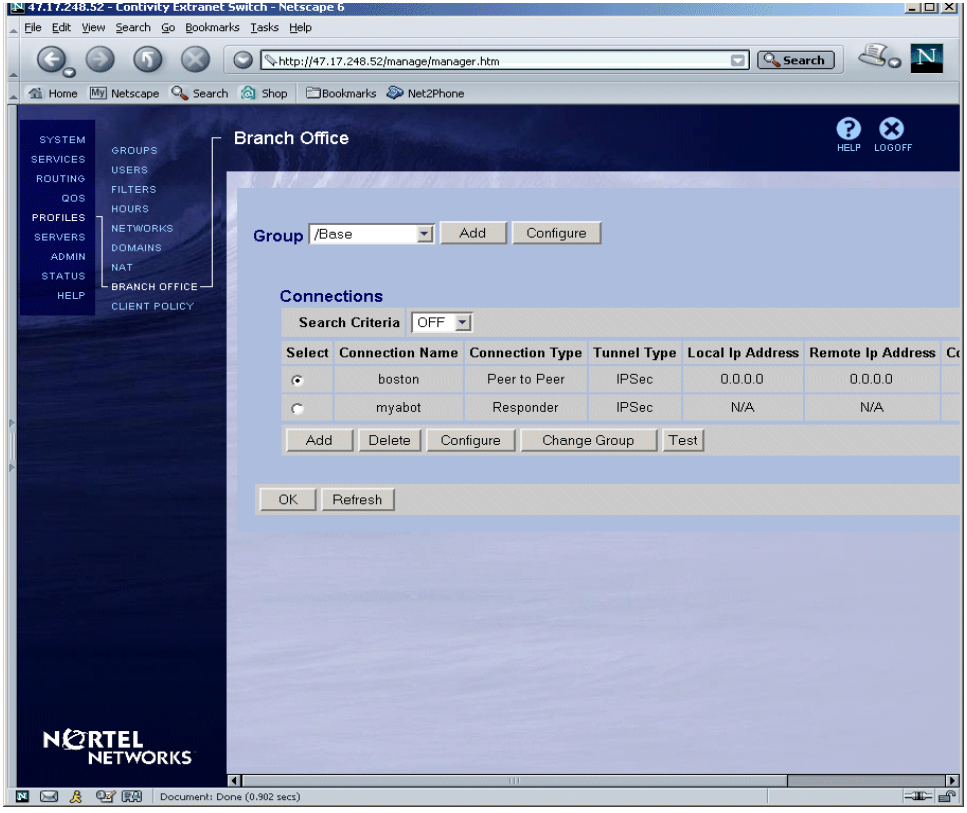
Use the Branch Office screen to create new branch office connections and to edit or delete existing connections. You can also add or edit the group that is associated with your branch office connection.

Note: Certain configuration changes are not reflected in the active branch office tunnel until it is disabled then re-enabled. Examples of these types of configuration changes are: changes to the tunnel filter used by the branch office (changing which filter is applied is reflected in the active branch office tunnel); changes to the NAT policy used by the branch office; routing changes, such as adding or deleting a default route.

To define a new branch office connection:

1 Go to the Profiles > Branch Office screen.

Figure 30 Branch office screen

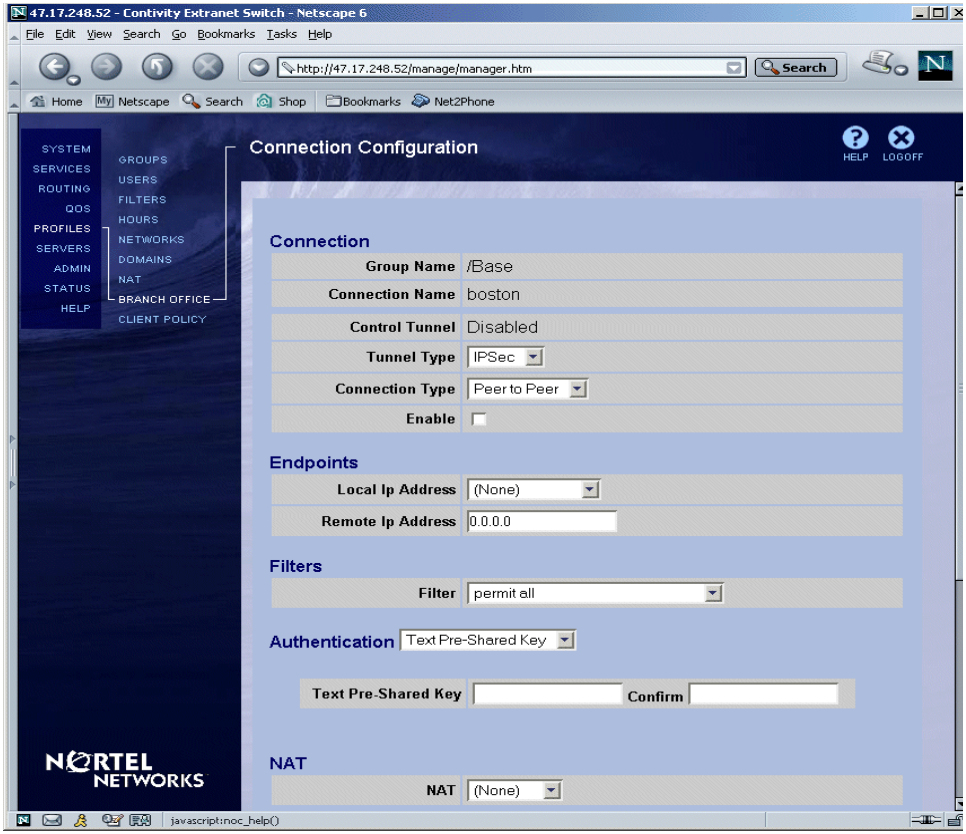


2. In the Group section, the list shows all the branch office groups on the Contivity. Select the group whose attributes you want the new group to inherit.
3. Click on the Add button to create a new group. The group name can be a maximum of 64 characters (spaces are permitted). The new group inherits the attributes (for example, Access Hours) of its parent group, which are then used by the branch office connection.
4. In the Connections section, select the search criteria: off, on, apply filter, or operator.
5. Click on the appropriate button to add, delete, configure, change group, or test the connection.

