Version 8.00

Part No. NN46110-502 02.01
315899-G Rev 01
13 October 2008
Document status: Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Configuration — Advanced Features



Copyright © 2008 Nortel Networks. All rights reserved.

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

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

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

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

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

Java is a trademark of Sun Microsystems.

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

Macintosh is a trademark of Apple Computer, Inc.

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

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

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

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

NDS is a trademark of Novell Inc.

OPENView is a trademark of Hewlett-Packard Company.

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

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

SPECTRUM is a trademark of Cabletron Systems, Inc.

All other trademarks are the property of their respective owners.

Restricted rights legend

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

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

Statement of conditions

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

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

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

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

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

Nortel Networks Inc. software license agreement

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

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

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

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

provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

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

4. General

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

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

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

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

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

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

Contents

Preface 11

Before you begin 11
Text conventions 11
Related publications 14
Printed technical manuals 15
How to get help 15
Finding the most recent updates on the Nortel Web site 16
Getting help from the Nortel Web site 17
Getting help over the phone from a Nortel Solutions Center 17
Getting help from a specialist by using an Express Routing Code 17
Getting help through a Nortel distributor or reseller 18

New in this release. 19

Feature changes 19
Other changes 19

Chapter 1
Advanced LAN and WAN configuration. 21

802.1Q VLAN configuration 21
Interface MTU and TCP MSS configuration 30
MTU configuration on an interface 31
TCP MSS clamping configuration 31
TCP MSS reset on an interface 32
MTU configuration on a tunnel 32
WAN interface setup 33
WAN interface configuration 34
Configuring E1 35
Configuring Fractional E1 37
Alarm generation 37

Healthcheck 37
Light emitting diodes 37
Single port T1/E1 38
Quad T1/E1 38
Obtaining statistics 38
Configuring with Quick Start 39
Event Log Messages 40
Circuitless IP configuration 41
Security Accelerator and Hardware Accelerator card configuration 45
VPN Router SA card 46
Hardware Accelerator card 46
Performance considerations 46
Support for IPsec encryption and authentication algorithms 47
Accelerator card security 47
Load-balancing between the CPUs and accelerator cards 48
Configuring the SA and Hardware Accelerator cards 49
Viewing statistics for accelerator cards 50

Chapter 2
T1 CSU/DSU configuration 51

Viewing status 52
Configuring a T1 CSU/DSU 52
56/64K CSU/DSU WAN 54

Chapter 3
ADSL and ATM configuration 59

ADSL WAN interface cards 59
ATM software 60
ADSL and ATM configuration 60
Configuring an ATM interface 60
Configuring an ATM virtual circuit 61
Configuring PPP authentication 63
Configuring PPP advanced parameters 64
Configuring PPPoE parameters 65

Chapter 4
PPP configuration 67

Configuring PPP settings 67

Chapter 5
PPPoE configuration 71

Overview 71
Configuring PPPoE settings 73

Chapter 6
Frame Relay configuration 75

Introduction 75
Permanent virtual circuits 78
RFC 1490 78
Traffic shaping 79
Committed information rate 79
Committed burst rate and excess burst rate 80
Traffic shaping configuration notes 81
Overview of Frame Relay configuration 81
Configuring Frame Relay settings 82
Configuring FRF.9 85
Configuring FRF.12 86
Frame Relay Forwarding Priority to a VC 90
Assigning priority to a PVC within a map class 90
Configuring VC with a map class 91
FR Forwarding Priority to a VC with FRF.12 93
Frame Relay monitoring 93
Frame Relay OM statistics 93
IP statistics 94

Chapter 7
Dial and Demand Services configuration 95

Dial interface configuration 95
Configuring the modem 97
Configuring PPP 98

Configuring ISDN BRI 99
Demand Services 102
Trigger modes 102
Dialing functionality 103
Backup interfaces 103
Configuring subinterfaces as backup interfaces 104
ABOT configuration for backup interfaces 104
Dial on Demand 105
Configuring Demand Services 105
Configuring Demand Services with an interface group trigger 106
Configuring Demand Services with an hour trigger 108
Configuring Demand Services with a route unreachable trigger 108
Configuring Demand Services with a ping trigger 110
Configuring Demand Services with a Traffic trigger 111
Configuring Demand dialout parameters 112
Configuring a remote network 112
System log messages 113
Healthcheck 114

Chapter 8
VPN Router Data Link Switching 115

Introduction 115
Supported functionality 120
Ethernet LLC Type 2 functionality 120
SDLC functionality 121
Single port V.35/X.21 serial card functionality 121
Configuring DLSw 122
VPN Router configuration commands example 125
DLSw local peer configuration 125
DLSw remote peer configuration 126
LLC Type 2 port configuration 126
SDLC port configuration 127
SDLC link station configuration 128
DLSw timers configuration 130
DLSw miscellaneous configuration 130

Single port V.35/X.21 configuration 130

Chapter 9
IPX configuration 131

Introduction 131
IPX client 132
Windows 95 and Windows 98 133
Windows NT 133
Enabling IPX for group users 133
Sample IPX VPN gateway topology 133

Chapter 10
Interoperability configuration 135

Configuring the Cisco 2514 router Version 11.3 136
Configuring the VPN Router for Cisco interoperability 138
Configuring the SafeNet/Soft-PK Security Policy Database Editor Version 1.0s 139
Connecting to IRE SafeNET/Soft-PK Security Policy Client 140
Configuring the VPN Router for IRE interoperability 143
Third-party client installation 144
Considerations for using third-party clients 145
Configuring the VPN Router as a branch office tunnel 147
Configuring the VPN Router as a user tunnel 148
. 150
Index 151

Preface

This guide describes the Nortel VPN Router advanced features. It provides configuration information and advanced WAN settings.

Before you begin

This guide is for network managers who set up and configure the Nortel VPN Router. This guide is based on the assumption that you have experience with Windows-based systems or graphical user interfaces (GUIs) and that you are familiar 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 choice. 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.

Related publications

For more information about the Nortel VPN Router, see the following publications:

- Release notes provide the most recent information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Nortel VPN Router Configuration — Client* (NN46110-306) provides information to install and configure client software for the VPN Router.
- *Nortel VPN Router Configuration — TunnelGuard* (NN46110-307) provides information to configure and use the TunnelGuard feature.
- *Nortel VPN Router Upgrades — Server Software Release 8.0* (NN46110-407) provides information to upgrade the server software to the most recent release.
- *Nortel VPN Router Installation and Upgrade — Client Software Release 8.01* (NN46110-409) provides information to upgrade the Nortel VPN Client to the most recent release.
- *Nortel VPN Router Configuration — Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration.
- *Nortel VPN Router Configuration — SSL VPN Services* (NN46110-501) provides instructions to configure services on the SSL VPN Module 1000, including authentication, networks, user groups, and portal links.
- *Nortel VPN Router Configuration — Advanced Features* (NN46110-502) provides configuration information for advanced features such as the Point-to-Point Protocol (PPP), Frame Relay, and interoperability with other vendors.
- *Nortel VPN Router Configuration — Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F).
- *Nortel VPN Router Configuration — Routing* (NN46110-504) provides instructions to configure the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), Equal Cost Multipath (ECMP), routing policy services, and client address redistribution (CAR).
- *Nortel VPN Router Using the Command Line Interface* (NN46110-507) provides syntax, descriptions, and examples for the commands that you can use from the command line interface (CLI).

- *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508) provides instructions to configure the Stateful Firewall and VPN Router interface and tunnel filters.
- *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.
- *Nortel VPN Router Troubleshooting — Server* (NN46110-602) provides information about system administrator tasks such as recovery and instructions to monitor VPN Router status and performance. This document provides troubleshooting information and event log messages.
- *Nortel VPN Router Administration* (NN46110-603) provides information about system administrator tasks such as backups, file management, serial connections, initial passwords, and general network management functions.
- *Nortel VPN Router Troubleshooting — Client* (NN46110-700) provides information to troubleshoot installation and connectivity problems with the Nortel VPN Client.

Printed technical manuals

To print selected technical manuals and release notes for 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 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 Web site at www.adobe.com to download a free copy of the Adobe Reader.

How to get help

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

Finding the most recent updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for updates to the most recent documentation and software for VPN Router, click one of the following links.

Link	Web site
Most recent software	Nortel page for **VPN Router** software located at support.nortel.com/go/main.jsp?cscat=SOFTWARE&poid=12325
Most recent documentation	Nortel page for **VPN Router** documentation located at support.nortel.com/go/main.jsp?cscat=DOCUMENTATION&poid=12325

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can perform the following activities:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also 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 following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to the following Web site:

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, contact the technical support staff for that distributor or reseller.

New in this release

The following sections detail what's new in *Nortel VPN Router Configuration — Advanced Features* (NN46110-502) for Release 8.0:

- "Feature changes" on page 19
- "Other changes" on page 19

Feature changes

Release 8.0 increases the upper limit of the forced logoff timer to 120 hours (5 days). For more information, see "Configuring the VPN Router as a user tunnel" on page 148.

Other changes

"Interoperability configuration" on page 135 includes content from *Nortel VPN Router Troubleshooting — Server* (NN46110-602).

Chapter 1
Advanced LAN and WAN configuration

This chapter provides the following configuration information:

- "802.1Q VLAN configuration" on page 21
- "Interface MTU and TCP MSS configuration" on page 30
- "WAN interface setup" on page 33
- "WAN interface configuration" on page 34
- "Circuitless IP configuration" on page 41
- "Security Accelerator and Hardware Accelerator card configuration" on page 45

802.1Q VLAN configuration

Use the Virtual LAN (VLAN) to control broadcast traffic and improve network performance. A VLAN is a collection of end nodes grouped logically, rather than by the physical location. The VPN Router assigns end nodes that frequently communicate with each other to the same VLAN, regardless of their physical location on the network. Users in separate areas or that connect to separate ports can belong to a single VLAN.

Create a VLAN based on

- Membership by port group—a port-based VLAN is a collection of ports on one or more switches. For example, the VPN Router assigns ports 1, 2, 3, and 4 to VLAN A and assigns ports 5, 6, 7, and 8 to VLAN B.

