Version 4.07

Part No. 315535-A Rev 00
June 2002

600 Technology Park Drive
Billerica, MA 01821-4130

New Features for the Contivity 1010/1050/1100

NORTEL NETWORKS™

Copyright © 2001 Nortel Networks

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

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

Trademarks

Nortel Networks, the Nortel Networks logo, Contivity, Preside, and Optivity are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

AXENT and OmiGuard Defender are trademarks of AXENT Technologies, Inc.

Check Point and Firewall 1 are trademarks of Check Point Software Technologies Ltd.

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

Entrust and Entrust Authority are trademarks of Entrust Technologies, Incorporated.

Java is a trademark of Sun Microsystems.

Linux and Linux FreeS/WAN are trademarks of Linus Torvalds.

Macintosh is a trademark of Apple Computer, Inc.

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

Netscape, Netscape Communicator, Netscape Navigator, and Netscape Directory Server are trademarks of Netscape Communications Corporation.

NETVIEW is a trademark of International Business Machines Corp (IBM).

NetWARE and Novel intraNetWare are trademarks of Novell, Inc.

NDS is a trademark of Novell Inc.

OPENView is a trademark of Hewlett-Packard Company.

SafeNet/Soft-PK Security Policy Database Editor is a trademark of Information Resource Engineering, Inc.

SecurID and Security Dynamics ACE Server are trademarks of RSA Security Inc.

SPECTRUM is a trademark of Cabletron Systems, Inc.

VeriSign is a trademark of VeriSign, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

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

This guide describes the new features for Nortel Networks* Contivity* 1010/1050/1100 series of switches.

Note: You cannot use this version of the software on any other Contivity VPN switch.

Before you begin

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

Text conventions

This guide uses the following text conventions:

`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`**}.
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.
asterisx (*)	Indicates a trademark.

Related publications

For more information about the Contivity VPN Switch, refer to the following publications:

- *Contivity 1010/1050/1100 Release Notes (V4.07)* (314963-A) provide the latest information and known problems and workarounds.
- *Reference for the Contivity VPN Switch Command Line Interface* (part number 314959-A) describes the commands that you can use from the command line interface.
- *Installing the Contivity 1010/1050/1100* (part number 314961-A) provides instructions on how to install the Contivity 1010, 1050, and 1100 and includes technical specifications.
- *Configuring the Contivity VPN Switch* (part number 314958-A) provides procedural information to help you configure, monitor, and troubleshoot your switch.
- *Connecting for Internet Access* (part number 314962-A) describes how to set up your Contivity 1010, 1050, or 1100 at the branch office site.

Acronyms

This guide uses the following acronyms:

BOT	branch office tunnel
CO	central office
BOQS	branch office quick start
CT	control tunnel
LAN	local area network
NOC	network operations center
WAN	wide area network
DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol
PPPoE	Point-to-Point Protocol over Ethernet
VPN	virtual private network

Hard-copy technical manuals

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

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

How to get help

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

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www130.nortelnetworks.com/cgi-bin/eserv/common/essContactUs.jsp URL.

Chapter 1
Overview

The features presented in this document are unique to the Contivity 1010/1050/1100 series switches. This document is for network administrators who are responsible for setting up and configuring a VPN switch. For information on existing features, see *Configuring the Contivity VPN Switch*.

The Contivity 1010/1050/1100 family of products is a low cost, low-end IP services platform that provides Virtual Private Networking (VPN), routing, and firewall services. It is useful for carrier and enterprise customers who may want to deploy them into their small business or home office locations. The hardware consists of the 1010 with dual 10/100 Ethernet port and a serial port, the 1050 with a single Ethernet port and a 4-port switch, and the 1100 with a single Ethernet port, a 4-port switch, and two I/O expansion slots. For detailed information on the hardware, see *Installing the Contivity 1010/1050/1100*.

This product offers the following features in addition to the existing Contivity VPN Switch features:

- Unique Default Configuration
- DHCP Server
- Point-to-Point Protocol over Ethernet (PPPoE)
- Branch office quick start utility
- DNS Proxy
- Compact flash disk

