Version 6.00

Part No. 315899-E Rev 00
August 2005

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring Advanced Features for the Contivity Secure IP Services Gateway

NORTEL

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.

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

Figures

Preface

This guide describes the Nortel* Contivity* Secure IP Services Gateway tunneling protocols. It provides configuration information and advanced WAN settings.

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:

BIS	backup interface service
DoD	dial on demand
FTP	File Transfer Protocol
IP	Internet Protocol
IKE	IPSec Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	integrated services digital network
ISP	Internet service provider
L2TP	Layer2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
LAN	local area network
OSPF	Open Shortest Path First routing protocol
PACE	Packet Context Engine
PDN	public data networks
POP	point-of-presence
PPP	Point-to-Point Protocol

PPTP	Point-to-Point Tunneling Protocol
RIP	routing information protocol
RPA	routing protocol application
RPS	routing policy server
RTM	route table manager
TCP	transmission control protocol
UDP	User Datagram Protocol
VPN	virtual private network
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 Basic Features for the Contivity Secure IP Services Gateway* introduces the product and provides information about initial setup and configuration.
- *Configuring SSL VPN Services on the Contivity Secure IP Services Gateway* provides instructions for configuring services on the SSL VPN Module 1000, including authentication, networks, user groups, and portal links.
- *Configuring Servers, Authentication, and Certificates for the Contivity Secure IP Services Gateway* provides instructions for configuring authentication services and digital certificates.
- *Configuring Firewalls, Filters, NAT, and QoS for the Contivity Secure IP Services Gateway* provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- *Configuring Tunneling Protocols for the Contivity Secure IP Services Gateway* configuration information for the tunneling protocols IPsec, L2TP, PPTP, and L2F.
- *Configuring Routing for the Contivity Secure IP Services Gateway* provides instructions for configuring BGP, RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Managing and Troubleshooting the Contivity Secure IP Services Gateway* provides information about system administrator tasks such as backup and recovery, file management, and upgrading software, and instructions for monitoring gateway status and performance. Also, provides troubleshooting information and inter operability considerations.
- *Reference for the Contivity Secure IP Services Gateway Command Line Interface* provides syntax, descriptions, and examples for the commands that you can use from the command line interface.
- *Configuring the Contivity VPN Client* provides information for setting up client software for the Contivity gateway.
- *Configuring TunnelGuard for the Contivity Secure IP Services Gateway* provides information about configuring and using the TunnelGuard feature.

Hard-copy technical manuals

To print selected technical manuals and release notes free, directly from the Internet, go to www.nortel.com/documentation, 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 the Adobe Systems website at www.adobe.com to download a free copy of the Adobe Acrobat Reader.

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best source of support for Nortel products is the Nortel Support Web site:

http://www.nortel.com/support

This site enables customers to:

- download software and related tools
- download technical documents, release notes, and product bulletins
- sign up for automatic notification of new software and documentation
- search the Support Web site and Nortel Knowledge Base
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you have a Nortel support contract and cannot find the information you require on the Nortel Support Web site, you can get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the Web site below and look up the phone number that applies in your region:

http://www.nortel.com/callus

When you speak to the phone agent, you can reference an Express Routing Code (ERC) to more quickly route your call to the appropriate support specialist. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

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

Chapter 1
Configuring advanced LAN and WAN settings

This chapter provides configuration information for the following:

- 802.1Q
- Interface MTU and the TCP MSS
- WAN interfaces
- Circuitless IP

Configuring 802.1Q VLAN

Virtual LAN (VLAN) allows you to control broadcast traffic and improve network performance. A VLAN is a collection of end nodes grouped logically, rather than by their physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of their physical location on the network. This allows users located in separate areas or connected to separate ports to belong to a single VLAN.

A VLAN is created based on:

- Membership by port group--A port-based VLAN is a collection of ports across one or more switches. For example, ports 1, 2, 3, and 4 on a switch may be assigned to VLAN A, while ports 5, 6, 7, and 8 on the switch may be assigned to VLAN B.
- Membership by MAC address--the MAC address of a network device determines its VLAN membership. To create a MAC address-based VLAN, a switch is configured with a list of MAC addresses that are associated with a particular VLAN. The source MAC address of a received frame is looked up to determine its associated VLAN.

- Membership by protocol--Protocol-based VLANs use layer 3 protocol type (such as IP, IPX, Appletalk) to determine membership. For example, you can create a VLAN for IPX protocol and place ports carrying IPX traffic into this VLAN. This will localize all IPX traffic (including IPX broadcasts) within the ports of that VLAN.
- Membership by network address--The network-layer address determines membership. For example, an IP-subnet-based VLAN can be created for IP subnet 128.1.1.0/24. The switch then inspects a packet's IP address to determine if it belongs to subnet 128.1.1.0/24. If it does, it is a member of that VLAN.

Hosts that are assigned to such a virtual LAN send and receive broadcast and multicast traffic as though they were all connected to a common network. Therefore, devices on the same VLAN function as a single LAN segment or broadcast domain. VLAN-aware switches isolate broadcast, multicast, and unknown traffic received from VLAN groups so that traffic from stations in a VLAN are confined to that VLAN.

By dividing the network into separate VLANs, separate broadcast domains are created. This arrangement conserves bandwidth, especially in networks supporting broadcast and multicast applications that flood the network with traffic.

Figure 1 on page 21 shows an example of a VLAN. Two buildings have separate internal networks and each building is connected to a VLAN-aware switch. The engineering and sales groups are in separate VLANs. If a workstation from the sales VLAN sends a broadcast, it is received by every workstation belonging to the sales VLAN regardless of the physical location of the workstation. At the same time, workstations on the engineering VLAN will have no knowledge of the broadcasts and sales broadcasts will not interfere with the engineering network.

Figure 1 Sample VLAN

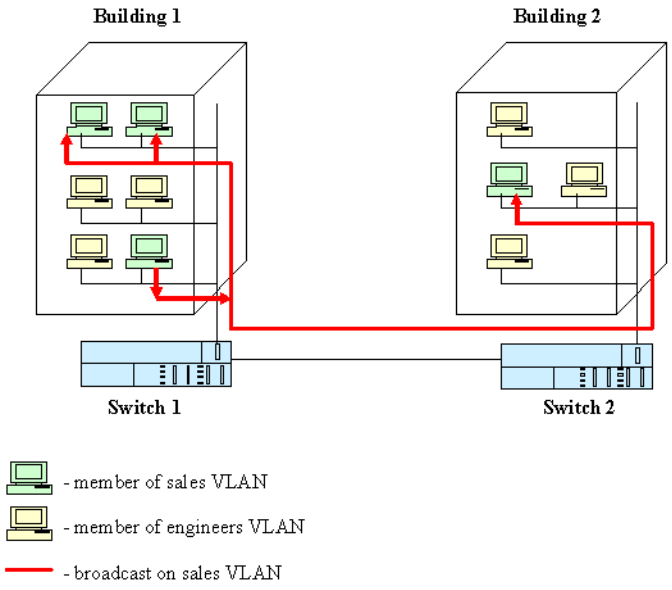


Figure 1

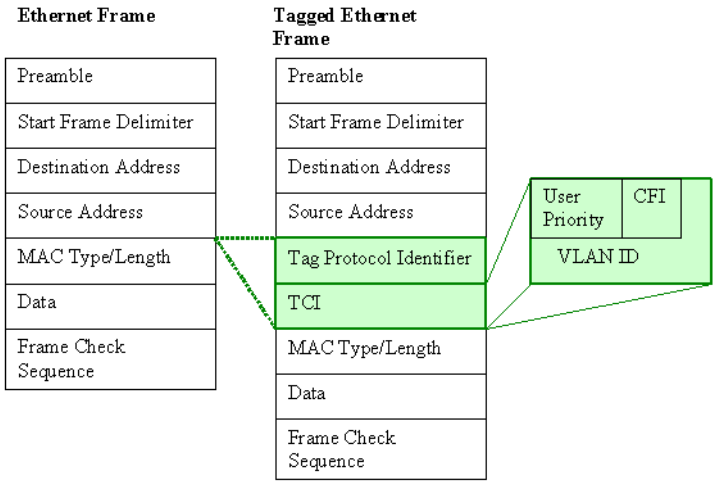
802.1Q is IEEE (Institute of Electrical and Electronics Engineers) specification for VLAN implementation in layer 2 switches with emphasis on Ethernet. 802.1Q provides a 32 bit (4 byte) header for VLAN tagging with VLAN membership information.

Frame tagging with 802.1Q information is done at the Data Link layer level and requires modification to Ethernet frame format. Each 802.1Q tag sits in the Ethernet frame between the source address field and the MAC (Media Access Control) client type/length field. It is the duty of the Ethernet switches to look at this tag and determine where the frame is to be delivered.

Figure 2 on page 22 shows the standard Ethernet frame and the 802.1Q modified Ethernet frame. The tagged frame has two new fields - Tag Protocol Identifier (TPI) and Tag Control Information (TCI) itself. TPI represents the Ether Type and is assigned a fixed value of 0x8100. If the frame has the TPI equal to 0x8100, the frame caries the 802.1Q tag. The tag itself is stored in the following two bytes (16 bits). The TAG contains: User Priority - 3 bits of 802.1p user priority level (0-7);

CFI - Canonical Format Indicator - 1 bit, indicates if the MAC addresses are in canonical format. This field is used for compatibility between Ethernet and Token Ring type networks. Ethernet uses value 0. Canonical MAC addresses are used in 802.3/Ethernet and transparent FDDI networks. Non-canonical MAC addresses are used in token ring and source-routed FDDI networks.VLAN ID (VID) - 12 bits, identification of VLAN, assigns a frame to one of the 4094 possible VLANs (1-4094, as values 0 and 4095 are reserved).

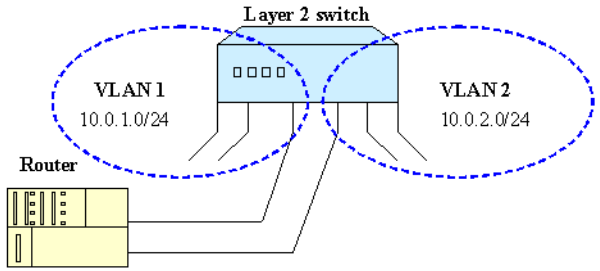
Figure 2 Ethernet frame and 802.1Q frames



When VLAN switch receives a frame it inspects the VLAN ID in the tag, if VLAN ID is specified, switch forwards the frame to a specific VLAN. If no ID is specified, switch forwards frame to a configured default VLAN.

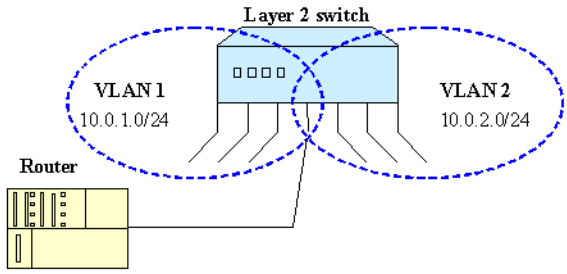
VLAN tagging simplifies the routing between VLANs. Tagging makes it easier and more cost effective for inter-VLAN routing. Based on the information in the tag, the router determines what VLAN the frame belongs to and routes the frame accordingly. Thus, a router that supports VLAN tagging is not required to have a dedicated link to each VLAN. A single tagged port could be used to perform inter-VLAN routing (Figure 3 on page 23).

Figure 3 Routing between VLANs



Tagging makes it easier and more cost effective for inter-VLAN routing. Based on the information in the tag, the router determines what VLAN the frame belongs to and routes the frame accordingly. Thus a router that supports VLAN tagging is not required to have a dedicated link to each VLAN, a single tagged port could be used to perform inter-VLAN routing (Figure 4).

Figure 4 VLAN tagging



Frame tagging on the Contivity gateway is used for routing between VLANs and traffic segregation. The Contivity gateway does not forward frames within the same VLAN as this is the responsibility of layer 2 switches.

802.1Q provides the Contivity gateway with the following capabilities:

- Receive and transmit 802.1Q tagged frames on Fast Ethernet (excluding the Intel i82557 chipset) and Gigabit Ethernet interfaces. When tagging is enabled the Contivity gateway receives and processes the tagged frames. If tagging is disabled, the Contivity gateway discards the tagged frames. Tagged frames are transmitted with tags identifying the outbound VLAN.
- Support for 802.1Q on public or private interfaces.
- Support for VLAN routing between VLANs.
- Support for VLAN tagging at the interface or subinterface level.
- An individual VLAN is mapped to an IP subnet.
- Support for routing services (static routes, RIP, OSPF, route policy service) and DHCP relay per VLAN on subinterfaces.
- Support interface filters, user and branch office tunnels using IPSec, PPTP, and L2TP per VLAN on subinterfaces.
- Display statistics for VLANs.

802.1Q tagging can be enabled at the interface or subinterface level.

When tagging is enabled at the interface level, the Contivity gateway can be configured to:

- Accept tagged frames when 802.1Q is enabled. A frame is tagged if it carries a 802.1Q tag with a non-null VLAN ID.
- Accept or discard untagged frames received by the interface (ingress behavior). A VLAN frame is untagged if it does not carry 802.1Q header or if the VLAN ID is set to null in the 802.1Q header (priority-tagged frames). The default behavior is to accept the untagged frames.
- Send tagged or untagged frames (egress behavior). The default behavior is set to send untagged frames. If egress frames are tagged, outbound frames include the 802.1Q header with the VLAN ID of the interface VLAN. If egress frames are untagged, outbound frames either do not include the 802.1Q tag header or include the 802.1Q header with null VLAN ID (when there is 802.1p user priority information in the frame).

A subinterface is a layer 2 entity. There can be multiple subinterfaces on a single interface, each representing a different network. The operational state of subinterfaces is dependent on the operational state of the associated base interface. If the base interface goes down, all subinterfaces over the interface also become non-operational.

When tagging is disabled, all frames are processed by the Contivity gateway as standard frames. If a tag is detected in some of the frames, these frames are discarded.

When tagging is enabled, the Contivity gateway uses the following rules to process a frame:

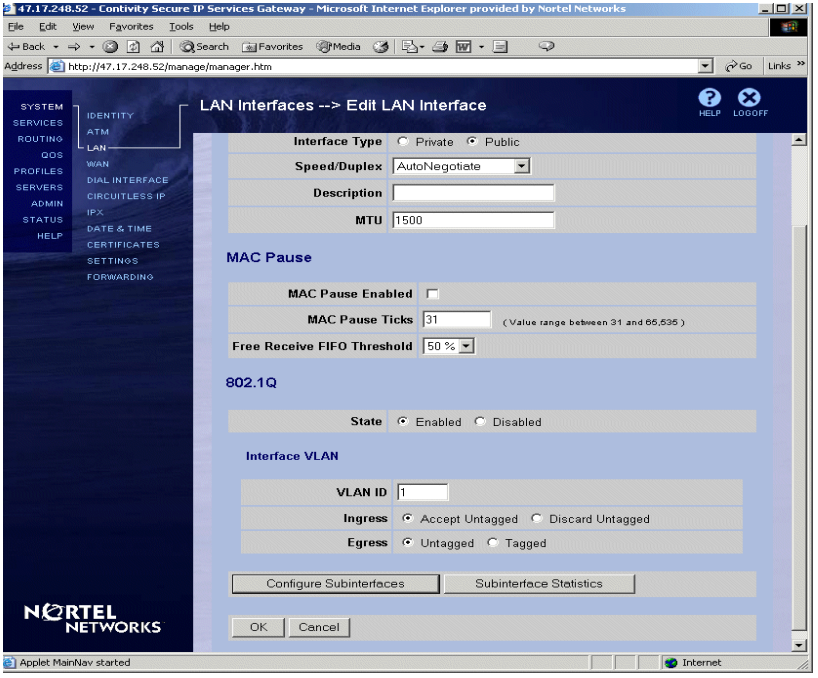
- Untagged frames are processed as standard frames by the LAN interface.
- Tagged frames with a VID between 1 and 4094 are processed by the corresponding VLAN. If the VID obtained from the frame does not mach any of those configured on the Contivity gateway VLANs, the frame is discarded.
- Tagged frame with a VID of 4095 is discarded.

To configure 802.1Q:

1. Go to the System > LAN screen and click on Configure next to the interface that you want to use for the 802.1Q. The Edit LAN Interface screen appears, as shown in Figure 5 on page 26.
2. Click on the Enable button for 802.1Q.

"802/1Q tagging" on page 26 shows the 802.1Q tagging screen.

Figure 5 802/1Q tagging



3 Once 802.1Q has been enabled on the interface the default behavior of accepting and sending untagged frames is applied to the interface.

a The VLAN ID for the interface is set to 1 by default. Enter the appropriate VLAN ID next to VLAN ID in the Interface VLAN section. Be sure to use different VLAN IDs at the interface and subinterface levels.

b Specify the Ingress behavior. Select whether to Accept Untagged frames or Discard Untagged frames on this interface. By default the Ingress behavior is set to Accept Untagged. If interface VLAN has been configured to Discard incoming Untagged frames, a confirmation screen appears stating that connectivity to the interface could be lost for the hosts that send untagged frames. Click on OK to apply the settings to the interface and discard all untagged frames.

c Specify the Egress behavior. Select whether the frames leaving the interface should be Tagged or Untagged. By default Egress behavior is set to Untagged. If interface VLAN has been configured to send Tagged frames, a confirmation screen appears stating that enabling this behavior

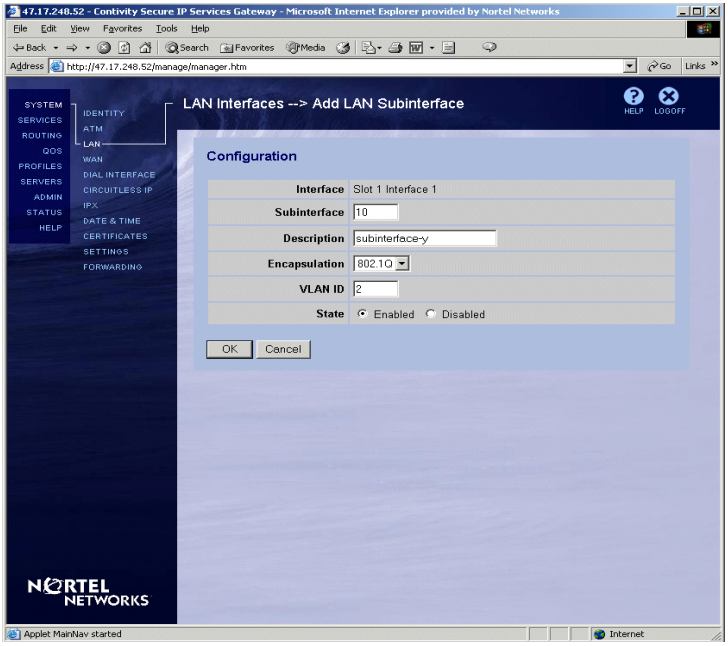
may cause a loss of connectivity with the hosts that do not support Tagged frames. Click on OK to apply the behavior.

d Click on OK. This returns you to the LAN Interfaces screen.

To configure VLAN at the subinterface level:

1. Go to the System > LAN screen and click on Configure next to the interface that you want to use for the VLAN. The Edit LAN Interface screen appears.
2. Click on Configure Subinterfaces on the LAN Interfaces > Edit LAN Interface screen. The LAN Interfaces > LAN Subinterfaces screen appears.
3. Initially no subinterfaces are configured. Click on Add Subinterface to add a subinterface.The LAN Interfaces > Add LAN Subinterface screen appears. Figure 6 shows the screen used to add LAN subinterfaces.

Figure 6 Adding LAN subinterfaces



The Interface field shows the current interface.

a Enter a number for a subinterface (1-65535) in the field next to Subinterface.

b Enter a Description (text up to 127 characters) for subinterface.

c Select Encapsulation (currently 802.1Q is the only option).

d Enter VLAN ID (value 1-4094). Be sure to use different VLAN IDs at the interface and subinterface levels.

e Select the Enabled State.

f Click on OK. The configured subinterface is listed on the LAN Subinterfaces screen. To change the configured parameters click on Configure next to subinterface. The Subinterface number cannot be changed once it is configured. The rest of the fields can be adjusted.

4 Click on Add IP to add an IP address to a subinterface.

5 The LAN Interfaces > Add IP Address screen appears.

a Enter the IP Address for subinterface.

b Enter the subnet mask associated with the address.

c Select the Interface Filter to be applied to subinterface.

d Click on OK.

The configured IP address and filter are listed under the subinterface.

6 To edit or delete the IP address click the appropriate button next to the IP address definition.

7 The LAN Interfaces > LAN Subinterfaces displays up to 10 subinterfaces; if the number of subinterfaces is greater than 10, the screen is subdivided into several screens. When all of the appropriate subinterfaces have been configured, click on Close.

8 When all of the parameters are configured, click on OK on the Edit LAN Interface screen.

To view subinterface statistics:

1 Go to the LAN Interfaces > Edit LAN interface screen.

2 Click on Subinterface Statistics. Statistics include total received/transmitted packets/octets, dropped packets/octets. To refresh the statistics, click on Refresh. To return to the LAN interfaces screen, click on Close. Initially all counters are cleared.

Scroll down to the 802.1Q statistics on the LAN Interfaces > Statistics screen to view the drop statistics for 802.1Q on the interface.

Routing (static routes, RIP, OSPF, route policies) can be configured on subinterfaces just like on any other interface. As with all interfaces, routing is supported for trusted interfaces only so if a subinterface is configured over a trusted interface, routing could be applied.

Go to Routing > Interfaces to configure OSPF and RIP for a subinterface. DHCP relay and IPSec/L2TP/PPTP tunnels on subinterfaces are configured in the same manner as for the regular interfaces.

Subinterfaces are displayed just like any other interfaces in the routing table. (Go to Routing > Route Table and click on Route Table.) Subinterfaces are also displayed in the forwarding table. (Go to Routing > Route Table and click on IP Forward Table.) Note that the subinterface is VC.

Configuring the interface MTU and the TCP MSS

For tunnels, you can configure the following:

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

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

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

Note: If you use SET for the DF bit in conjunction with packet capture on the outgoing interface and you receive an ICMP error packet, fragmentation may be occurring. If so, you can use the MTU value in the ICMP packet to set the tunnel MTU to avoid fragmentation. Then if you need to, you can adjust MTU limitations.

You can configure the following parameters for interfaces:

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

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

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

The default MTU value for each interface is based on the media type adjusted for Layer 2 encapsulation (Table 1).

Table 1 Default MTU by interface media type

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

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

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

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

Configuring the MTU on an interface

To change the MTU on an interface:

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

Configurable TCP MSS clamping

You can configure the TCP maximum segment size (MSS) on all interfaces. The TCP MSS specifies the largest TCP payload that a client is able to accept from a peer server, for example FTP or HTTP. You can configure the TCP MSS independently from the MTU size.

Note: On most PCs and the Contivity gateway, the default value for the TCP MSS is 1460 (MTU 1500 – 40 bytes; 20 bytes IP header + 20 bytes TCP header.

TCP MSS *clamping* is the substitution of the configured MSS value for the MSS value negotiated between TCP peers. To implement TCP MSS clamping, you must configure it on the interfaces that will receive or transmit the plain-text packets.

Note: Tunnels do not support clamping. To achieve clamping across tunnels, you must configure TCP MSS clamping on the ingress private side network.

Resetting the TCP MSS on an interface

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

- For a LAN interface, go to the System > LAN Edit screen, select the Enabled or Disabled option, and enter the TCP MSS value.

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

Configuring the MTU on a tunnel

For tunnels, you can configure the following:

- For all tunnels (IPSec, L2TP & PPTP), tunnel MTU can be configured.
- For IPsec tunnels only, DF (don't fragment) Bit behavior can be configured.

Tunnel MTU determines the largest size tunnel packet that will be transmitted. This MTU size includes the IPsec header and IP transport header layers. The default tunnel MTU behavior is, Enabled @ 1788 bytes. If tunnel MTU is disabled, then the tunnel MTU is derived from the interface MTU.

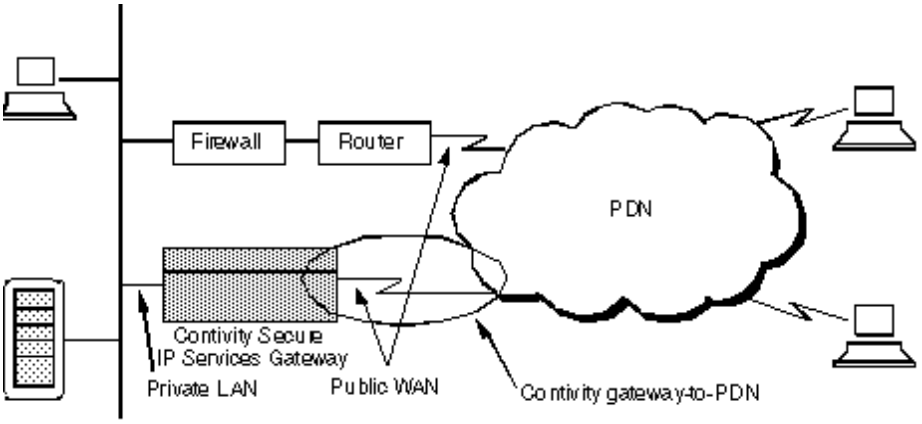
For IPsec tunnels, the DF bit in the outer IP transport header is now configurable. The default behavior is to CLEAR the bit. You can SET the bit or COPY the bit from the inner IP header.