To configure a connection:

1. Select the radio button next to connection name and click on Configure

Figure 31 Connection configuration screen



2 Select the tunnel type for the connection from the list. The default type is IPsec. Click the drop-down list and select either IPsec, PPTP, or L2TP.

Note: If you change the tunnel type, the fields in the Authentication portion of this screen change to reflect the different configuration requirements for the selected tunnel type.

3 Select the type of Branch Office connection that you want this branch office to use.

- Peer to peer connection type is the traditional branch office tunnel, where either side can initiate traffic.

- Initiator, where with Asynchronous Branch Office Tunnels (ABOT), one side must be configured as the initiator and the other as the responder. Only the Initiator can bring up the tunnel. When the connection type is set to initiator, there is no need to define a local endpoint. You should only configure an IPsec tunnel type. IPsec authentication requires an initiator ID.



Note: Asynchronous branch office tunnels work only on public interfaces.

- Responder, where neither local or remote endpoints are required. You must configure IPsec authentication to specify the same initiator ID as in the associated initiator branch office tunnel.

4 Click on Enable to enable the branch office connection.



Note: For security, the Enable Branch Office Connection selection is automatically disabled when you attempt to save an incorrect configuration.

5 Select the Endpoint Address fields to specify the public interface IP addresses of the Contivity gateways that form the branch office connection. The Local Endpoint address is the public interface IP address of the Contivity whose management interface you are using. The Remote Endpoint address is the public interface IP address of the Contivity that forms the opposite end of the branch office connection.

6 Click the drop-down list and choose the filter that you want this branch office connection to use. The default is permit all. You can specify one filter. Packet filtering controls the types of access allowed for users of this branch connection. Filters are based on various parameters, including protocol ID, direction, IP addresses, source, port, and TCP connection establishment. Filters are defined on the Profiles > Filters screen.

7 For Authentication, configure the authentication that is used between the local and remote branch office. The fields that appear in this screen depend on whether you are using an IPsec, PPTP, or L2TP tunnel type.



Note: If you create a branch office connection using any IPsec certificate and you choose IP address as the alternate name, you must use the IP address of the public interface that is on the branch office end of the connection.

8 Under NAT, select either PortNAT or none. NAT enables you to build your VPN without requiring that you reconfigure or rename your existing network. NAT sets are defined on the Profiles > NAT screen. For further information on NAT, see *Configuring Firewalls, Filters, and NAT for the Contivity Secure IP Services Gateway* book.

9 For IP Configuration, select either Static or Dynamic routing for this branch office connection:

- If you choose Static routing, you must manually specify the Accessible Networks (the private internal networks behind a gateway that can be accessed via the branch office connection).
- If you choose Dynamic, the routing protocol automatically determines the accessible networks based on information that is entered on the System > LAN Interfaces > Edit IP Address screen.

10 Click on the Create Local Network button to go the Profiles > Networks screen and define a local network. The Local networks are the subnetworks on the private internal network of the local gateway.If you want to edit an existing local network, select it from the list and the Connection Configuration screen appears. These networks have been previously set up on the Profiles > Networks screen.

11 To specify the remote network, click on the Add button to go to the Add Networks screen and add the remote networks for the branch office configuration. Remote networks are the subnetworks on the private network of the remote gateway.

Sample branch office procedure

To create a dynamic peer-to-peer branch office tunnel over ISDN with local/peer authentication that includes MS-ChapV2 and RC4-40 encryption, enabled compression and a permit all filter:

1. Launch the Web browser and enter the IP of the Contivity.
2. Enter the user name and password.
3. Select Profiles > Branch Office.
4. Clic on the Add Group name and OK.
5. Select your group from the group pull down menu.
6. Click on Add Connection.
7. Connection screen, enter the connection name (up to 128 characters).
8. Select the tunnel type PPTP and Peer to Peer and Click on OK.
9. On the Connection Configuration screen:
    a. Select the Locap IP from the Endpoints and enter the remote IP that this PPTP tunnel will connect to.
    b. In the Authentication section, enter a local UID and the remote peer UID and password (must match the remote tunnel).
    c. Select the MS-CJAP V2 authentication and RC4-40 emcru[topm/
    d. Enable Compression and Compression Stateless Mode.
    e. Select Dynamic from the IP Configuration menu, and keep the RIP and OSPF defaults.
    f. Click on OK.
10. Configure the other end of the tunnel with the same information.
11. Click on the Test button on each end of the tunnel to verify connectivity.
12. Try to ping from on PC to the other PC through the branch office.

Chapter 6
Configuring control tunnels

Control tunnels are special tunnels that allow you to securely manage a Contivity Secure IP Services Gateway over the Internet. The primary reasons for creating control tunnels are secure management and network data integrity. Control tunnels provide secure access to a customer's remote Contivity so that you can manage it over a network. Control tunnels also guarantee that no data from the network behind that customer's Contivity could be accessed by anyone on the network who manages the Contivity.