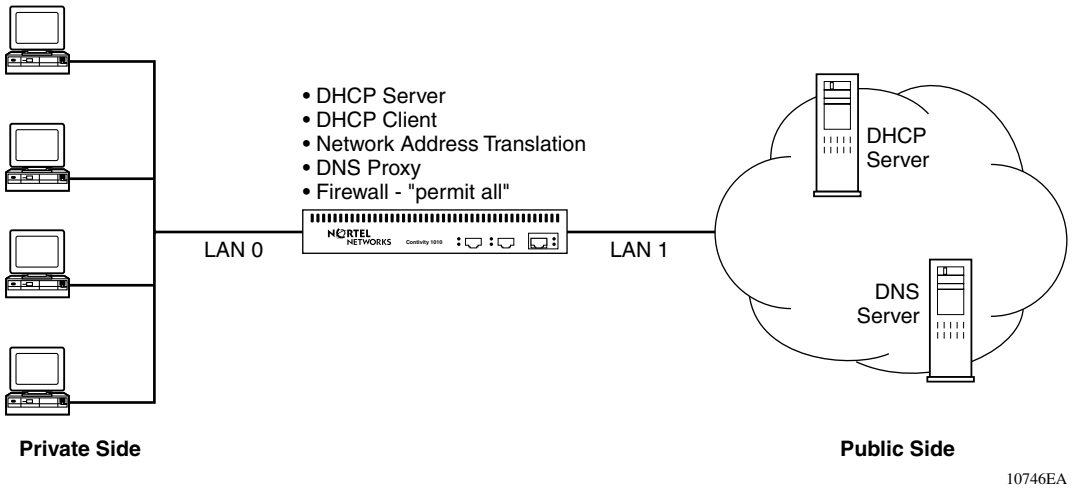
Internet Explorer 5.5 or 6.0 and Netscape 4.7.*x* or 6.2 are the supported Web browsers.

Default configuration

The Contivity 1010/1050/1100 series of switches uses a unique default configuration to simplify setup in the small office or home office environment.

Figure 1 shows the default configuration.

Figure 1 Default configuration



DHCP Server

Dynamic Host Configuration Protocol (DHCP) dynamically assigns IP configuration parameters to clients and provides for centralized network administration. DHCP pushes configuration information to clients, including network address parameters and standard options. It also provides for interaction with DNS.

DHCP uses the concept of IP address leases. When a DHCP client requests an IP address, a DHCP server grants the client exclusive use of an assigned IP address for a specified period of time.

The Contivity 1010, 1050, and 1100 switches include a full implementation of a DHCP server that is in compliance with RFC 2131 and RFC 2132.

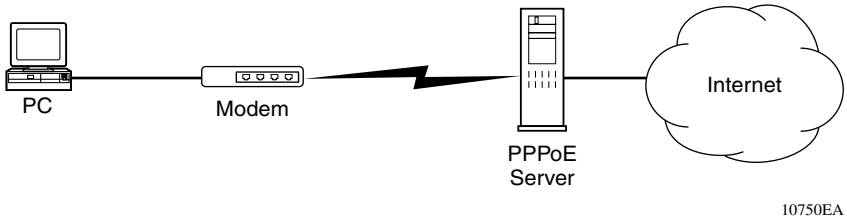
PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) allows PPP to run over Ethernet. Typically, PPP runs over serial interfaces and in most cases runs over phone lines connected to a server.

With DSL and cable modems, where a personal computer is connected to the Ethernet interface of the modem, ISPs cannot run PPP because PPP cannot run directly over Ethernet. ISPs often prefer to use PPP to provide features such as user authentication and bandwidth monitoring.

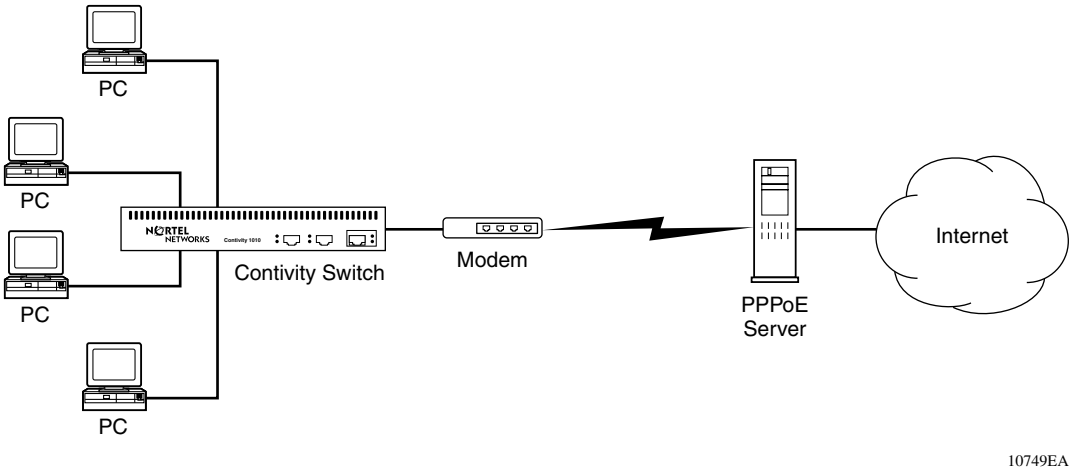
Typically, PPPoE is set up in two different configurations: PPPoE for the single user (Figure 2) or PPPoE on a local network. For locations with single computers, the PPPoE client is typically loaded on the computer and it reaches the PPPoE server through the Ethernet connection via the DSL modem. The DSL modem then forwards the packets to the WAN interface without interpreting the PPPoE packets. The PPPoE packets reach their final destination (PPPoE server) for further handling. This is in compliance with RFC 2516.