Note: If you use SET/COPY for the DF bit in conjunction with a packet capture utility on the outgoing interface, and you may receive an ICMP error packet signifying fragmentation is needed (the result of the tunnel packets being too large). If so, you can use the MTU value reported in the ICMP error packet to reset the tunnel MTU to avoid fragmentation.

Setting up WAN interfaces

You assign WAN interface connections between the Contivity gateway and the PDN. Figure 7 on page 33 shows the connection attributes that you must configure. These attributes assign WAN interface connections between the Contivity gateway and the ISP.

Figure 7 Contivity gateway-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).

Note: If you are using a 32 bit subnet mask for a WAN interface, you must specify the local WAN interface as the remote gateway when you define a default route that will go out form the WAN.

Configuring WAN interfaces

The System > WAN interfaces screen shows the WAN interfaces currently installed in the Contivity gateway, 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 select to configure or disable a WAN card, or view statistics.

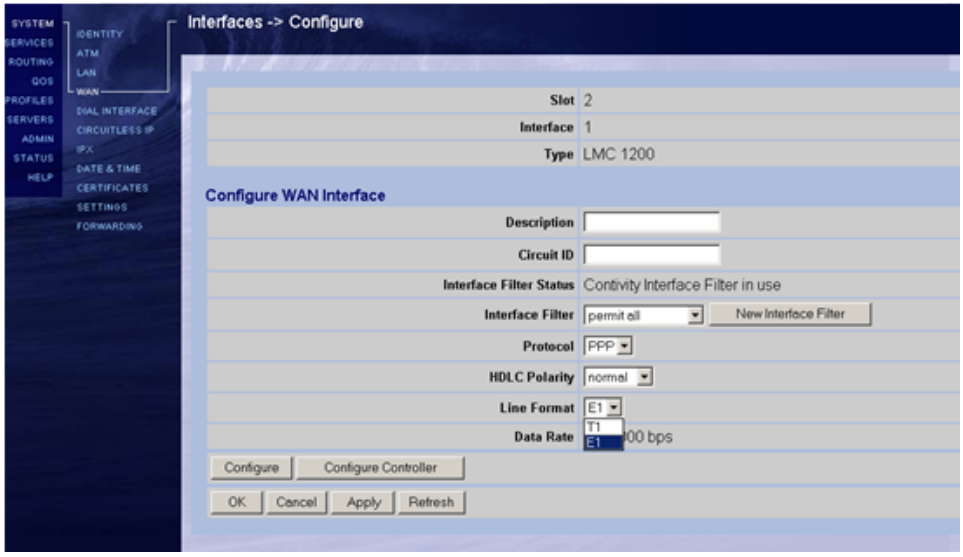
Note: To change the IP address of a WAN link, you must disable the interface, change the address and re-enable the interface. This automatically disables static routes for the interface. If you change the IP address back to the original address, you must manually re-enable static routes.

To configure the WAN interface:

1. Select System > WAN.
2. Click the radio button next to the adapter you wish to configure.
3. Click Configure.

Figure 8 on page 35 shows the WAN Interfaces > Configure page.

Figure 8 WAN Interfaces > Configure page



4 Type a description in the Description field.

5 Enter the Circuit ID in the Circuit ID field.

The Circuit ID parameter is configured on a per-interface basis, but is available to all WAN interfaces.

6 Select an option from the Interface Filter menu.

7 Select an option from the Protocol menu.

8 Select an option from the HDLC Polarity menu.

If line framing is Extended Super Frame (ESF), HDLC polarity is normal. If line framing is SF, HDLC polarity is inverted.

9 Select an option from the Line Format menu.

The line format controls the physical line impedance, which is set to 120 Ohms for E1 service.

10 Click Configure to configure the Protocol.

11 Click Configure Controller to open the Controller page.

12 Click one of the following buttons:

- Click OK to accept the changes and return to the prior page.

- Click Cancel to ignore any changes made to the page. The prior values are reset.
- Click Apply to apply the changes to the page.
- Click Refresh to redraw the page.

Configuring E1

A local exchange carrier provides a T1 and E1 service to a customer. The CSU/DSU is the interface between the carrier transmission and the customer premises equipment. T1 is available in North America, and E1 is available in Europe and internationally. Nortel provides a T1/E1 interface for the Contivity Extranet Switch (CES) platform with an integrated CSU/DSU.

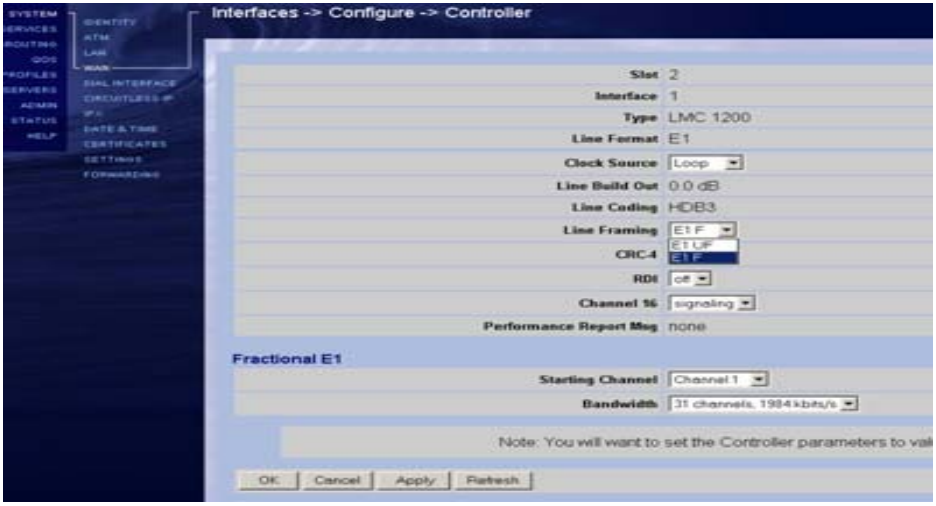
You can configure all of the parameters for E1 with the GUI, Quickstart, or NNCLI.

To configure E1 with the GUI:

1. On the WAN Interface screen, click the radio button of the E1 adapter you want to configure.
2. Click Configure.
3. Enter the information from the Configuring WAN procedure.
4. Click Configure Controller to open the Controller page.

Figure 9 on page 37 shows the Configure Controller page, which is used to configure E1.

Figure 9 Configure > Controller page



5 Select Loop from the Clock Source menu.

The clock source is typically set to loop when connected to a live E1 service. Internal clocking is used only for local or test applications.

There are no Line Build Out options.

There are no E1 Line Coding options. E1 always uses HDB3 line coding.

6 Select an option from the Line Framing menu.

There are two choices for E1 line framing: framed E1 and unframed E1. The advantage of framed E1 is that it permits fractional E1 services. It supports 30 or 31 DS0 channels. The advantage of unframed E1 is that it permits the maximum E1 user bandwidth, 32 DS0 channels. This parameter is determined by the E1 service provider.

7 Select an option from the CRC-4 menu.

E1 CRC-4 is only for framed mode. The CRC-4 generation may be turned on or off. This setting is determined by the service provider.

8 Select an option from the RD1 menu.

E1 RDI generation is only for framed mode. The E1 RDI may be turned on or off. This setting is determined by the service provider.

9 Select an option from the Channel 16 menu.

For a framed E1, channel 16 may be set to signaling or to data. This parameter is determined by the E1 service provider. For framed E1 with channel 16 signaling, there are 30 (1—15, 17—31) channels available. For framed E1 with channeling 16 data, there are 31 (1—31) channels available. For unframed E1, there are always 32 channels (0—31).

10 There is no PRM for E1.

11 Click **OK** to accept the changes and return to the prior page.

Configuring Fractional E1

Fractional E1 allows for fractional E1 circuit through timeslot provisioning. Fractional E1 is more affordable than clear channel circuit in that you choose how many channels you want, from 1 - 30, and pay for what you have chosen.

To configure fractional E1:

1 From the WAN Interfaces > Configure Controller page, select a channel from the Starting Channel menu.

2 Select a bandwidth from the Bandwidth menu.

Alarm generation

The integrated CSU/DSU generates Alarm Indication/Remote Defect Indication (RAI/RDI), which is a yellow alarm.

RAI/RDI is generated on the outgoing E1 signal when the CSU/DSU detects a red alarm, which indicates a loss of signal or loss of framing. The format of the RAI signal depends on the line framing used.

Healthcheck

Table 2 shows descriptions of the health status.

Table 2 Health Status

Status	Description
Green	Interface enabled and link up (ok)
Red	Interface enabled and link down (alert)
Magenta	Interface disabled (warning)

Light emitting diodes (LEDs)

Single port T1/E1

Table 3 shows the LEDs for a single port T1/E1. The LMC 1200 is a single port T1/E1. All LEDs off indicates the interface is disabled.

Table 3 Single port T1/E1 LEDs

LED	Condition
Green	Interface functioning normally
Red	Receiving red alarm (receiver loss of signal or loss of framing)
Yellow	Receiving yellow alarm (RAI/RDI)

Quad T1/E1

A quad T1/E1 has one green LED per port. The LMC 150x card is a quad T1/E1. Table 4 shows the quad T1/E1 LEDs state.

Table 4 Quad T1/E1 LEDs

LED state	Condition
Off	Interface disabled
On	Interface enabled and functioning normally
Flashing	Interface enabled and in an alarm state (red, yellow, or blue)

Obtaining statistics

To obtain statistics on a WAN adapter:

1. From the WAN > Interfaces page, select a radio button for the desired WAN adapter.
2. Click Statistics.

Configuring with Quick Start

Quick Start is a comprehensive initial configuration page that includes WAN configuration. To complete the Quick Start page to set up your Contivity Secure IP Services Gateway:

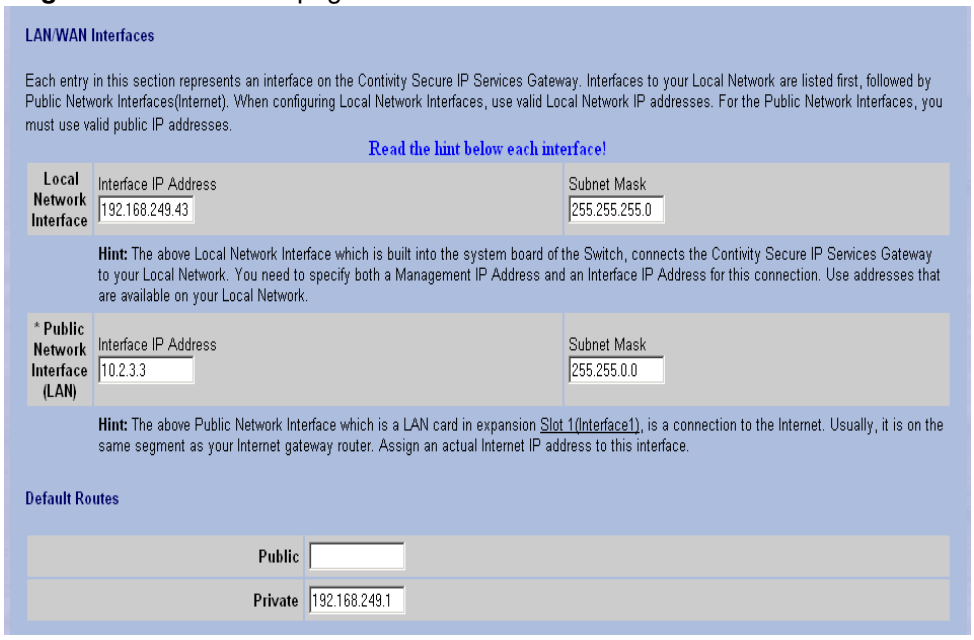
1. From the Welcome to the Contivity Secure IP Services Gateway, click Quick Start.
2. Read the information on the page.

   This page tells you the requirements and information you must complete for QuickStart.

3. Click Continue Quick Start. This single page allows you to:
   - Configure the switch interfaces
   - Create up to three user accounts
   - Change the default admin ID and password
   - Change the switch's date and time

Figure 10 on page 41 shows the section of the Quick Start page you use to configure WAN.

Figure 10 Quick Start page



4 Complete this page to setup your Contivity Secure IP Services Gateway.

5 Click Complete Quick Start.

Event Log Messages

The following is an example of start-up and shut-down event log messages:

Start-up

1 01/12/2005 03:43:18 (LMCIK) INFO IO WANT1 Code 1 Port 0 enabled

2 01/12/2005 03:43:18 (Syslog) INFO SYSTEM SYSTEMLOG Code 6 Interface[258] Enabled changed from ‘False’ to ‘1’ by user ‘admin’ @ ‘10.254.1.44’

3 01/12/2005 03:43:18 (LMCIK) INFO IO WANT1 Code 4 Port 0 link coming up

4 01/12/2005 03:43:18 (Syslog) INFO SYSTEM SYSTEMLOG Code 215 PortUp devLoc 0x102

Shut-down

1 01/12/2005 03:41:03 (LMCIK) INFO IO WANT1 Code 2 Port 0 disabled

2 01/12/2005 03:41:03 (LMCIK) INFO IO WANT1 Code 10 Slot 2 started but not running

3 01/12/2005 03:41:03 (Syslog) INFO SYSTEM SYSTEMLOG Code 6 PppIntf[258] LinkLayerUp changed from 'TRUE' to 'FALSE' by user 'admin' @ '10.245.1.44'

4 01/12/2005 03:41:03 (LMCIK) INFO IO WANT1 Code 5 Port 0 link going down

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 gateway 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

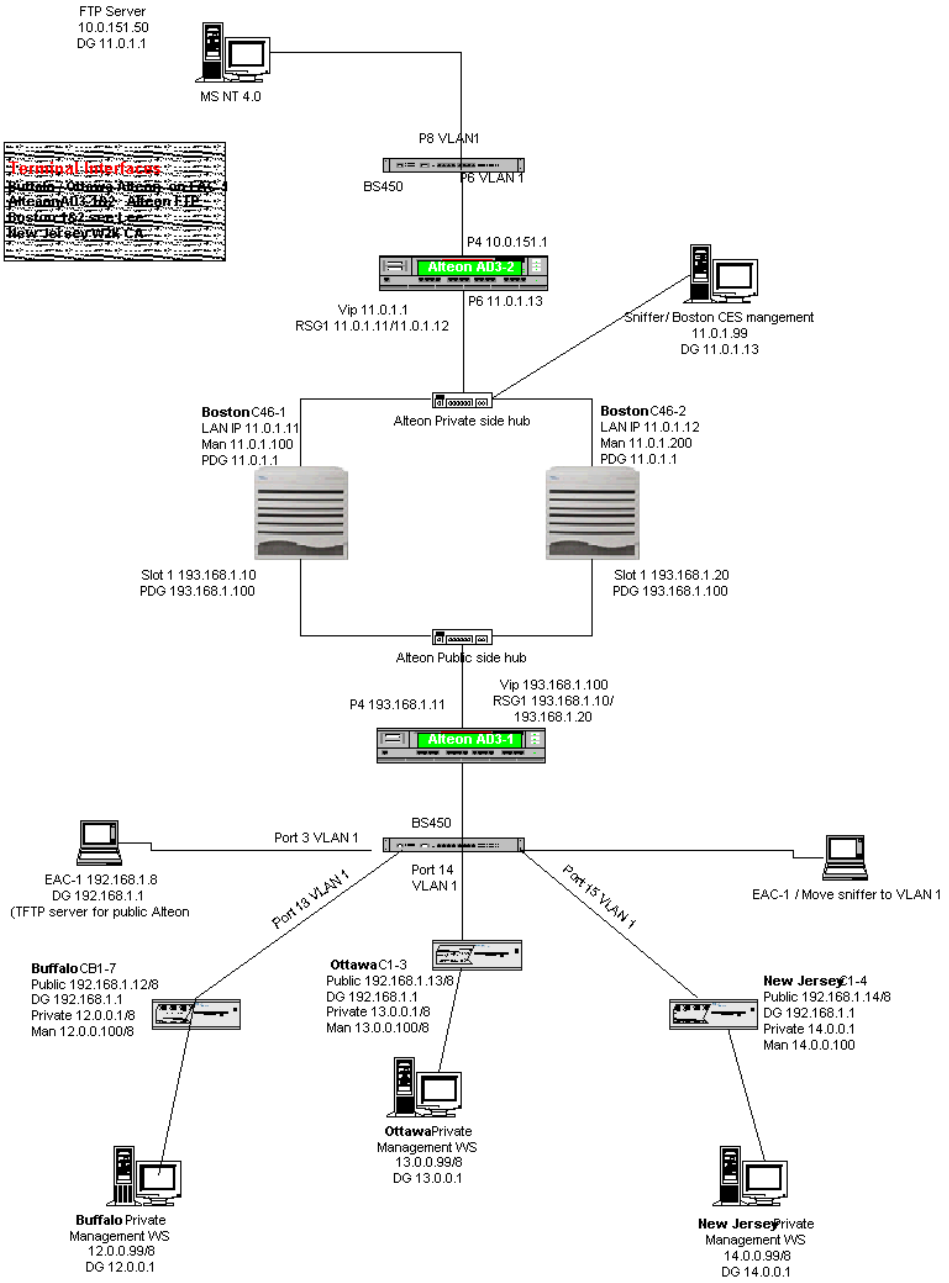
All current tunnelling protocols are supported, including: IPSec, L2TP and PPTP. Tunnel terminations are allowed based on tunnel types. Peer-to-peer, ABOT, and client tunnel types are supported. You can use CLIP addresses for load balancing with an Alteon switch where the same CLIP address is used by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

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 11 on page 44 the private Alteon WebOS switch is configured to direct returning data back to the client through the same Contivity gateway 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 gateway load balancers as basic configuration.

Figure 11 CLIP network topology



To configure CLIP:

1. Go to System > Circuitless IP and under Configured Circuitless IP, click on the Add button.
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.
2. Select CLIP as the route source for the protocol.
3. Click on OK.

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.

Configuring the Contivity Security Accelerator (CSA) and Hardware Accelerator cards

Nortel supports two PCI-based option cards for encryption and compression:

- Contivity Security Accelerator (CSA) card
- Hardware Accelerator card

The Contivity Security Accelerator card and the Hardware Accelerator card perform bulk encryption and compression algorithms for IPsec tunnel traffic to improve tunnel throughput. Because the accelerator cards offload bulk IPsec encryption duties from the main CPUs, Contivity gateways that support accelerator cards run faster and more efficiently.

Table 5 lists the Contivity gateways that support the CSA card and the Hardware Accelerator card.

Table 5 Contivity platform support for CSA and Hardware Accelerator cards

Contivity platform	CSA card supported?	Hardware Accelerator card supported?	Maximum number supported (1 or 2)[1]
1700	No	Yes	1
1740	Yes	Yes	1
2600	No	Yes	1
2700	Yes	Yes	2
4600	Yes	Yes	2
5000	Yes	Yes	2

1 You can install two CSA cards, two Hardware Accelerator cards, or one of each type of card.

The CSA card has one green LED; the Hardware Accelerator card has no LEDs.

Contivity Security Accelerator (CSA) card

The CSA card uses a single Hifn* 7854 chip for encryption and compression and has 64 MB of onboard RAM. It supports AES-128 cryptography with SHA-1 authentication and triple DES cryptography with either MD5 or SHA-1 authentication on packets flowing over preestablished IPsec tunnels.

The CSA card supports ISAKMP and encryption key generation for Groups 1, 2, and 5. The card also provides random number generation.

The CSA card is the successor to the Hardware Accelerator card. Along with providing support for AES, the CSA card provides increased encryption throughput and improved compression performance. For example, on the CSA card, compressed tunnels use less bandwidth than uncompressed tunnels, but on the Hardware Accelerator card, compressed tunnels use more bandwidth than uncompressed tunnels.

Hardware Accelerator card

The Hardware Accelerator card uses a single Hifn 7811 chip for encryption and compression. It performs triple DES and DES cryptography, LZS* compression, and MD5 or SHA-1 authentication on packets flowing over preestablished IPsec tunnels.

Performance considerations

Some packets expand when the LZS compression algorithm is applied. If the tunnel is assigned to the Hardware Accelerator card, the packets will be sent through the card a second time with compression disabled. Therefore, compressed packets are single threaded through the Hardware Accelerator card.

This consideration does not apply to the CSA card. If the tunnel is assigned to the CSA card, the CSA card will automatically encrypt the uncompressed version of the packet when it detects that the compression algorithm causes the packet to expand. In this way, multiple packets are queued up for processing.

Support for IPsec encryption and authentication algorithms

Table 6 lists the IPsec encryption and authentication algorithms supported by the Contivity Security Accelerator card and the Hardware Accelerator card. The CPU supports all algorithms.

Table 6 Support for IPsec encryption and authentication algorithms

Encryption/authentication algorithm	CSA card	Hardware Accelerator card
256-AES with SHA1	No	No
128-AES with SHA1	Yes	No

Table 6 Support for IPsec encryption and authentication algorithms (continued)

Encryption/authentication algorithm	CSA card	Hardware Accelerator card
Triple DES with SHA1 or MD5	Yes	Yes
56-bit DES with SHA1 or MD5	No	Yes
40-bit DES with SHA1 or MD5	No	Yes
SHA1 or MD5 authentication only	No	No
HMAC with SHA1 or MD5 authentication only	No	No
UDP wrapped	No	Yes

Accelerator card security

At startup, whenever an accelerator card is manually enabled, or whenever the accelerator recovers from a failure, the power-on self-test (POST) verifies the integrity of the hardware. This test includes validation of the accelerator's encryption, MAC, and compression algorithms against their software counterparts. In the event POST fails, the accelerator is set offline.

Load-balancing between the CPUs and accelerator cards

When one or two accelerator cards are installed, Contivity software tries to ensure optimal tunnel throughput by balancing tunnels across available system resources, that is, the CPUs and the accelerator cards. When a tunnel is established or rekeyed, the Contivity gateway evaluates several parameters—in particular the number of active tunnels and the encryption algorithm—to determine where to assign the new tunnel.

Note: If an accelerator card fails, all tunnel sessions running on that card are automatically moved to a CPU. A rekey is requested for each tunnel on the failed accelerator card.

The Contivity gateway automatically performs load-balancing of tunnel sessions across the accelerator cards and the main CPUs.

1. When the gateway is booted, the CPUs and the accelerator cards are assigned initial bandwidth allocations as follows:
   - The initial bandwidth assigned to a CPU is based on the CPU speed.
   - If the gateway has two CPUs, the bandwidth allocation of the boot CPU is set to a smaller value than the allocation for the non-boot CPU. Because the boot CPU handles functions other than packet processing—for example, route table updates—tunnels are assigned more aggressively to the non-boot CPU.
   - Because the CSA card provides greater throughput and performance, the CSA card is assigned a proportionally higher bandwidth allocation than the Hardware Accelerator card. For this reason, tunnels are assigned more aggressively to the CSA card.
2. When a new IPsec tunnel is established, the gateway assigns the tunnel to the CPU or to the accelerator card that currently has the largest amount of available bandwidth.
3. After a tunnel is assigned to the accelerator card or to a CPU, the amount of bandwidth on the card or CPU is correspondingly decreased.

Note: After a tunnel has been assigned to an accelerator card or CPU, the gateway does not dynamically reassign the tunnel to a new resource.

Configuring the CSA and Hardware Accelerator cards

You must have Administrator privileges to configure an accelerator card. You can configure the following settings for the Contivity Security Accelerator and the Hardware Accelerator card:

- Enable or disable the accelerator card.
- Enable or disable automatic recovery in case the card stops running.

When you enable automatic recovery and the gateway detects a recoverable failure, all sessions fail over and are handled by the software. As soon as the accelerator card recovers, new tunnels and re-keyed tunnels will be assigned to it.