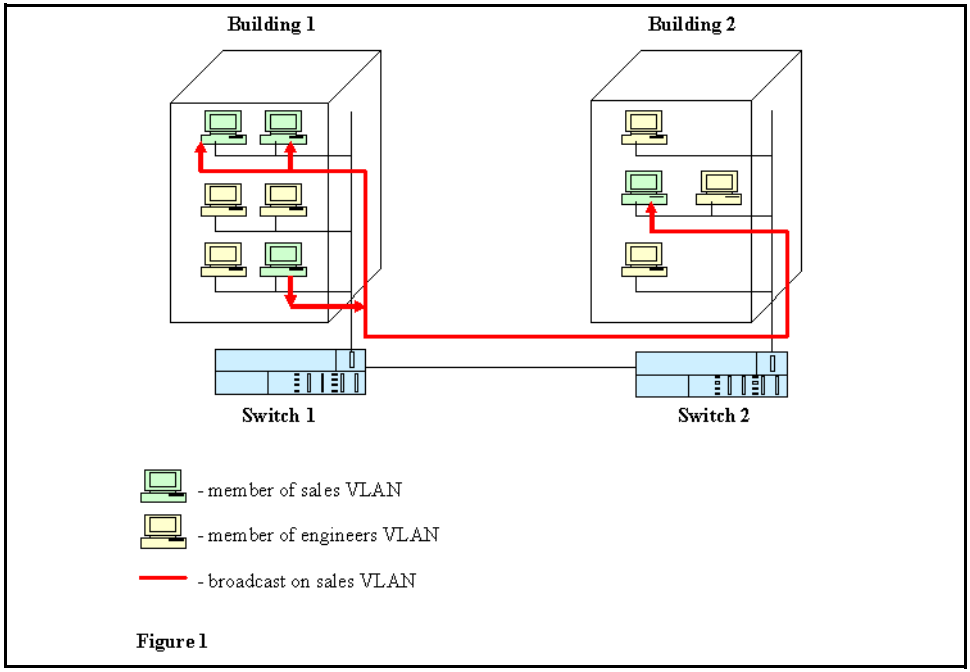
- Membership by MAC address—the MAC address of a network device determines the VLAN membership. To create a MAC address-based VLAN, configure a VPN Router with a list of MAC addresses associated with a particular VLAN. The VPN Router looks up the source MAC address of a received frame to determine the associated VLAN.
- Membership by protocol—protocol-based VLANs use Layer 3 protocol type, for example, IP, Internetwork Packet Exchange (IPX), or Appletalk to determine membership. For example, you can create a VLAN for the IPX protocol and place ports that carry IPX traffic into this VLAN. This localizes all IPX traffic (including IPX broadcasts) within the ports of that VLAN.
- Membership by network address—the network-layer address determines membership. For example, you can create an IP-subnet-based VLAN for IP subnet 128.1.1.0/24. The VPN Router then inspects a packet IP address to determine if it belongs to subnet 128.1.1.0/24. If it does belong to that subnet, it is a member of the VLAN.

Hosts assigned to a virtual LAN send and receive broadcast and multicast traffic as though they all connect 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 remain within that VLAN.

Divide the network into separate VLANs to create separate broadcast domains. This arrangement conserves bandwidth, especially in networks that support broadcast and multicast applications that flood the network with traffic.

"Sample VLAN" on page 23 shows an example of a VLAN. Two buildings use separate internal networks and each building connects to a VLAN-aware switch. The engineering and sales groups exist in separate VLANs. If a workstation from the sales VLAN sends a broadcast, every workstation that belongs to the sales VLAN receives the broadcast, regardless of the physical location of the workstation. At the same time, workstations on the engineering VLAN have no knowledge of the broadcasts. Sales broadcasts do not interfere with the engineering network.

Figure 1 Sample VLAN



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

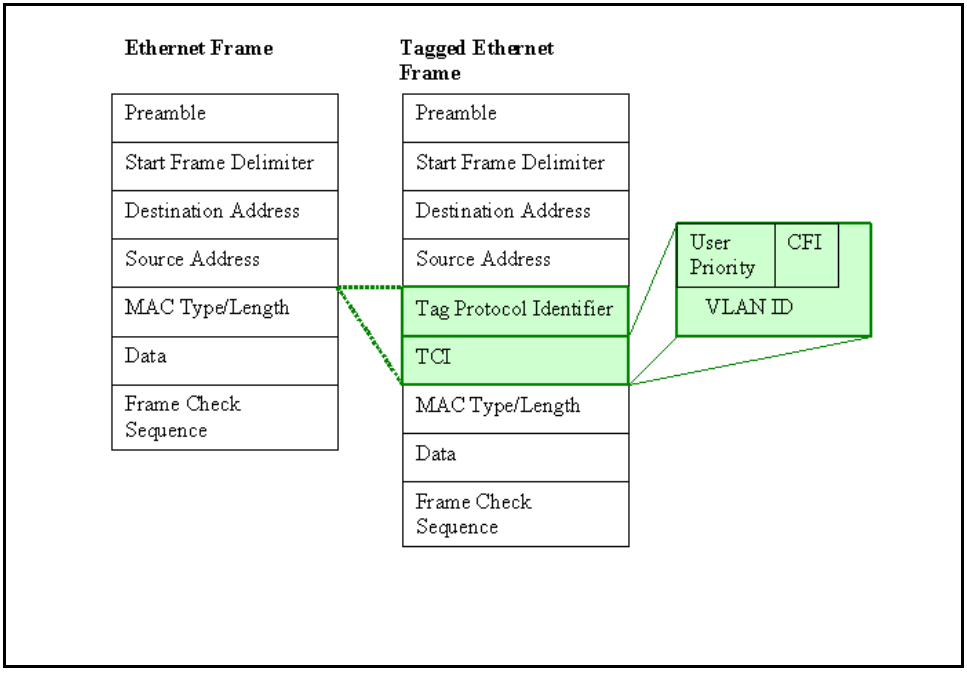
Frame tagging with 802.1Q information performs at the Data Link layer level and requires modification to Ethernet frame format. Each 802.1Q tag sits in the Ethernet frame between the source address field and the MAC client type and length field. Ethernet switches use this tag to determine where to deliver the frame.

"Ethernet frame and 802.1Q frames" on page 24 shows a standard Ethernet frame and an 802.1Q modified Ethernet frame. The tagged frame uses two new fields—Tag Protocol Identifier (TPI) and Tag Control Information (TCI). TPI represents the Ether Type and uses a fixed value of 0x8100. If the frame uses the TPI equal to 0x8100, the frame carries the 802.1Q tag. The following two bytes (16 bits) stores the tag. The tag contains the following bits:

- User Priority—3 bits of 802.1p user priority level (0–7)

- Canonical Format Indicator (CFI)—1 bit that indicates if the MAC addresses use the canonical format. This field provides compatibility between Ethernet and Token Ring type networks. Ethernet uses value 0. 802.3/Ethernet and transparent Fiber Distributed Data Interface (FDDI) networks use Canonical MAC addresses. Token ring and source-routed FDDI networks use noncanonical MAC addresses.
- VLAN ID (VID)—12 bits that identifies the VLAN and assigns a frame to one of the 4094 possible VLANs (1 to 4094, as values 0 and 4095 are reserved).

Figure 2 Ethernet frame and 802.1Q frames



After a VLAN switch receives a frame, it inspects the VLAN ID in the tag. If the tag specifies the VLAN ID, the VPN Router forwards the frame to a specific VLAN. If the tag does not specify the ID, the VPN Router forwards the frame to a configured default VLAN.

VLAN tagging simplifies the routing between VLANs. Tagging makes it easy and cost-effective for inter-VLAN routing. Based on the information in the tag, the router determines which VLAN the frame belongs to and routes the frame accordingly. Therefore, a router that supports VLAN tagging does not need a dedicated link to each VLAN. You can use a single tagged port to perform inter-VLAN routing (see "Routing between VLANs" on page 25 and "VLAN tagging" on page 25).

Figure 3 Routing between VLANs

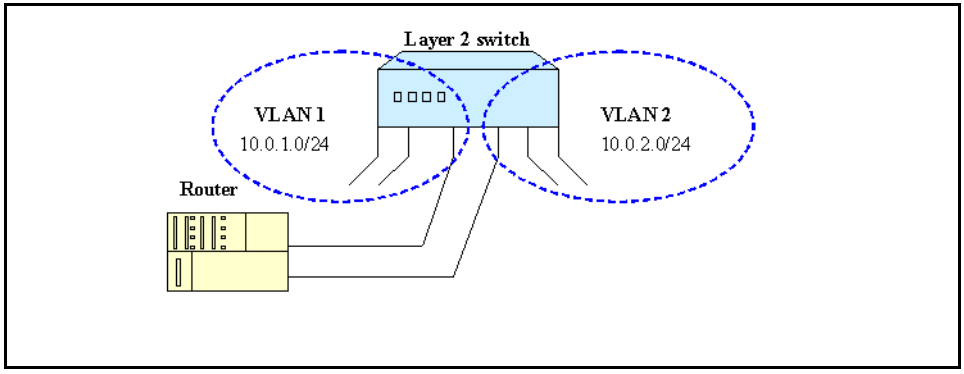
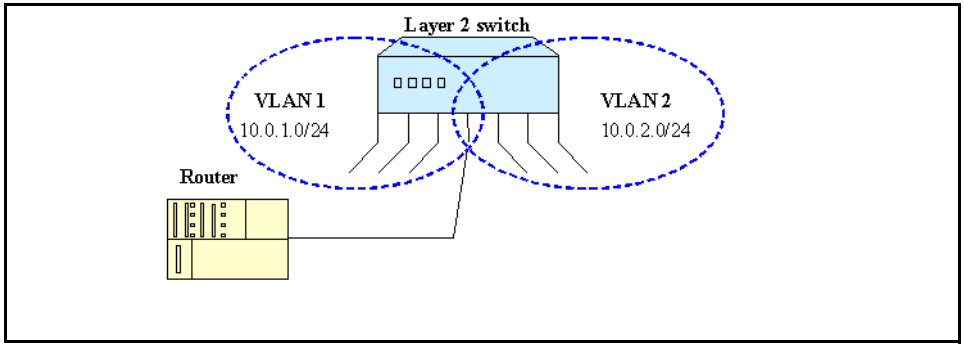


Figure 4 VLAN tagging



Use frame tagging on the VPN Router for routing between VLANs and traffic segregation. The VPN Router does not forward frames within the same VLAN; Layer 2 switches perform this function.