Figure 2 PPPoE for single user



The second configuration is usually seen in multi-computer locations, small offices, or branch offices where the entire LAN is connected to the Internet via DSL or cable modem. In this case, either the modem or the gateway acts as a PPPoE client. Figure 3 shows how the Contivity 1100 switch connected to the DSL modem acts as the PPPoE client. In this configuration, the PPPoE client encapsulates the LAN traffic in the PPPoE header and forwards it to the PPPoE server.

Figure 3 PPPoE on a local network

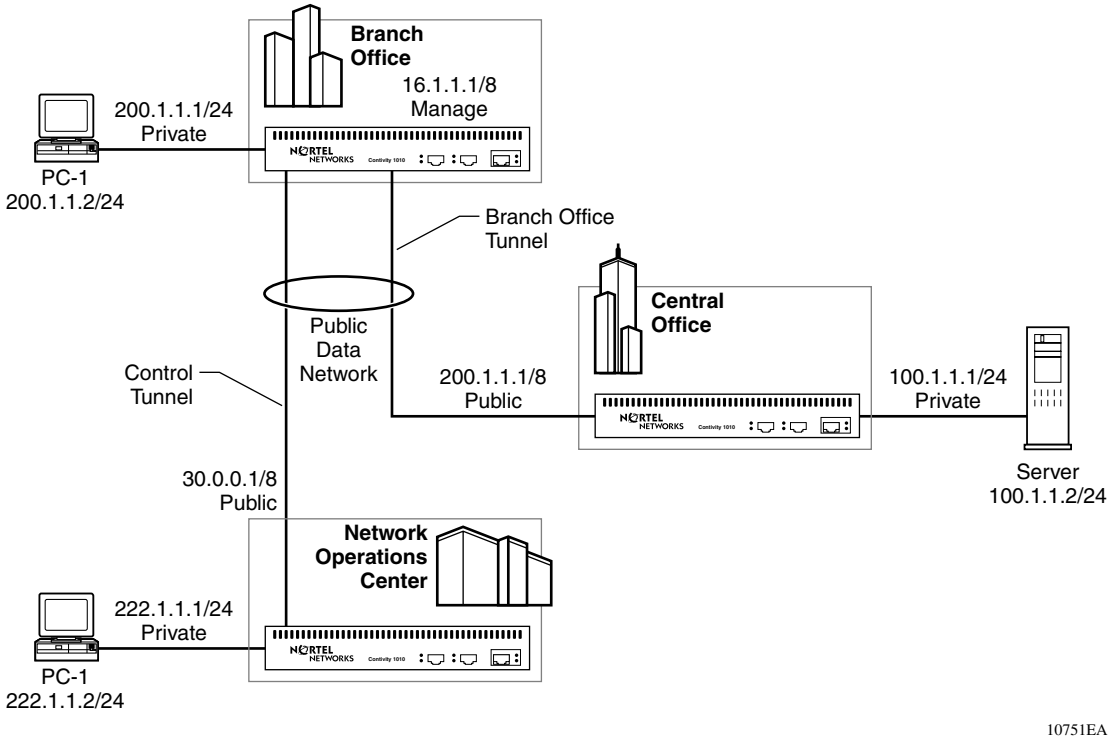


Branch office quick start utility

The branch office quick start utility (BOQS) simplifies deployment of switches in the branch office environment. BOQS converts your Contivity 1010, 1050, or 1100 device from an Internet Access Gateway into a Secure Access Gateway by provisioning a virtual private network (VPN) connection to a Central Office or optionally, to a Network Operation Center. BOQS adds VPN functionality to basic internet access connectivity. It allows a NOC or central office management to access the Contivity 1010, 1050, or 1100 so that network administrators can further configure the it without going to the remote site.

Figure 4 shows a view of the network after VPN services are provisioned.