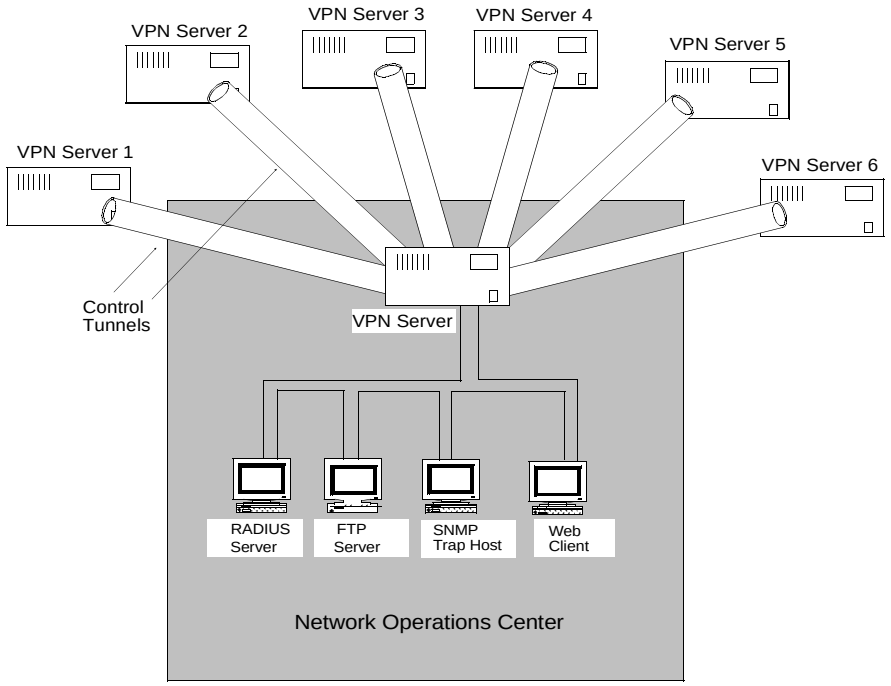
You can allow access to FTP, DHCP, RADIUS, and DNS servers from the Contivity through the control tunnel. Control tunnels allow you to easily configure secure tunnels to any Contivity that you want to manage. This allows you to set up an encrypted tunnel to a customer's Contivity. Through that tunnel you can perform all the necessary management tasks, such as HTTP, FTP, SNMP, and Telnet.



Note: To establish a control tunnel over a NAT connection, use IPSec-capable NAT. Control tunnels cannot establish a connection while the Contivity Stateful Firewall is enabled when you use the Autodetect IPSec-capable NAT feature.

Figure 32 shows a sample branch office control tunnel environment where a central VPN server can control several VPN devices and configure services, such as RADIUS, FTP backup, SNMP Traps through Web client management, or Telnet.

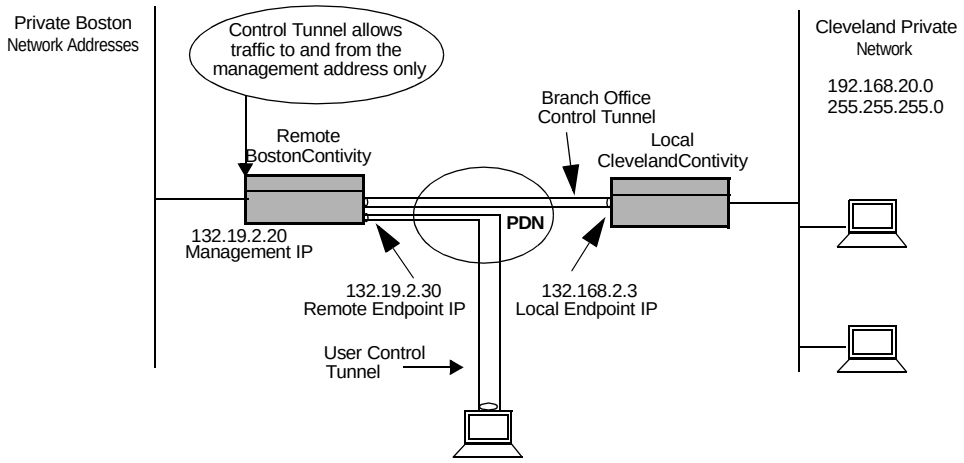
Figure 32 Branch office control tunnel



Control tunnel types

There are two types of control tunnels: a branch office control tunnel and a user control tunnel. With both tunnel types, you can establish a secure IPsec tunnel to a system that you want to manage. The traffic inside the tunnels is limited to the Contivity's management IP address only, which is unique to control tunnels. Figure 33 shows a special branch office control tunnel from a network operations center in Cleveland, and also a user control tunnel.

Figure 33 Sample control tunnel environment



Branch office control tunnels allow anyone on the configured network to communicate with the Contivity being managed. This allows a Contivity to communicate with various systems within a company's network operations center or corporate headquarters (the Cleveland private network).

A user control tunnel allows a Contivity VPN Client to communicate with a Contivity that is being managed. This allows network management personnel from anywhere in the world access to the management tasks.

If you work at a NOC in Cleveland and you manage a customer's Contivity that is located in Boston, you would want to use control tunnels. On one end of the control tunnel (the Contivity under management), access is always restricted to the management address only. Access to the Boston Contivity is limited. The Cleveland end of the tunnel could allow access to its entire private network. This allows multiple systems in your Cleveland NOC to communicate with the management address only of the Boston Contivity; or for the Boston Contivity to use remote servers (FTP, DHCP, RADIUS, and DNS servers) on the Cleveland private network.

In this environment, the remote Boston Contivity is a control tunnel to the local Cleveland Contivity. From any system on the Cleveland network, you can access the management address for the Boston Contivity. This allows systems on the Cleveland network to initiate management operations on the Boston Contivity, such as HTTP, FTP, and Telnet. Yet because it is a control tunnel, users on the Cleveland private networks cannot exchange packets with users on the private Boston Network.

Additionally, a user control tunnel is configured so that a remote user can establish a control tunnel when using the IPsec client. You create this user account with password authentication in the Control Tunnels group using the serial port.

Restricted mode

The Restricted mode feature prevents management of the Contivity except through a control tunnel. This limits the scope of management to someone who has the proper credentials both to set up the tunnel (if it is an end user) and to log in as an administrator (administrative access privileges). Having the proper access privileges acts as a level of security. Additionally, since in restricted mode you are forced to manage the Contivity through a tunnel, you are guaranteeing data protection through encryption.

You enable Restricted mode through the Serial Interface menu or the command line interface available through Telnet. In Restricted mode, you can perform the key management functions through the control tunnel, including HTTP, FTP, SNMP, and Telnet. All other attempts to perform these actions outside of the control tunnel will fail. You cannot enter Restricted mode unless there is an active control tunnel. This ensures there is a mechanism to manage the Contivity in restricted mode.