The VPN Router uses 802.1Q to perform the following

- Receive and transmit 802.1Q tagged frames on Fast Ethernet (excluding the Intel i82557 chipset) and Gigabit Ethernet (GbE) interfaces. After you enable tagging, the VPN Router receives and processes the tagged frames. If you disable tagging, the VPN Router discards the tagged frames. The VPN Router transmits tagged frames with tags that identify the outbound VLAN.
- Support 802.1Q on public or private interfaces.
- Support VLAN routing between VLANs.
- Support VLAN tagging at the interface or subinterface level.
- Map an individual VLAN to an IP subnet.
- Support routing services, for example, static routes, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and route policy service and the Dynamic Host Configuration Protocol (DHCP) relay for each VLAN on subinterfaces.
- Support interface filters, user and branch office tunnels using IPsec, Point to Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP) for each VLAN on subinterfaces.
- Display statistics for VLANs.

You can enable 802.1Q tagging at the interface or subinterface level.

If you enable tagging at the interface level, you can configure the VPN Router to perform the following activities:

- Accept tagged frames after you enable 802.1Q. The VPN Router tags a frame if it carries a 802.1Q tag with a non-null VLAN ID.
- Accept or discard untagged frames received by the interface (ingress behavior). The VPN Router does not tag a VLAN frame if it does not carry the 802.1Q header or if the VLAN ID is null in the 802.1Q header (priority-tagged frames). The default behavior accepts the untagged frames.
- Send tagged or untagged frames (egress behavior). The default behavior sends untagged frames. If the router tags egress frames, outbound frames include the 802.1Q header with the VLAN ID of the interface VLAN. If the router does not tag egress frames, outbound frames do not include the 802.1Q tag header or the frames include the 802.1Q header with null VLAN ID (when 802.1p user priority information exists in the frame).

A subinterface is a Layer 2 entity. You can use multiple subinterfaces on a single interface, each representing a different network. The operational state of subinterfaces depends on the operational state of the associated base interface. If the base interface goes down, all subinterfaces over the interface also become nonoperational.

After you disable tagging, the router processes all frames as standard frames. If the router detects a tag in some of the frames, the router discards these frames.

After you enable tagging, the VPN Router uses the following rules to process a frame:

- The LAN interface processes untagged frames as standard frames.
- The corresponding VLAN processes tagged frames with a VLAN ID (VID) from 1 to 4094. If the VID in the frame does not match a VID on the VPN Router VLANs, the VLAN discards the frame.
- The router discards a tagged frame with a VID of 4095.

To configure 802.1Q

1. Choose **System, LAN**.

   The LAN Interfaces window appears.

2. Click **Configure** next to the interface that you want to use for the 802.1Q.

   The LAN Interfaces > Edit LAN Interface window appears.

3. Select **Enabled** for **802.1Q State**.

   After you enable 802.1Q on the interface, the default behavior of accepting and sending untagged frames applies to the interface.

4. In the **Interface VLAN** section, type the appropriate VLAN ID. The default is 1. Use different VLAN IDs at the interface and subinterface levels.

5. For the ingress behavior, select an option. The default is **Accept Untagged**. After you configure an interface VLAN to **Discard Untagged**, a confirmation window appears that states that the hosts that send untagged frames can lose connectivity to the interface. Click **OK** to apply the settings to the interface and discard all untagged frames.

6 For the egress behavior, select an option. The default is **Untagged**. After you configure an interface VLAN to send tagged frames, a confirmation window appears that states that enabling this behavior can cause a loss of connectivity with the hosts that do not support tagged frames. Click **OK** to apply the behavior.

7 Click **OK**.

Configure VLAN at the subinterface level

1 Choose **System, LAN.**

The LAN Interfaces window appears.

2 Click **Configure** next to the interface that you want to use for the VLAN.

The LAN Interfaces > Edit LAN Interface window appears.

3 Click **Configure Subinterfaces**.

The LAN Interfaces > LAN Subinterfaces window appears.

4 Click **Add Subinterface** to add a subinterface.

The LAN Interfaces > Add LAN Subinterface window appears. Interface shows the current interface.

5 In the **Subinterface** box, type a number for a subinterface (1 to 65535).

6 In the **Description** box, type a description (up to 127 characters).

7 Select an encapsulation method (currently 802.1Q is the only option).

8 Type the **VLAN ID** (value 1 to 4094). Use different VLAN IDs at the interface and subinterface levels.

9 Select **Enabled** for the state.

10 Click **OK**. The LAN Subinterfaces window lists the configured subinterface. To change the configured parameters, click **Configure** next to subinterface. You cannot change the Subinterface number. You can adjust the other fields.

11 To add an IP address to a subinterface, click **Add IP**.

12 In the **IP Address** box, type an IP Address.

13 Type the subnet mask associated with the address.

14 Select the **Interface Filter** you want to apply to the subinterface.

15 Click **OK**.

The configured IP address and filter appear under the subinterface.

16 To edit or delete the IP address, click the appropriate option next to the IP address definition.

17 The LAN Interfaces, LAN Subinterfaces window shows up to 10 subinterfaces. If the number of subinterfaces is greater than 10, the window divides into several windows. After you configure all appropriate subinterfaces, click **Close**.

18 After you configure all parameters, on the Edit LAN Interface window, click **OK**.

Viewing subinterface statistics

1 Select **System, LAN.**

The LAN Interfaces window appears.

2 Click **Configure** next to the interface that you want to use for the VLAN.

3 The LAN Interfaces > Edit LAN Interface window appears.

4 Click **Subinterface Statistics**.

The LAN Interfaces > Statistics window appears. Statistics include total received and transmitted packets and octets, and dropped packets and octets.

5 To refresh the statistics, click **Refresh**.

6 To return to the LAN interfaces window, click **Close**. Initially, all counters are zero (clear).

7 Use **System**, **LAN**, **Statistics** to view the drop statistics for 802.1Q on the interface.

Configure routing (static routes, RIP, OSPF, route policies) on subinterfaces the same as you configure other interfaces. As with all interfaces, only trusted interfaces support routing.

Configure OSPF and RIP for a subinterface on the Routing, Interfaces window. Configure DHCP relay and IPsec, L2TP, and PPTP tunnels on subinterfaces the same as you configure regular interfaces.

To display subinterfaces, perform one of the following actions:

- In the routing table—select **Routing, Route Table,** and then click **Route Table**.
- In the forwarding table—select **Routing, Route Table** and click **IP Forward Table**. The subinterface is a VC.

Interface MTU and TCP MSS configuration

You can configure the following interface parameters:

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

The MTU assigns the maximum size of a data packet transmitted from the interface. The MTU does not affect the size of a packet accepted by the interface. The interface either fragments or drops packets larger than the MTU. The do not fragment (DF) bit in the IP header determines the action to take.

For optimal network performance, configure the largest MTU value possible. Because certain network topologies do not handle large packets, you can lower the MTU to decrease the size of the packets you send.

The media type adjusted for Layer 2 encapsulation determines the default MTU value for each interface, see the following table.

Table 1 Default MTU by interface media type

Media	Default MTU (bytes)
Ethernet	1500
Frame Relay	1496
ISDN	1500
PPPoE	1492

Table 1 Default MTU by interface media type

Media	Default MTU (bytes)
Serial	1500
WAN (T1/T3)	1500

You can reset the MTU on the following interfaces to these values:

- LAN interfaces: 576 through 1500 bytes
- Point-to-Point Protocol Over Ethernet (PPPoE) interfaces: 576 through 1492
- WAN interfaces: 576 through 1788 bytes
- Branch office tunnels: 576 through 1788 bytes

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

MTU configuration on an interface

To change the MTU on an interface

- For a LAN interface, choose **System, LAN**, click **Configure**, and then type the MTU value.
- For a WAN interface, choose **System, WAN**, click **Configure, Configure**, and then type the MTU value.

TCP MSS clamping configuration

You can configure the TCP MSS on all interfaces. The TCP MSS specifies the largest TCP payload that a client can accept from a peer server; for example, File Transfer Protocol (FTP) or Hypertext Transfer Protocol (HTTP). You can configure the TCP MSS independently from the MTU size.

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

TCP MSS clamping substitutes the configured MSS value for the MSS value that TCP peers negotiate. To implement TCP MSS clamping, you must configure it on the interfaces that 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.

TCP MSS reset on an interface

To change the current TCP MSS of an interface

- For a LAN interface, choose **System, LAN, Edit**, select the TCP MSS option (enabled or disabled), and then type the TCP MSS value.
- For a WAN interface, choose **System, WAN, Configure, Configure**, select the TCP MSS option (enabled or disabled), and then type the TCP MSS value.

MTU configuration on a tunnel

For tunnels, you can configure the following

- For all tunnels (IPsec, L2TP, and PPTP), you can configure tunnel MTU.
- For IPsec tunnels only, you can configure DF bit behavior.

Tunnel MTU determines the largest size tunnel packet for transmission. This MTU size includes the IPsec header and IP transport header layers. The default tunnel MTU behavior is enabled at 1788 bytes. If you disable tunnel MTU, the tunnel MTU is calculated based on the interface MTU.

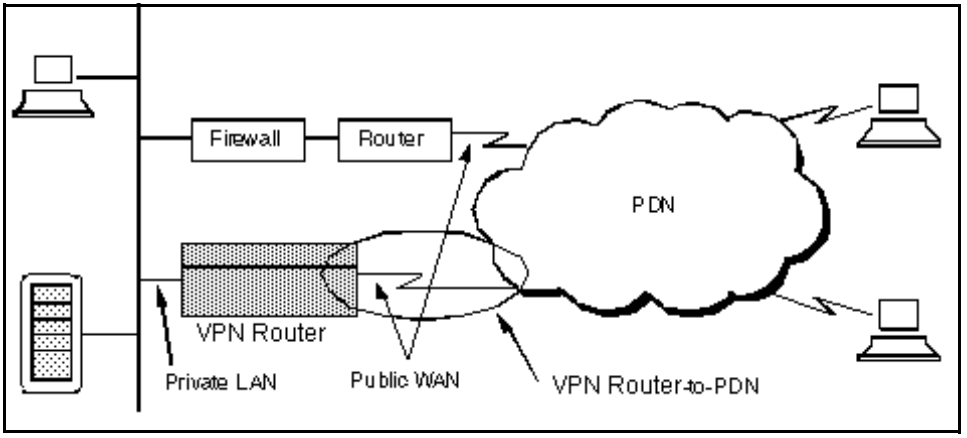
For IPsec tunnels, you can configure the DF bit in the outer IP transport header. The default behavior clears the bit. You can set the bit or copy the bit from the inner IP header.