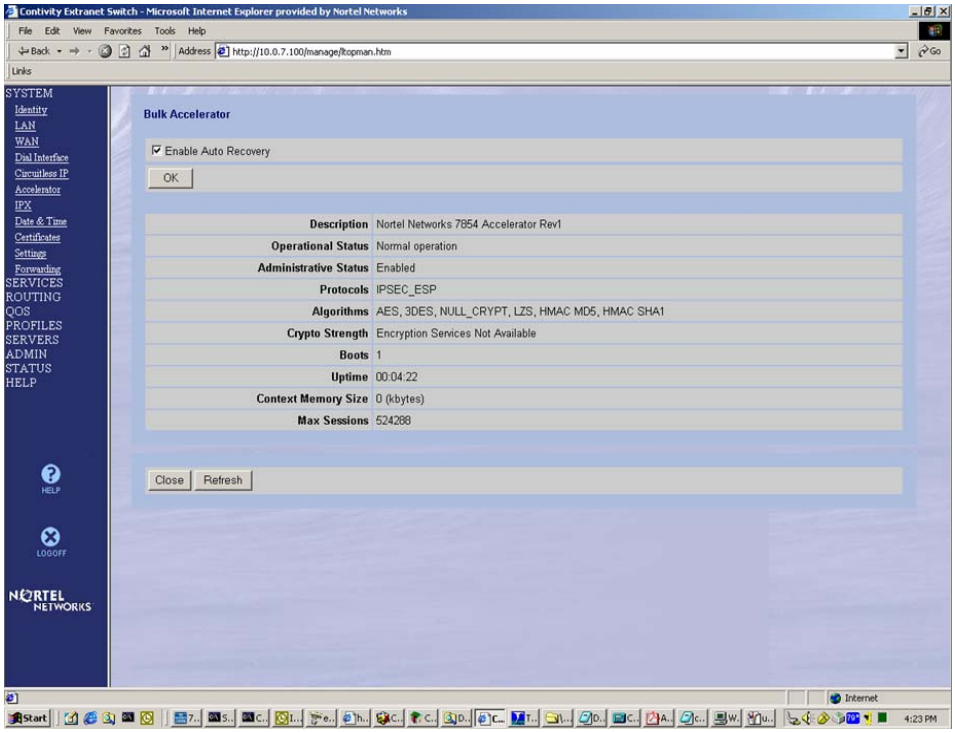
To enable or disable a CSA or Hardware Accelerator card:

1 Choose System > Accelerator.

The Hardware Accelerator screen shows the operational status that the gateway reports for the card, as shown in Figure 12.

2 Click on Disable or Enable.

Figure 12 Hardware Accelerator screen



To enable or disable automatic recovery of a CSA or Hardware Accelerator card:

1 Choose System > Accelerator (see Figure 12 on page 50).

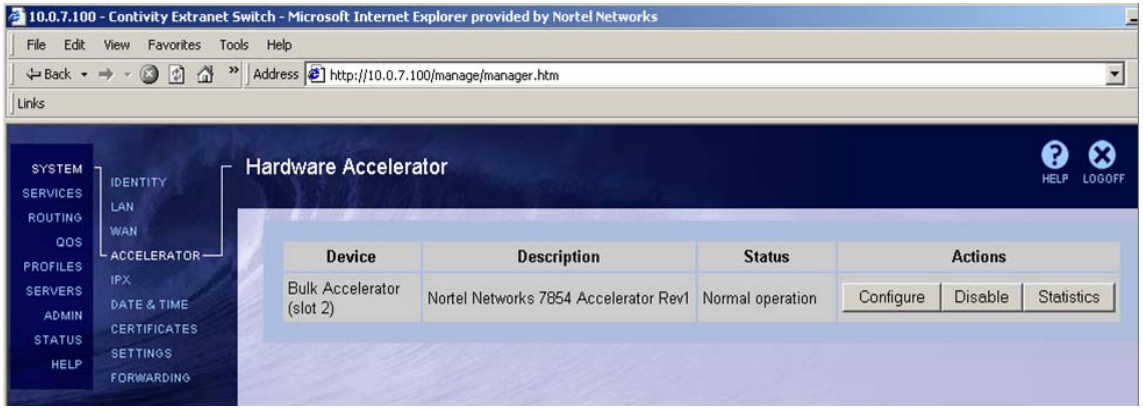
2 Click on Configure.

The Hardware Accelerator Configuration screen appears (Figure 13).

3 Select or clear the Enable Auto Recovery option.

When you enable this option, all sessions will fail over to the software if the accelerator card experiences a recoverable failure.

Figure 13 Hardware Accelerator Configuration screen



You cannot configure the other fields on the Hardware Accelerator Configuration screen. Following is a brief description of these fields.

- Description: Type of accelerator card installed in the gateway: 7854 (Contivity Security Accelerator card) or 7811 (Hardware Accelerator card).

- Operational Status
  - — Disabled
  - — Normal Operation (“Active” on Status > Statistics: HwAccelInfo screen)
  - — Shutdown (indicates that automatic recovery is disabled; you can manually reenable the card after a recoverable failure has been detected)
  - — Failed (indicates that the card is not operating properly; contact Nortel Customer Support for additional information)
- Administrative Status: either Enabled or Disabled (enabled by default).
- Protocols: Shows the protocols supported by the card.
- Algorithms: Shows the encryption and authentication protocols that the card supports (see Table 6 on page 47).
- Crypto Strength: AES, 3DES, or DES (Hardware Accelerator card only), depending upon the maximum key length.
- Boots: Number of times that the card has been restarted.
- Uptime: Length of time that the accelerator card has been running (days:hours:minutes:seconds) since it was last restarted.
- Context Memory Size: Amount of context memory on the card.
- Max Sessions: Maximum number of sessions. Divide this number by 2 to obtain the number of tunnels (2048 sessions represents 1028 tunnels).
- POST Results: Shows the passing and failure indications for each power-on self-test (POST) type. This field displays when there is a POST failure only.

Viewing statistics for accelerator cards

To view information or statistics about a CSA or Hardware Accelerator card, choose Status > Statistics > Hw Accel Info or Status > Statistics > Hw Accel Stats.

You can also execute these CLI commands:

- show status statistics hardware hw-accel-info
- show status statistics hardware hw-accel-stats

Chapter 2
Configuring a T1 CSU/DSU

Management screens that you access from the System > WAN Interfaces > Configure screen enable you to configure the settings for a T1 with an integrated CSU/DSU, including extended super frame (ESF) framing parameters and adding fractional T1 channels.

The Quad T1/E1 is a four-port version of the single port T1 card that is optional with Contivity platforms. The Quad T1/E1 is used in situations where there is a need to terminate multiple T1/E1 circuits utilizing clear text routing at a regional or headquarters location.

Terminating multiple T1/E1 circuits is typically a mid-range or regional application. The advantages for local loop technology to mid-range locations are reoccurring cost, bandwidth and reliability.

Newer T1 services use extended super frame (ESF) framing, which uses out-of-band signaling. The configuration parameters with ESF are:

- Line framing is ESF.
- Line coding is B8ZS.
- HDLC polarity is normal.
- Performance report message value is determined by the T1 service provider.

Older T1 services use super frame (SF) framing, which uses in-band signaling. The configuration parameters with SF are:

- Line framing is SF.
- Line coding is AMI.
- HDLC polarity is inverted.
- Performance report message should be set to “none” as it has no effect in SF framing.

Because SF framing uses in-band signaling, the data can generate a false yellow alarm. These false yellow alarms can be eliminated by setting one fractional T1 channel to “off.” If you have the option of using SF or ESF framing, Nortel recommends ESF framing because it provides better diagnostics and does not generate false yellow alarms.

Viewing status

Following is a list of screens that allow you to either configure or view status for the T1 interface with an integrated CSU/DSU:

- System > WAN
- System > WAN > Configure
- Admin > Health Check
- Status > Statistics > WAN Status

Initial configuration takes place when you install the card, and configuration changes are necessary when adding additional fractional T1 channels.

Note: You must restart the gateway after adding a T1 card or after enabling a fractional T1 line.

All of the CSU/DSU commands can be configured through the Web interface, the serial interface, or the command line interface.

Configuring a T1 CSU/DSU

To configure a T1 CSU/DSU:

1. Click on Configure on the System > WAN Interfaces > Configure PPP/Frame Relay screen. The Configure CSU/DSU screen appears.
2. Set the Circuit ID. This field is specified by the circuit vendor and is useful for communicating with the vendor during troubleshooting.

3. Set the Clock Source. This field sets where the timing is being determined, from the gateway (Internal) or from the T1 service provider (Loop). The clock source is usually set to Loop when connected to a live T1 service. Internal clocking is used for local or test applications only.

4. Set the Line Build Out (dB) value. The line build out value is a power level that is set based on the distance from the CSU/DSU to the T1 service provider's gateway. If the CSU/DSU card is close by, the gateway requires less power and the line build out value is lower; if the card is far away, the gateway requires more power and the line build out value is higher. This setting is determined by the T1 service provider. Valid options are:

   - 0.0
   - -7.5
   - -15.0
   - -22.5

5. Set the Line Coding value. This field sets the method of encoding binary digits on the line. The line coding value is supplied by the T1 service provider. Valid options are AMI and B8ZS.

6. Select the HDLC Polarity. This field determines whether or not the user data is inverted. This field must be synchronized with the AMI line coding; otherwise, you might violate the AMI specification. Both the local and the remote CSU/DSU must terminate the T1 data circuit with the same setting: either both using Normal or both using Inverted. Valid options are Normal and Inverted.

7. Set the Line Framing value. This field determines the low-level protocol between the T1 service provider and the gateway. It determines how the data is encapsulated and it handles the signaling for alarms and loopbacks. The newer ESF framing uses out-of-band signaling, while the older SF framing uses in-band signaling. The line framing value is supplied by the T1 service provider. Valid options are SF and ESF.

8. Select the Performance Report Message setting. The Performance Report Message parameter is a part of the ANSI T1 specification. It generates messages that state how many errors there are per second. This value is used with ESF framing only. When using SF framing, this parameter has no effect but should be set to None to avoid any confusion. The Performance Report Message value is supplied by the T1 service provider and are None and ANSI.

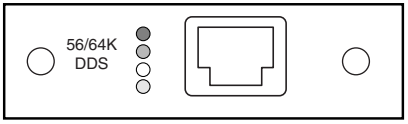
9. Enable Fractional T1. A T1 service consists of up to 24 channels. Typically, you purchase the number of necessary channels from the service provider, and

you can add additional channels (up to 24) as growth requires. When you add a fractional T1 channel, you must enable it through this parameter and restart the system. Valid options for each of the 24 DS-0 channels are On (checked) and Off (unchecked).

56/64K CSU/DSU WAN

The 56/64K CSU/DSU WAN interface card has a single RJ-48 connector that provides the signals needed to interface to network equipment. Figure 14 shows the 56/64K CSU/DSU WAN interface card. This card can be run on any platform supported by Version 5.00 except the Contivity 4500.

Figure 14 56/64K CSU/DSU WAN interface card



10972EA

The connector on the 56/64K CSU/DSU WAN interface card accommodates an 8-pin RJ-48 modular patch cord. These cables are commonly sold as Category 5, or Ethernet, cables.

Note: Nortel does not supply an interface cable with the 56/64K CSU/DSU WAN interface card.

The cable you use should be wired in accordance with EIA-568-A wiring style. This wiring style ensures that the transmit signal (pins 1 and 2) and the receive signal (pins 7 and 8) are carried on a twisted pair inside the patch cord. The use of factory-made patch cords is strongly recommended.

You connect the 56/64K CSU/DSU WAN interface card to the service provider network using a straight-through cable or a crossover cable, depending on how the service provider wired its jack.

- For a straight-through connection, you can use a standard Category 5 (Ethernet) straight-through cable.

- For a crossover connection, you cannot use a standard Category 5 crossover cable. The 56/64K CSU/DSU crossover cable and the Ethernet crossover cable are not interchangeable.

Table 7 provides the 56/64K CSU/DSU cable pinouts for a crossover connection.

Table 7 56/64K CSU/DSU cable pinouts for crossover connection

Nortel termination		Remote termination	
Signal	**Pin # to Pin #**		**Signal**
Transmit tip	1	7	Receive tip
Transmit ring	2	8	Receive ring
not used	3	3	not used
not used	4	4	not used
not used	5	5	not used
not used	6	6	not used
Receive tip	7	1	Transmit tip
Receive ring	8	2	Transmit ring

The cable will operate properly if pins 3, 4, 5, and 6 are not connected.

Caution: For crossover connections, do not use Ethernet cable. The link will not be established.

Table 8 provides the 56/64K CSU/DSU cable pinouts for a straight-through connection.

Table 8 56/64K CSU/DSU cable pinouts for straight-through connection

Nortel termination		Remote termination	
Signal	**Pin # to Pin #**		**Signal**
Transmit tip	1	1	Transmit tip
Transmit ring	2	2	Transmit ring
not used	3	3	not used
not used	4	4	not used

Table 8 56/64K CSU/DSU cable pinouts for straight-through connection

Nortel termination		Remote termination	
not used	5	5	not used
not used	6	6	not used
Receive tip	7	7	Receive tip
Receive ring	8	8	Receive ring

Figure 15 shows the LEDs on the 56/64K CSU/DSU WAN interface card.

Figure 15 LEDs on the 56/64K CSU/DSU WAN interface card

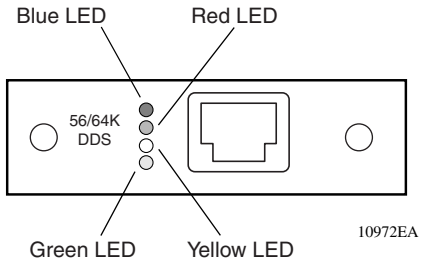


Table 9 describes the LEDs on the 56/64K CSU/DSU WAN interface card.

Table 9 LED indicators on the 56/64K CSU/DSU WAN interface card

LED	Description
Blue	Blue alarm LED is lit when receiving an upstream failure denoted by an alarm indication signal (AIS).
Red	Red alarm LED is lit when a loss-of-signal (LOS) or out-of-frame (OOF) condition is detected on the receive signal.
Yellow	Yellow alarm LED is lit when the far-end equipment is in the red alarm condition.
Green	Normal operation.

The Contivity gateway provides for direct connection to Digital Data Service (DDS) with 56/64K DDS interface with an integrated CSU/DSU. This is data rate-selectable (56 Kbps / 64 Kbps) and supports PPP and FR protocols over 56/64K DDS leased lines.

It supports PPP and Frame Relay protocols over 56/64K DDS leased lines.

Clock Source is one of the following:

- Internal – clock source is originated from the chip. Only for 56kbps data rate.
- Loop (default setting) – clock source is the network

To configure the 56/64K DDS Interface, click on Configure CSU/DSU on the System > WAN Interfaces > Configure PPP/Frame Relay screen. The Configure CSU/DSU screen appears.

Figure 16 56/64K DDS interface 1

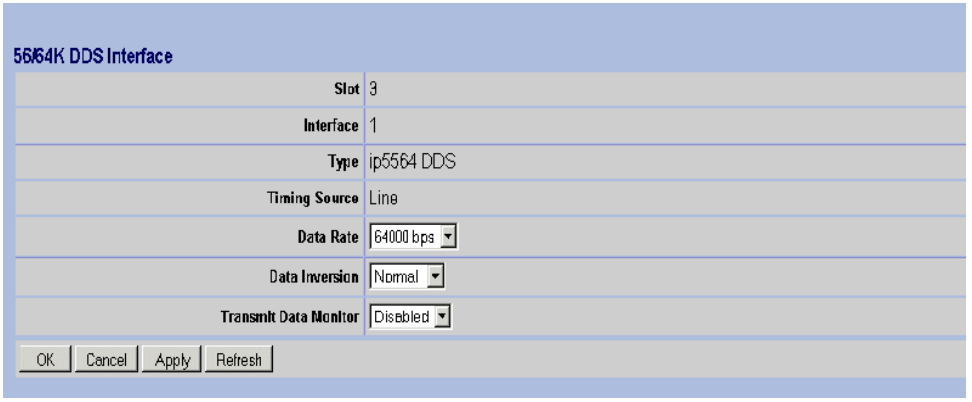
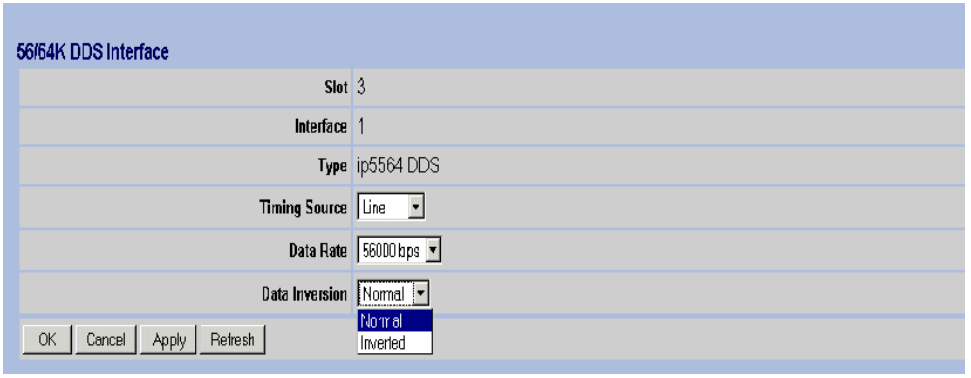


Figure 17 56/64K DDS interface 2



Chapter 3
Configuring ADSL and ATM

Asymmetric digital subscriber line (ADSL) service provides high-bandwidth digital information using the existing telephone network (or POTS—plain old telephone service). ADSL simultaneously accommodates voice (analog) information on the same line.

ADSL is “asymmetric” in that most of its two-way bandwidth is allocated to the downstream direction to send data to the customer. Typically, ADSL provides downstream data rates from 512 Kb/s to 6 Mb/s.

Note: When ADSL receives large numbers of packets from an FTP session, PPP keep-alive packets may be delayed. You can reset the PPP parameter to help alleviate this problem.

ADSL WAN interface cards

The Contivity 1100 supports two ADSL WAN interface cards: one card that supports Annex A and a second card that supports Annex B. The two cards support the following ADSL line protocols:

- ADSL Annex A interface card supports these line protocols:
  - — ANSI DMT over analog/POTS (specified in ANSI T1.413)
  - — G.lite over analog/POTS (specified in ITU-T G.992.2)
  - — G.DMT Annex A over analog/POTS (specified in ITU-T G.992.1 Annex A)
- ADSL Annex B interface card supports the G.DMT Annex B line protocol over digital/ISDN BRI (specified in ITU-T G.992.1 Annex B).

ATM software

ADSL is the physical layer protocol; asynchronous transfer mode (ATM) is the link layer protocol. ATM on the ADSL interface supports one virtual circuit (VC) that uses ATM Adaptation Layer 5 (AAL5) to format packets.

IP packets are encapsulated within AAL5 frames. The following AAL5 encapsulation types are supported on the ATM VC:

- MPoA routed (as described in RFC 2684, “Multiprotocol Encapsulation over ATM Adaptation Layer 5”)
- PPPoA
- PPPoE

Each ATM VC has an IP address (static or dynamic) and an associated VPI/VCI.

Configuring ADSL and ATM

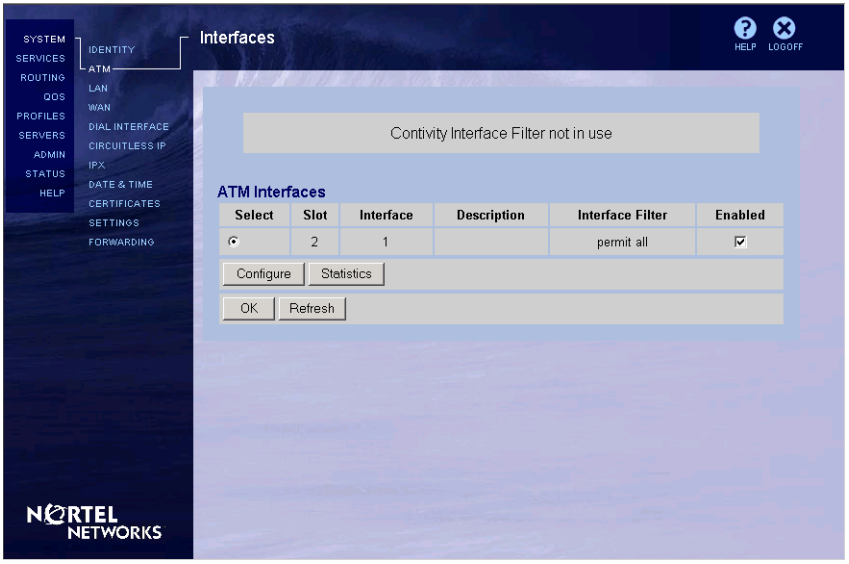
This section provides instructions for using the GUI to configure ADSL and ATM.

Configuring an ATM interface

To configure an ATM interface:

1 From the left menu bar of the GUI, choose System > ATM. The ATM Interfaces screen opens, as shown in Figure 18 on page 63.

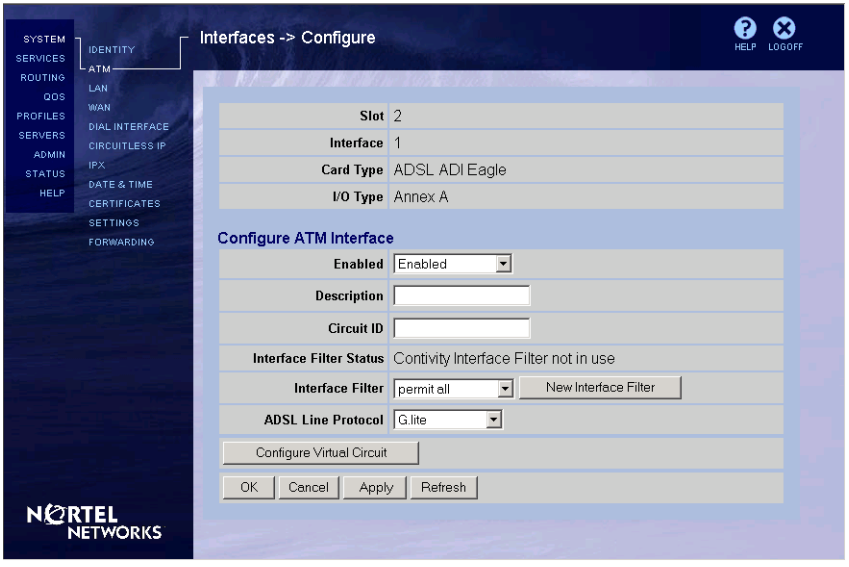
Figure 18 ATM Interfaces screen



2 Select the interface that you need to configure and click on Configure.

The ATM Interfaces Configure screen opens, as shown in Figure 19.

Figure 19 ATM Interfaces Configure screen



3 Configure ATM interface parameters as follows:

   a Enable or disable the interface. You can also enable or disable the interface with debugging enabled.

   b In the Description field, you can type a text description for the physical interface (this field is optional).

   c In the Circuit ID field, type the vendor's circuit identifier (the telephone company supplies this ID). This ID is useful for troubleshooting.

   d From the Interface Filter list, choose an existing filter or click on New Interface Filter to create a new one. The default filter is "deny all."

   e From the ADSL Line Protocol list, choose the appropriate line protocol.

   The line protocol must be compatible with the I/O type specified at the top of the screen (see Figure 19 on page 63). For example, if the I/O type is Annex A, you cannot set the ADSL line protocol to G.dmt Annex B.

4 Click on OK or Apply.

5 To configure the ATM virtual circuit for this interface, click on Configure Virtual Circuit (see the next section, "Configuring an ATM virtual circuit").

Configuring an ATM virtual circuit

You can configure one ATM virtual circuit (VC) on an ADSL interface. The VC uses ATM Adaptation Layer 5 (AAL5) to encapsulate IP packets within AAL5 frames. Each ATM VC has an IP address and an associated VPI/VCI.

To configure an ATM virtual circuit:

1 From the left menu bar of the GUI, choose System > ATM.

   The ATM Interfaces screen opens (see Figure 18 on page 63).

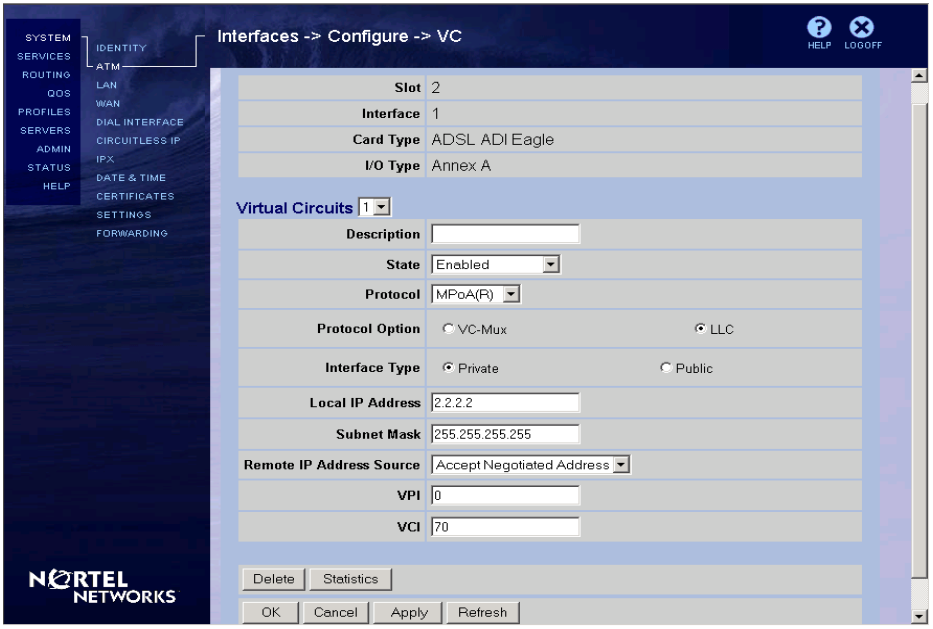
2 Select the interface that you need to configure and click on Configure.

   The ATM Interfaces Configure screen opens (see Figure 19 on page 63).