Figure 4 Network view

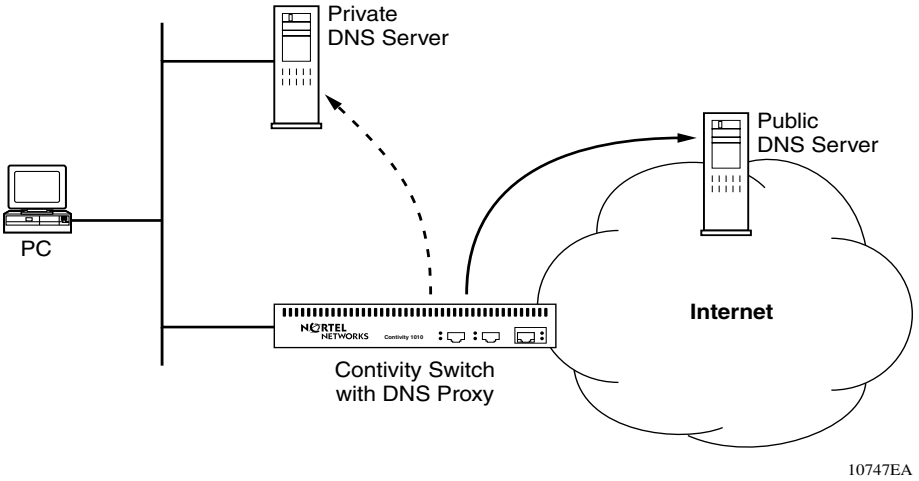


DNS proxy

The Domain Name Service (DNS) is a method for mapping host names to IP addresses. It allows the Internet to provide an updated set of mappings for all Internet devices. A DNS server holds the segment of the DNS database for which it has authority. DNS clients are any TCP/IP applications that refer to hosts by host name. When an application needs to convert a host name to its IP address, it uses the client portion, which creates a DNS query specifying the host name and sends the query to a server. The server tries to find the host IP address by looking in its database or by making queries to other servers. Eventually, a DNS response is returned to the application, which contains the IP address or an error indicating that the host name is unknown.

It is common for companies to set up their own domain name system internally, and leave it to the ISP to handle all external DNS. These companies have their own DNS servers, but use the external DNS servers for non-company names. This *splits* the DNS names into two separate systems: the private, company-controlled DNS names and the Internet DNS names.

Figure 5 Split DNS



You can configure the Contivity 1010, 1050, or 1100 as a DNS proxy, which means that it can act like a DNS server for any PC on the private network. The PCs are configured to send their DNS queries to the DNS proxy, which in turn passes the query to its set of *true* DNS servers. Whether you have configured DHCP client or PPPoE determines which DNS servers will respond. When the DNS proxy receives a DNS query form a PC, it passes the query on to the DNS servers until it receives a response, which is subsequently returned to the PC.

Compact flash disk

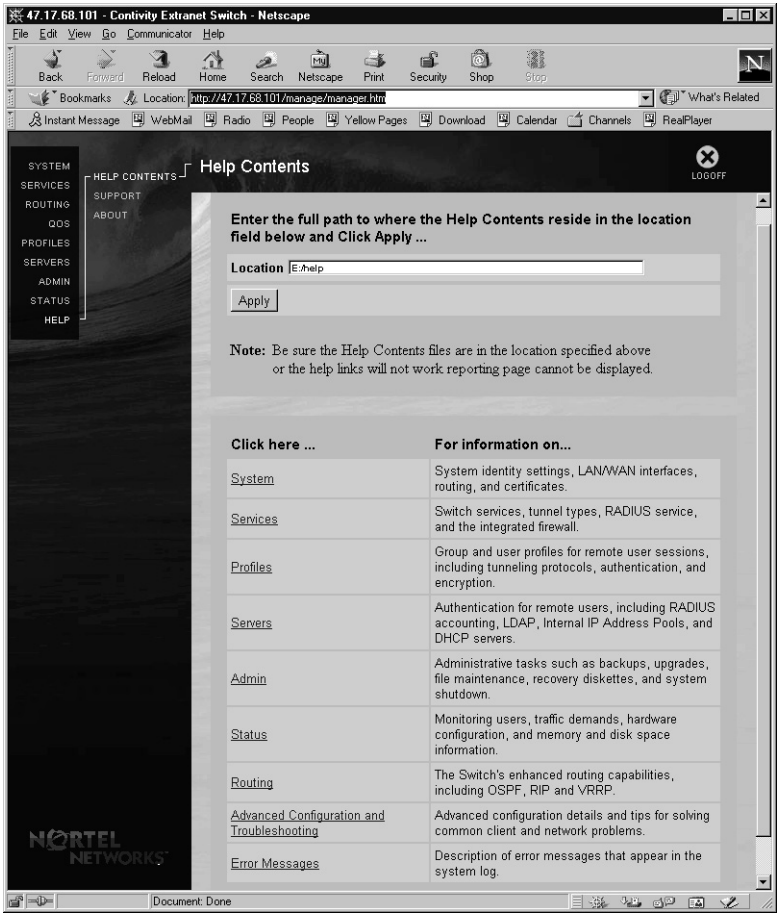
The Contivity 1010/1050/1100 series of switches uses a compact flash disk instead of a traditional hard disk. The compact flash disk provides 32 MB of flash disk storage. Because of the limited storage capacity, the following functionality is not provided:

- 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. You can copy the help files from the CD to a directory on a server. When you click on Help→Help Contents (Figure 6), you are prompted to enter the location of the help files. If the help files cannot be located on the CD or a server, you can find them on the Nortel Networks documentation Web site.

Figure 6 Help Contents screen



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

CLI commands

Following is a list of new CLI commands implemented for the Contivity 1010, 1050, and 1100. For further information and command descriptions, see *Reference for the Contivity VPN Switch Command Line Interface*.

Table 1 Contivity 1010/1050/1100 CLI commands

DHCP server commands
bootfile
description
excluded-address
hardware-address
host
included-address
ip dhcp server pool
lease
next-server
option
option client-identifier
option default-router
option dns-server
option domain-name
option netbios-name-server
option netbios-node-type

Table 1 Contivity 1010/1050/1100 CLI commands

server-name
service dhcp enable
service dhcp restart
show ip dhcp server
PPPoE commands
interface
pppoe admin-state enable
pppoe cost
pppoe enable
pppoe idle-timeout
pppoe ip local
pppoe on-demand enable
pppoe ppp authentication
pppoe ppp ipcp vj-connect-id-compression-negotiation
pppoe ppp ipcp vj-max-slots
pppoe ppp ipcp vj-negotiation
pppoe ppp lcp echo-fault-threshold
pppoe ppp lcp echo-interval
pppoe ppp lcp protocol-field-compression
pppoe ppp username
show interface fastethernet pppoe
FTP core dump commands
ftp-coredump
ftp-coredump enable
show ftp-coredump
DNS proxy commands
ip name-server
show ip name-server
split-dns enable

Chapter 2
Getting started

This chapter provides more detailed information on configuring the features that are unique to the Contivity 1010/1050/1100 series of switches.

The Contivity 1010, 1050, and 1100 provide 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.

Full details on hardware installation, including adding local area network (LAN) or wide area network (WAN) cards, are in *Installing the Contivity 1010/1050/1100*. You should complete the hardware installation before starting this chapter.

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 gateway.
- 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 gateway 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.

DHCP server

DHCP pushes configuration information to clients and provides for interaction with DNS.The following restrictions apply to the DHCP server:

- DHCP server is enabled by default on the private (trusted) interface
- DHCP Relay and the DHCP Server are mutually exclusive on a physical port.

Because the Contivity 1010, 1050, and 1100 have the DHCP server enabled by default, Nortel Networks recommends that branch office users set up their PC to accept the IP addresses that the DHCP server will provide the LAN 0 (**private**) ports. See the Connecting for Internet access section for this procedure.

Figure 7 shows the DHCP server screen on the Contivity VPN Switch.

Figure 7 DHCP server screen

To configure the DHCP server:

1. Go to the Servers→DHCP screen.
2. Click on the Enable/Disable Server button to select the state of the DHCP server.
3. In the Default Options section, specify the lease time in the ddd:hh:mm:ss format or select Infinite to indicate an unspecified period of time.

4. Click Add in the Standard Options section to access the Add Option screen. The standard options section shows the current status of any added options and lets you add new options:
   - Select the desired options from the drop-down list.
   - Select the desired Type from the drop-down list.
   - Enter the appropriate value.
5. In the Pool section, click on the Add button to add a pool. The Add Pool screen appears:
   a. Enter the base IP address for the pool.
   b. Enter the subnet mask for the pool.
   c. Enter a description of the pool.
   d. Click on OK.
6. Select Pool and click on the Configure button to return to the Pool screen.
7. The Inclusion Range section allows you to add blocks of IP addresses that you can then give out.
   a. Under Inclusion Range, click on the Add button. The Pool Inclusion screen appears.
   b. Enter the base IP address for the Start Address.
   c. Enter the End IP address.
   d. Click on OK.
8. Optionally, you can select an Exclusion Range for further control of the IP addresses that you give out. For example, if you have a pool with the range 2.0.1.1 to 2.0.1.255 and want to exclude 2.0.1.50, you would specify 2.0.1.50 as both the start and end address.
   a. Under Exclusion Range, click on the Add button. The Pool Exclusion screen appears.
   b. Enter the Start Address for the range.
   c. Enter the End Address for the range.
   d. Click on OK.
9. Optionally, you can force the DHCP server to assign a fixed IP address to a host every time it logs in. You can do this with host reservations under the Host section.

a Click on the Add button. The Host screen appears.

b Enter the host name that is registered with DNS.

c Enter the IP address that you always want to reserve.

d Enter the Ethernet (MAC) address.

e Click on OK.