Note: If you use set or copy for the DF bit with a packet capture utility on the outgoing interface, you can receive an Internet Control Message Protocol (ICMP) error packet that signifies you need fragmentation (the result if tunnel packets are too large). If this situation occurs, use the MTU value that appears in the ICMP error packet to reset the tunnel MTU to avoid fragmentation.

WAN interface setup

You assign WAN interface connections between the VPN Router and the private dial-up network (PDN). "VPN Router-to-PDN configuration" on page 33 shows the connection attributes that you must configure. These attributes assign WAN interface connections between the VPN Router and the Internet service provider (ISP).

Figure 5 VPN Router-to-PDN configuration



You configure WAN devices with local and remote IP addresses and Point-to-Point Protocol (PPP)-related settings on the System, WAN, Configure window. After you click PPP Authentication or Advanced Settings, the associated configuration window appears. Use this window to specify the interface filter for the firewall. The IP Control Protocol (IPCP) uses these addresses, which communicates IP addresses to peer connections over PPP. Your ISP provides many of these values.

Note: If you use a 32-bit subnet mask for a WAN interface, you must specify the local WAN interface as the remote VPN Router when you define a default route sent from the WAN.

WAN interface configuration

The System, WAN interfaces window shows the WAN interfaces currently installed in the VPN Router, the slot in which the cards reside, an interface description (optional), and the current state. This window also indicates if the firewall is active and identifies the interface filter that is in use. From this window, you can 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 reenable the interface. This automatically disables static routes for the interface. If you reset the IP address to the original address, you must manually reenable static routes.

To configure the WAN interface

1 Choose **System, WAN**.

The WAN Interfaces window appears.

2 Select the adapter that you want to configure, and then click **Configure**.

3 In the **Description** box, type a description.

4 In the **Circuit ID** box, type the Circuit ID.

You configure the Circuit ID parameter for each interface, but it is available to all WAN interfaces.

5 From the **Interface Filter** list, select an option.

6 From the **Protocol** list, select an option.

7 From the **HDLC Polarity** list, select an option.

If line framing is Extended Super Frame (ESF), High-Level Data Link Control (HDLC) polarity is normal. If line framing is SF, HDLC polarity is inverted.

8 From the **Line Format** list, select an option.

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

9 To configure the protocol, click **Configure**.

10 To open the **Controller** window, click **Configure Controller**.

11 Click one of the following options:

- Click **OK** to accept the changes and return to the prior window.
- Click **Cancel** to ignore changes made to the window. The previous values reset.
- Click **Apply** to apply the changes to the window.
- Click **Refresh** to redraw the window.

Configuring E1

A local exchange carrier provides T1 and E1 service to a customer. The Channel Service Unit/Data Service Unit (CSU/DSU) is the interface between the carrier transmission and the customer premises equipment. T1 is available in North America; E1 is available in Europe and internationally. Nortel provides a T1 and E1 (T1/E1) interface for the VPN Router with an integrated CSU/DSU.

You can configure all parameters for E1 by using the GUI, Quickstart, or the CLI.

To configure E1 by using the GUI

1 On the **WAN Interface** window, select the E1 adapter you want to configure.

2 Click **Configure**.

3 Configure the WAN interface, see on "WAN interface configuration" on page 34.

4 Click **Configure Controller** to open the Controller window.

5 From the **Clock Source** list, select **Loop**. The clock source typically loops if it connects to a live E1 service. Use internal clocking only for local or test applications.

No Line Build Out options exist.

No E1 Line Coding options exist. E1 always uses HDB3 line coding.

6 From the **Line Framing** list, select either E1F (framed E1) or E1UF (unframed E1). Framed E1 permits fractional E1 services and supports 30 or 31 DS0 channels. Unframed E1 permits the maximum E1 user bandwidth, 32 DS0 channels. The E1 service provider determines this parameter.

7 From the **CRC-4** list, select an option.

E1 CRC-4 is only for framed mode. You can turn the CRC-4 generation on or off. The service provider determines this setting.

8 From the **RD1** list, select an option.

E1 RDI generation is only for framed mode. You can turn the E1 RDI on or off. The service provider determines this setting.

9 From the **Channel 16** list, select an option.

For a framed E1, you can set channel 16 to signaling or to data. The E1 service provider determines this parameter. For framed E1 with channel 16 signaling, 30 (1–15, 17–31) channels exist. For framed E1 with channeling 16 data, 31 (1–31) channels exist. For unframed E1, 32 channels (0–31) exist.

10 No PRM is available for E1.

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

Configuring Fractional E1

Fractional E1 provides a fractional E1 circuit through timeslot provisioning. Fractional E1 is more affordable than clear channel circuit because you choose the number of channels you want, from 1 to 30, and pay only for that number of channels.

To configure fractional E1

1. Select **WAN Interfaces, Configure Controller**.
2. From the **Starting Channel** list, select a channel.
3. From the **Bandwidth** list, select a bandwidth.

Alarm generation

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

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

Healthcheck

The following table describes 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

The following section explains the light emitting diodes (LED) for the T1/E1 card.

Single port T1/E1

The following table shows the light emitting diodes (LED) for a single port T1/E1. The LMC 1200 is a single port T1/E1. All LEDs off indicates that the interface is disabled.

Table 3 Single port T1/E1 LEDs

LED	Condition
Green	Interface functions 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 uses one green LED for each port. The LMC 150x card is a quad T1/E1. The following table 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. Select **WAN, Interfaces**.
2. Click the desired WAN adapter.
3. Click **Statistics**.

Configuring with Quick Start

Quick Start is a comprehensive initial configuration window that includes WAN configuration. To use the Quick Start window to configure your VPN Router

1. From the Welcome to the VPN Router message, click **Quick Start** or choose **Admin, Quick Start**.

   The Quick Start window appears.

2. Read the information that appears.

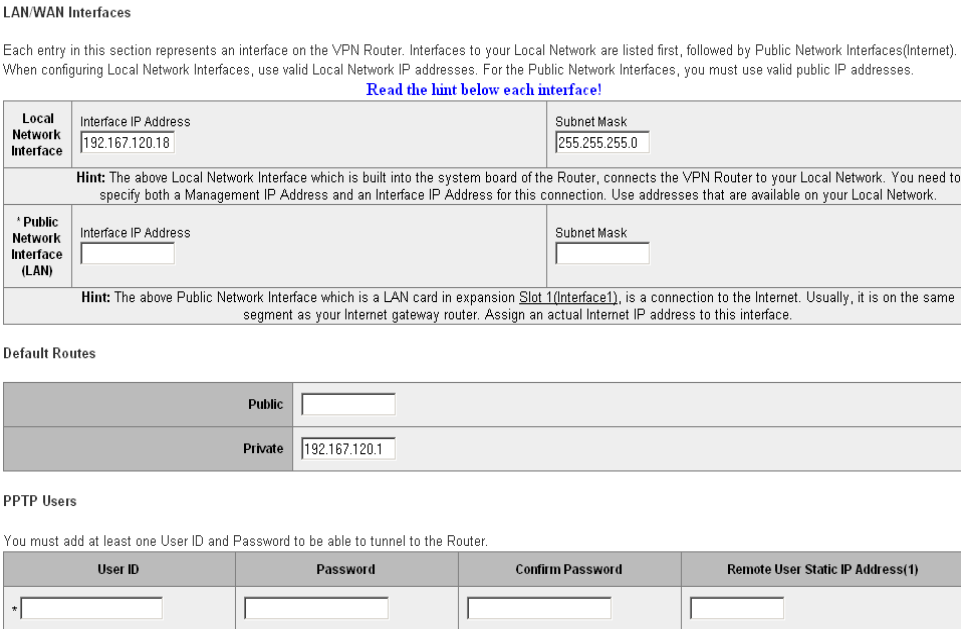
   This window lists the requirements and information you must complete for QuickStart.

3. Click **Continue Quick Start**. From this single window, you can

   - configure the VPN Router interfaces
   - create up to three user accounts
   - change the default administrator (admin) ID and password
   - change the date and time

"Quick Start window" on page 40 shows the section of the Quick Start window you use to configure WANs.

Figure 6 Quick Start window



4 Enter the values in this window to setup your VPN Router.

5 Click **Complete Quick Start**.

Event Log Messages

The following is an example of startup and shutdown event log messages.

Startup

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

Shutdown

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

Circuitless IP configuration

You use a circuitless IP (CLIP) to define virtual addresses as termination points, such as TCP connections, for branch office and client tunnels. You can use the VPN Router CLIP to build tunnel and ICMP filters for the public side, the private side, or both.