3 Click on Configure Virtual Circuit at the bottom of the Interfaces Configure screen.

   The ATM Configure VC screen opens, as shown in Figure 20 on page 65.

Figure 20 ATM Configure VC screen



4 Configure VC parameters as follows:

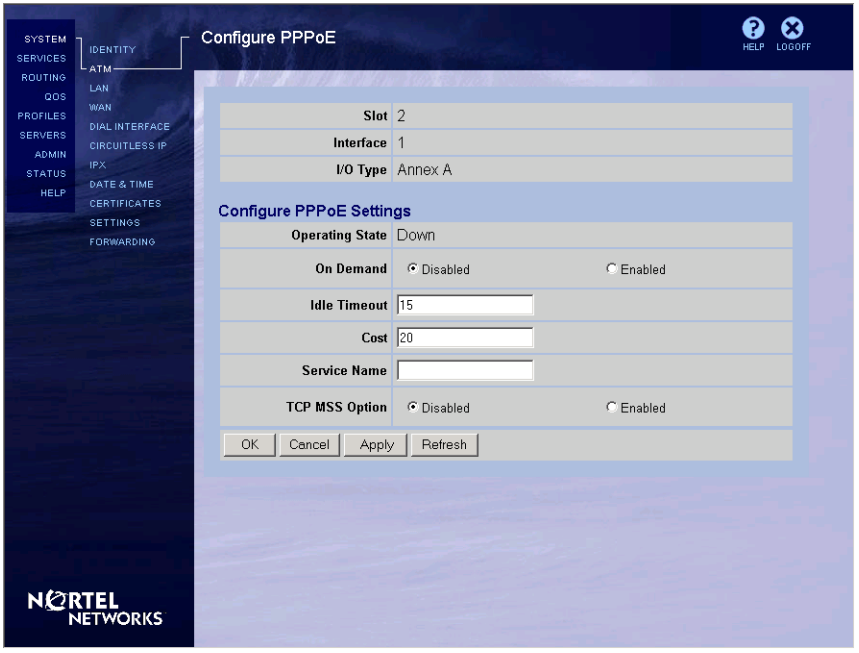
a In the Description field, you can type a text description for the VC (this field is optional).

b Enable or disable the VC. You can also enable or disable the VC with debugging enabled.

c From the Protocol list, choose the encapsulation protocol for the VC: MPoA routed (the default value), PPP over AAL5 (PPPoA), or PPP over Ethernet (PPPoEoA).

If you set the protocol to PPPoA or PPPoEoA, several new fields are displayed, as shown in Figure 21 on page 66. (The MAC CRC field appears only when the protocol is set to PPPoEoA.)

Figure 21 ATM Configure VC screen with PPPoEoA encapsulation



d Select a protocol option: VC-MUX or LLC.

VC-MUX is a null encapsulation that allows only one protocol to run over the VC. The LLC (LLC/SNAP) option allows multiple protocols to run over the virtual circuit.

Note: If the protocol is set to MPoA(R), set the protocol option to LLC.

e If you set the protocol to PPPoEoA, set the MAC CRC option to include or exclude the Ethernet MAC CRC in MPoA bridged frames.

f Set the Interface Type option to indicate whether the VC is on the private side of the gateway (the default value) or the public side.

g If you set the protocol to PPPoA or PPPoEoA, enable or disable the Use Default Route option. By default, this option is enabled.

The Use Default Route option configures the default route to use the dynamically learned IP address for the VC and to update that address when it changes.

h If you set the protocol to PPPoA or PPPoEoA, use the Local IP Address Source field to specify whether the IP address for this VC will be acquired dynamically or whether you will enter an address and subnet mask.

Note: If you set the protocol to MPoA(R), you must type a static IP address and mask.

i If you set the Local IP Address Source option to Specify IP Address, type an IP address and mask in the Local IP Address and Subnet Mask fields.

j Use the Remote IP Address Source field to specify whether the peer IP address will be acquired dynamically or whether you will enter the address.

k If you set the Remote IP Address Source option to Specify IP Address, type the IP address for the remote peer in the Remote IP Address field.

l In the VPI and VCI fields, type the virtual path identifier and the virtual circuit identifier for this VC.

5 Click on OK or Apply.

6 If you set the protocol to PPPoA or PPPoEoA, see the following sections:

- "Configuring PPP authentication" on page 67
- "Configuring PPP advanced parameters" on page 69

7 If you set the protocol to PPPoEoA, you can also set PPPoE parameters (see "Configuring PPPoE parameters" on page 71).

Configuring PPP authentication

If you set the protocol on the Configure VC screen to PPPoA or PPPoEoA (see Figure 21 on page 66), you can configure PPP authentication parameters.

To configure PPP authentication parameters:

1 From the left menu bar of the GUI, choose System > ATM.

The ATM Interfaces screen opens (see Figure 18 on page 63).

2 Select the interface that you need to configure and click on Configure.

The ATM Interfaces Configure screen opens (see Figure 19 on page 63).

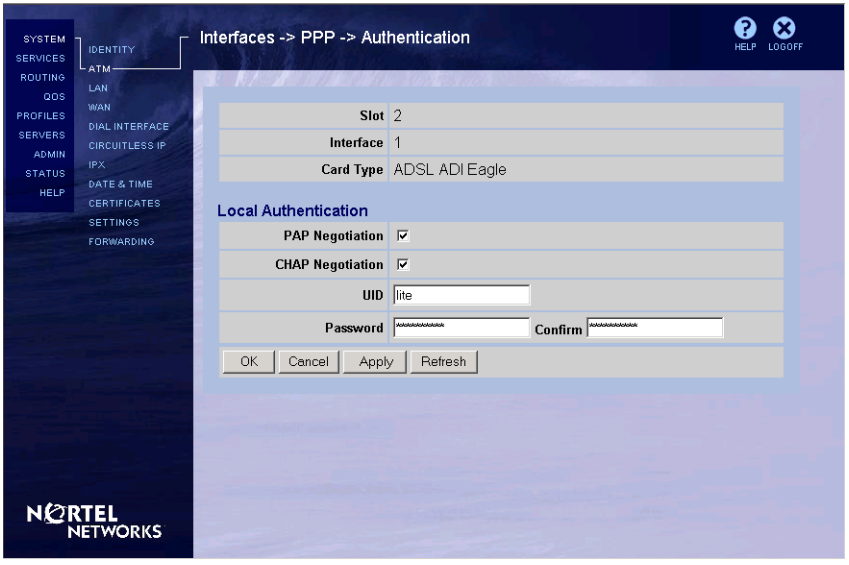
3 Click on Configure Virtual Circuit at the bottom of the Interfaces Configure screen.

The ATM Configure VC screen opens (see Figure 21 on page 66).

4 In the Configure PPP Settings section at the bottom of the Configure VC screen, click on Authentication Settings.

The PPP Authentication screen opens, as shown in Figure 22.

Figure 22 PPP Authentication screen



5 Select PAP negotiation, CHAP negotiation, or both, by placing a check mark in the appropriate check box.

When you select CHAP or PAP, you enable the protocol for PPP sessions on the ATM VC.

6 In the UID and Password fields, type the user ID and password that the gateway will use for PAP and CHAP authentication.

7 In the Confirm field, retype the password.

8 Click on OK.

You return to the Configure VC screen (see Figure 21 on page 66).

9 If you need to set PPP advanced parameters, go to"Configuring PPP advanced parameters" on page 69.

10 If you set the protocol to PPPoEoA and you need to set PPPoE parameters, see "Configuring PPPoE parameters" on page 71.

Configuring PPP advanced parameters

If you set the protocol on the Configure VC screen to PPPoA or PPPoEoA, you can configure PPP advanced parameters.

To configure PPP advanced parameters:

1 From the left menu bar of the GUI, choose System > ATM.

The ATM Interfaces screen opens (see Figure 18 on page 63).

2 Select the interface that you need to configure and click on Configure.

The ATM Interfaces Configure screen opens (see Figure 19 on page 63).

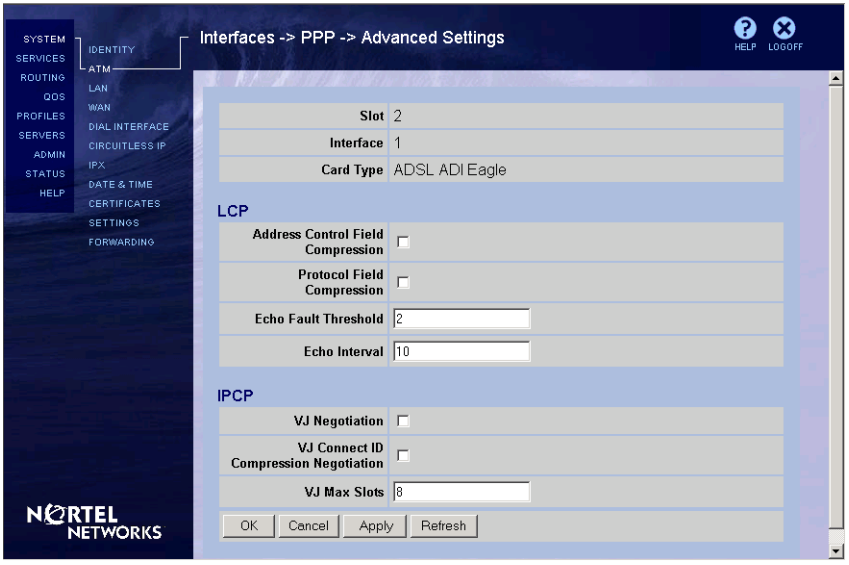
3 Click on Configure Virtual Circuit at the bottom of the Interfaces Configure screen.

The ATM Configure VC screen opens (see Figure 21 on page 66).

4 In the Configure PPP Settings section at the bottom of the Configure VC screen, click on Advanced Settings.

The PPP Advanced Settings screen opens, as shown in Figure 23 on page 70.

Figure 23 PPP Advanced Settings screen



5 Set Link Control Protocol (LCP) parameters as follows. (The LCP negotiates various link options between the gateway and the ISP.)

a Select the Address Control Field Compression option to enable LCP address control field compression. This option compresses the address control field in the packet header and reduces packet overhead by 1 byte.

b Select the Protocol Field Compression option to enable LCP protocol field compression. This option compresses the protocol field in the packet header and reduces packet overhead by 1 byte.

c In the Echo Fault Threshold field, type a value for the LCP echo fault threshold. The echo fault threshold is the number of consecutive unanswered echo requests that LCP sends before it disconnects the link. Type an integer from 0 through 255 (0 disables this option).

d In the Echo Interval field, type the number of seconds between LCP echo requests. You can use this interval with the echo request threshold to determine whether the link has been disconnected. Type an integer from 0 through 255.

6 Set IP Control Protocol (IPCP) settings as follows. (The IPCP specifies certain dial-up networking attributes, such as address assignment and configuration of DNS or WINS server settings.)

a. Select the VJ Negotiation option to enable Van Jacobson (VJ) compression negotiation. VJ compression compresses the TCP/IP header fields on a per TCP/IP flow basis and reduces packet overhead.

b. Select the VJ Connect ID Compression Negotiation option to enable VJ connect ID compression. In conjunction with VJ compression negotiation, VJ connect ID compression negotiation further reduces the TCP/IP packet header to increase packet transmission performance.

c. In the VJ Max Slots field, specify the maximum number of concurrent VJ compressed TCP/IP flows. Type an integer from 2 through 16 (the default is 8).

7. Click on OK.

   You return to the Configure VC screen (see Figure 21 on page 66).

8. If you need to set PPP authentication parameters, go to"Configuring PPP authentication" on page 67.

9. If you set the protocol to PPPoEoA and you need to set PPPoE parameters, see the next section, "Configuring PPPoE parameters."

Configuring PPPoE parameters

If you set the protocol on the Configure VC screen to PPPoEoA, you can configure PPPoE parameters.

To configure PPPoE parameters:

1. From the left menu bar of the GUI, choose System > ATM.

   The ATM Interfaces screen opens (see Figure 18 on page 63).

2. Select the interface that you need to configure and click on Configure.

   The ATM Interfaces Configure screen opens (see Figure 19 on page 63).

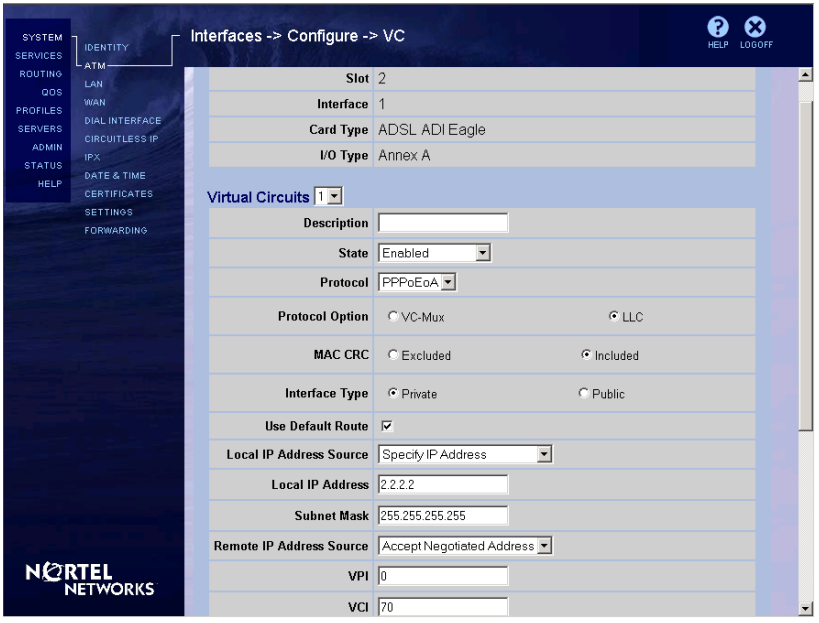
3. Click on Configure Virtual Circuit at the bottom of the Interfaces Configure screen.

   The ATM Configure VC screen opens (see Figure 21 on page 66).

4 In the Configure PPPoE Settings section at the bottom of the Configure VC screen, click on Edit PPPoE Interface.

The Configure PPPoE screen opens, as shown in Figure 24.

Figure 24 Configure PPPoE screen



5 Enable or disable the On Demand option to enable on-demand connections or to enable only nailed-up connections.

6 If you enabled the On Demand parameter, enter a value for the Idle Timeout parameter.

In the Idle Timeout field, type the number of minutes that can elapse with no activity before the interface terminates the on-demand connection.

7 In the Cost field, you can set the cost of the PPPoE interface.

8 In the Service Name field, you can specify a service name to be associated with this PPPoE interface. Enter a description of the PPPoE connection.

9 Enable or disable the TCP MSS option.

PPPoE enforces an MTU size of 1492 bytes. For this reason, all PCs that connect to the Contivity gateway also need to enforce an MTU of 1492 bytes, instead of the usual 1500 bytes. If it is impractical to change the MTU for your PCs, you can enable this option. For more information, see "Configuring the interface MTU and the TCP MSS" on page 29.

10 Click on OK.

You return to the Configure VC screen (see Figure 21 on page 66).

Chapter 4
Configuring PPP

The Point-to-Point Protocol (PPP) is a standard for transporting multi-protocol datagrams over point-to-point links. PPP has three main components:

- Encapsulation for multi-protocol datagrams.
- A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
- Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

For more information, see RFC 1661.

Configuring PPP settings

To configure PPP settings:

1. Select System > WAN on the Contivity Secure IP Services Gateway menu. The System > WAN Interfaces screen appears.
2. Select the interface that you want to configure by clicking the associated radio button in the Select column and then clicking Configure. The System > WAN Interfaces > Configure screen appears. The System WAN Configure screen contains information common to all WAN link protocols and interfaces.
3. Enter an optional description of the interface in the Description field.
4. Enter a unique text name in the Circuit ID field.
5. Select an Interface Filter from the list.
6. Select PPP from the Protocol list. The default is PPP.

7. Click Configure. The System > WAN Interfaces > Configure > Configure PPP screen appears. Information about the interface is given at the top of the screen, including the slot number and interface number.
8. Enter a description.
9. Enter the IP address.
10. Specify the remote IP address setting.
11. Select the interface type, public or private.
12. Click PPP Authentication settings to configure the PPP authentication settings for this interface, including Local PAP and CHAP User IDs and Passwords. The System > WAN Interfaces > Configure PPP > Authentication screen appears. (To configure a CSU/DSU, click Configure CSU/DSU. Refer to Chapter 2, “Configuring a T1 CSU/DSU,” on page 53.)
13. Select the appropriate authentication type, PAP or CHAP, as required by the ISP. If authentication is not required, select None.
14. The ISP providing the WAN connection to the gateway might require a user ID and password. If so, enter and confirm the password. Click OK to save the settings and return to the Configure PPP screen.
15. You can optionally click Configure PPP Advanced Settings to further configure the PPP interface, including Link Control Protocol (LCP) and IP Control Protocol (IPCP) settings. The PPP Advanced Settings screen appears.
16. The Link Control Protocol (LCP) session negotiates various link options between the gateway and the ISP.

    Click Address Control Field Compression to enable Address Control Field Compression, which then compresses the Address Control Field and reduces packet overhead by one byte. Address Control Field compression is Disabled by default.

    Click Protocol Field Compression to enable Protocol Field Compression, which then compresses the Protocol Field and reduces packet overhead by one byte. Protocol Field Compression is disabled by default.

    Set the Echo Fault Threshold. You can set the number of times LCP attempts an Echo request without receiving a reply. The link is dropped when the number of echo requests exceeds the number in the Echo Fault Threshold box. The range is 0 to 255 (0 indicates disabled); default is 1.

Set the Echo Interval. You can set the Echo request Interval in seconds. Use this interval along with the value of the Echo Fault Threshold box to determine if a link has been disconnected. The range is 0 to 255; default is 0 (disabled).

17 The IP Control Protocol (IPCP) settings allow you to specify certain dial-up networking attributes. Typically, IPCP handles address assignment and configuration of domain name system (DNS) or windows Internet naming service (WINS) server settings.

Set the VJ Negotiation. Click to enable Van Jacobson (VJ) Compression Negotiation VJ Compression compresses the TCP/IP header fields on a per TCP/IP flow basis and reduces packet overhead. VJ Negotiation is disabled by default.

Set the VJ Connect ID Compression Negotiation. Click to enable Van Jacobson (VJ) Connect ID Compression, which then further reduces the VJ compression header and increases packet transmission performance. This option is used only when a single TCP/IP flow is active at any single time over the link. VJ-style TCP/IP header compression identification is **Disabled** by default.

Set the VJ Max Slots. This is the Maximum number of concurrent VJ-compressed TCP/IP flows. The range is from 2 to 16; default is 8.

18 In the LCP/NCP section of the screen, set the Interface Debug option, if needed. This option, under the Link Control Protocol/Network Control Protocol, sends PPP control packets to the Event log. This is a Nortel internal Customer Support utility that helps diagnose and troubleshoot WAN interface problems.

19 Click OK to save the settings and return to the System > WAN Interfaces > Configure > Configure PPP screen.

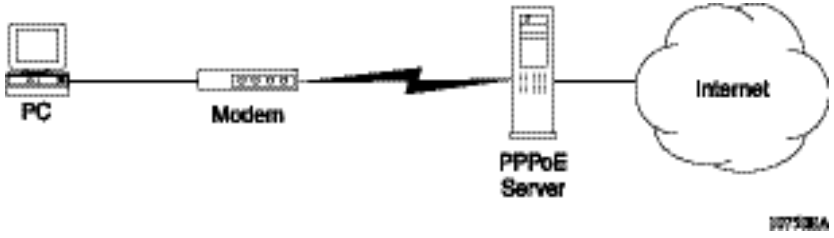
Chapter 5
Configuring PPPoE

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.

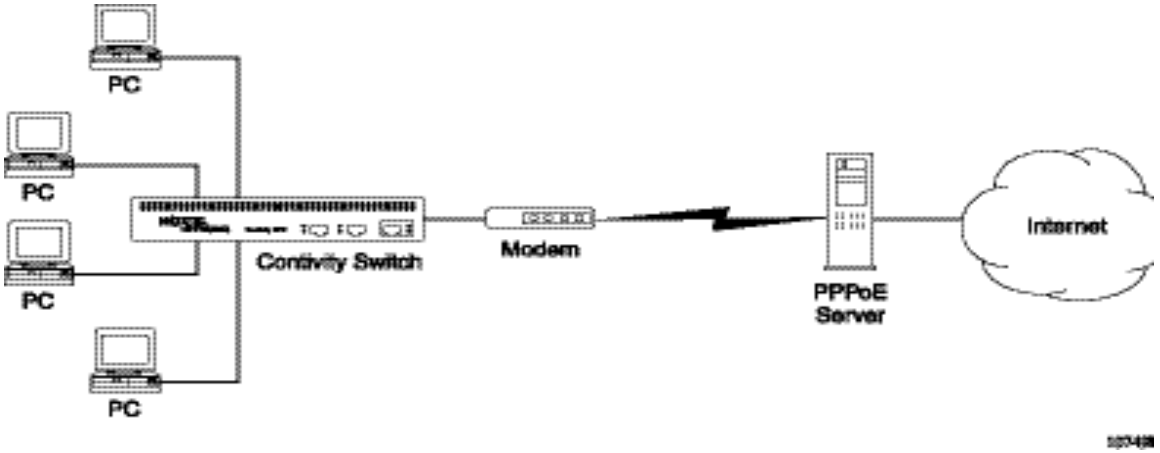
Typically, PPPoE is set up in two different configurations: PPPoE for the single user (Figure 25) or PPPoE on a local network. For locations with single computers, the PPPoE client is typically loaded on the computer and it reaches the PPPoE server through the Ethernet connection via the DSL modem. The 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 implementation is in compliance with RFC 2516.

Figure 25 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 26 shows how a Contivity 1100 gateway 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 26 PPPoE on a local network



PPPoE has the following usage restrictions:

- PPPoE MTU limitation of 1492 bytes. (Reset PC from MTU=1500 to MTU=1492)
- Must set the appropriate filter (deny all by default)
- PPPoE changes are not dynamically applied (must bounce service for edits)
- Must be set on a public Ethernet interface
- Must set the Administrative State to enabled (disabled by default)
- PPPoE is supported as only one session on one interface
- Cannot use dynamic routing on PPPoE interfaces (unless tunneling)

Note: Due to DNS-Ping packet traffic on the PPPoE on demand link, it does not go into IDLE/ TIMEOUT state. In the process of doing a health check on the DNS servers, it sends out DNS-Ping packet traffic, which sends traffic over the PPPoE link if there is a DNS server configured that can be reached over this link. This keeps the PPPoE link up. The status of the DNS servers can be checked using the HealthCheck and the System > Identity screens on the GUI. The Alert LED will not come on if there is a DNS Server Alert.

Configuring PPPoE settings

To configure PPPoE:

1. Go to the System > LAN screen.
2. Choose a public interface, select PPPoE from the Protocol list, and click on Apply.
3. On the Add PPPoE Interface screen, select permit all for the Interface Filter and click on OK.
4. From the System > LAN screen, click on the Edit button, and the Edit PPPoE Interface screen appears.
   a. Enable the administrative state to activate.
   b. Enable On Demand. The default is disabled (nailed PPPoE service).

c Enter the Idle Timeout parameter value from the range specified on the screen to specify *n* minutes of inactivity after which to tear down the connection.

d Enter a value from the range specified on the screen to indicate the cost of the connection.

e Optionally, enter a service name that describes the connection. You should use this field only if the ISP has provided a service name.

f Enter the local IP address, which is dynamically assigned to the interface. The default 0.0.0.0 indicates that the address will dynamically come from the ISP server.

5 For PPP Authentication Settings, click on Configure. The default authentication is None. The PPP Local Authentication screen appears.

a Select either PAP or CHAP.

b Enter the UID.

c Enter a password.

d Click on OK.

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

a Configure the appropriate LCP and IPCP options.

b Click on OK.

Chapter 6
Configuring Frame Relay

Frame Relay is a high-speed, packet-switching WAN protocol that connects geographically dispersed LANs. Frame Relay (FR) is usually offered by a public network provider; however, private organizations can acquire and manage their own Frame Relay networks as well. You can configure Frame Relay on any WAN interface on the gateway.

Frame Relay is a connection-oriented protocol, which means that it relies on end-to-end paths between devices connected across the network. It implements these connections using permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). Contivity Secure IP Services Gateway supports PVCs.

The Contivity gateway functions as a Frame Relay access device (FRAD) in a Frame Relay network. In Frame Relay, there are multiple virtual point-to-point connections (virtual circuits) on a single physical interface. Each virtual circuit has a unique local IP/remote IP point-to-point connection.

Each PVC on the Contivity gateway is a separate IP address. With Frame Relay, IP addresses are assigned to virtual circuits, and the virtual circuit is in turn associated with a physical interface. Also, there may be multiple PVCs on a single physical interface, and hence multiple IP interfaces on a single physical interface. In PPP, there is only a single IP address per physical interface.

Figure 27 on page 84 shows a single public interface to an ISP. In this scenario, a Frame Relay PVC is configured between Contivity 1 and the ISP for Contivity 2 and 3. The PVC replaces a dedicated PPP connection. The Frame Relay PVC is generally less expensive than the dedicated PPP link.