Nailed-up control tunnels

You may want to have some control tunnels remain up even when there is no traffic traversing the control tunnel. This is generally the case for branch office versus end user control tunnels.



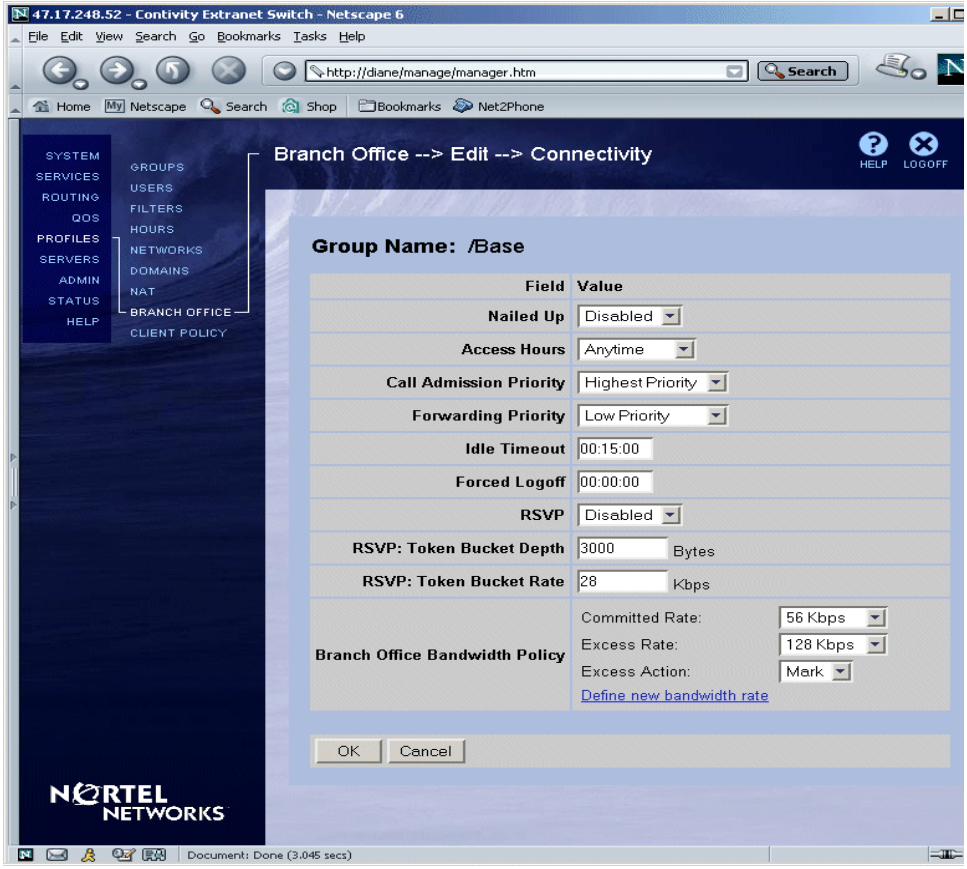
Note: If you change any settings to the branch office connection when using nailed up tunnels, you must bring down the tunnel for the changes to take effect.

To create a nailed-up control tunnel using the nailed-up parameter:

1. Go to Profiles > Branch Office screen and click on the Edit button next to the group that you want to have nailed up.
2. On the Edit Group screen, click on the Configure button under the Connectivity section.
3. On the Connectivity screen, when you click on the Configure button next to the Nailed Up field, a drop-down list gives you the option to select Enabled or Disabled. You should enable this parameter only on the initiating side of the tunnel.

Another way to nail up control tunnels, is to create a script that continuously sends ping packets to the management IP address of the Contivity on the customer premise through the control tunnel from a host at the network operations center. The pings must occur at an interval that is less than the Idle Timeout value. These pings act as a liveliness detection and perform keepalive signals for the end connection, and report to the sender that the packet was received or that there was no response.

Figure 34 Edit Connectivity screen



4 Click on Enabled. Disabled is the default.

5 Click on OK.

Creating control tunnels

To create a special branch office connection, you must create a control tunnel definition on the remote customer Contivity. There are two methods you can use to create control tunnels:

- On the Contivity's GUI, use the Profiles > Branch Office screens to create the branch office connection and specify that it is for a control tunnel.

- For the command line interface, use the Contivity's command line interface (described in *Reference for the Contivity Secure IP Services Gateway Command Line Interface*) to set up the connection as a control tunnel. This procedure is described in the following example.

To configure the local Contivity:

1. Initiate a Telnet session to the customer's Contivity.
2. Enter the appropriate control create string, following the required control create parameters already described. A sample string follows:

```
control create boston bostoncleveland 132.19.2.20 132.19.2.30
192.168.2.3 192.168.20.0 255.255.255.0
```

   Management Only (a special control tunnel filter) is used by default with control tunnels to maximize security.

3. To view Help, enter control help create. These are control create parameters that you must enter:

```
CONTROL CREATE <name> <password> <MGMT/Local_P> <Local_endpoint>
<Remote_endpoint> <Remote_Subnet_Address> <Remote_Subnet_Mask>
```

   If you are using the local Contivity current Management IP address (132.19.2.20) rather than a substitute, then the network address translation feature is unnecessary. If not, enable control on the remote Contivity and enter the control address through the command line interface. If you enter an address other than the management IP address (MGMT), NAT creates a NAT set with a static rule. The NAT set is called Control plus the name of the connection (for example, Control Boston). This also creates a network definition that is named Control and the name of the connection. The network definition contains the NAT management address. In this case, the branch office connection automatically fills in the correct NAT rule and accessible network. When using the control create commands, you must enter them in a complete string. The Contivity that you are controlling sets a management only filter by default that restricts access to the management IP address only. You can verify the control tunnel connection from the Profiles > Branch Office: Control Tunnels connection field.