A CLIP interface provides

- 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

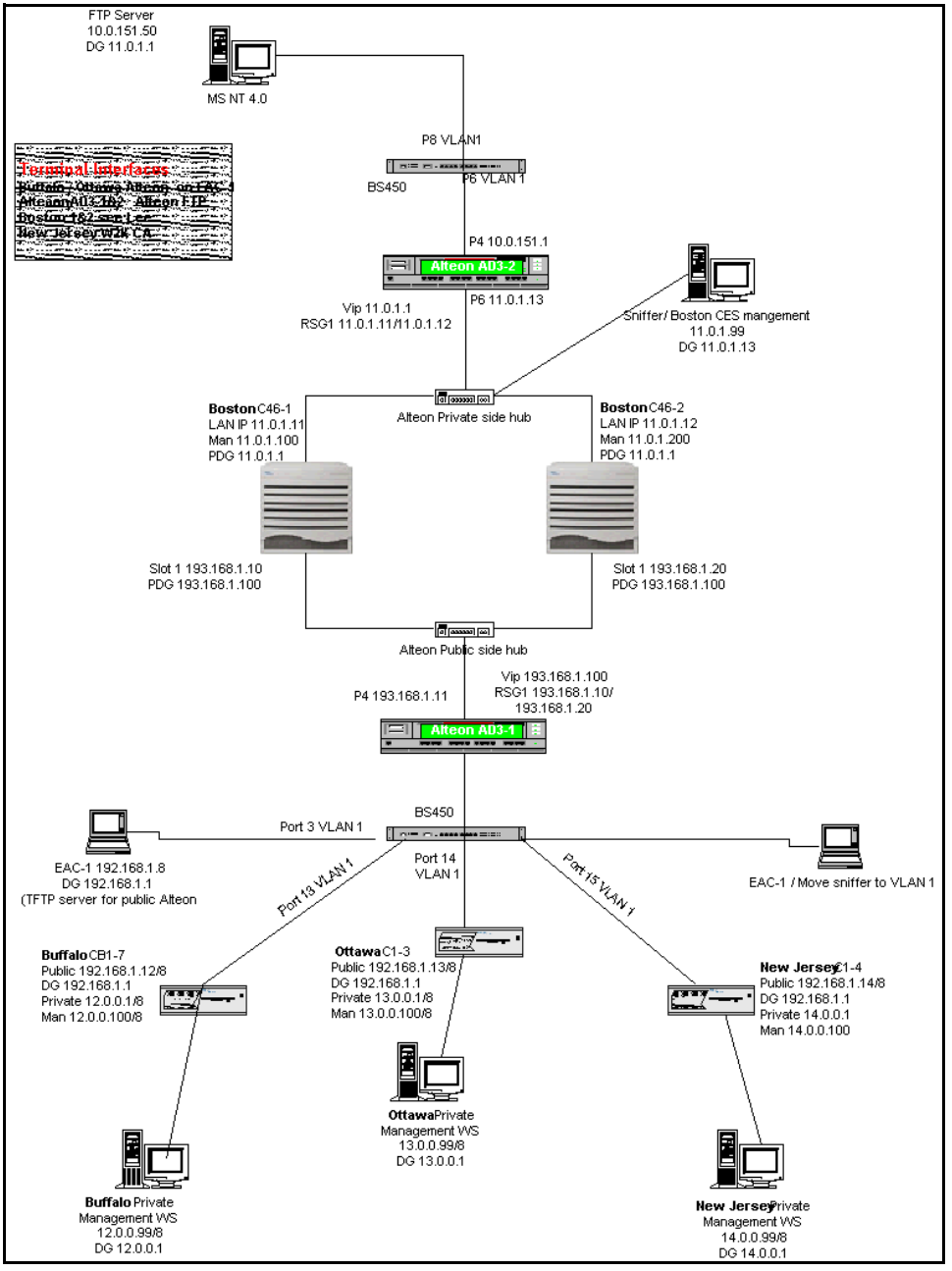
The VPN Router supports all current tunnelling protocols, including IPsec, L2TP, and PPTP. The router permits tunnel terminations based on tunnel types. The VPN Router supports peer-to-peer, asynchronous branch office tunnel (ABOT), and client tunnel types. You can use CLIP addresses for load balancing with an Alteon switch when multiple VPN Routers behind the Alteon switch use the same CLIP address.

For client or remote branch office tunnels, the VPN Router servers (load balancers) appear as one device. You configure the VPN Router servers with a common CLIP, although each server uses a unique interface IP address. The CLIP address is also unique within each VPN Router.

For VPN Router servers supporting branch offices, use the asynchronous branch office tunnel. Also, configure the VPN Router servers as responders and the remote clients as initiators.

As shown in "CLIP network topology" on page 43, the private Alteon WebOS switch directs returning data to the client through the same VPN Router as the ingress traversal through the VPN load balancing function. The Alteon WebOS supports up to 255 port connections. However, the network topology supports only eight VPN Router load balancers as the basic configuration.

Figure 7 CLIP network topology



To configure CLIP

1. Choose **System, Circuitless IP**.

   The Circuitless IP window appears.

2. Under Configured Circuitless IP, click **Add**.

   The Circuitless IP > Add window appears.

3. Type the CLIP address.
4. For the **Interface Type**, select either **Public** or **Private**. You can configure up to six CLIP addresses.
5. For the **Allowed Services**, select either **Public** or **Private** for each tunnel type.
6. Click **Apply** and **OK**.
7. After you complete the configuration, select **Enabled**, and then click **OK**.
8. Click **Allowed Services** to view the status of the allowed services. Click **Refresh** to view the changes.

To enable CLIP redistribution through dynamic routing protocols

1. Choose **Routing, Policy**.

   The Policy window appears.

2. Select **CLIP** as the route source for the protocol.
3. Click **OK**.

As part of the network management support, you can obtain real-time statistical information by clicking Allowed Services on the Circuitless IP window. The statistics include circuitless IP address information as well as connected session information.

Security Accelerator and Hardware Accelerator card configuration

Nortel supports the following two Peripheral Component Interconnect (PCI)-based option cards for encryption and compression:

- VPN Router Security Accelerator (SA) card
- Hardware Accelerator card

The VPN Router SA 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, VPN Routers that support accelerator cards run fast and efficiently.

The following table lists the VPN Routers that support the SA card and the Hardware Accelerator card.

Table 5 VPN Router platform support for SA and Hardware Accelerator cards

VPN Router platform	SA card supported?	Hardware Accelerator card supported?	Maximum number supported (1 or 2)
1700	No	Yes	1
1740	Yes	Yes	1
2600	No	Yes	1
2700	Yes	Yes	2
4600	Yes	Yes	2
5000	Yes	Yes	2

You can install two SA cards, two Hardware Accelerator cards, or one of each type of card. The SA card uses one green LED; the Hardware Accelerator card does not use LEDs.

VPN Router SA card

The SA card uses a single Hifn 7854 chip for encryption and compression and uses 64 MB of onboard RAM. The SA card supports Advanced Encryption Standard (AES)-128 cryptography with Secure Hash Algorithm (SHA)-1 authentication and triple Data Encryption Standard (DES) cryptography with either Message Digest 5 (MD5) or SHA-1 authentication on packets flowing over preestablished IPsec tunnels.

The SA card supports Internet Security Association and Key Management Protocol (ISAKMP) and encryption key generation for Groups 1, 2, and 5. The card also provides random number generation.

The SA card is the successor to the Hardware Accelerator card. As well as providing support for AES, the SA card provides increased encryption throughput and improved compression performance. For example, on the SA 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. The card performs triple DES and DES cryptography, Lempel-Ziv Stac (LZS) compression, and MD5 or SHA-1 authentication on packets flowing over preestablished IPsec tunnels.

Performance considerations

Some packets expand after you apply the LZS compression algorithm. If you assign the tunnel to the Hardware Accelerator card, the packets transmit through the card a second time with compression disabled. Therefore, the router single threads compressed packets through the Hardware Accelerator card.

This consideration does not apply to the SA card. If you assign the tunnel to the SA card, the SA card automatically encrypts the uncompressed version of the packet after it detects that the compression algorithm causes the packet to expand. In this way, multiple packets queue for processing.

Support for IPsec encryption and authentication algorithms

The following table lists the IPsec encryption and authentication algorithms supported by the VPN Router Security Accelerator card and the Hardware Accelerator card. The CPU supports all algorithms.

Table 6 Support for IPsec encryption and authentication algorithms

Encryption or authentication algorithm	SA card	Hardware Accelerator card
256-AES with SHA1	No	No
128-AES with SHA1	Yes	No
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
Hashed message authentication code with SHA1 or MD5 authentication only	No	No
User Datagram Protocol wrapped	No	Yes

Accelerator card security

At startup, whenever you manually enable an accelerator card or whenever the accelerator recovers from a failure, the power-on self-test (POST) verifies the integrity of the hardware. This test validates encryption on the accelerator, MAC, and compression algorithms against the software counterparts. If POST fails, the accelerator goes offline.

Load-balancing between the CPUs and accelerator cards

After you install one or two accelerator cards, VPN Router software ensures optimal tunnel throughput by balancing tunnels across the CPUs and the accelerator cards. When a tunnel establishes or rekeys, the VPN Router 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 automatically move to a CPU. The router requests a rekey for each tunnel on the failed accelerator card.

The VPN Router automatically performs load-balancing of tunnel sessions across the accelerator cards and the main CPUs in the following ways:

- After the VPN Router boots, it assigns CPUs and the accelerator cards initial bandwidth allocations as follows:
  - The initial bandwidth assigned to a CPU is based on the CPU speed.
  - If the VPN Router uses two CPUs, the bandwidth allocation of the boot CPU is assigned a smaller value than the allocation for the nonboot CPU. Because the boot CPU handles functions other than packet processing—for example, route table updates—the router assigns tunnels more aggressively to the nonboot CPU.
  - Because the SA card provides optimal throughput and performance, the router assigns a proportionally higher bandwidth allocation to the SA card than the Hardware Accelerator card. For this reason, the router assigns tunnels more aggressively to the CSA card.
- After the establishment of a new IPsec tunnel, the VPN Router assigns the tunnel to the CPU or to the accelerator card that currently provides the largest amount of available bandwidth.
- After the router assigns a tunnel to the accelerator card or to a CPU, the amount of bandwidth on the card or CPU correspondingly decreases.



Note: After the VPN Router assigns a tunnel to an accelerator card or CPU, it does not dynamically reassign the tunnel to a new resource.

Configuring the SA and Hardware Accelerator cards

You need administrator privileges to configure an accelerator card. You can enable or disable the following components for the Security Accelerator and the Hardware Accelerator card:

- the accelerator card
- automatic recovery if the card stops running

After you enable automatic recovery and the VPN Router detects a recoverable failure, all sessions fail over and the software handles them. As soon as the accelerator card recovers, the VPN Router assigns it new tunnels and rekeyed tunnels.

To enable or disable an SA or Hardware Accelerator card

1. Choose **System, Accelerator**.

   The Hardware Accelerator window shows the operational status that the VPN Router reports for the card.