Figure 27 Frame Relay single public interface to ISP

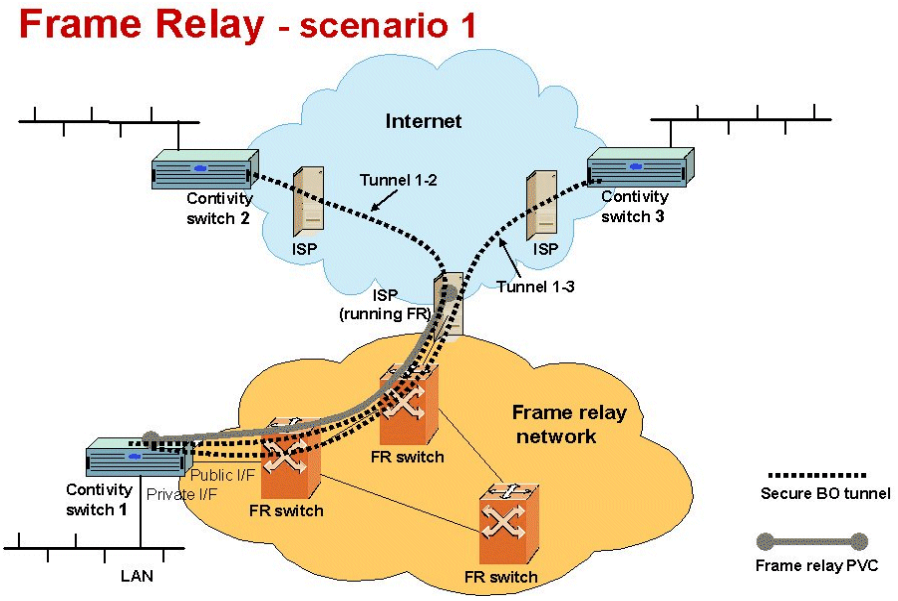


Figure 28 on page 85 shows three Frame Relay PVCs (logical connections) running over a single interface on Contivity 1. These logical connections would not be possible using PPP. The connections in this example do not have to be branch office tunnels. They could also be unsecure, clear text connections over the secure Frame Relay private network.

Figure 28 Frame Relay multiple public interfaces

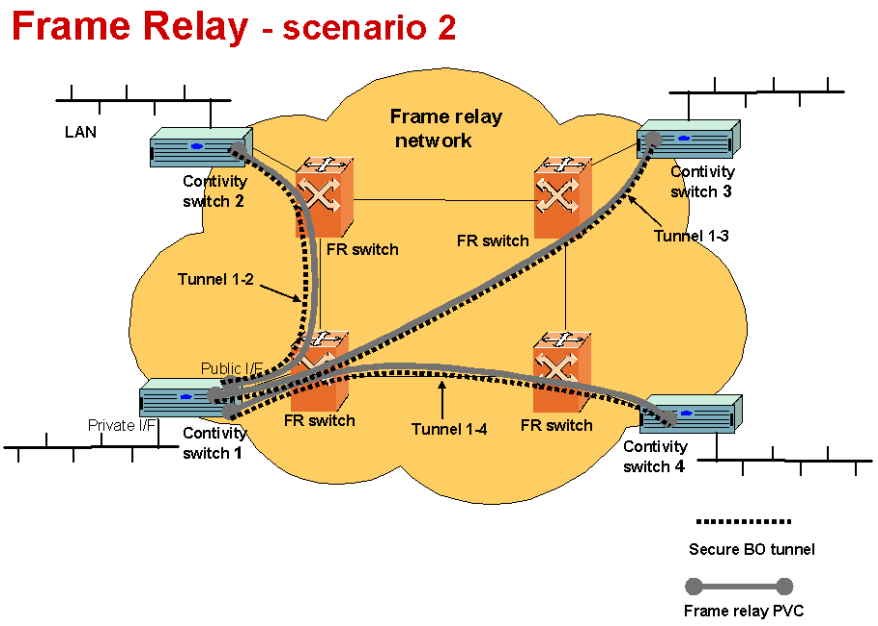
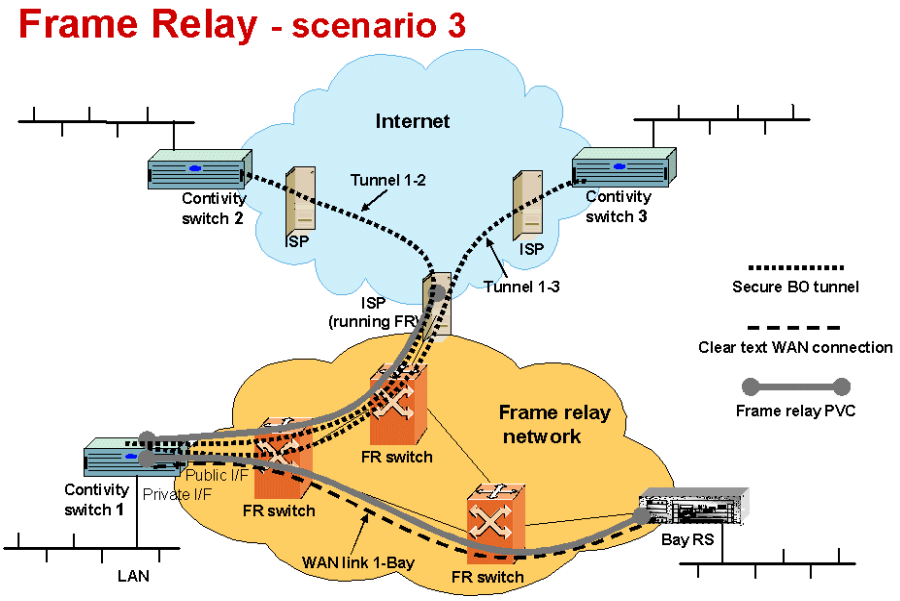


Figure 29 on page 86 shows a gateway between an existing Frame Relay network and a new IP VPN network. Contivity 1 acts as a gateway between the newer unsecure public network (Internet) and the older, secure Frame Relay private network. Contivity 1 is connected to Contivity 2 and 3 using a branch office tunnel over a Frame Relay PVC. Contivity 1 is also connected to the BayRS router using a clear text WAN connection over another Frame Relay PVC, which takes advantage of the WAN as secure interface.

Figure 29 Gateway between Frame Relay network and VPN network



Permanent virtual circuits

A permanent virtual circuit (PVC) is a dedicated logical path that connects two devices over a network. When configured, a PVC is always available to the connected devices; a PVC does not require setup before data can travel across the network, nor does it need to be disconnected after data has passed. Because many PVCs can coexist for one physical line, devices can share the bandwidth of the transmission line.

RFC 1490

RFC 1490 defines the encapsulation method for sending data across a Frame Relay network. Nortel routers implement RFC 1490 for all protocols that Nortel supports over Frame Relay networks.

Traffic shaping

Traffic shaping relieves bottlenecks in topologies with high-speed connections to the central site, and low-speed connections at remote sites. Committed information rate enforcement and quality of service are the major components of Nortel traffic shaping. The traffic shaping parameters are defined in CCITT I.370.

Committed information rate

The committed information rate (CIR) is the rate at which the network supports data transfer under normal operations. Its name is descriptive: you have a contract with your carrier, who is committed to providing a given throughput, here called the committed information rate. The CIR is measured in bits per second. You configure this value that the carrier provides per virtual circuit.

When configuring the CIR, consider the following:

• CIR of 0

You can contract with a carrier for a CIR of 0, which yields best-effort service at low cost. The carrier transmits data, but does not commit to providing a specified throughput. To configure a CIR of 0, set both the throughput (which is the CIR) and the committed burst (B_c) to 0, and set the excess burst (B_e) to a value greater than 0. For more information about burst rates, see the next section, "Committed burst rate and excess burst rate."

• Maximum CIR

The maximum CIR should not be greater than the speed of the access line on the slower end of a virtual circuit. In a big pipe/little pipe topology, likely CIRs at the remote sites would be 32 Kb/s, 56 Kb/s, or 64 Kb/s. If you configure CIRs for these virtual circuits at the central site, you can use CIR enforcement (described in the next topic) to prevent the big pipe from sending traffic that exceeds the PVC CIRs.

• CIR enforcement

CIR enforcement means restricting the speed of outbound traffic to a rate no faster than the CIR. It is the major component of traffic shaping. You can configure CIR enforcement to operate over Synchronous, High-Speed Serial Interface (HSSI), T1, E1, and Integrated Services Digital Network (ISDN) lines, for Frame Relay backup, demand, bandwidth-on-demand, and leased lines at the virtual circuit level. CIR enforcement operates on whole frames only. It controls congestion either by bringing down the virtual circuit, or by throttling the traffic.

Committed burst rate and excess burst rate

ANSI T1.618 issues implicit congestion notification from the network to the user device. The committed burst size (B_c) defines the number of bits that the network will transmit over a specified time interval (T_c) when no congestion is occurring. The excess burst size (B_e) defines the number of extra bits that the network attempts to send over the T_c when there is no congestion. Both the B_c and the B_e are values that you can configure.

The sum of the B_c and the B_e is the maximum amount of traffic that can travel across the network per T_c when there is no congestion. If you set the B_e to a value greater than zero, the router can send traffic exceeding the CIR. To enforce the CIR, that is, to limit traffic that the router can send to the amount of the CIR, set the B_e to 0.

Traffic shaping configuration notes

Traffic shaping is best used at central offices to prevent the “big pipe” from sending too much data too quickly to remote sites with “little pipes.” This concept should guide your decisions about how to configure traffic shaping.

Consider the following when you configure traffic shaping:

- In general, the value you assign to the B_c should equal 1/4 of the CIR to avoid excessive queuing and dropped packets.

If, however, you are sending frames that exceed the size of the B_c, data travels slowly because the router must use multiple time periods to accommodate the packet size and avoid exceeding the CIR. If setting the B_c to 1/4 of the CIR yields a value lower than the packet size, set the B_c to 1/3 or even 1/2 of the CIR.

For example, a typical TFTP frame is 548 bytes. If the CIR is 16,000 bits, the B_c configured according to the 1/4 guideline would be 4,000 bits, or 500 bytes, which is not big enough to accommodate a TFTP frame.

If you set the B_c to 16,000/2, or 1/2 CIR, the result is 8,000 bits, or a packet size of 1,000 bytes, which works, but may result in excessive queuing because the T_c is 1/2 second. If you set the B_c to 16,000/3, or 1/3 CIR, the result is a B_c of 5,333 bits or 666 bytes, much closer to the 548 TFTP frame size.

- If you cannot predict the typical frame size, monitor Frame Relay shaping statistics for numbers of large frames and dropped frames. If either of these numbers is increasing constantly or dramatically, adjust the B_c to a higher value in small increments.

Overview of Frame Relay configuration

Each physical WAN interface can be configured to run either PPP or Frame Relay as a link protocol, but not both simultaneously. However, in a Contivity gateway with multiple WAN interfaces, one interface may run PPP and another interface may run Frame Relay. PPP is the default link protocol.

Frame Relay on the Contivity gateway acts as a UNI device; it does not support NNI. Each WAN link can be configured to run either PPP (the default) or Frame Relay. Each Frame Relay link can be a switched (default) or direct connection.

Note: The WANic 700 High-Speed Serial Interface (HSSI) does not support switched Frame Relay on the DigiLink, model DL3100.

The gateway type is set on a per-link basis. The possible setting are ITU-T and ANSI. This determines both the LMI format and the FECN/BECN processing. The LMI Poll Interval Timer and Poll Interval Counter may be configured when LMI is enabled.

Note: Only ~1500 byte (Ethernet maximum) sized frames are supported. Any larger frames will be discarded as excessively long frames. This is an implementation limitation, not a protocol limitation.

Configuring Frame Relay settings

To configure Frame Relay settings:

1. Select System > WAN on the Contivity Secure IP Services Gateway screen. The System > WAN Interfaces screen appears.
2. Select the interface that you want to configure by clicking the associated radio button in the Select column and then clicking Configure.

   The System > WAN Interfaces > Configure screen appears. The System WAN configure screen contains information common to all WAN link protocols and interfaces.
3. Enter an optional description of the interface in the Description field.
4. Enter a unique text name in the Circuit ID field. This field is optional. This is a character string specified by the circuit vendor. It can be useful when communicating with the vendor during troubleshooting.

Note: Note that while Circuit ID is defined in the T1/E1 MIB (RFC 1406) it is applicable to almost any WAN connection, and so it is configured at the interface level.

5. Select an Interface Filter from the list.
6. Select FR from the Protocol list. The default is PPP.

Note: When you change from Frame Relay to PPP, you lose all configured Frame Relay virtual circuits.

7 Click Configure. The System > WAN Interfaces > Configure > Frame Relay screen appears.

8 Enable the Debug box to have packet information logged in the Event Log.

Choose the connection type, either switched or direct.

To connect to a Frame Relay gateway, the connection type must be set to "switched." In this mode, the gateway type is user configurable. The gateway type determines both the LMI format and the FECN/BECN processing.

Two Contivity gateways can be directly connected without an intervening Frame Relay gateway via the interface connection type "direct." When direct mode is selected, LMI messages are disabled and FECN/BECN processing is not performed. The UNI is defined by FRF 1.1.

9 Select the gateway type, either ITU-T, ANSI or ILMI.

10 Enter a value for the LMI (Local Management Interface) poll interval timer. The gateway supports LMI, as defined in ITU-T Q.933 annex A and ANSI T1.617 Annex D. The LMI type is determined by the gateway type parameter when the physical interface is in the switched mode. This parameter also determines the FECN/BECN processing. LMI is disabled when the physical interface is in the direct mode.

- Minimum: 5
- Maximum: 30
- Default: 10

11 Enter a value for the LMI (Local Management Interface) poll interval counter.

- Minimum: 1
- Maximum: 255
- Default: 6

12 Click Configure Virtual Circuit. The System > WAN Interfaces > Configure > Frame Relay > VC screen appears. Each Frame Relay PVC is individually configured.

13 Enter a description. This is the same user-entered text description used by the existing physical interfaces.

14 Select the state for the VC. This is the same as the physical interface enable/disable. There are 4 values: TRUE, TRUE_DEBUG, FALSE,

FALSE_DEBUG. The _DEBUG values cause the packet to displayed in the event log.

15 Select the VC protocol, IP MPoFR.

16 Specify the Local IP address (static).

17 Select the interface. This is the same public/private (or untrusted/trusted) parameter used by the existing physical interfaces.

18 Specify the remote IP address (static).

19 Enter a value for the DLCI (Data Link Connection Identifier) parameter.

20 Enter a value for the CIR (Committed Information Rate) parameter. The supported range is 0 to the maximum line speed. The default is 0.

The Contivity gateway supports traffic shaping and congestion control as defined in CCITT I.370. The traffic shaping parameters, CIR, B_c, and B_e, are configured on a per-VC basis. FECN/BECN processing is supported as defined in ANSI T1.618 Annex A. The DE flag is not set. CLLM is not supported.

21 Enter a value for the B_c (Committed Burst Size) parameter. The supported range is 0 to the maximum line speed. The default is 0.

22 Enter a value for the B_e (Excess Burst Size) parameter. The supported range is 0 to the maximum line speed. The default is the maximum line speed.

23 Click Statistics to view collected statistics for the interface.

24 Use the Add button to create and define additional PVCs on the interface.

Configuring FRF.9

Frame Relay compression, as offered by FRF.9, provides L2 type compression. When transporting encrypted traffic over a Frame Relay link, it is not necessary to run FRF.9 compression. This is due to the nature of encryption and compression. Compression finds patterns in data to take out common bit patterns at the transmitting end and re-insert these data patterns at the receiving end, while encryption eliminates bit patterns, thus making it harder for anyone eavesdropping to decipher the data.

The Contivity gateway Frame Relay software supports FR data compression as defined in FRF.9. Each FR virtual circuit can have FRF.9 compression enabled or disabled, with disabled as the default. Only LZS compression algorithm is supported.

If FRF.9 is enabled, the Contivity gateway attempts to negotiate an LZS compression algorithm. If the remote end does not support FRF.9, or if it supports FRF.9 but does not support LZS compression, data compression is not performed on the VC. There are three valid combinations of the FRF.9 compression and FRF.9 algorithm fields, as shown in Table 10. The fourth combination in the table is not valid.

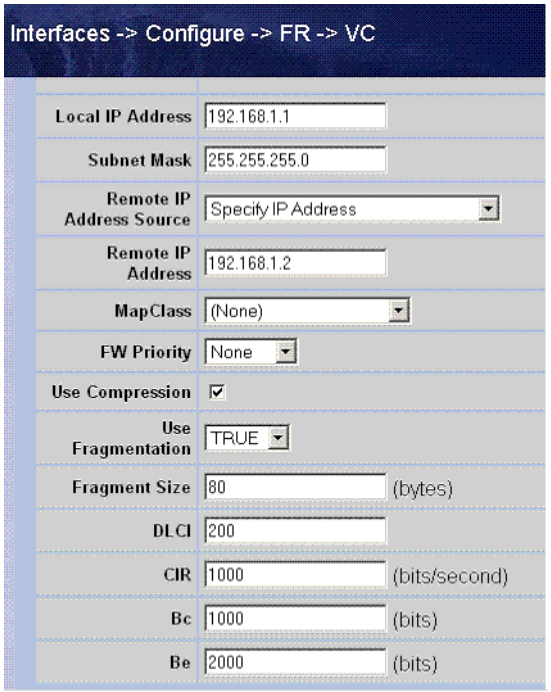
Table 10 FRF.9 compression and algorithm fields

Compression	Algorithm	Result
FALSE	NONE	no negotiation
TRUE	NONE	negotiation unsuccessful
TRUE	LZS	negotiation successful
FALSE	LZS	not valid

To configure FRF.9:

1. Select System > WAN Interfaces > Configure > FR > VC. Figure 30 on page 94 shows the screen that appears.
2. Click the checkbox beside Use Compression. This enables FRF.9.
3. Click OK.

Figure 30 FRF.9 compression



Configuring FRF.12

FRF.12 fragmentation allows high-priority packets of one VC to be sent (interleaved) between fragments of lower priorities of the same VC or other VCs (see Table 11 on page 95).

!**IMPORTANT!**: For full functionality, FRF.12 must be enabled for the PVC, and interleaving must be enabled for the associated interface. Enabling/disabling Interleaving does not cause a circuit restart.

FRF.12 Fragmentation is a configurable, non-negotiable option for a PVC (see Table 12 on page 96). Enabling/disabling FRF.12 Fragmentation causes a circuit restart. Both sides of the circuit must be configured for FRF.12 Fragmentation.

FRF.12 is supported for speeds of < 1MB.

Although an interleaving scheme is not explicitly defined in FRF.12, this fragmentation allows high-priority packets of one VC to be sent (interleaved) between fragments of lower priorities of the same VC or other VCs.

Such fragmentation and interleaving is required to ensure high voice quality for VoIP packets when transmitting voice and data over a WAN. Fragmentation is only required over WANs operating with speeds less than 1Mbps. Fragmentation and interleaving ensures that larger data packets do not introduce variable delay (jitter) to the smaller voice packets. The packets fragment to a fixed configurable size as they transmit over the WAN. Ideally, solution packets interleave so that each subsequent voice packet is always less than a fixed amount of delay (one packet fragment time) from the previous voice packet. For example:

Packets arriving at the router (V = voice packet, D = large data packet)

VDDVDDDDVV

Packets as transmitted over WAN after Fragmentation and Interleaving

DDDVDVDVDV

The FRF.12 fragmentation is implemented within Frame Relay stack, and the associated interleaving is implemented within QoS queues. Interleaving uses two classes of packets, voice and non-voice, and no reordering of packets occur within either class.

Table 11 Interleave values

OM Member Name	Index	Type	Access	Values	Default Values	Description
Interleave	False	Enumeration	RW	0 or 1	0	Enable/disable interleaving
Interleaved Packets	False	UINT32	RW	0 - 4294967295	0	The number of interleaved packets

Table 12 Fragmentation values

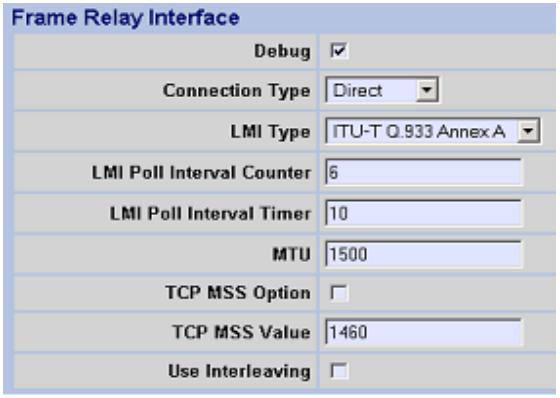
OM Member Name	Index	Type	Access	Values	Default Values	Description
Fragmentation	False	Enumeration	RW	0 or 1	0	Enable/disable fragmentation
FragSize	False	Integer	RW	40 – 800–no fragmentation	80	Fragment size in bytes

To configure FR:

1 Complete steps 1—12 in "Configuring Frame Relay settings" on page 90. Ensure that Use Interleaving checkbox is enabled (see Figure 31 on page 96).

2 Click OK.

Figure 31 Enable interleaving



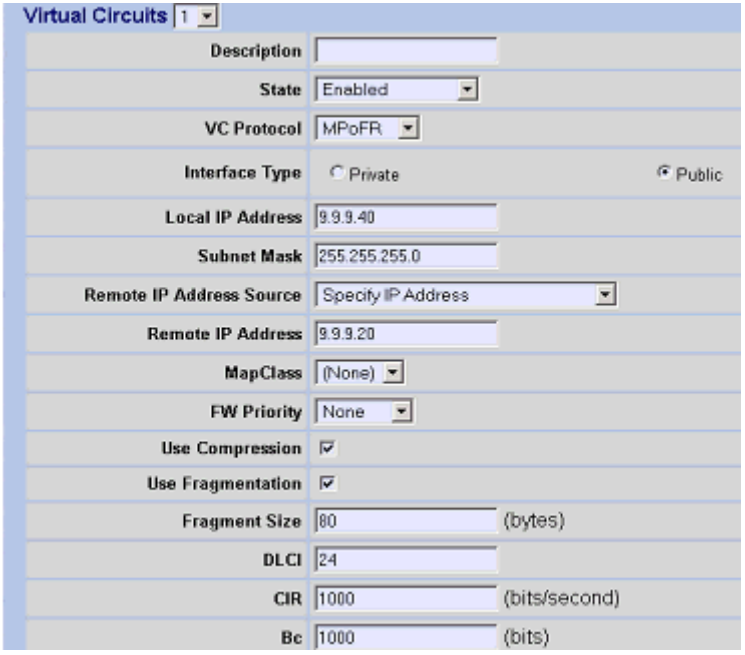
3 Complete steps 13-25 in "Configuring Frame Relay settings" on page 90 and ensure the following (see Figure 32 on page 97):

a Use Fragmentation is enabled.

b Fragmentation size values (see Table 12 on page 96) are entered into the Fragmentation Size box. Set the Fragment size to be the same as, or as close to, the size of the voice packet size to optimize voice performance.

4 Click OK.

Figure 32 Enable fragmentation



Frame Relay Forwarding Priority to a VC (virtual circuit)

The FR Forwarding Priority to a VC provides an interface-level priority queuing scheme in which prioritization is based on the destination of a permanent virtual circuit (PVC) rather than the destination of the packet contents. For example, FR Forwarding Priority to a VC allows you to configure a PVC transporting voice traffic to have absolute priority over a PVC transporting signaling traffic, and a PVC transporting signaling traffic to have absolute priority over a PVC transporting data. FR Forwarding Priority to a VC provides three levels of priority: Low(1), Medium(2), High(3).

The Frame Relay packet is examined at the interface for the data link connection identifier (DLCI) value. The packet is then sent to the correct priority queue based on the priority level configured for that DLCI.

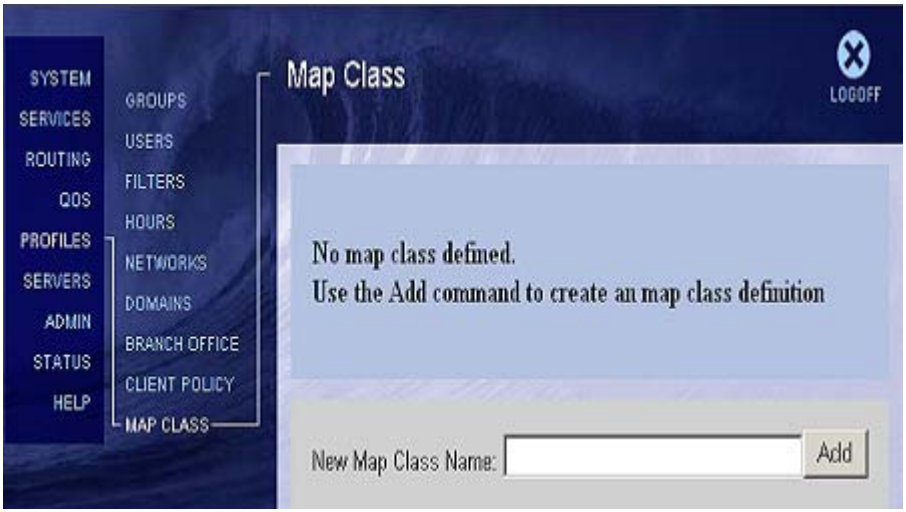
Assigning priority to a PVC within a map class

You assign priority to a PVC within a Frame Relay map class. All PVCs using or inheriting that map class are classed according to the configured priority.