After you configure the local Contivity, you must configure the Contivity located at the remote site. Complete the following steps to define the branch office connection for the remote Contivity.

To create a new group:

1. Access the Profiles > Branch Office screen.
2. Click on the Add Group button.
3. From the list, select the parent group whose attributes the new group inherits; for example, /Base.
4. Enter the name for the new group. Click on OK to save the settings and return to the Profiles > Branch Office screen. You can use the Edit button next to the group name on the Profiles > Branch Office screen to review or modify the group's attributes.

To define the branch office connection, specify a name for the connection, then associate the connection with a group:

1. On the Profiles > Branch Office screen, click on Define Branch Office Connection.
2. On the initial Define Connection screen, name the connection, for example vpn_to_boston which is specified on the Profiles > Networks screen.
3. Click on the name in the list to associate the connection with the group, for example /Base/cleveland.
4. Click on OK. The configuration screen for the new branch office connection appears.

On the Define Connection configuration screen, you enter required configuration information for the local branch office connection, for example, static routing and the IPsec tunnel type.

1. Enable the branch office connection by selecting the check box.
2. Click on the list and select the routing type that you want to use for your branch office connection, for example, static routing. You *cannot* use control tunnels with RIP.
3. Specify the addresses of the public interfaces of the two Contivity gateways forming the connection.
    a. For the local endpoint address, click on the list and select the address of the local Contivity (for example, 132.168.2.3).

b In the remote endpoint address field, enter the address of the remote Contivity (for example, 132.19.2.30) that you want to form the opposite end of the branch office connection.

4 Specify the private subnetworks that can be reached through the tunnel connections of this branch office connection.

a Click on the list and select the network address(es), for example, the cleveland entry previously created. The local network is the Contivity's private network, which is specified on the Profiles > Networks screen.

b Click on Add in the Remote Endpoint field, and enter the Management IP address of the local Contivity and its mask (for example, a host mask of 255.255.255.255).

5 Click on the list, then select the No NAT Translation option.

6 Click on the desired filter for the connection.

7 Select the IPsec tunnel type.

8 Set up the authentication method for the connection, for example, text pre-shared key. Enter the key (for example, bostoncleveland), then retype it in the Confirm Text String field.

9 Click OK to save the configuration settings.

Next, you should verify your branch office connection by sending ping packets to the management IP address of the local Contivity. Or, you can establish a Web connection to the local Contivity and attempt to configure it.

Creating a user control tunnel from the serial interface

You can create a user tunnel using the serial interface. Control tunnels allow the management of the Contivity without access to anything on the network other than the management IP address. This is used to force management through an encrypted tunnel and restricts access to the local resource such as outsourcing management of a Contivity. You create the control tunnel user in the group /Base/Control Tunnels.

1 Open a connection to the serial interface.

2 Type **5** to Create a user management tunnel.

3. Enter a user name and password.
4. When prompted for an IP address, enter an address that would be a static IP address for the control tunnel or leave it blank to use the IP Addr Pool. This creates a group called Control and places this user within this group.

Chapter 7
Configuring networks, domains, and client policies

When you enable either split tunneling or a branch office, you can associate networks to groups. If you are using the auto connect feature, you can specify domains and group them into sets. If you are using split tunneling, you can use the client policy feature to prevent potential security violations.

Configuring networks

You can specify network routes that are tunneled when you enable the split tunneling or branch office features. After you specify networks, you associate them to specific groups for tunneling capabilities through the Profiles > Groups > Connectivity Edit screen. You specify branch office networks through the Profiles > Branch Office Edit screen..

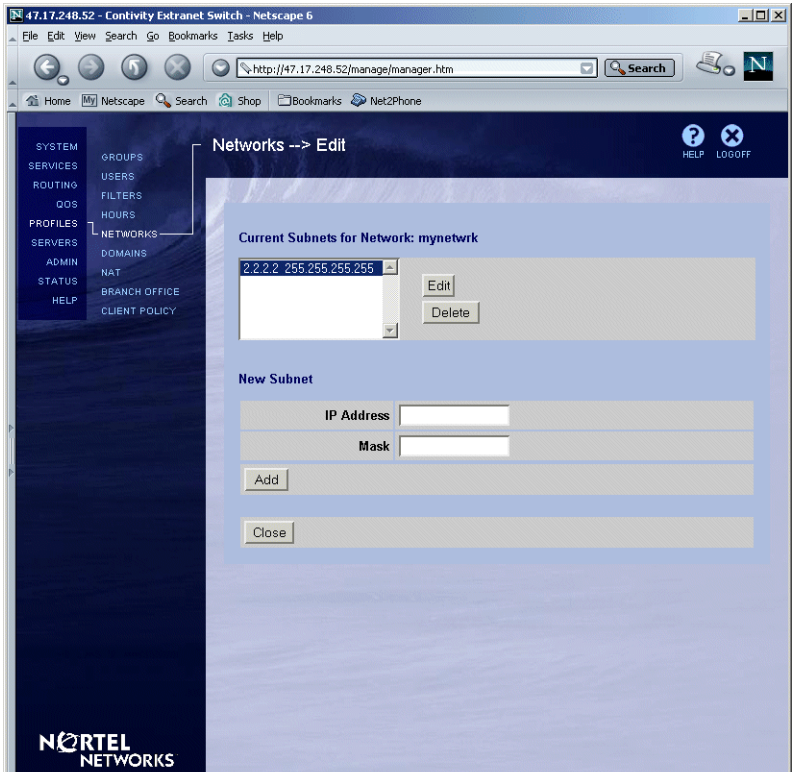


Note: A maximum of 16 routes are allowed on the August 1995 version of Windows 95 systems; the gateway displays more than 16 routes, but you cannot tunnel through them.

To configure a network:

1. Go to Profiles > Networks > Create and enter the network name in the edit box.
2. Click on the Create button.
3. The Networks Edit screen allows you to assign IP addresses and subnet masks to the networks. Click on the network that you want to modify and then click on the Edit button. The Filter Rules for that group appear.