2. Click **Disable** or **Enable**.

To enable or disable automatic recovery of an SA or Hardware Accelerator card

1. Choose **System, Accelerator**.
2. Click **Configure**.
3. Select or clear **Enable Auto Recovery**.

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

You cannot configure the other fields on the Hardware Accelerator Configuration window. The following list provides a brief description of these fields:

- Description—type of accelerator card installed in the VPN Router: 7854 (Security Accelerator card) or 7811 (Hardware Accelerator card)
- Operational Status
  - Disabled

  - — Normal Operation—Active on Status, Statistics: HwAccelInfo window.
  - — Shutdown—indicates that automatic recovery is disabled. You can manually re-enable the card after the router detects a recoverable failure.
  - — Failed—indicates that the card does not operate properly. Contact Nortel Customer Support for additional information.
- Administrative Status—either Enabled or Disabled (enabled by default)
- Protocols—shows the protocols that the card supports
- Algorithms—shows the encryption and authentication protocols that the card supports (see "Support for IPsec encryption and authentication algorithms" on page 47)
- Crypto Strength—AES, 3DES, or DES (Hardware Accelerator card only), depending on the maximum key length
- Boots—number of times the card restarts
- Uptime—length of time the accelerator card runs (days:hours:minutes:seconds) since the last restart
- 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 pass and fail indications for each power-on self-test (POST) type (This field appears only if the POST fails)

Viewing statistics for accelerator cards

You can view information or statistics about an SA or Hardware Accelerator card from either of the following windows:

- Status, Statistics, Hw Accel Info
- Status, Statistics, Hw Accel Stats

You can also view the SA or Hardware Accelerator card information or statistics by running the following CLI commands:

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

Chapter 2
T1 CSU/DSU configuration

You configure the settings for a T1 with an integrated Channel Service Unit/Data Service Unit (CSU/DSU), including extended super frame (ESF) framing parameters and adding fractional T1 channels on the management windows that you access from the System, WAN Interfaces, Configure window.

The Quad T1/E1 is a four-port version of the single-port T1 card that is optional with VPN Router platforms. Use the Quad T1/E1 in situations when you need to terminate multiple T1/E1 circuits by using clear text routing at a regional or headquarters location.

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

New T1 services use ESF framing, which uses out-of-band signaling. You can configure the following ESF parameters:

- Line framing is ESF.
- Line coding is Binary 8-Zero Substitution (B8ZS).
- High-Level Data Link Control (HDLC) polarity is normal.
- The T1 service provider determines the performance report message value.

Old T1 services use super frame (SF) framing, which uses in-band signaling. You can configure the following SF parameters:

- Line framing is SF.
- Line coding is alternate mark inversion (AMI).
- HDLC polarity is inverted.
- Performance report message has a value of none as it has no effect in SF framing.

Because SF framing uses in-band signaling, the data can generate a false yellow alarm. To eliminate these false yellow alarms, set one fractional T1 channel to off. If you can use SF or ESF framing, Nortel recommends that you use ESF framing because it provides better diagnostics than SF framing and does not generate false yellow alarms.

This chapter includes the following topics:

- "Viewing status" on page 52
- "Configuring a T1 CSU/DSU" on page 52
- "56/64K CSU/DSU WAN" on page 54

Viewing status

You can configure or view the status for the T1 interface with an integrated CSU/DSU from the following menu paths:

- System, WAN
- System, WAN, Configure
- Status, Health Check
- Status, Statistics, WAN Status

Initial configuration occurs after you install the card, and you must change the configuration after you add additional fractional T1 channels.



Note: You must restart the VPN Router after you add a T1 card or after you enable a fractional T1 line.

You can configure all CSU/DSU commands through the Web interface, the serial interface, or the command line interface (CLI).

Configuring a T1 CSU/DSU

To configure a T1 CSU/DSU

1. Choose **System**, **WAN Interfaces, Configure PPP/Frame Relay**.
2. Click **Configure**.
3. Configure the **Circuit ID**. The circuit vendor specifies this field; it is useful for communicating with the vendor during troubleshooting.
4. Configure the **Clock Source**. This field specifies where to determine the timing, from the VPN Router (Internal) or from the T1 service provider (Loop). The clock source is usually configured to Loop when the router connects to a live T1 service. You use internal clocking for local or test applications only.
5. Configure the **Line Build Out** (dB) value. The line build out value is a power level based on the distance from the CSU/DSU to the VPN Router of the T1 service provider. If the CSU/DSU card is near, the VPN Router requires less power and the line build out value is lower; if the card is far away, the VPN Router requires more power and the line build out value is higher. The T1 service provider determines this setting. The valid options are
   - 0.0
   - –7.5
   - –15.0
   - –22.5
6. Configure the **Line Coding** value. This field configures the method of encoding binary digits on the line. The T1 service provider supplies the line coding value. The valid options are AMI and B8ZS.
7. Select the **HDLC Polarity**. This field determines whether the user data is inverted. You must synchronize this field with the AMI line coding; otherwise, you can 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. The valid options are Normal and Inverted.
8. Configure the **Line Framing** value. This field determines the low-level protocol between the T1 service provider and the VPN Router. Line framing determines how to encapsulate the data and handles the signaling for alarms and loopbacks. The new ESF framing uses out-of-band signaling, while the old SF framing uses in-band signaling. The T1 service provider supplies the line framing value. The valid options are SF and ESF.
9. Select the **Performance Report Message** setting. The Performance Report Message parameter is part of the ANSI T1 specification. This parameter

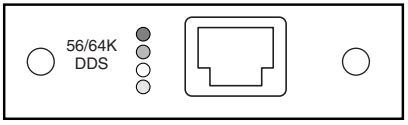
generates messages that state the number of errors for each second. This value applies to ESF framing only. Although this parameter has no effect when you use SF framing, configure it to **None** to avoid confusion. The T1 service provider supplies the Performance Report Message value. The values are None and ANSI.

10 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 add additional channels (up to 24) as growth requires. After 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 (selected) and Off (cleared).

56/64K CSU/DSU WAN

The 56/64K CSU/DSU WAN interface card uses a single RJ-48 connector that provides the signals needed to interface to network equipment. "56/64K CSU/DSU WAN interface card" on page 54 shows the 56/64K CSU/DSU WAN interface card. You can run this card on a platform supported by Version 5.00—except the VPN Router 4500.

Figure 8 56/64K CSU/DSU WAN interface card



10972EA

The connector on the 56/64K CSU/DSU WAN interface card accommodates an eight 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.

Wire the cable in accordance with the 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) transmit on a twisted pair inside the patch cord. Nortel strongly recommends that you use a factory-made patch cord.

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

- For a straight-through connection, use a standard Category 5 (Ethernet) straight-through cable.
- For a crossover connection, you cannot use a standard Category 5 crossover cable. You cannot interchange the 56/64K CSU/DSU crossover cable and the Ethernet crossover cable.

The following table 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 operates properly if pins 3, 4, 5, and 6 do not connect.



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

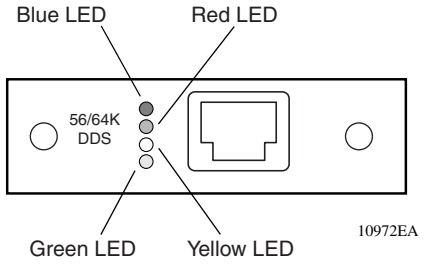
The following table provides the 56/64K CSU/DSU cable pinouts for a straight-through connection.

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
Not used	5	5 Not used
Not used	6	6 Not used
Receive tip	7	7 Receive tip
Receive ring	8	8 Receive ring

The following table shows the LEDs on the 56/64K CSU/DSU WAN interface card.

Figure 9 LEDs on the 56/64K CSU/DSU WAN interface card



The following table 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 lights after the router receives an upstream failure denoted by an alarm indication signal (AIS).
Red	Red alarm LED lights after the router detects a loss-of-signal (LOS) or out-of-frame (OOF) condition on the receive signal.
Yellow	Yellow alarm LED lights if the far-end equipment is in the red alarm condition.
Green	Normal operation.

The VPN Router provides for direct connection to Digital Data Service (DDS) with 56/64K DDS interface with an integrated CSU/DSU. This connection is data rate-selectable (56 Kb/s or 64 Kb/s) 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.

The clock source is one of the following

- Internal—clock source originates from the chip; only for 56 Kb/s data rate.
- Loop (default setting)—clock source is the network.

To configure the 56/64K DDS interface

1. Choose **System**, **WAN Interfaces, Configure PPP/Frame Relay**.
2. Click **Configure CSU/DSU**.
3. Select the **Timing Source**.
4. Select the **Data Rate**.
5. Select the **Data Inversion**.
6. Enable or Disable the **Transmit Data Monitor**.
7. Click **Apply**.

Chapter 3
ADSL and ATM configuration

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

ADSL is asymmetric in that most of the two-way bandwidth allocates 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: After ADSL receives large numbers of packets from a File Transfer Protocol (FTP) session, the Point-to-Point Protocol (PPP) keep-alive packets occasionally experience a delay. To alleviate this issue, reset the PPP parameter.

This chapter includes the following topics:

- "ADSL WAN interface cards" on page 59
- "ADSL and ATM configuration" on page 60

ADSL WAN interface cards

The VPN Router 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 the following line protocols:
  - American National Standards Institute (ANSI) Discrete Multi-tone (DMT) over analog or POTS (specified in ANSI T1.413)

  - — G.lite over analog/POTS (specified in ITU-T G.992.2)
  - — G.DMT Annex A over analog or 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 or Integrated Services Digital Network (ISDN) Basic Rate Interface (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.

AAL5 frames encapsulate IP packets. The ATM VC supports the following AAL5 encapsulation types:

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

Each ATM VC uses an IP address (static or dynamic) and an associated virtual path identifier (VPI) or virtual circuit identifier (VCI).

ADSL and ATM configuration

This section provides instructions to configure ADSL and ATM.

Configuring an ATM interface

To configure an ATM interface

1. Choose **System, ATM**.

   The ATM Interfaces window appears.

2. Select the interface that you want to configure, and click **Configure**.

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

4 In the **Description** box, type a description for the physical interface (this field is optional).

5 In the **Circuit ID** box, type the circuit identifier of the vendor (the telephone company supplies this ID). Use this ID for troubleshooting.

6 From the **Interface Filter** list, select an existing filter or click **New Interface Filter** to create a new one. The default filter is deny all.

7 From the **ADSL Line Protocol** list, select the appropriate line protocol.

The line protocol must be compatible with the I/O type you specify at the top of the window. For example, if the I/O type is Annex A, you cannot set the ADSL line protocol to G.dmt Annex B.