To add a map class for a PVC:

1 Select Profiles > Map Class. Figure 33 on page 99 shows the Map Class window that appears.

Figure 33 Adding a map class for Frame Relay



2 In the New Map Class Name dialog box, enter the name of the new map class.

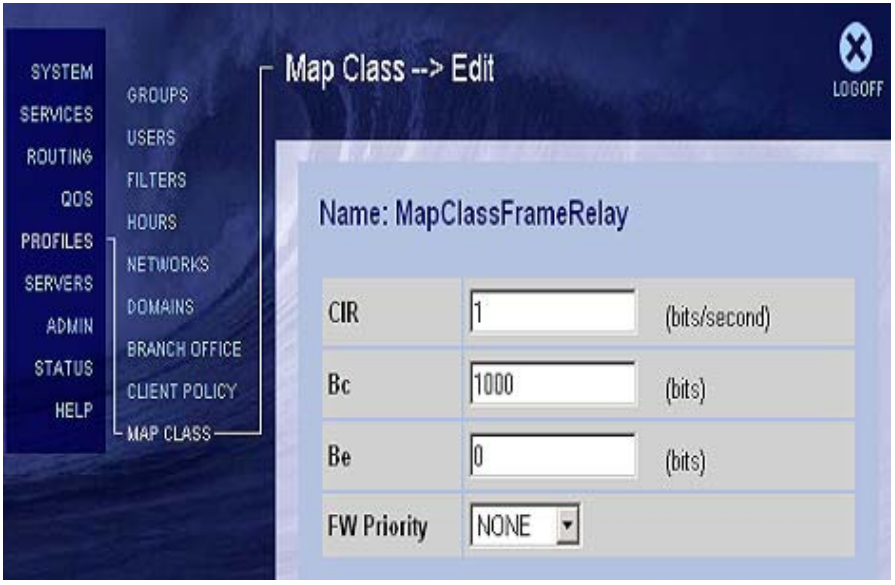
3 Click ADD.

To edit a Map Class associated with a PVC:

1 Select Profiles > Map Class.

2 Select a Map Class Name, click Edit. The Map Class Edit window appears. Figure 34 on page 100 shows the Map Class Edit window.

Figure 34 Editing a map class



3 Enter a value for the following:

- CIR (Committed Information Rate) parameter: The supported range is 0 to the maximum line speed. The default is 0.
- Bc (Committed Burst Rate) parameter: The supported range is 0 to the maximum line speed. The default is 0.
- Be (Excess Burst Rate) parameter: The supported range is 0 to the maximum line speed. The default is the maximum line speed.

Note: If a PVC does not have a map class associated with it, or if the map class associated with it does not have priority explicitly configured, then the packets on that PVC are queued on the default **none** priority forwarding.

- FW Priority: Select one of the following from the options: None(0), Low(1), Medium(2), High(3), Highest(4).

4 Click OK.

To delete a Map Class:

1 Select Profiles > Map Class.

2 Select a Map Class name and click Delete.

3 A confirmation window appears, as shown in Figure 35. Click OK.

Figure 35 Deleting a map class

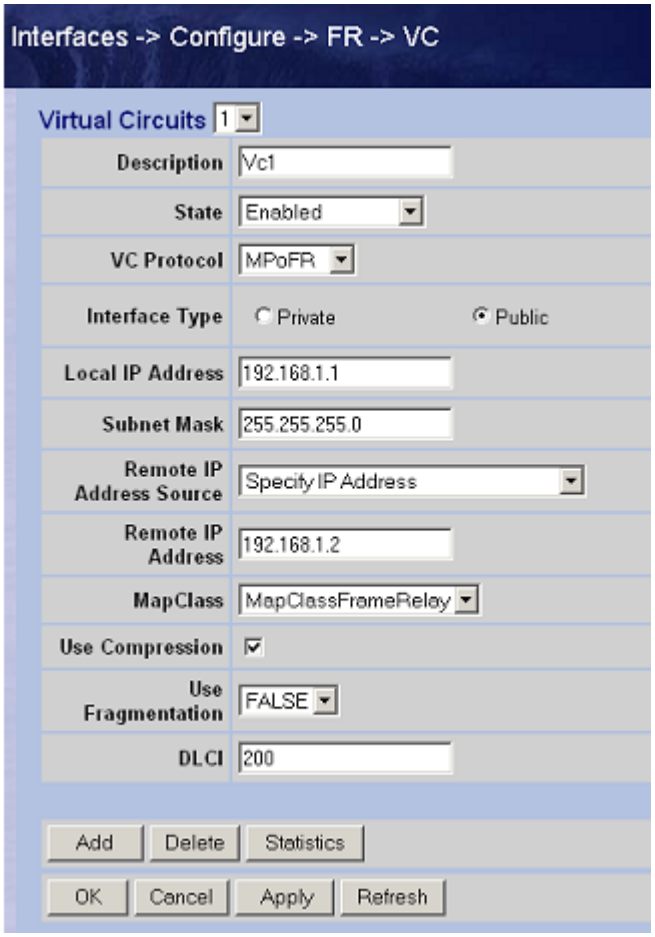
Configuring VC with a map class

If you do not enable FR Forwarding Priority to a VC on the interface using the priority number command in interface frame-relay subinterface <slot>/<port> mode, configuring PVC priority within a map class is not effective.

To use map class in VC:

1 Select System > WAN > Configure > Frame Relay > Virtual Circuits. Figure 36 on page 102 shows the VC window that appears. Figure 37 on page 104 shows the window that appears when using fragmentation.

Figure 36 Map Class in VC with fragmentation disabled



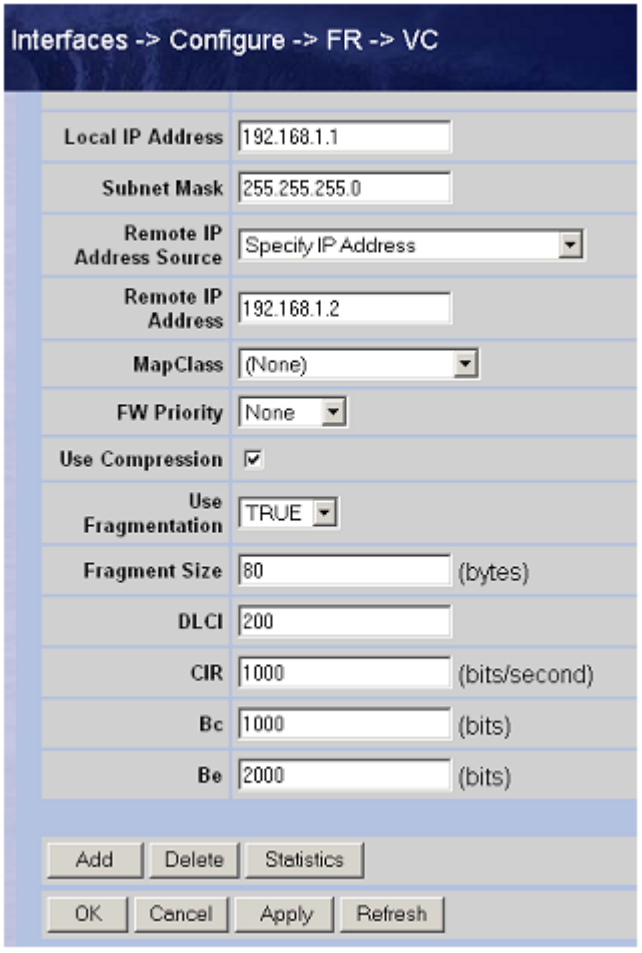
2 Select the following fields:

a For VC with fragmentation disabled, see Figure 36:

- Virtual Circuits: Select the virtual circuit you want to configure using the list box.
- Description: Enter an optional description.
- State: Select the state for the virtual circuit.
- VC Protocol: Select MPoFR (MultiProtocol interconnect over Frame Relay) (IETF RFC 2427).
- Interface Type: Select the interface type, either public or private.
- Local IP Address: Enter the local IP address for the virtual circuit.

- Subnet Mask: Enter a subnet address.
- Remote IP Address Source: Select the remote IP source from the box.
- Remote IP Address: Enter the remote IP address for the virtual circuit.
- Map Class: Select a Map Class from the box.
- Use Compression: Check to use compressions.
- Use Fragmentation: Select True or False. Selecting True initiates.
- DLCI: Enter a value for the DLCI (Data Link Connection Identifier) parameter.

Figure 37 Map Class in VC with fragmentation enabled



b For VC using fragmentation, see Figure 37:

- Local IP Address: Enter the local IP address for the virtual circuit.
- Subnet Mask: Enter a subnet address.
- Remote IP Address Source: Select the remote IP source from the box.
- Remote IP Address: Enter the remote IP address for the virtual circuit.
- FW Priority: Select one of the following from the options: None(0), Low(1), Medium(2), High(3), Highest(4).
- Use Compression: Check to use compressions.
- Use Fragmentation: TRUE is selected.

- Fragment Size: The supported range is 40 - 800. The default is 80.
- CIR (Committed Information Rate) parameter: The supported range is 0 to the maximum line speed. The default is 0.
- Bc (Committed Burst Rate) parameter: The supported range is 0 to the maximum line speed. The default is 0.
- Be (Excess Burst Rate) parameter: The supported range is 0 to the maximum line speed. The default is the maximum line speed.

3 Click Apply, and then click OK.

FR Forwarding Priority to a VC with FRF.12

FR Forwarding Priority to a VC works with or without FRF.12. The interface-level priority forwarding takes the place of the FIFO queuing or dual FIFO queueing normally used by FRF.12.

PVC priority assigned within FR Forwarding Priority to a VC takes precedence over FRF.12 priority, which means that all packets destined for the same PVC queue on the same interface queue, regardless of whether or not they were fragmented.

This method ensures that time or delay-sensitive traffic, such as voice, has absolute priority over signalling traffic, and that signaling traffic has absolute priority over data traffic, provided different PVCs are used for the different types of traffic.

To configure FRF.12 with FR Forwarding Priority:

1 To complete the configuration steps for FRF.12., see"Configuring FRF.12" on page 94.

2 To configure the FRF.12 VC, follow the procedures in "Frame Relay Forwarding Priority to a VC (virtual circuit)" on page 98.

Frame Relay monitoring

Statistics are collected on both a per-link and a per-PVC basis, and are displayed through MIBs, CLI, and the Admin > Healthcheck screen. Statistics are divided into two categories: generic statistics and frame-relay specific statistics. The generic statistics apply to any data link and are reported through the MIB-II ifTable (RFC 2233). All of the statistics are reported, even if they are not collected. Any statistic that is not collected is reported as zero.

Frame Relay OM statistics

All of the Frame Relay related statistics are displayed through the Admin > Healthcheck screen and through the CLI. Statistics not collected are reported as zero. Statistics are initialized to 0 when an object is enabled.

These statistics support the CLI show interface serial command.

IP statistics

The current per-WAN interface statistics are collected on a per-PVC basis. They are not collected on a per-Frame Relay interface basis.

Chapter 7
Configuring dial services and Demand Services

Support for asynchronous serial interfaces over the serial port and V.90 internal modem provides support for dial backup scenarios. With the serial port, this is achieved using an external modem. The modem can be used as a backup service for a leased-line connection between the remote and central offices or between two branch offices. If the primary connectivity goes down, a circuit-switched connection is established and traffic is rerouted. When the primary link is restored, traffic is redirected to the leased line, and the modem call is released.

In addition to backup services applications, these interfaces are also used to dial into the gateway to manage it using the browser-based management interface windows. The serial ports allow you to run the serial menu through a direct cable connection.

Dial interfaces

The following procedure pertains to the configuration of the Contivity gateway's serial (COM) port as a dial interface. The V.90 configuration has not been included separately. However, the configuration of V.90 interface is similar to the configuration of the Serial Port except in the following:

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

Note: To use a dial interface as the backup interface in Demand Services, configure the PPP Authentication protocol under the Dial Interfaces PPP configuration. Configure the user-name and password parameters under the Demand Services configuration.

To configure dial interfaces:

1. Select System > Dial Interfaces on the Contivity Secure IP Services Gateway menu. The Dial Interface window appears. (For information about specific fields or parameters in the windows, refer to the online help.)
2. Use the Select radio button to select a specific interface to configure. You can then configure the interface or view statistics about it.
3. Click Configure. The Interface Configuration window appears. The fields in the Interface Configuration window are different, depending on the Port Mode setting. You use the Interface Configuration window to configure the dial interface settings for the currently selected interface.
4. The port mode setting, either Serial Menu, PPP, Auto Detect, or AOT, is shown as it is currently set on the Switch Settings window. If the port mode is PPP, the window changes to allow you to configure PPP specific parameters.
5. Click Modify System Settings to access the System > Switch Settings window to change the port mode. You can select PPP to support modem communications, Serial Menu to support a direct connection through the gateway serial port, Auto Detect, or AOT.
6. The Interface Filter Status indicates if the Contivity Interface Filter is enabled and in use or disabled. The filter can be enabled and disabled using the Services > Firewall NAT window.
7. Select the interface filter from the list of available filter options. You can click New Interface Filter to access the Profiles > Filters window if you want to create a new interface filter to apply to this dial interface.
8. Enter a description for the interface.
9. Provide an ID for the circuit.
10. Enter the dial out phone number.
11. Select whether the interface is private or public.
12. Click the Configure PPP button to access the "Configuring PPP" on page 109 to configure IP addresses, if desired.

Configuring the modem

To configure the modem:

1. Select Configure Modem in the Dial Interfaces > Interface Configuration window to access the Configure Modem window. Use this window to set the modem parameters. You can also access the Modem Commands window from the Configure Modem window.

   The fields in the top section of the window provide information about the dial interface being configured, including the slot in which the interface is installed, the interface number, the type of interface, Serial or Com, and the port mode setting.

2. Select the desired baud rate from the list of options available.
3. Select from the list of available options to set the Auto Answer setting.
4. Enter the initialization string that you want to use with the modem. The default is +++ATZ.
5. Enter the termination string that you want to use with the modem. The default is +++ATH.
6. Enter the dial prefix string that you want to use with the modem. The default is +++ATDT.
7. To send commands directly to the modem, click Modem Commands.

   The modem commands window appears when you select the Modem Commands button in the Configure Modem window. This window enables you to send commands and receive responses from the modem.

8. Enter the modem command in this field.
9. Click Apply.
10. The modem response section shows the modem's reply to commands entered.

Configuring PPP

The fields in the top section of the window provide information about the dial interface being configured, including the slot in which the interface is installed, the interface number, the type of interface, Serial or Com, and the port mode setting.

To configure PPP:

1. Enter a text description for the connection in the Description field.
2. The default IP local and remote address settings are set to Accept Negotiated Address. You can change the local and/or the remote IP addresses to specific values by selecting Specify IP Address.
3. If you select Specify IP Address, enter the IP address and the subnet mask you want to apply to the local end of the connection.
4. Click Authentication Settings to go to the Authentication Settings window in order to configure the authentication parameters for the interface. See the online help for information about specific fields in the PPP Authentication Settings window.

Note: The authentication client and server settings apply to the PPP connection only. The authentication client information is designed to be used by the Contivity gateway when dialing and logging into a Dial-In Server. The authentication server settings on a Contivity gateway are only used when some one dials into that Contivity gateway (the Contivity gateway is acting as the dial-in server). To prevent anyone from dialing into a Contivity gateway and getting access to the network, incoming authentication is always enabled and the default user name and password are the same as what is stored in memory. The default user name and password can be overridden through the Authentication Server username and password fields. Authentication Server is less often used for dial-out calls. You can use it to effect bi-directional authentication.

5. Click Advanced Settings to access the Advanced Settings window, which provides additional, advanced parameters for PPP. See the online help for information about specific fields in the PPP Advanced Settings window.

Configuring ISDN BRI

The fields in the top section of the window provide information about the dial interface being configured, including the slot in which the interface is installed, the interface number, the type of interface, Serial or Com, and the port mode setting.

To configure ISDN BRI:

1. Enter a text description for the connection in the Description field.
2. Provide an ID for the circuit.
3. Select the interface filter from the list of available filter options. You can click New Interface Filter to access the Profiles > Filters window if you want to create a new interface filter to apply to this dial interface.
4. Enter the ISDN dial out phone number.
5. Select whether the interface is private or public.
6. To configure the PPP settings for the connection, click Configure PPP. The Configure PPP window appears. See "Configuring PPP" on page 109 for more information.
7. Click Configure ISDN BRI to configure ISDN device parameters. The BRI Configuration window appears.
8. Select the Country Code for which country or continent this Contivity gateway will operate in. When you select this command, the gateway automatically loads country-specific information. Each country or continent has a set of valid ISDN switch types.

Note: Not all ISDN parameters are valid for all countries.

9 Use this option to enable and disable the automatic switch detection option for ISDN BRI. This command applies to type NI-2 ISDN switches only (North America only).

- Auto - Specifies that the ISDN switch type will be automatically detected.
- Disable - Disables automatic ISDN switch type detection.
- On-reset - Specifies that the ISDN switch type will be automatically detected after the gateway is reset.

10 Select the switch type based on your location.

Location	Switch types
Europe	ETSI
Hong Kong	HKT
Japan	KDD
	NTT
Korea	KOR
North America	Lucent 5E10
	DMS-100
	NI-2

11 Enable the DOVBS option to implement data over voice bearer services (DOVBS). An adaptation rate of 56 Kb/s is typically used to send digital data over a call line that is used for voice communication.

Note: This command does not apply to all countries and all switch types. Check with your local ISDN provider.

12 Use the Auto SPID Detect option to enable automatic detection of the service profile ID (SPID) for ISDN BRI. This command applies only to NI-2 ISDN switches (North America only). Automatic detection of the SPID is set to disabled by default.

13 Enter Local Phone Numbers 1 and 2 for SPID 1 and 2.

14 Set the SPID 1 and SPID 2 options to set the service profile IDs (SPID) for registration of the B channel with the service provider's ISDN switch. If you

do not have an SPID number (used mostly in North America), select **none** as the SPID number.

15 Set the Manual TEI option to specify that the terminal end-point identifier (TEI) will be entered manually. Some switches do not support automatic TEI. The TEI number is obtained from the local ISDN provider.

16 Use the Dial Out MultiLink option to enable multilink for outgoing calls. If enabled, outgoing calls are a bundling of two B-channels into a 128 Kbps pipe to provide higher bandwidth on an as needed basis.

17 Use the Dial In MultiLink option to enable multilink for an incoming call. If enabled, incoming call will be negotiated for multilink, if the other side is capable of doing multilink. If it is not capable, the call will fall back to plain PPP, and the incoming call will be negotiated for no multilink.

18 Enable Auto Answer to enable automatic answering of incoming calls. Select Disable to disable the automatic answering of incoming calls. The default is disabled.

19 Click OK to save the ISDN device settings and return to the System > Dial Interfaces > Interface Configuration window.

20 Click Connect to make the defined ISDN connection.

Demand Services

Demand Services brings up a backup interface based on one of the following triggers: traffic, interface group, hour, unreachable route, or ping. Demand Services has two sets of functionality: backup interfaces, formerly known as BIS, and Dial on Demand (DoD). Backup interfaces provide an automated mechanism to enable a backup interface when a designated primary connection fails. DoD activates the dial interface when traffic needs to be routed over a dial interface route, and then deactivates the dial interface when there is no traffic to be routed.

The dial interfaces, including the V.90 modem, serial port, or ISDN connection, can be used for backup services.

Note: Only nailed up circuits are supported as primary circuits. However, secondary (or backup) circuits can include demand circuits.

Trigger modes

You configure Demand Services so that a backup interface assumes the role of the primary connection when one of the following triggers occurs:

- Interface group failure
- Route unreachability
- Ping failure
- Hour

You configure Demand Services to activate an interface when the following trigger occurs:

- Traffic

Note: Both backup interfaces and DoD interfaces are configured in the same demand windows. Backup interfaces and DoD interfaces work in the background, depending on the trigger that causes an event to occur.

Each demand interface is assigned a priority by the user. This priority is used when a contention for the dial interface is encountered. A demand interface can be:

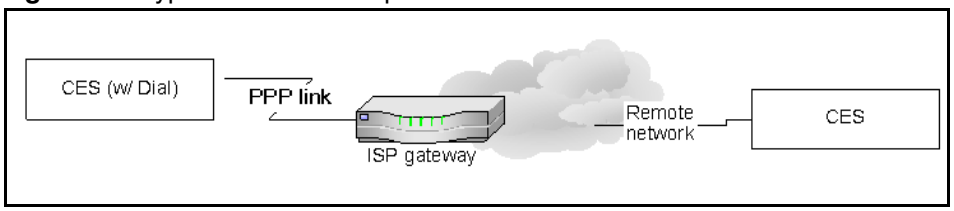
- Idle—trigger event has not occurred
- Active—trigger event has occurred
- Connecting—connection attempts are in progress
- Connected—connection completed, traffic flowing

Note: Many demand interfaces can be activated at any time, but only the one with the highest priority will be connecting or connected. The demand interface with the lowest number has the highest priority.

Demand Services runs on all CES platforms capable of running software release 6.0. Demand Services is a basic feature and does not require a key.

Figure 38 on page 115 shows a typical demand setup.

Figure 38 Typical demand setup



Dialing functionality

A maximum of three numbers is allowed for dialing out the dial interface. You configure the number of times each number is retried before dialing the next number. The delay between each redial is also a configurable parameter.

Backup Interfaces

Demand Services provides an automated mechanism to enable a backup interface when a designated primary connection fails. The types of primary connections are: interface group, specific route, and connection to a specific destination.

When the primary connection goes down, Demand Services enables the backup interface using parameters configured in the demand profile. The demand profile specifies the primary connection to be backed up, the backup interface, and other failover parameters.

You can configure any Contivity interface as a backup interface, not only dial or ISDN interfaces. For example, you can designate any of the following interfaces as a backup interface for a primary T1 circuit on your gateway:

- ISDN interface
- Ethernet interface attached to a DSL modem
- Dial interface (V.90 modem)

The interface selected as the backup interface must already be installed and configured before it is used in a backup interface configuration.

Note: The ping default route feature pings an address to ensure that the route is valid before that route is added to the routing table. If you turn the ping default route feature on, you can use it to validate a backup route. See Configuring Routing for the Contivity Secure IP Services Gateway for more information on the ping default route feature.

Configuring subinterfaces as backup interfaces

The following Contivity subinterfaces and virtual circuits (VCs) cannot be configured as backup interfaces:

- 802.1Q VLAN subinterfaces
- Interfaces with virtual circuits (Frame Relay and ADSL/ATM)

Configuring an ABOT for backup interfaces

When configuring an asynchronous branch office tunnel (ABOT) for use over a primary link and a backup link, you must enable the Aggressive Mode Initial Contact Payload parameter on both the initiator and responder side of the ABOT. This parameter is found under the IPsec parameters on the Profiles > Branch Office > Groups > Configure window.

If you do not enable the Aggressive Mode Initial Contact Payload parameter on both sides of the tunnel, the change from the primary interface to the backup interface (or vice versa) will fail for a period of time equal to the ABOT idle timeout on the responder side. You can work around the issue by lowering the idle timeout value until the outcome is satisfactory. You may need to fine-tune the idle timeout value; if you set the idle timeout too low, it can cause unnecessary tunnel teardowns when there is a break in traffic.

Dial on Demand

DoD is used in situations where users must connect a LAN to the Internet or to a corporate Remote Access Service (RAS), and the only available technology is either a low frequency of occurrence or dial-up. The typical use for DoD is for remote offices that do not have access to a higher speed WAN technology, either because of availability or cost.

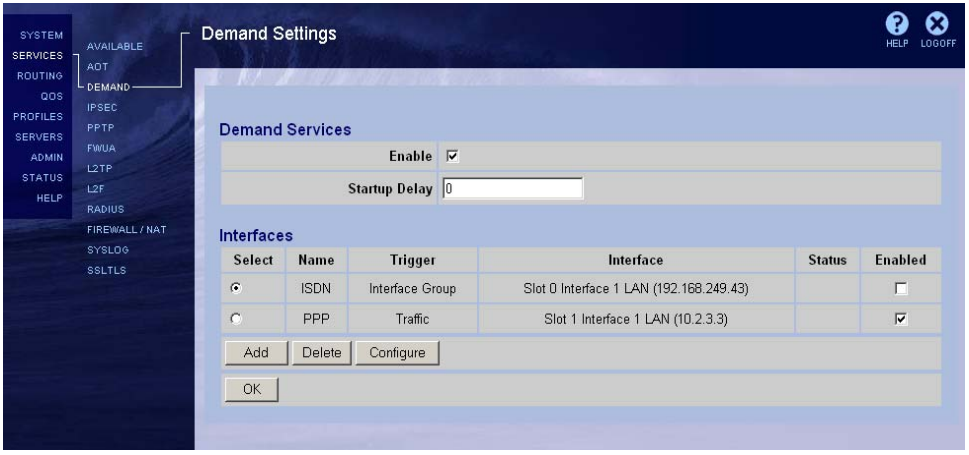
The normal state of a DoD connection is down. DoD activates the dial interface when a private-side device attempts to establish a connection to a network that is accessible through the dial interface route.