Figure 35 Editing networks



4 The Current Subnets For section shows the currently configured IP addresses and subnet masks for the network that you are editing. In the New Subnets For section, enter the IP address and subnet mask for the network. This field allows you to define an access network within a group profile that permits users access only if they tunnel from the defined network.

a If you use this feature, you must go to Profiles > Groups > *Group Name* > Edit.

b In the Connectivity section, click on Configure.

c For Access Network Name, select the name you chose and click on OK.

5 Click on Add.

Configuring domains

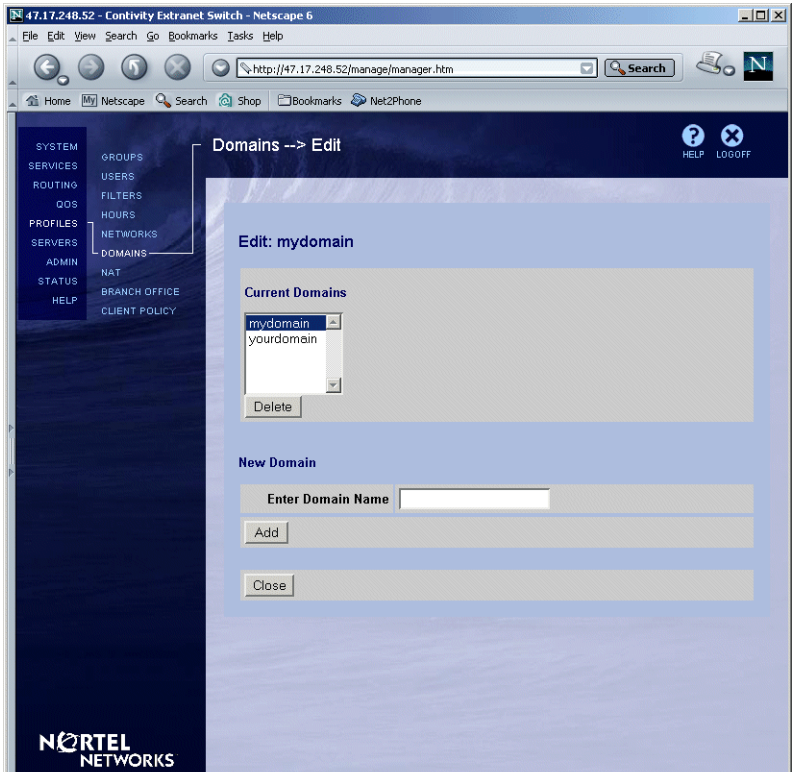
You can specify the domains that are used by the client auto connect feature to simplify management by grouping domains into sets. You can then specify which sets of domains are used for particular IPsec tunnels on the Profiles > Groups > Edit IPsec screen.

When a remote client user attempts to connect to a location, such as a Web site, that is in a specified domain or set of domains, the client cuto connect feature is started.

To configure domains:

1. If you want to creat a new domain, enter the domain name in the edit box. The Current Domain Sets section shows the currently configured sets of domains that you can use when specifying the Client Auto Connect feature.
2. Click on the domain set that you want to modify, then click the Edit button. The Edit Domain Set screen appears.

Figure 36 Editing domains



3 Enter the name of the new domain set.

4 Click on the Create Domain button. The new name is added to the Current Domain Sets field. You can then edit the domain set and add the names of the domains that you want included in the set.

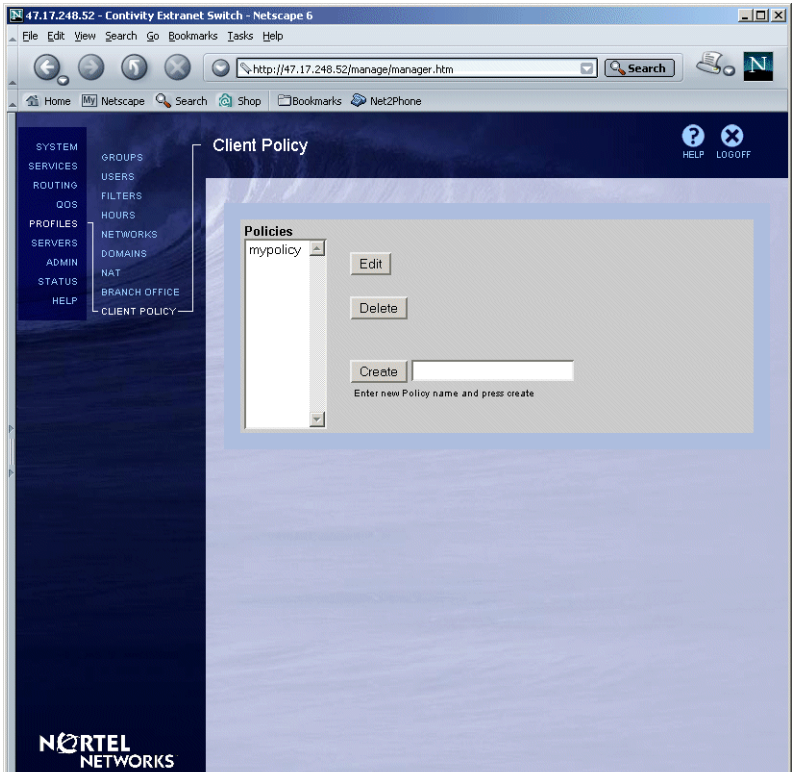
Client policy

Client policy helps prevent potential security violations that could occur when you are using the split tunneling feature. Split tunneling allows client data to travel either through a tunnel to the enterprise network or directly to the Internet. Although a powerful feature, this could allow an application on the client to maliciously forward packets from the Internet to the enterprise network.

To configure a client policy:

1. If you want to create a new policy, enter the name in the edit box and click on the Create button.
2. Click on the policy that you want to modify, then click the Edit button. The Edit Client Policy screen appears.