8 Click **OK** or **Apply**.

Configuring an ATM virtual circuit

You can configure one ATM VC on an ADSL interface. The VC uses AAL5 to encapsulate IP packets within AAL5 frames. Each ATM VC uses an IP address and an associated VPI and VCI.

To configure an ATM virtual circuit

1 Select **System, ATM**.

The ATM Interfaces window appears.

2 Select the interface that you want to configure and click **Configure**.

3 Click **Configure Virtual Circuit**.

4 In the **Description** box, type a description for the VC (optional).

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

6 From the **Protocol** list, select the encapsulation protocol for the VC: MPoA routed (the default value), PPPoA, or PPPoEoA.

If you configure the protocol to PPPoA or PPPoEoA, several new fields appear (for example, the MAC CRC field appears only when the protocol is PPPoEoA.)

7 If you configure the protocol to PPPoEoA, configure the **MAC CRC** option to include or exclude the Ethernet MAC CRC in MPoA bridged frames.

8 If you configure the protocol to PPPoA or PPPoEoA, perform the following steps:

   a Enable or disable **Use Default Route**. The default is enabled.

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

   b In the **Local IP Address Source** box, specify whether this VC dynamically acquires the IP address or whether you type an address and subnet mask.

9 If you configure the protocol to MPoA(R), perform the following steps:

   a Type a static IP address and mask.

   b Configure the protocol option to **LLC**.

10 Select a **protocol** option: VC-MUX or LLC.

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

11 Configure the **Interface Type** to private or public. The default value is private.

12 If you configure 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.

13 If you configure the Remote IP Address Source option to **Specify IP Address**, type the IP address for the remote peer in the Remote IP Address field.

14 In the **VPI** and **VCI** boxes, type the virtual path identifier and the virtual circuit identifier for this VC.

15 Click **OK** or **Apply**.

If you configure the protocol to PPPoA, see the following sections:

- “Configuring PPP authentication” on page 63
- “Configuring PPP advanced parameters” on page 64

If you configure the protocol to PPPoEoA, you can also configure PPPoE parameters (see “Configuring PPPoE parameters” on page 65).

Configuring PPP authentication

If you configure the protocol on the Configure VC window to PPPoA or PPPoEoA, you can configure PPP authentication parameters.

To configure PPP authentication parameters

1. Choose **System, ATM**.

   The ATM Interfaces window appears.

2. Select the interface that you want to configure, and then click **Configure**.
3. Click **Configure Virtual Circuit**.
4. In the Configure PPP Settings section, click **Authentication Settings**.
5. Select **PAP negotiation**, **CHAP negotiation**, or both.

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

6. In the **UID** and **Password** boxes, type the user ID and password for PAP and CHAP authentication.
7. In the **Confirm** box, retype the password.
8. Click **OK**.

   You return to the Configure VC window.

To configure PPP advanced parameters, see “Configuring PPP advanced parameters".

To configure PPPoE parameters, see “Configuring PPPoE parameters” on page 65.

Configuring PPP advanced parameters

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

To configure PPP advanced parameters

1. Choose **System, ATM**.

   The ATM Interfaces window appears.

2. Select the interface that you want to configure, and then click **Configure**.
3. Click **Configure Virtual Circuit**.
4. In the Configure PPP Settings section, click **Advanced Settings**.
5. Configure **Link Control Protocol** (LCP) parameters as follows: The LCP negotiates various link options between the VPN Router and the ISP.
   a. Select **Address Control Field Compression** to compress the address control box in the packet header and reduce packet overhead by 1 byte.
   b. Select **Protocol Field Compression** to compress the protocol box in the packet header and reduce packet overhead by 1 byte.
   c. Type a value for the **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 to 255 (0 disables this option).
   d. Type the number of seconds between LCP echo requests in the **Echo Interval** box. You can use this interval with the echo request threshold to determine whether the link disconnects. Type an integer from 0 to 255.
6. Configure **IP Control Protocol** (IPCP) settings as follows: The IPCP specifies certain dial-up networking attributes, such as address assignment and configuration of Domain Name System (DNS) or Windows Internet Naming Service (WINS) server settings.
   a. Select **VJ Negotiation** to enable Van Jacobson (VJ) compression negotiation. VJ compression compresses the TCP/IP header fields on individual TCP/IP flows and reduces packet overhead.
   b. Select **VJ Connect ID Compression Negotiation** 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** box, specify the maximum number of concurrent VJ compressed TCP/IP flows. Type an integer from 2 to 16 (the default is 8).

7 Click **OK**.

You return to the Configure VC window.

To configure PPP authentication parameters, see "Configuring PPP authentication" on page 63.

To configure PPPoE parameters, see "Configuring PPPoE parameters".

Configuring PPPoE parameters

If you configure the protocol to PPPoEoA, you can configure PPPoE parameters.

To configure PPPoE parameters

1 Choose **System, ATM**.

The ATM Interfaces window appears.

2 Select the interface that you want to configure, and then click **Configure**.

3 Click **Configure Virtual Circuit**.

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

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

6 If you enabled the On Demand parameter, in the **Idle Timeout** box, type the number of minutes that can elapse with no activity before the interface terminates the on-demand connection.

7 In the **Cost** box, configure the cost of the PPPoE interface.

8 In the **Service Name** box, specify a service name associated with this PPPoE interface. Enter a description of the PPPoE connection.

9 Enable or disable **TCP MSS**.

PPPoE enforces a maximum transmission unit (MTU) size of 1492 bytes. For this reason, all PCs that connect to the VPN Router must also 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 "Interface MTU and TCP MSS configuration" on page 30.

10 Click **OK**.

You return to the Configure VC window.

Chapter 4
PPP configuration

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

- encapsulation for multiprotocol datagrams
- Link Control Protocol (LCP) to establish, configure, and test the data-link connection
- Network Control Protocols (NCPs) to establish and configure various network-layer protocols

For more information, see RFC 1661. This chapter includes the following topic:

- "Configuring PPP settings" on page 67

Configuring PPP settings

To configure PPP settings

1. Choose **System**, **WAN**.

   The WAN Interfaces window appears.

2. Select the interface that you want to configure, and then click **Configure**.
3. (Optional) Type a 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 window appears. Information about the interface appears at the top of the window, including the slot number and the interface number.

8 Enter a description.

9 Enter the IP address.

10 Specify the remote IP address setting.

11 Select either **public** or **private** for the interface type.

12 Click **PPP Authentication settings** to configure the PPP authentication settings for this interface, including local Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP) user IDs and passwords.

The WAN Interfaces > Configure PPP > Authentication window appears. To configure a Channel Service Unit/Data Service Unit (CSU/DSU), see Chapter 2, “T1 CSU/DSU configuration,” on page 51.

13 Select the appropriate authentication type, PAP or CHAP, as required by the ISP. If you do not require authentication, select **None**.

14 The ISP that provides the WAN connection to the VPN Router can 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 window.

15 You can optionally click **Configure PPP Advanced Settings** to further configure the PPP interface, including LCP and IP Control Protocol (IPCP) settings.

16 The LCP session negotiates the following link options between the VPN Router and the ISP:

- Enable **Address Control Field Compression** and reduce packet overhead by one byte. The default is disabled.
- Enable **Protocol Field Compression** and reduce packet overhead by one byte. The default is disabled.
- Configure the **Echo Fault Threshold** to configure the number of times LCP attempts an Echo request without receiving a reply. The link drops after the number of echo requests exceeds the number in the Echo Fault Threshold box. The range is 0 to 255 (0 indicates disabled); the default is 1.

- Configure the **Echo Interval** in seconds. Use this interval with the value of the Echo Fault Threshold box to determine if a link disconnects. The range is 0 to 255; the default is 0 (disabled).

17 You use the IPCP settings 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.

Enable **Van Jacobson (VJ) Compression Negotiation** to compress the TCP/IP header fields on an individual TCP/IP flow basis and reduce packet overhead. The default is disabled.

Enable **Van Jacobson (VJ) Connect ID Compression** to further reduce the VJ compression header and increase packet transmission performance. Use this option only when a single TCP/IP flow is active at one time over the link. The default is disabled.

Configure the **VJ Max Slots**. This option 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 window, select **Interface Debug**, if needed. This option sends PPP control packets to the Event log. This option is a Nortel internal customer support utility that diagnoses and troubleshoots WAN interface problems.

19 Click **OK** to save the settings.

Chapter 5
PPPoE configuration

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

This chapter includes the following topics:

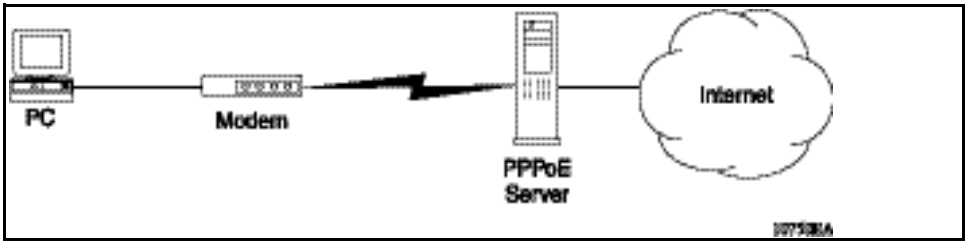
- "Overview" on page 71
- "Configuring PPPoE settings" on page 73

Overview

With Digital Subscriber Line (DSL) and cable modems, where a personal computer connects to the Ethernet interface of the modem, Internet service providers (ISP) 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.

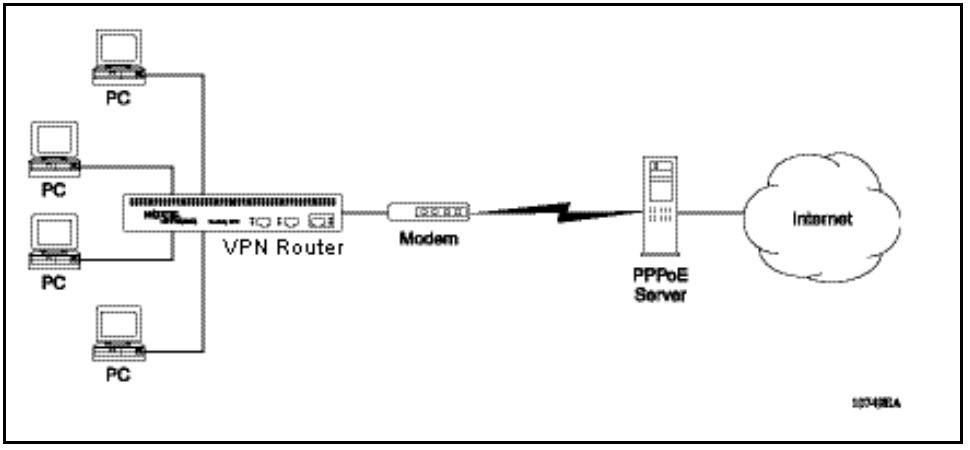
PPPoE can use two configurations: PPPoE for the single user "PPPoE for single user" on page 72 or PPPoE on a local network. For locations with single computers, the PPPoE client runs on the computer and reaches the PPPoE server through the Ethernet connection through the DSL modem. The DSL modem then forwards the packets to the WAN interface without interpreting the PPPoE packets. The PPPoE packets reach the destination (PPPoE server) for further handling. This implementation complies with RFC 2516.