Configuring Demand Services

To configure Demand Services:

1 Go to Services > Demand. The Demand Settings window appears. Figure 39 shows the Demand Settings window. (For information about specific fields or options on the windows, refer to the online Help.)

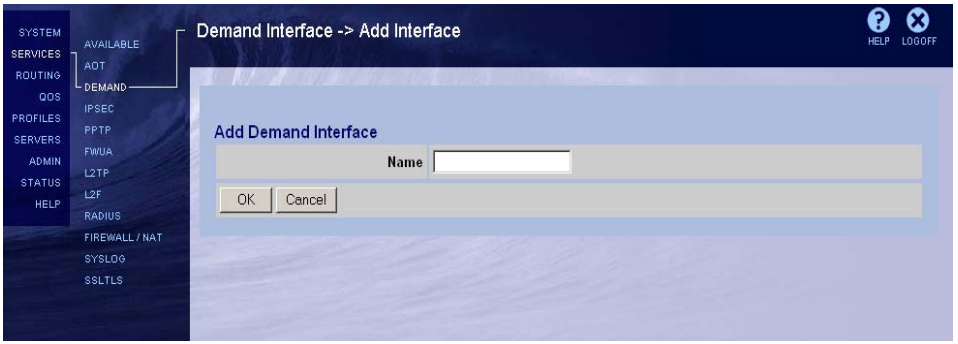
Figure 39 Demand Settings window



2 Check the Enable box in the top section of the window to globally enable Demand Services on the Contivity Secure IP Services Gateway.

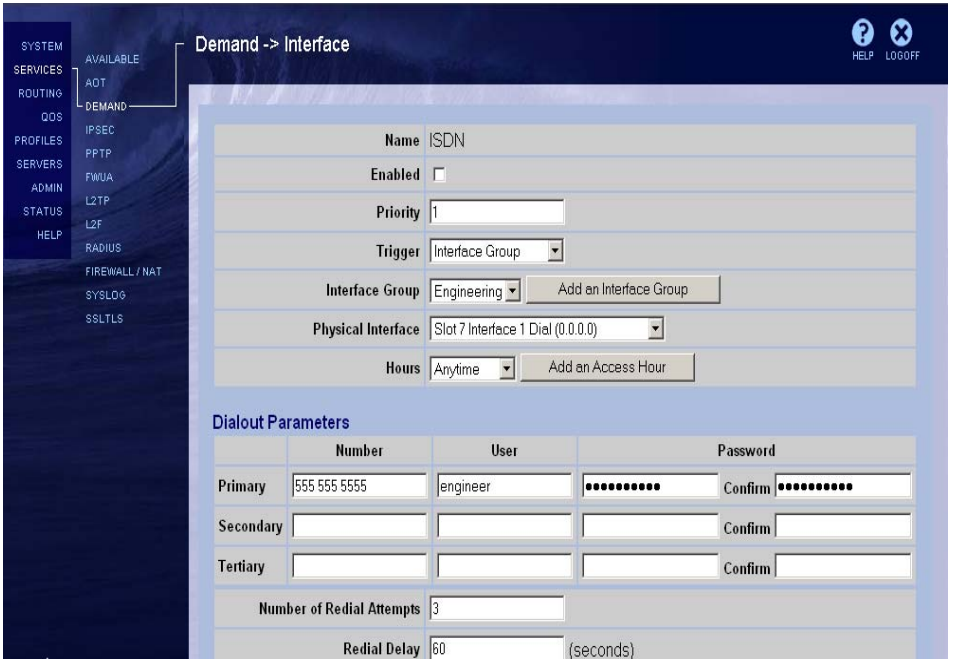
3 Click the Add button in the Interfaces section of the window to add a backup interface. The Demand Interface > Add Interface window appears. Figure 40 shows the Add Interface window.

Figure 40 Demand Interface > Add Interface window



4 Enter a descriptive name for the Demand Interface profile configuration and click OK. The Demand > Interface window appears. Figure 41 shows the Demand > Interface window, which is used to configure the Demand profile that you created on the Add Interface window.

Figure 41 Demand > Interface window



5 Check the Enabled box to enable this specific Demand profile.

6 Assign a priority for the interface in the Priority box.

7 Select a trigger option for this Demand profile from the list. The trigger options are Traffic, Interface Group, Hour, Route Unreachable, and Ping.

After you select the trigger, the window is refreshed to include parameters that must be configured for that specific type of trigger. See the following sections for information about configuring each trigger type.

Configuring Demand Services with an interface group trigger

In the context of Demand Services, an interface group can consist of branch office tunnels, physical interfaces, or a combination of tunnels and interfaces. When you configure an interface group as the trigger, Demand Services assumes the backup role when all components of the interface group are down.

Note: To back up a single physical interface, you can configure an interface group that contains only that single physical interface. A physical failure—for example, on a WAN interface, the loss of synchronization clocking— triggers Demand Services.

When you configure an interface group as a trigger, include business-critical tunnels in the group (for example, a tunnel to corporate headquarters). You can include non-business-critical tunnels in an interface group, especially if the backup interface is a dial or ISDN interface.

When you configure Demand Services to activate the backup interface upon failure of an interface group, you can include tunnels and physical interfaces in the interface group.

The time that it takes to detect a failure depends on these factors:

- Tunnels: The Contivity gateway detects the loss of IPsec keepalives on the tunnels included in an interface group. By default, IPsec keepalive messages are sent every 15 minutes, so 15 minutes could elapse before the backup interface is triggered. You can reduce the IPsec keepalive interval; however, more frequent keepalive messages can burden the central site Contivity gateway.
- Physical interfaces: The Contivity gateway checks the status of a physical interface included in an interface group every 30 seconds. If a physical interface fails immediately after this check, 30 seconds will elapse before the Contivity gateway discovers the failure and activates the backup interface.

To configure an Interface Group as the trigger:

When you select Interface Group as the trigger, the Interface Group trigger parameters display in the top section of the window (see Figure 41 on page 118).

1. Enable the interface.
2. Assign a priority for the interface in the Priority box.
3. Select the interface group to be backed up from the Interface Group menu.

   To create a new interface group to add to the list, click Add an Interface Group to display the Routing > Interface Group window, where you create a new interface group.

4. Select the backup interface for this Demand profile from the Physical Interface menu.

   Demand interfaces are assigned a priority level, allowing the system to create multiple definitions for a single physical interface.

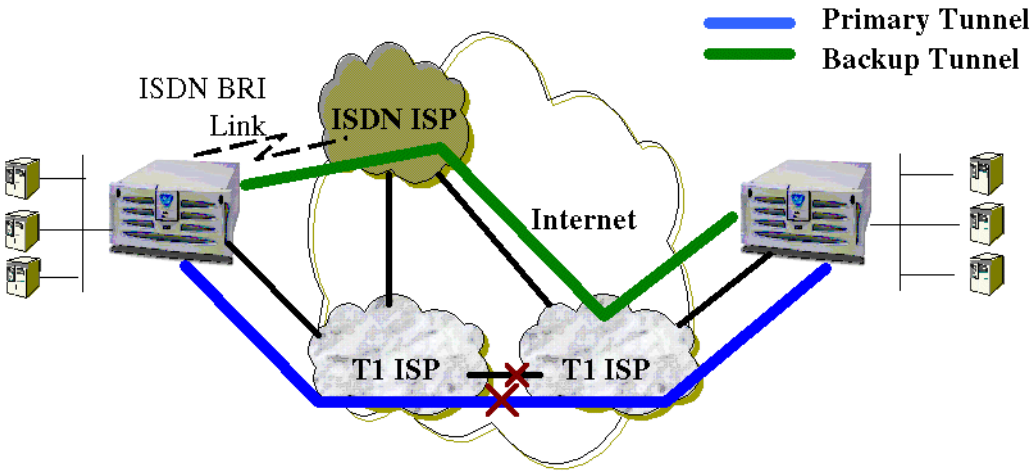
5. You can configure the Demand profile to activate only during certain days and hours by selecting a time specification from the Hours list. To create a new time specification, click the Add an Access Hour button.
6. Configure the dialout parameters for the backup interface. To configure dialout parameters, see “Configuring Demand dialout parameters” on page 127.
7. Click OK or Apply.

Configuring Demand Services with an hour trigger

You can configure Demand Services to become active at a specific time of day or on specific days of the week. (To configure a time specification, execute the **`access-hours`** command in Global Configuration mode or go to the Profiles > Hours window.)

Figure 42 on page 121 illustrates a Demand Services configuration with an hour trigger.

Figure 42 Demand Services configured with an hour trigger



You can also use a time-of-day specification in conjunction with one of the other trigger types: ping, interface group, traffic, or route unreachable. For example, you can configure Demand Services to activate when a specific interface group fails, but only during the hours 8:00 through 17:00 Monday through Friday.

To configure Demand Services with an hour trigger:

When you select Hour as the trigger, the Hour trigger parameters display in the top section of the window.

1. Enable the interface.
2. Assign a priority for the interface.

3 Select the backup interface for this Demand profile from the Physical Interface menu.

4 From the Hours list, select a time specification to activate this Demand profile. To create a new time specification, click the Add an Access Hour button.

If a Demand backup connection is established when the endpoint specified in the time specification arrives, the connection is torn down.

5 Configure the dialout parameters for the backup interface. To configure dialout parameters, see "Configuring Demand dialout parameters" on page 127.

6 Click OK or Apply.

Configuring Demand Services with a route unreachable trigger

You can configure Demand Services to become active when a specific route times out in the routing table. (To configure a route, execute the **`network`** command in Global Configuration mode or go to the Profiles > Networks window.)

This type of trigger is useful only if your IP network uses RIP or OSPF and if alternative routes exist between endpoints. If you have not configured redundant routing paths into your network, route timeout and, therefore, Demand activation, can take several minutes to failover as the Contivity gateway waits for the routing protocol to determine that the route no longer exists.

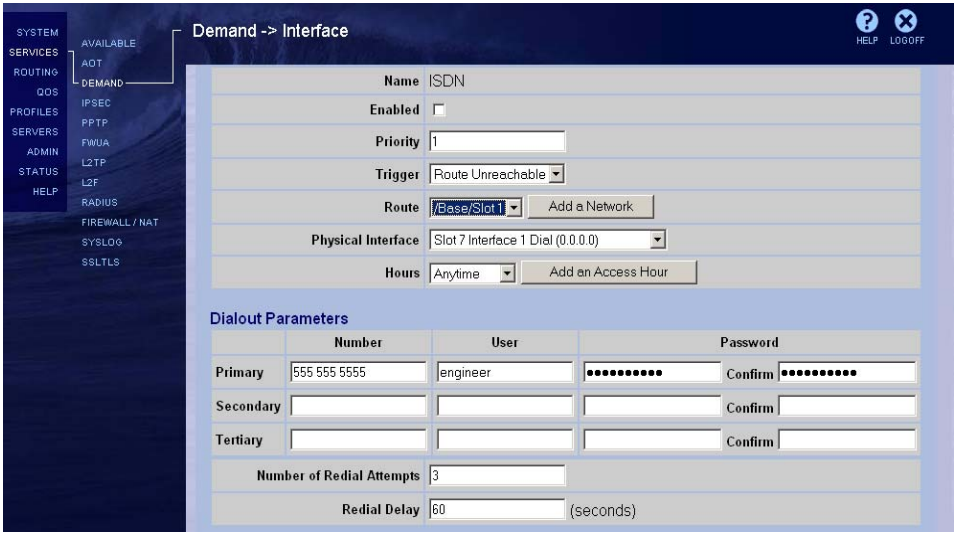
For example, if you have a direct route and one or more multiple-hop routes to your corporate headquarters, and the direct route fails, RIP or OSPF steers the traffic through a multi-hop path. If the connection is completely lost, the route times out in the routing table and triggers Demand Services. Several minutes could elapse, however, before Demand Services is triggered.

For this type of trigger to work properly, the primary and backup tunnels must use similar routing protocols, and the primary tunnel must be configured with the lower-cost routes.

To configure Demand Services with a Route Unreachable trigger:

When you select Route Unreachable as the trigger, the route unreachable parameters display in the top section of the window. Figure 43 on page 123 shows the Demand > Interface window with Route Unreachable as the trigger.

Figure 43 Demand > Interface window with Route Unreachable as the trigger



1. Enable the interface.
2. Assign a priority for the interface.
3. From the Route list, select the network route connection to monitor. Use the Add a Network button to define a network route and add it to the list.
4. Select the backup interface for this Demand profile from the Physical Interface menu.
5. To configure the Demand profile to activate only during certain days and hours, select a time specification from the Hours list. To create a new time specification, click the Add an Access Hour button.
6. Configure the dialout parameters for the backup interface. To configure dialout parameters, see "Configuring Demand dialout parameters" on page 127.
7. Click OK or Apply.

Configuring Demand Services with a ping trigger

You can configure Demand Services to trigger by the failure of a ping to a specified destination. The main application for the ping trigger is DSL with attached Ethernet DSL modem. The Contivity gateway pings the device on the other end of the local loop, for example, a DSLAM. In this way, the Contivity gateway determines whether there is a local loop failure or a failed connection to the Internet service provider (ISP).

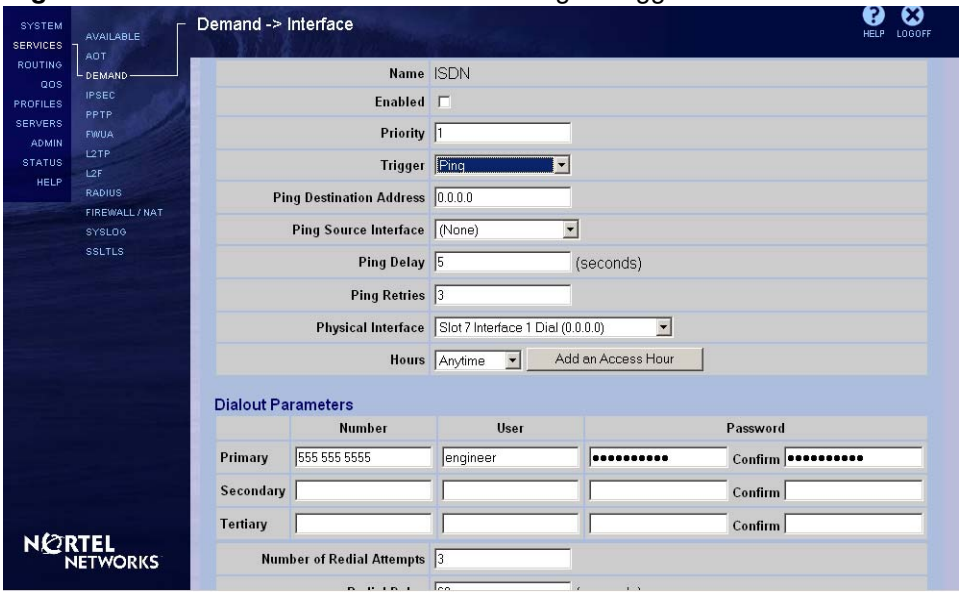
Note: In order for the **test** button on a ping trigger demand interface to have a successful test, the ping destination must be unreachable during the test. You can accomplish this by using a temporary fake ping destination address while performing the test.

If you use this type of trigger with a Branch Office, you must configure at least one static route in the Demand profile so that the Contivity gateway can reach the tunnel end point through the backup interface.

To configure Demand Services with Ping as the trigger:

When you select Ping as the trigger, the ping trigger parameters displays in the top section of the window. Figure 44 on page 125 shows the Demand Interface window with Ping selected as the trigger.

Figure 44 Demand Interface window with Ping as trigger



1 Enable the interface.

2 Assign a priority for the interface.

3 In the Ping Destination Address field, enter the IP address that you want to regularly ping. This connection is the entity that is backed up.

4 From the Ping Source Interface list, enter the interface on this Contivity gateway that is the source of the ping.

5 In the Ping Delay field, enter the maximum number of seconds that the Contivity gateway waits to receive an ICMP reply before it assumes that the connection has failed and triggers the backup interface. Enter an integer from 1 through 900. The default value is 5.

6 In the Ping Retries field, enter the maximum number of ping retries allowed before the Contivity gateway assumes that the connection has failed and triggers the backup interface. Enter an integer from 1 through 6. The default value is 3.

7 Select the backup interface for this Demand profile from the Physical Interface menu.

8 You can configure the Demand profile to activate only during certain days and hours by selecting a time specification from the Hours list. To create a new time specification, click the Add an Access Hour button.

9 Configure the dialout parameters for the backup interface. To configure dialout parameters, see "Configuring Demand dialout parameters" on page 127.

10 Click OK or Apply.

Configuring Demand Services with a Traffic trigger

The dial session is policed by an inactivity timer to prevent uptime when there is no traffic. Sometimes the line is billed per minute of operation, so do not keep it up unnecessarily.

The inactivity threshold timer has a default of 120 seconds. The timer starts when no traffic has arrived for one second. On expiration of the timer, any tunnel configured over the dial interface is brought down, cleared of state information, and the session is terminated.

Each Demand interface remembers its status independent of other Demand interfaces. If a Demand interface deactivates and other Demand trigger events occur, the Demand interface with the next highest priority becomes active.

To configure Demand Services with Traffic as the trigger:

When you select Traffic as the trigger, the Traffic parameters displays in the top section of the window. Use this option when you want only a line to activate when there is traffic.

1 Enable the interface.

2 Assign a priority for the interface.

3 Select the backup interface for this Demand profile from the Physical Interface menu.

4 In the Idle Timeout box, define how long the line is idle before being brought down.

The range is 30 to 3600 seconds, with a default of 120.

5 To configure the Demand profile to activate only during certain days and hours, select a time specification from the Hours list. To create a new time specification, click the Add an Access Hour button.

6 Configure the dialout parameters for the backup interface. To configure dialout parameters, see "Configuring Demand dialout parameters.

7 Click OK or Apply.

Configuring Demand dialout parameters

To configure dialout parameters:

1 In the Dialout Parameters section, type the primary number in the Primary box.

2 In the Secondary box, type the secondary number.

3 In the Tertiary box, type the tertiary number.

4 In the User box, type the assigned username.

5 There are three separate usernames and passwords assigned to each of the three phone numbers, allowing for dial to different accounts. In the Password box, type the assigned password.

6 In the Confirm box, retype the password.

7 In the Number of Redial Attempts box, type the number of times to try before moving to the next number.

Select between 1 and 10, with a default of 3.

If the number of redial attempts is set to three, the system dials the primary number three times before moving to the secondary number. The system then dials the secondary number three times and if the secondary number fails, it dials the tertiary number three times.

8 In the Redial Delay box, type the number of seconds to wait between retries.

Select between 1 and 500, with a default of 60.

Configuring a remote network

You configure the IP address, mask, cost, and enabled or disabled state of a remote network in the remote network page.

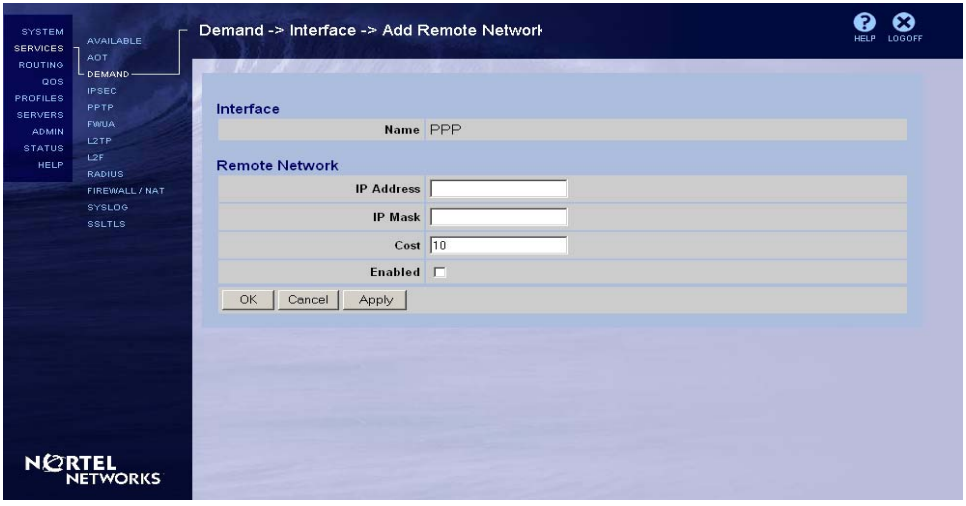
Note: You can define an infinite number of static routes. To define a default route, simply define a remote network of 0.0.0.0.

To configure a remote network:

1 To add a Remote Network, click Add under the Remote Networks section of the Demand > Interface window. The Demand > Interface > Add Remote Network window opens.

Figure 45 shows the Add Remote Network window.

Figure 45 Demand remote network



2 Type the IP address in the IP Address box.

3 Type the IP mask in the IP Mask box.

4 Type the cost in the Cost box.

Note: Cost is configured like any other static route. To configure a Demand interface, set the cost appropriately to ensure that the connected Demand route has a lower cost than the primary routes. The default is 10.

5 Click the Enable box to enable the Remote Network.

6 Click OK.

7 To configure the remote network, select the remote network you want to configure and click Configure.

8 The Edit Remote Network window opens. Repeat Steps 2 to 6 in this procedure.

System log messages

The system generates eventlog for the following situations:

- The Demand line connects—identifies what brought up the line.
- The Demand line disconnects—indicates the reason for the disconnect:
  - inactivity
  - line error
  - line drop
- Other miscellaneous messages regarding Demand status.

Healthcheck

Table 13 describes the healthcheck status of each Demand interface.

Table 13 Healthcheck status

Demand status	Description	Healthcheck status
Idle Active Connecting Connected	Normal Demand interface status	OK/green
Not configured/disabled	Demand interface cannot activate	Disabled/yellow
Error	Internal error	Error/red

Note: In the case of more than one Demand line, the healthcheck status is an accumulation of the individual statuses: green if all are green; red if one is red; yellow for all other combinations.

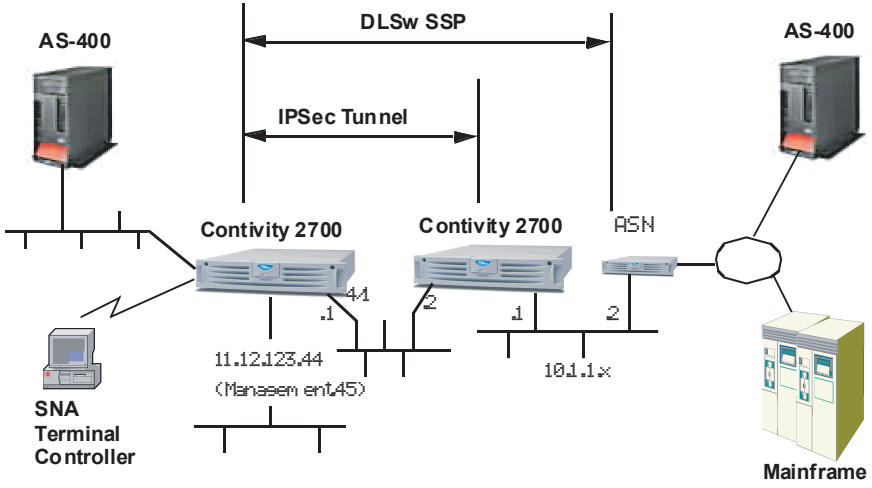
Chapter 8
Contivity DLSw

DLSw (Data Link Switching) provides support for IBM* SNA protocol networking in IP networks. This includes IP encapsulation and session-oriented IP networking and support for SDLC and LLC2 interfaces for integration of native SNA traffic. It provides the ability to deploy Contivity gateways to support future application migration from SNA to IP in a secure IP environment.

DLSw is a forwarding mechanism for the IBM SNA and IBM NetBIOS protocols. It does not provide full routing, but instead provides switching at the Data Link layer and encapsulation in TCP/IP for transport over the Internet.

Because SNA and NetBios are basically connection-oriented protocols, the Data Link Control procedure that can be used on the LAN is IEEE 802.2 Logical Link Control (LLC) Type 2. Data link switching also accommodates SNA protocols over WAN links via the SDLC protocol, as shown in Figure 46.