Figure 37 Client policy screen



3. In the Permitted Applications section, click on the application and click on Add.
4. For Protocol, select either TCP or UDP.
5. Enter the port number. The default is
6. For Application Type, select either Client or Server.
7. Click on Apply.

Appendix A
Branch office quick start template

The branch office quick start template provides a list of values that the local Contivity 1010/1050/1100 users will need to enter on the BOQS screen. You can enter the appropriate values in the right-hand column and then fax, send, or E-mail the template to the local user along with any other information that they may need, such as who to contact for further information or questions.

Central office tunnel configuration	**Your value**
Central office tunnel name	
Central office tunnel password	
Central office public IP address	
Central office DNS server IP address	
Central office WINS sever IP address	
Private network IP address	
Private network mask	
Network Operation Center tunnel configuration	**Your value**
Network operation center tunnel name	
Network operation center tunnel password	
Network operations center public IP address	
Network operations center private network IP address	
Network operations center private net mask	
Branch office switch management IP address	

Glossary

acknowledgement (ACK)

A type of message sent to indicate that a block of data arrived at its destination without error.

address masks

IP addresses used to represent a series or range of IP addresses.

authentication

A security procedure where a user verifies his identity before accessing networks protected by a firewall.

bandwidth

The difference between the highest and lowest frequencies of a transmission channel; amount of data that can be sent through a given communications circuit.

certification authority (CA)

An authority that issues digital certificates and manages the life cycle of certificates.

Challenge Handshake Authentication Protocol (CHAP)

A peer entity authentication method for PPP, using a randomly-generated challenge and requiring a matching response that depends on a cryptographic hash of the challenge and a secret key.

client

A system or process that requests a service of another system or process.

default route

A route that is used when the switch receives traffic for which no matching route is in the routing table.

Diffie-Helman

A key agreement algorithm that does key establishment, not encryption. However, the key it produces may be used for encryption, for further key management, or any other cryptography.

digital certificate

A certificate document in the form of a digital data object to which is appended a computed digital signature value that depends on the data object.

distinguished name (DN)

An identifier that uniquely represents an object in the X.500 Directory Information Tree. An X.509 public-key certificate or CRL contains a DN that identifies its issuer, and attribute certificate identifies its subject.

Domain Name System (DNS)

A general purpose distributed, replicated, data query service used to look up host IP addresses based on host names. DNS applications can perform name-to-address and address-to-name translations.

dynamic routes

Routes that are learned via the switch's RIP support, and are used for branch office connections and the private interface.

encryption

The manipulation of a packet’s data to prevent any but the intended recipient from reading the data.

encryption certificate

A public-key certificate that contains a public key that is intended to be used for encrypting data, rather than for verifying digital signatures or performing other cryptographic functions.

Federal Information Processing Standards (FIPS)

Technical guidelines for U.S. Government procurements of information processing system equipment and services.

File Transfer Protocol (FTP)

A TCP-based application layer Internet Standard protocol that transfers files to and from a remote host.

firewall

A collection of hardware and software components that controls communication between two networks, such as a private network and the Internet. All information passed between the two networks must pass through the firewall. The firewall allows only authorized traffic to pass between the networks.

gateway

A communications device or program that passes data between networks having similar functions but dissimilar implementations.

interface

The connection between a router and one of its attached networks. An interface to a network has a single IP address and mask associated with it.

Internet

The single, interconnected, worldwide system of commercial, government, educational, and other computer networks that share a set of protocols.

Internet Protocol (IP)

The transport layer protocol used by the Internet Protocol family for transporting information among computers.

Internet Security Association and Key Management Protocol (ISAKMP)

Defines how encryption keys for sessions are initiated and updated.

intranet

A computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.

IP address

The identifiers used by the protocols that govern Internet information exchange. The Internet Network Information Center assigns these numbers to uniquely identify different machines on the Internet.

IPsec

A tunneling protocol that offers a strong level of encryption, integrity protection. It uses digital certificates, password-based keys, and tokens for authentication.

IPsec Key Exchange (IKE)

An Internet IPsec key-establishment protocol that puts in place authenticated keying information for use with ISAKMP and for other security associations.

key agreement

A method for negotiating a key value without transferring the key, even in an encrypted form, such as Diffie-Helman.

Layer2 Tunneling Protocol (L2TP)

Tunneling protocol that enables secure remote access to enterprise networks across the Internet.

Lightweight Directory Access Protocol (LDAP)

Protocol based on directory entries that provide access for management and browser applications that provide read/write interactive access to the X.500 directory.

local area network (LAN)

A data network intended to serve an area of only a small area to optimize data transfer rates.

management information base (MIB)

The set of parameters an SNMP management station can query or set in the SNMP agent of a network device, such as a router.

management IP address

The IP address that is used to manage all system services from a Web browser, such as HTTP, FTP, and SNMP. This address must be accessible from one of the switch's private physical interfaces. To be accessible, the Management IP Address must map to the same network as one of the private interfaces.

medial access control (MAC) address

The hardware address of a device connected to a shared media.

Network Address Translation (NAT)

A mechanism that converts an internal network’s private addressing scheme to an acceptable Internet address, thereby enabling the internal systems to communicate on the Internet.

Network Time Protocol (NTP)

Synchronizes the clocks of various devices across networks.

Open Shortest Path First (OSPF)

OSPF is a link-state routing protocol that maintains a database from which a routing table is constructed from the shortest path, using a minimum of routing protocol traffic.

packet

The unit of data sent across a network. Typically, it refers to application data units.

PING

A program used to test reachability of destinations by sending an ICMP echo request and waiting for a reply.

Point-to-Point Protocol (PPP)

A protocol that provides a method for transmitting packets over serial point-to-point links.

Point-to-Point Tunneling Protocol (PPTP)

A tunneling protocol that is used as a security tool.

port

A transport layer demultiplexing value. Each application has a unique port number associated with it.

private default route

The default routes that are used for traffic that comes into the switch via a public interface, through a tunnel, or from the switch's public interface address.

protocol

A formal description of message formats and the rules two computers must follow to exchange those messages. A protocol can describe low-level details of machine-to-machine interfaces or high-level exchanges between allocation programs.

public default route

The default routes that are used for traffic that comes into the switch via a private interface or from the switch's private interface address.