10 The server does not implement configuration changes until it is restarted. Return to the Server→DHCP screen and select the Restart Server option to restart the DHCP server.

11 To verify the configuration changes, go to the Status→Health Check screen or click on the DHCP Stats button on the Status→Statistics screen.

Configuring PPPoE

Point-to-Point Protocol over Ethernet allows PPP to run over Ethernet. It is used by DSL or cable modem users for access to the Internet. PPPoE has the following usage restrictions:

- Cannot use dynamic routing on PPPoE interfaces
- PPPoE can only be supported on one interface at a time
- Must be set on a public Ethernet interface
- Must set the Administrative State to enabled (disabled by default)
- Must set the appropriate filter (deny all by default)
- PPPoE changes are dynamically applied

Figure 8 shows the System→LAN screen.

Figure 8 System→LAN screen

To configure PPPoE:

1. Go to the System→LAN screen.
2. From the Select Protocol list, select PPPoE and click on Apply. The Add PPPoE Interface screen appears.
3. For Administrative State, click on Enable.
4. For Interface Filter, select permit all.
5. Go back to the System→LAN screen and click on Edit.The Edit PPPoE Interface screen appears.

6 For PPP Authentication Settings, click on Configure. The PPP Local Authentication screen appears.

7 Select either PAP or CHAP and enter the UID and password.

8 Click on OK.

9 To verify the state of PPPoE, you can look at the Operational State in the System→LAN screen of the PPPoE. This indicates that PPPoE session is up. To verify that IP/PPP/PPPoE is established, you can either check the event log and search for PPPoE to see if IP is established or you can check the forwarding table to see if a public default route is entered through the PPPoE interface.

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

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

2 Go to the System→LAN screen, select PPPoE from the Select Protocol list and click on Apply. The Add PPPoE Interface screen appears.

3 For Administrative State, click on Enable and for Interface Filter, select permit all.

4 Click on OK.

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

Static IP addressing

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

1 Open your Web browser and type http://192.168.1.2.

2 Enter **admin** and **setup** as the username and password.

3 Go to the System→LAN screen.

4 From the Select Protocol list, select IP and click on Apply. The Add IP Address screen appears.

5 Select the Static option.

6 Enter the IP address and the subnet mask.

7 Click on OK

Branch office quick start

Network administrators and service providers can use the branch office quick start for provisioning of IP-based VPN services on a large scale. It provides VPN services using Contivity 1010, 1050, and 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, and 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, or 1100 must be connected to a public network and have access to the Internet before local users can use BOQS. The unique Contivity default configuration allows easy deployment of Contivity 1010, 1050, and 1100 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, and 1100 must be configured manually before local users can use BOQS.

Note: It is possible to have a successful configuration of the tunnel and due to other factors have the tunnel test fail. If this occurs the following error messages are displayed: Test Branch Office Tunnel: Test FAILURE, ERROR Code: 1 and Branch Office Quick Start successfully created tunnel to Central Office.

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 at the local sites, you must 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 2 shows how offices with approximately 50 workstations can each have subnets assigned.

Table 2 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, and 1100.

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 Contivity 1010, 1050, and 1100 devices. 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 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 1010/1050/1100 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. The 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 / Mask fields.