Figure 46 Contivity DLSw configuration



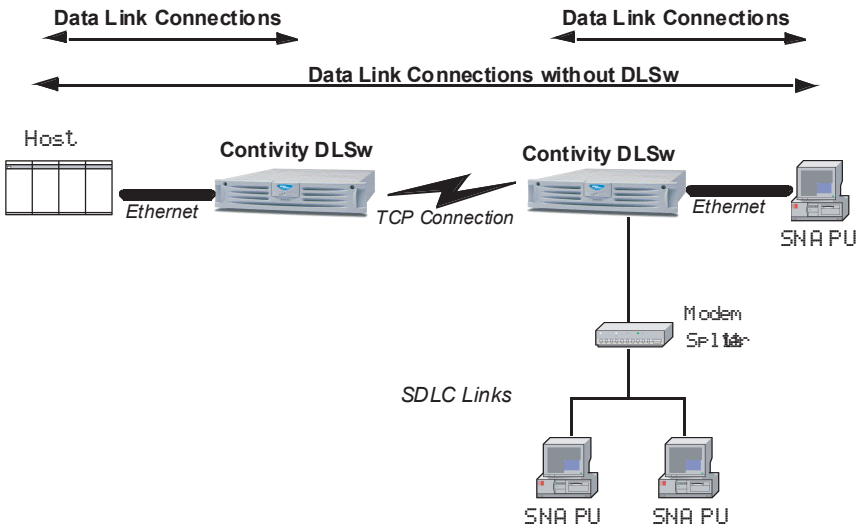
Data Link Switching supports:

- SNA {Physical Unit (PU) Type 2, PU 2.1, PU 4 and PU 5} systems attached to Ethernet (DIX) V2 or IEEE 802.3/802.2 compliant Local Area Networks
- SNA (PU 1 and PU 2, PU 2.1 (primary or secondary) and PU 4) systems attached to IBM Synchronous Data Link Control (SDLC) links. The SDLC attached systems are provided with a LAN appearance within the Data Link Switch (each SDLC PU is presented to the SSP (Switch to Switch Protocol) protocol as a unique MAC/SAP address pair).
- Contivity DLSw supports all PUs transparently

The major difference between data link switching and bridging is that DLS terminates the data link control and bridging does not. In traditional bridging, the data link control is end-to-end. Data link switching terminates the LLC Type 2 connection at the switch. This means that the LLC Type 2 connections do not cross the wide area network.

Figure 47 shows data link connections without DLSw.

Figure 47 Data Link Connections without DLSw

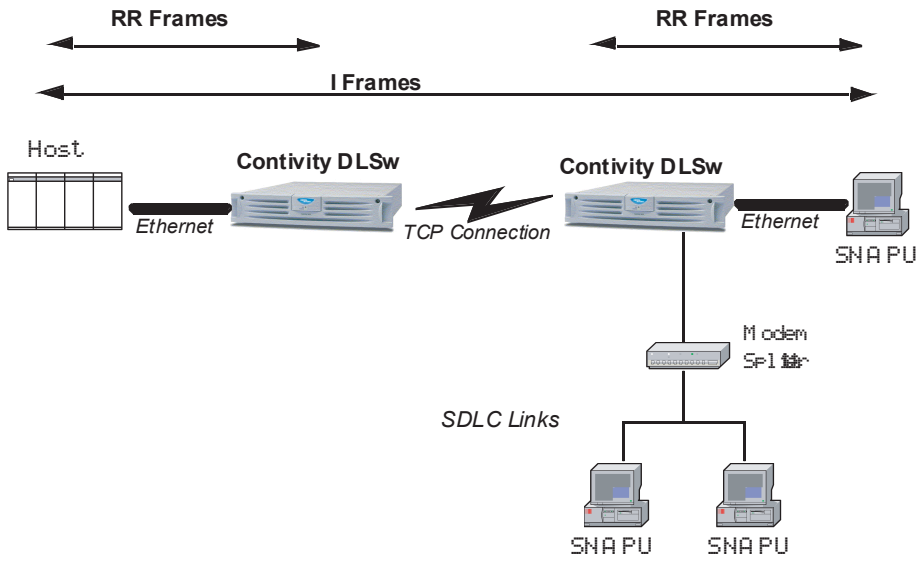


The DLS multiplexes LLC connections onto a TCP connection to another DLS. The LLC connections at each end are independent from each other. It is the responsibility of the data link switch to deliver frames that it has received from an LLC connection to the other end. As a result of this design, LLC time-outs are

limited to the local LAN (i.e., they do not traverse the wide area). Also, the LLC Type 2 acknowledgments (RR's) do not traverse the WAN, reducing traffic across the wide area links. For SDLC links, polling and poll response occur locally, not over the WAN.

Figure 48 shows the data link with DLSw.

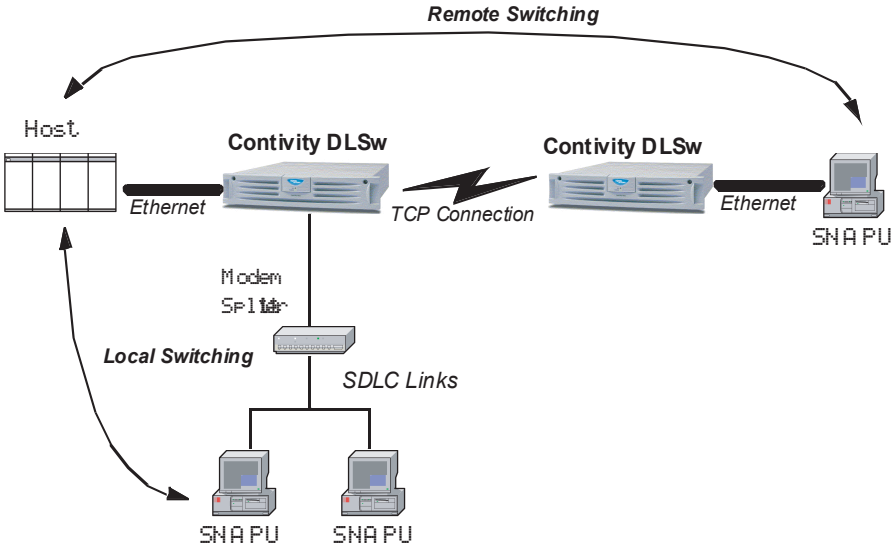
Figure 48 Data Link with DLSw



Data Link Switches can be in used in pairs or by themselves. A Single DLS internally switches one data link to another without using TCP (local switching case). A paired DLS multiplexes data links over a reliable transport using a Switch-to-Switch Protocol (SSP) (in the remote switching case). A number of RFCs document the frame formats and protocols for this multiplexing between Data Link Switches.

Figure 49 on page 134 shows local and remote switching.

Figure 49 Local and Remote Switching



Before Data Link Switching can occur between two routers, they must establish a TCP connection between them. Once this connection is established, the DLS employs SSP to establish an end-to-end circuit over the transport connection. Each DLS maintains a list of DLS-capable routers and their status (active/inactive).

Contivity DLSw fully supports RFC 1434 and RFC 1795. RFC 2166 is partially supported. Contivity DLSw does not support UDP services as defined in RFC 2166. It supports TCP services only.

When initiating a connection, Contivity DLSW first tries to connect using RFC 2166. If this fails, Contivity DLSW then tries connecting according to RFC 1795. If this also fails, it connects as RFC 1434.

Supported functionality

Listed below are functions specifically supported by the Contivity DLSw implementation:

- Contivity DLSw is configured through use of the CLI. The initial release does not support configuration through the GUI.
- Feature licensable using a license key
- Local Peer configurable on private/Circuitless IP (CLIP) addresses
- Full back-level inter operability with RFC1434
- Full support for DLSw Standard Version 1 (RFC 1795)
- Full support for TCP only portion of DLSw Standard Version 2 (RFC 2166)
- Preferred Peer support via an assigned cost.
- Unconfigured peers that allows Contivity device to accept DLSw peering where the remote peer is not pre-configured.
- Global command to enable/disable DLSw without loss of the DLSw configuration.
- Local and Remote switching for both Ethernet LANs for SNA traffic and SDLC stations
- SDLC and LLC2 support on private interfaces
- Marking of the Contivity-generated DLSw IP packets with a fixed DSCP value equal to AF21.
- Clear Circuit: A circuit is a single end-to-end SNA connection carried across the DLSw switch. This functionality provides the ability to delete a specific circuit or group of circuits. A cleared circuit may or may not automatically re-establish.

Contivity DLSw does not support the following functionality:

- DLSw MIBs are not supported.
- NetBios traffic is not supported.
- UDP and IP Multicast are not supported between DLSw peers.

Ethernet LLC2 functionality

Ethernet LLC2 functionality supports:

- Support for SNA LLC2 traffic on all Private Ethernet interfaces
- Support for Type I and II LLC communications
- Support for simultaneous SNA and non-SNA traffic
- Ethernet MAC including auto-sensing of 802.3/DIX2 Ethernet formats by Link Station
- Provision of IBM's Dynamic Window Algorithm for controlled restart of I-frame traffic after LAN congestion

Ethernet LLC2: MAC address translation:

- Provides the optional ability to translate the LLC2 MAC Addresses for traffic transiting the Contivity LLC2 interfaces
- This ability addresses the occasional need to change the Mainframe or Data Center without requiring the re-configuring of the Host MACs across many branches' Ethernet LANs.

SDLC functionality

SDLC provides support for:

- Synchronous serial SNA SDLC protocol traffic on serial interfaces
- Primary, secondary and negotiable link station roles
- Primary and secondary multi-drop configurations
- Leased lines (no support for switched lines)
- Full-duplex and half-duplex modes
- Normal (modulo 8) and extended (modulo 128) sequence numbering
- Configurable special polling using SNRM, DISC, TEST, XID messages (XID is sent by the primary station and Contivity DLSw uses it to poll the secondary)

Single port V.35/X.21 serial card functionality

Single port V.35/X.21 serial card provides support for:

- V.28 (EIA-232c compatible with RS-232) as well as V.35, X.21 interfaces
- DCE (internal clock) mode on the single port V.35/X.21 to give clock to locally connected SDLC devices
- NRZI/NRZ line encoding on the Single Port V.35/X serial card
- Flag streaming between frames while not idle on the single port V.35/X.21 serial card for communication with AS/400

Configuring DLSw

To configure DLSw:

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

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

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

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

4. Enable DLSw globally using the DLSw CLI license command and your specific license key.

   ```
   CES(config)#license install dlsw <license-key>
   ```

5 Start DLSw local peer on the CLIP/private interface.

```
CES(config)#dlsw local-peer 11.12.123.45
```

6 Ping the remote peer using the source address of the local peer to determine that it is reachable:

```
CES#ping 10.10.20.1 11.12.123.45
PING 10.10.20.1: 36 data bytes
64 bytes from 10.10.20.1: icmp_seq=0. time=<16 ms
64 bytes from 10.10.20.1: icmp_seq=1. time=<16 ms
64 bytes from 10.10.20.1: icmp_seq=2. time=<16 ms
64 bytes from 10.10.20.1: icmp_seq=3. time=<16 ms ----10.10.20.1
PING Statistics---- 4 packets transmitted, 4 packets received,
0% packet loss round-trip (ms) min/avg/max = <16/<16/<16
```

7 Connect to the remote peer.

```
CES(config)#dlsw remote-peer 10.10.20.1
```

8 Create and enable LLC2 port. Enter interface configuration mode on the private interface (slot 0/1 for example).

```
CES(config)#interface fast 0/1
CES(config-if)#llc2 enable
```

9 Create SDLC port. Configure SDLC parameters. In this example, you have an external modem eliminator or equipment that is providing clock.

```
CES(config)#interface serial 3/1
CES(config-if)#clock-type external
CES(config-if)#line-speed 19200
CES(config-if)#encapsulation sdlc
```

To configure the serial interface, you must have a minimum serial board frimware revision level of 7. You can determine the revision level using the CLI command **show interface serial** *x/x* **statistics**. The revision level is shown in the last line of the example below as the **PHY ID rev**.

```
CES#show int ser 3/1 statistics
Date 09/24/2003  Time 21:40:33
WAN Slot 3 Interface 1
        PHY: Up
        Administrative State: Enabled
        Link Protocol: SDLC
   (Various output typically appearing here
   has been deleted for brevity.)
Hardware Information
====================
PHY ID model:   0x4
PHY ID rev:     0x7
```

10 Reboot the Contivity gateway after you set SDLC on the serial interface card. (You do not need to reboot before completing the configuration; however, the link station cannot be enabled or started until the reboot is complete.)

11 After restarting the Contivity gateway, configure the SDLC port role, if required. The default is primary.

```
CES(config-if)#sclc rold {pri|neg|sec}
```

12 Enable the SDLC port.

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

13 Create and configure SDLC link station on the same interface.

```
CES(config-if)#sdlc link-station polladdress 37
CES(config-ls)#(lmac lsap) lmac 00-00-11-11-22-22 lsap 04
CES(config-ls)#(rmac rsap) rmac 40-00-00-00-00-07 rsap 04
CES(config-ls)#enable
CES(config-ls)#start
```

You must set up the local mac/sap and remote mac/sap pairs. Also, you should enable and start the SDLC link station. In this example, the poll frame is the default one, SNRM. The remote peer can be created after you create the llc2 port or sdlc port.

Contivity configuration commands example

The following CLI commands are used to configure Contivity DLSw in the example configuration.

```
dlsw local 11.12.123.45
   dlsw remote 10.10.20.1 rfc1795only
   interface fast 2/1
      llc2 enable
   interface serial 3/1
      clock-type external
      line-speed 64000
      encaps sdlc
      sdlc role primary
      sdlc link poll 37
         lmac 00-00-11-11-22-22 lsap 04
         rmac 40-00-00-00-00-07 rsap 04
         proxy 01712345
         enable
         start
```

DLSw local peer configuration

To configure a DLSw local peer, use the following basic steps and related commands. Many of these steps are optional; the default values are typically sufficient for proper operation.

1. Create a DLSw local peer on a specific private/CLIP address. This DLSw local peer listens for and accepts incoming connections. Contivity DLSw currently supports one (1) local peer.
2. Enable or disable MAC address translation. The default value is disabled.
3. Configure MAC cache limit. Default value is 0.
4. Enable/disable backlevel flow control. Default value is disabled. It is recommended that this be enabled for RFC 1434 type peers.
5. Enable/disable the local peer. The IP address used by local peer can be changed only if local peer is administratively disabled.
6. Enable/disable un-configured peer support. The default value is disabled.

DLSw remote peer configuration

To configure DLSw remote peer, use the following basic steps and related commands. Many of these steps are optional; the default values are typically sufficient for proper operation.

1. Create the DLSw remote peer with a reachable IP address.
2. Configure the receive initial pacing parameter. This parameter is used when two peers negotiate connection capability. Default value is 1.

Note: These steps are optional. Nortel recommends that the defaults be used for the llc2 timers, counters, lan-type and window parameters unless changes are required to resolve specific issues.

3. Configure circuit inactivity timeout. For RFC2166 peers you can set the time after which a connection without circuits is moved to a standby state. Default value is 0.
4. Configure the remote peer cost. Peer cost is used in preferred peer feature (all peers with the same cost are broadcast on the same time). Default value is 5 (minimum).
5. Enable/disable the remote peer.
6. Create the DLSw remote peer as backup peer.
7. Configure a backup peer for a specific connection.

LLC2 port configuration

To configure the LLC2 port, use the following basic steps and related commands. Many of these steps are optional; the default values are typically sufficient for proper operation.

1. Create the LLC2 port.
2. Configure values for LLC2 port timers.
3. Configure port retry counter.

4 Configure lan-type. Supported LAN types are 802.3 and DIX. Default value is 802.3 and DIX.

5 Configure port maximum received window. Default value is 7 (modulo 8).

SDLC port configuration

To configure an SDLC port use the following steps. Many of these steps are optional; the default values are typically sufficient for proper operation.

1 Create SDLC port.

2 Configure activation sequence used when a primary port is activating (remote peer first or local device first). The default is local device first.

Note: Use the default of local-device-first to avoid repeated outage failure messages on the host for PU Type 2 devices, which would occur if the local device is not powered on. Use Peer-first if you want the Contivity to establish the host connection first prior to polling the local device.

Troubleshooting hint: You can use this parameter to test local or remote communications under conditions when a connection could not normally be tested.

3 Configure values for port timers.

Note: It is important to set these timers consistent with the link speed of the SDLC link. Incorrect settings can result in unexpected errors and link disconnects.

4 Configure port counters.

5 Enable/disable debug. To display all in/out SDLC packets in the Event Log, debug has to be enabled. Default value is disabled.

6 Enable/disable interframe-fill. The default value is disabled.

7 Configure port maximum received window. Default value is 7 (modulo 8).

8 Configure SDLC port poll address.

9 Enable/disable full-duplex communications for primary port. The default value is disabled.

Note: The primary and secondary full duplex settings are not Constant Carrier. Very few IBM devices support true full duplex. Therefore, it is almost always incorrect to enable full duplex. If the line is primary/secondary two-way alternating communications, do NOT enable these options.

10 Enable/disable full-duplex communication for secondary port. The default value is disabled.

11 Configure SDLC port role (primary, negotiable, secondary). The default value is primary.

12 Enable/disable transmission of REJECT frame. The default value is disabled.

SDLC link station configuration

To configure SDLC link station, use the following steps and related commands. Many of these steps are optional; the default values are typically sufficient for proper operation.

1 Create SDLC link station. Assign a poll address to link station. In CLI it is a new link station configuration mode.

2 Configure local MAC/SAP used for outgoing/incoming circuits.

3 Configure remote MAC/SAP used for outgoing/incoming circuits.

4 Configure SDLC link station counters.

Note: Nortel recommends that these settings not be changed unless required to address a specific configuration issue.

5 Configure values for SDLC link station timers.

Note: The fast-poll and slow-poll timers are critical for good response time for devices on the SDLC link. By default, the device will be polled at a 400 ms interval for 16 tries, and thereafter at 1 second intervals until a productive response (an I-Frame) to a poll is received. This results in an average response time typically approaching 1 second. More aggressive settings of 100 ms for fast-poll and 400 ms for slow-poll result in a much more responsive terminal.

6 Configure SDLC link station received window. Default value is 7 (modulo 8).

Note: Nortel recommends that these settings not be changed unless required to address a specific configuration issue.

7 Configure SDLC link station send window. Default value is 7 (modulo 8).

Note: Nortel recommends that these settings not be changed unless required to address a specific configuration issue.

8 Configure group poll address. Group poll is optional, and is only used for an IBM 3174 controller which is being used as a LAN Gateway.

9 Configure proxy XID. Proxy XID is only required for PU Type 2 devices. Do not configure for PU Type 1, PU Type 2.1, and PU Type 4.

10 Configure the SDLC link station poll frame. The default value is SNRM. The poll frame default should work in the majority of cases, and should only be modified if required for the particular attached device. Nortel recommends that it not be changed unless the device is not responding to normal re-activation polling.

11 Enable/disable the SDLC link station. Default value is disabled.

12 Start/stop the SDLC link station in order to activate/de-activate it.

DLSw timers configuration

Configure global timer values at the local peer level:

```
dlsw timer tcp-connect-retry connectretry
dlsw timer test-timeout conntimeout
dlsw timer explorer-timeout circtimeout
dlsw timer explorer-wait-timeout multicirctimeout
dlsw timer explorer-delay value
dlsw timer circuit-ack-timeout acktimeout
dlsw timer idle-timeout idletime
```

DLSw miscellaneous configuration

Miscellaneous DLSw configuration includes the following:

- Configure local/remote MAC address translation tables.
- Delete circuits with the same local SAP/with a specific local-remote SAP pair or all circuits.
- Configure DLSw debug level. Default value is Low.
- Enable/disable internal DLSw signal tracing. The default value is disabled. dlsw ips-trace should only be used under instructions from Nortel technical support.
- Delete entries in MAC-cache.

Single port V.35/X.21 configuration

Configuration of the single port V.35/X.21 serial card involves the following:

1. Configure clock-type (external, internal, loopback). The default is internal.
2. Configure line coding (NRZ/NRZI). The default line encoding is NRZI when you set the line type to SDLC. For non-SDLC line type, the default is NRZ.
3. Configure line speed.

Chapter 9
Configuring IPX

The Internetwork Packet Exchange (IPX protocol is the Novell* adaptation of the Xerox Networking System (XNS) protocol. IPX has the following characteristics:

- It is a connectionless datagram delivery protocol. A datagram is a unit of data that contains all of the addressing information required for it to be delivered to its destination.
- It does not guarantee the delivery of packets. Higher-level protocols assume the responsibility for reliability.

The gateway supports IPX by encapsulating IPX traffic within PPTP client connections.

Note: The gateway IPX support is not available for the IPsec tunneling protocol.

IPX is the network-layer routing protocol used in the Novell NetWare* environment. The primary tasks of IPX are addressing, routing, and switching information packets from one location to another on a network. In a LAN-based client the network interface card (NIC) provides network node addressing; in a tunneled environment, the gateway provides the network node addressing.

Network addresses form the basis of the IPX internetwork addressing scheme for sending packets between network segments. Every network segment of an internetwork is assigned a unique network address by which routers forward packets to their final destination network. On the gateway, all public interfaces are treated as a single network segment with a unique network address. A network address in the NetWare environment consists of eight hexadecimal characters. In the following example, 0x indicates that this is a hexadecimal number, and *n* is any hexadecimal character.

`0x`*`nnnnnnnn`*

Socket numbers are the basis for an IPX *intranode address* (the address of an individual entity within a node). They allow a process (for example, IPX Routing Information Protocol [RIP] and Service Access Points [SAP]) to distinguish itself to IPX. To be able to communicate on the network, the process must request a socket number. Any packets IPX receives addressed to that socket are then passed on to the process within the node.

The gateway uses IPX RIP and SAP to dynamically learn and advertise IPX routes and services. The gateway assigns IPX addresses to tunneled clients; remote users cannot configure the IPX tunnel address for their systems.

The gateway does not forward IPX packets from a private nontunneled LAN to another private nontunneled LAN, nor does it propagate routing or server tables from a private nontunneled LAN to another private nontunneled LAN.

IPX client

On the PPTP client (for example, Microsoft Dial-Up Networking), you must enable the dial-up networking IPX option. Enabling the IPX option allows you to tunnel using IPX, IP, or IPX and IP according to the dial-up networking selections.

Windows 95 and Windows 98

When running Windows 95 or Windows 98, load the intraNetWare client, which is available from the Novell Web site:

`http://www.novell.com`

Note: The NetWare client for Windows 95 and Windows 98 does not function properly; therefore, you must use the Novell intraNetWare client when using IPX with PPTP.

Windows NT

The NetWare client is already on Windows NT systems. You can use that or the Novell intraNetWare client, which you can access from the Novell Web site at http://www.novell.com.

Enabling IPX for group users

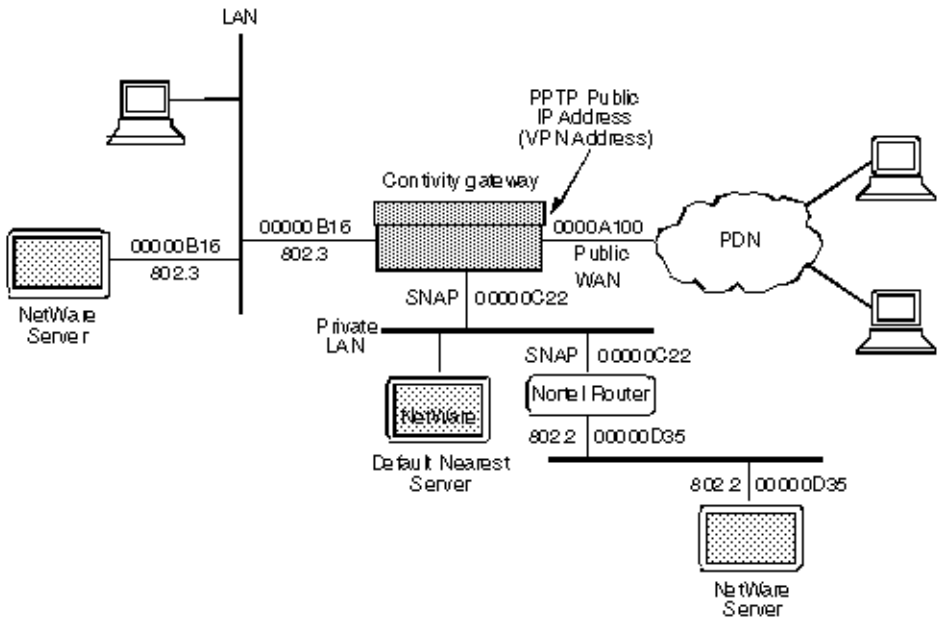
IPX is disabled on a per-group basis by default. Therefore, you must enable IPX for group users to access IPX. Enable IPX for group users from the Profiles > Groups > Edit > Connectivity screen.

Sample IPX VPN gateway topology

Regardless of the number of IPX public interfaces that are configured on the gateway, they all use the same IPX network address. You must enable the private interfaces that you want to use for IPX traffic, and for each private interface you must configure the IPX network address and IPX frame type. The IPX network address that you configure must match the IPX network address for that LAN, and the IPX frame type must match the IPX frame type for that LAN. In the following figure, the public interface IPX network address that the gateway provides is 0000A100.

In Figure 50 on page 150, the private interface network address to the NetWare server is 00000B16 and the Frame Type is 802.3; similarly, the private interface network address to the Nortel Router is 00000C22 and the Frame Type is SNAP.

Figure 50 IPX topology



Note: The Private LAN can also carry IP and IPX traffic simultaneously. The IP addresses are not shown in this figure.

Index

Numbers

A

B

C

D

E

H

I

L

M

N

P

R

S

T

V

W