Resource Reservation Protocol (RSVP)

A protocol used to signal QoS requests and confirmations.

route

The path that network traffic takes from its source to its destination.

router

A device that forwards traffic between networks. The forwarding decision is based on network layer information and routing tables.

routing

The process of selecting the correct interface and next hop for a packet being forwarded.

Routing Information Protocol (RIP)

A distance vector, as opposed to link state, routing protocol.

RSA digital signature

A public-key encryptographic system that may be used for encryption and authentication.

server

A provider of resources, such as file servers and name servers.

Simple Network Management Protocol (SNMP)

The Internet standard protocol developed to manage nodes on an IP network.

split horizon

A method that RIP uses to avoid routing problems caused by including routes in updates sent back to the gateway from which they were learned. The simple split horizon scheme omits routes learned from one neighbor in updates sent back to that neighbor. An extension to this method is called split horizon with poisoned reverse. It includes the learned routes, but assigns them a cost of infinity, which causes an update.

static routes

Routes that are manually configured in the switch's routing table.

stub network

A network that only carries packets to and from local hosts. Even if it has paths to more than one other network, it does not carry traffic for other networks.

subnet

A portion of a network, which may be a physically independent network segment, that shares a network address with other portions of the network and is distinguished by a subnet number.

Telnet

A command protocol used to establish login sessions on a remote host.

triggered update

A method used by RIP in which a new routing table is sent almost immediately after a routing change has been made. This is in contrast to the poison reverse method, in which routes are updated after a cost of infinity is reached, a process that can take much time.

User Datagram Protocol (UDP)

An Internet standard transport layer protocol. It is a connectionless protocol that adds a level of reliability to an multiplexing to IP.

Uniform Resource Locator (URL)

A standard for identifying objects on the Internet accessible through the Web.

Virtual Router Redundancy Protocol (VRRP)

A protocol that handles private interface failures. VRRP targets hosts that are configured with static next-hop routing addresses or default gateways. It provides a means of rerouting traffic in the event of a system/interface failure.

Wide Area Network (WAN)

A network, usually constructed with serial lines, that covers a large geographic area.

Index

A

access hours 79, 82, 91
accessible networks 92, 93, 113
administrator 30
asymmetric branch office tunnel (ABOT) 91
authentication
  branch office 103
authentication methods 91

B

base group 76
branch office
  access hours 91
  authentication 103
  authentication methods 91
  configuring 91
  encryption settings 93
  indirectly connected switches 93
  routing 103
  sample configurations 92
  sample procedure 95
branch office quick start 40
  template 46
branch office quick start paramenters 45
branch office quick start template 121
branch office quick start utility 40
branch office tunnels
  asymmetric 91
  peer to peer 91

C

call admission
  priority 79
cards
  LAN 23
  WAN 23
children of base group 76
client policy 118
Command Line Interface (CLI) 22
compact flash disk 49
configuration
  checklist 34
  choices 37
  IP address 25
  perparing for 33
  Web interface options 33
configuring
  branch offices 91
  serial interface 27
Confivity 1010/1050/1100 39
connection types
  initiator 102
  responder 102
Contivity 1010/1050/1100
  branch office quick start 40
  compact flash disk 49
  default configuration parameters 39
  enterprise requirements 42
  ISP environment 43
  setting up 46
control tunnels 105
  branch office 107
  creating 110, 111

nailed-up 108
restricted mode 108
sample 107
user 107
current subnetworks 116
customer support 18

D

data collection
interval 73
data rates
WAN interfaces 66
default
gateway 27
login 32
password 32
default route
branch office 93
DHCP
client 54
DNS
host name 52
server address 52

E

encryption
settings for branch office 93
Extranet Access 19

F

FIPS
overview 22
firewall
branch office 92
interaction with branch office 93
license key 21
flash disk system
compressed files 49
forwarding priority 79

G

getting started 23, 51
group
associations 77
guided configuration
requirements 38

I

idle timeout 80
indirectly connected switches 93
inheritance, group 82
interface
filter 56
Internet domain 52
IP address 27
assigning 23
branch office 102
configuration utility 25
currently assigned 55
reconfiguring values 31
IPX 25
ISP 63
tunnels 76

L

LAN
card 57
LAN interfaces 53
last name search 90
LDAP
attribute search 90
license keys
advanced routing 21
firewall 21
tunnel 21
licenses 37
log file
configuration 73

life time 73
login 32

M

MAC Pause 58
management
Extranet Access Switch 37
management IP address 31, 51

N

navigational menu 38
Network Address Translation (NAT) 94
Network Time Protocol (NTP) 68
new subnetworks 116

P

password 32
Peer to peer 101
port speed 58
primary administrator 30
primary DNS server 53
private LAN 53
product support 18
proxy ARP 73
public data network (PDN) 54
publications
hard copy 17

Q

Quick Start 38

R

register 37, 38
relative distinguished name 78
remote access 20
routing
advanced licence key 21

S

Safe mode 32, 70
search for users 90
secondary DNS server 53
serial interface
configuration 27
prerequisites 27
serial number search 26
services 37
subnet mask 27, 55
subnetworks 91
support, Nortel Networks 18
Switch concepts 19
Symmetric Branch Office tunnel 91
system identity 51

T

technical publications 17
technical support 18
template 46, 121
terminal emulator 28
tertiary DNS server 53
tunnel license key 22
tunnel types 84
tunnels, configuring 75

U

Uniform Resource Locator (URL) 32
user
ID search 90
user control tunnel
serial interface 113
user groups

adding 85
searching 89
user profile
adding 86
user tunnels 82

W

WAN interfaces
configuration 63
configuring data rates 66
currently installed 64
web browser interface 32
Web interface options 33
Welcome display 36