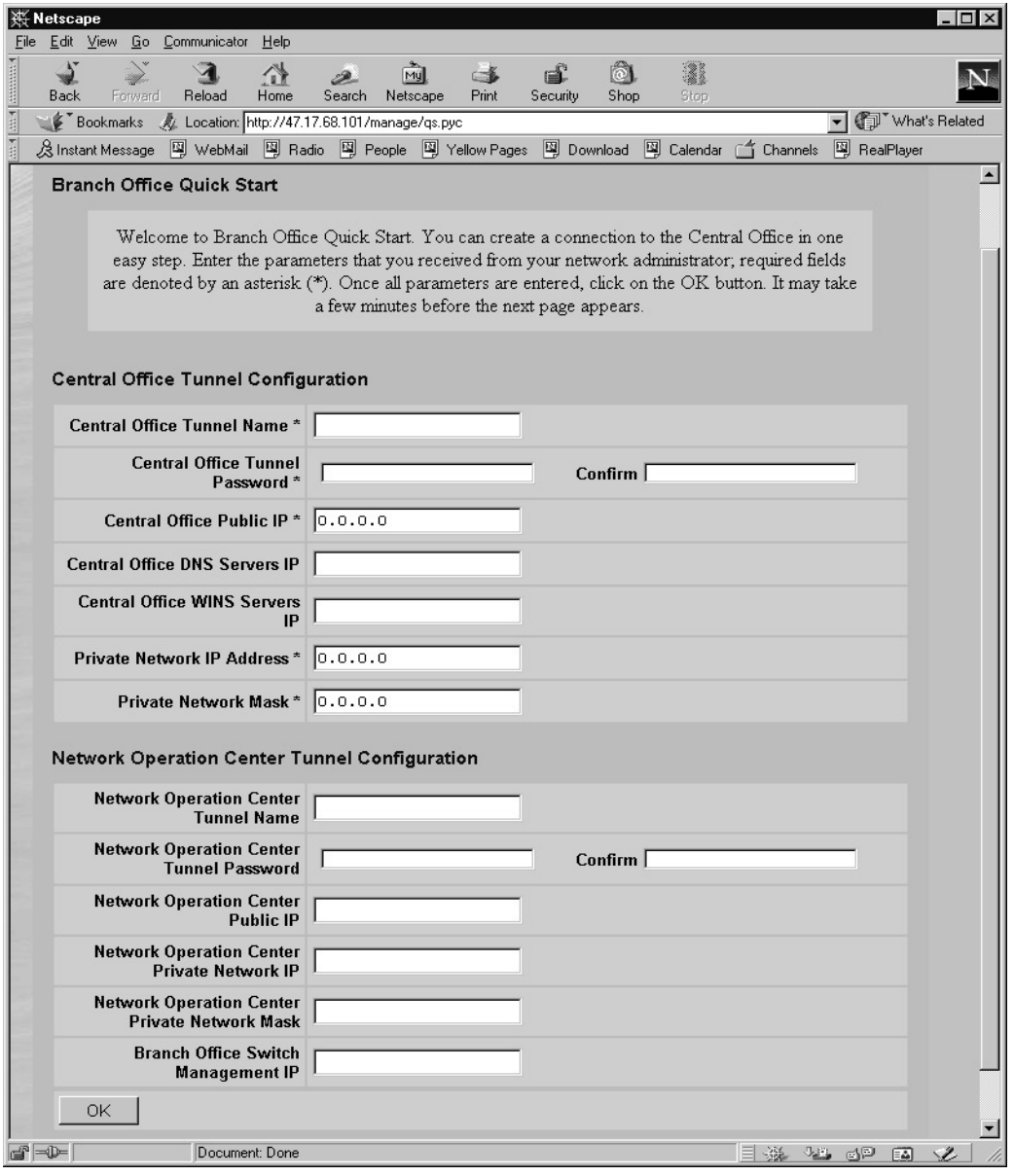
Table 3 contains the BOQS parameters.

Table 3 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

See Appendix A, "Branch office quick start template" for a template of this information. Figure 9 shows the branch office quick start screen.

Figure 9 Branch office quick start screen



Connecting for Internet access

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

To setup your Contivity 1010, 1050, or 1100:

1. Plug the power cord into an AC power outlet, plug the power cord into the external power supply and 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 using a standard Ethernet cable (not included with the Contivity unit). If you need the LAN 1 MAC address, it is located on the back of the unit.
3. If you want to connect a PC directly to the Contivity 1010, use the cable that ships with it. If you want to connect more devices to the Contivity 1010, you must connect an Ethernet switch or hub to the LAN 0 port and then connect the devices. If you want to connect more devices to the Contivity 1050 or 1100, you must connect them with standard Ethernet cables to the LAN 0 (**private)** ports labeled A-D.
4. Because the Contivity 1010, 1050, and 1100 have the DHCP server enabled by default on the LAN 0 port, you should set up the PC 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 (192.168.1.3 to 192.168.1.254).

   For other operating systems, see the user documentation for those systems.
5. 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 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 enter **http://192.168.1.2**.

b Click on Manage Switch and enter **admin** and **setup** as the username and password.

c Go to the System→LAN screen, select PPPoE from the Select Protocol list and click on Apply. The Add PPPoE Interface screen appears.

d For Administrative State, click on Enable.

e For Interface Filter, select permit all.

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 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**.

b Click on Manage Switch and enter **admin** and **setup** as the username and password.

c Go to the System→LAN screen. s

d Select IP from the Select Protocol list.

e Click on Apply. The Add IP Address screen appears.

f Select the Static option and type the IP address and the subnet mask.

g Click on OK.

h 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 gateway (for example, 47.17.2.1):

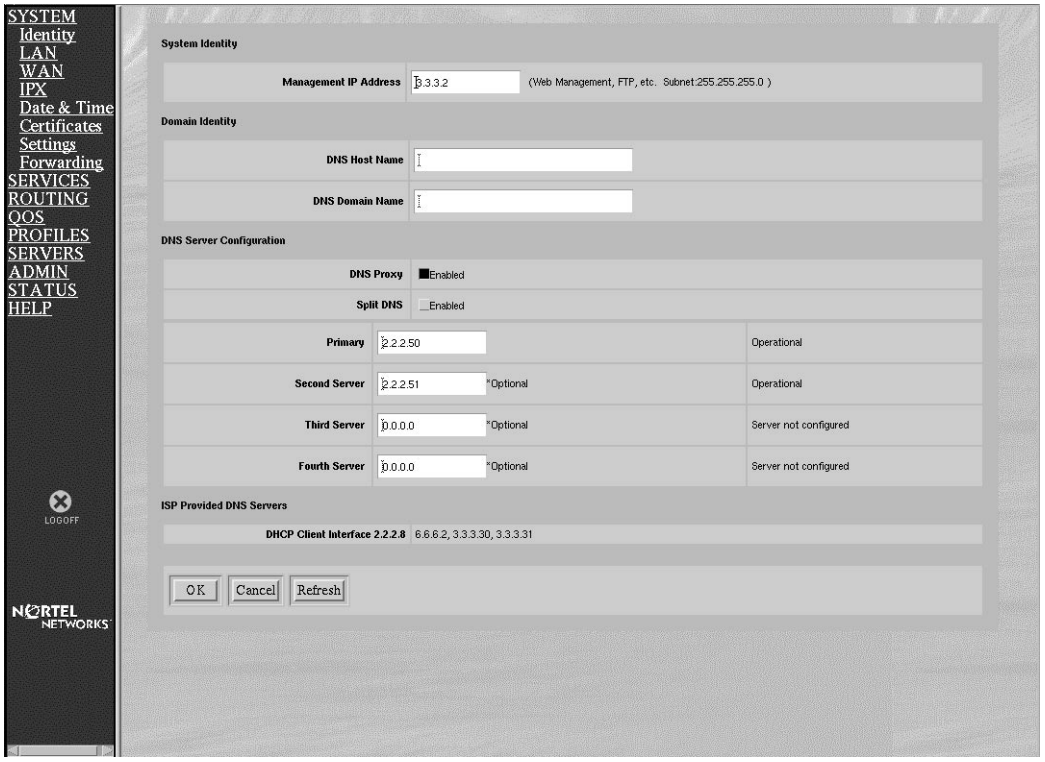
```
interface fastethernet 1/1
ip address type static
ip address 47.17.2.33 255.255.255.0
ip route 0.0.0.0 0.0.0.0 47.17.2.1 enabled
exit
```

Configuring a DNS server

You can configure up to four DNS servers. The ISP can assign more than one DNS server, which are displayed on the screen, but cannot be changed. You should enable split DNS if your DNS name space has been split into private names and public names; a DNS server knows the private names while another server knows the public Internet DNS names.

Figure 10 shows the System→Identity screen

Figure 10 System→Identity screen



To configure a DNS server:

1. Got to the System→Identity screen.
2. The DNS Proxy Enabled/Disabled check box allows you to select whether you want the DNS Proxy to act as a DNS server to the private side. It it enabled by default.
3. Click on the Split DNS check box if you have a split name space.
4. For Primary, enter the address of the DNS server that the DNS proxy tries to contact first.
5. For Second, enter an address for the Second Domain Name System (DNS) server. If the Primary DNS server doesn't respond in a few seconds, service is requested of the Second DNS server (if present).

6 For Third, enter an address for the Third Domain Name System (DNS) server. If the Primary and Secondary DNS servers doesn't respond, service is requested of the third DNS server (if present).

7 For Fourth, enter an address for the Fourth Domain Name System (DNS) server. If the preceding servers doesn't respond, service is requested of the fourth DNS server (if present).

8 Click on OK. The switch checks all of the DNS addresses to see if they respond and then provides an operational or error status.

Compact flash disk

The compact flash disk provides 32 MB of flash disk storage. 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→Administrator 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.

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	

Index

T

W