Figure 10 PPPoE for single user



The second configuration is usually in multicomputer locations, small offices, or branch offices where the entire LAN connects to the Internet through DSL or cable modem. In this case, either the modem or the VPN Router acts as a PPPoE client. "PPPoE on a local network" on page 72 shows how a VPN Router 1100 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 11 PPPoE on a local network



The following list identifies the restrictions of PPPoE:

- PPPoE maximum transmission unit (MTU) limitation of 1492 bytes. (Reset PC from MTU=1500 to MTU=1492)
- must configure the appropriate filter (deny all by default)
- PPPoE changes do not dynamically apply (must restart the service for edits)
- must exist on a public Ethernet interface
- must configure the Administrative State to enabled (disabled by default)

- can support only one session on one interface
- cannot use dynamic routing on PPPoE interfaces (unless tunneling)



Note: Due to Domain Name System (DNS)-Ping packet traffic on the PPPoE on-demand link, the administrative state does not go into IDLE/TIMEOUT state. While performing a health check on the DNS servers, the router sends out DNS-Ping packet traffic, which sends traffic over the PPPoE link if a DNS server exists and is reachable over this link. This process keeps the PPPoE link up. To check the status of the DNS servers, use the HealthCheck and the System, Identity windows. The Alert LED does not light if a DNS Server Alert exists.

Configuring PPPoE settings

To configure PPPoE

1 Choose **System**, **LAN**.

The LAN Interfaces window appears.

2 Select a public interface, select **PPPoE** from the **Protocol** list, and click **Apply**.

The LAN Interfaces > Add PPPoE Interface window appears.

3 Select **permit all** for the **Interface Filter**, and then click **OK**.

4 From the **LAN Interfaces** window, click **Edit** for the PPPoE interface.

The LAN Interface > Edit PPPoE Interface window appears.

5 On the **Edit PPPoE Interface** window, perform the following steps:

a For **Administrative State**, select **Enabled**.

b For **On Demand,** select **Enabled**. The default is disabled (nailed PPPoE service).

c In the **Idle Timeout** box, type a value within the range specified on the window to specify the minutes of inactivity after which to tear down the connection.

d In the **Cost** box, type a value within the range specified on the window to indicate the cost of the connection.

e (Optional) Type a service name that describes the connection. Use this box only if the ISP provides a service name.

f (Optional) Select **Use Default Route** to enable the default route for this interface.

g Type the local IP address, which is dynamically assigned to the interface. The default 0.0.0.0 indicates that the address dynamically comes from the ISP server.

h (Optional) For **TCP MSS Option**, select Enabled to enable TCP MSS clamping. The default is disabled.

i (Optional) For **TCP MSS Value**, specify the maximum segment size (MSS) of the largest TCP packet (in bytes) that can be sent.

6 For **PPP Authentication Settings**, click **Configure**. The default authentication is None.

The PPP Local Authentication window appears.

7 Perform the following steps:

a Select an authentication method, either **PAP Negotiation** or **CHAP Negotiation**.

b Type the user ID.

c Type and confirm the password.

d Click **OK**.

8 For **PPP Advanced Settings**, click **Configure**.

The PPP Advanced window appears.

9 Perform the following steps:

a Configure the appropriate Link Control Protocol (LCP) and IP Control Protocol (IPCP) options.

b Select **Interface Debug** to send PPP control packets to the Event log. Nortel Technical Support uses this log to diagnose and troubleshoot interface problems.

c Click **OK**.

Chapter 6
Frame Relay configuration

Frame Relay (FR) is a high-speed, packet-switching WAN protocol that connects geographically dispersed LANs. Public network providers offer Frame Relay; however, private organizations can acquire and manage their own Frame Relay networks. You can configure Frame Relay on a WAN interface on the VPN Router.

This chapter includes the following topics:

- "Introduction" on page 75
- "Permanent virtual circuits" on page 78
- "RFC 1490" on page 78
- "Traffic shaping" on page 79
- "Overview of Frame Relay configuration" on page 81
- "Configuring Frame Relay settings" on page 82
- "Configuring FRF.9" on page 85
- "Configuring FRF.12" on page 86
- "Frame Relay Forwarding Priority to a VC" on page 90
- "Frame Relay monitoring" on page 93

Introduction

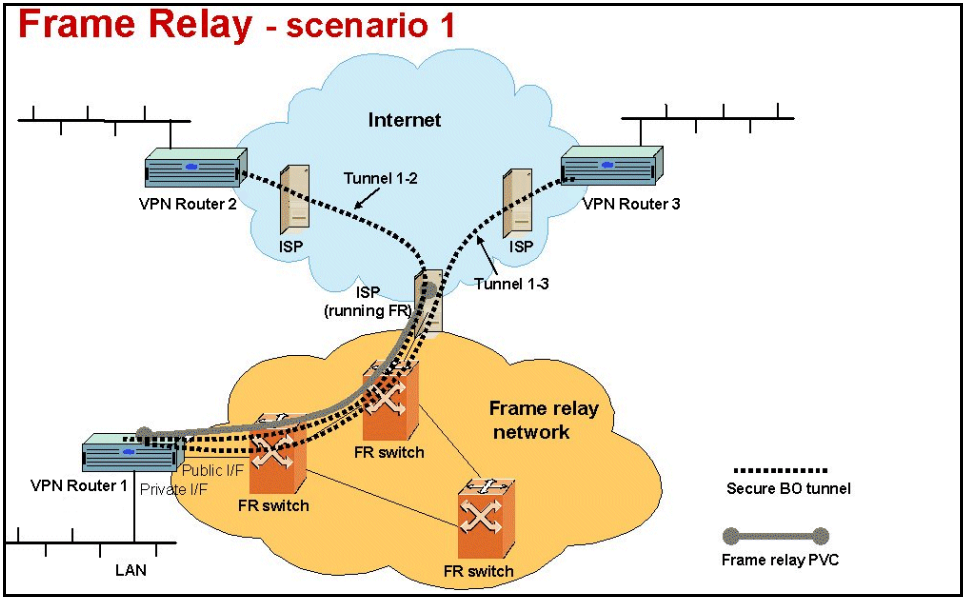
Frame Relay is a connection-oriented protocol and relies on end-to-end paths between devices that connect across the network. Frame Relay implements these connections using permanent virtual circuits (PVC) or switched virtual circuits (SVC). VPN Router supports PVCs.

The VPN Router functions as a Frame Relay access device (FRAD) in a Frame Relay network. In Frame Relay, multiple virtual point-to-point connections (virtual circuits) exist on a single physical interface. Each virtual circuit uses a unique local IP and remote IP point-to-point connection.

Each PVC on the VPN Router is a separate IP address. With Frame Relay, the router assigns IP addresses to virtual circuits and associates the virtual circuit with a physical interface. Multiple PVCs can exist on a single physical interface and, hence, multiple IP interfaces on a single physical interface. In PPP, only a single IP address exists for each physical interface.

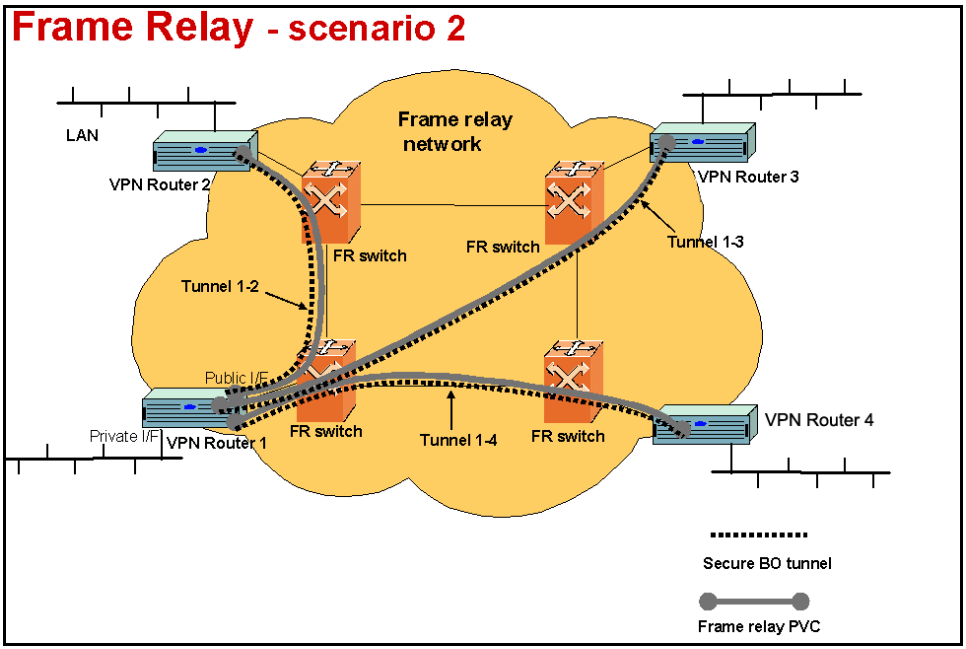
"Frame Relay single public interface to ISP" on page 76 shows a single public interface to an Internet service provider (ISP). In this scenario, a Frame Relay PVC exists between VPN Router 1 and the ISP for VPN Router 2 and 3. The PVC replaces a dedicated Point-to-Point Protocol (PPP) connection. The Frame Relay PVC is generally less expensive than the dedicated PPP link.

Figure 12 Frame Relay single public interface to ISP



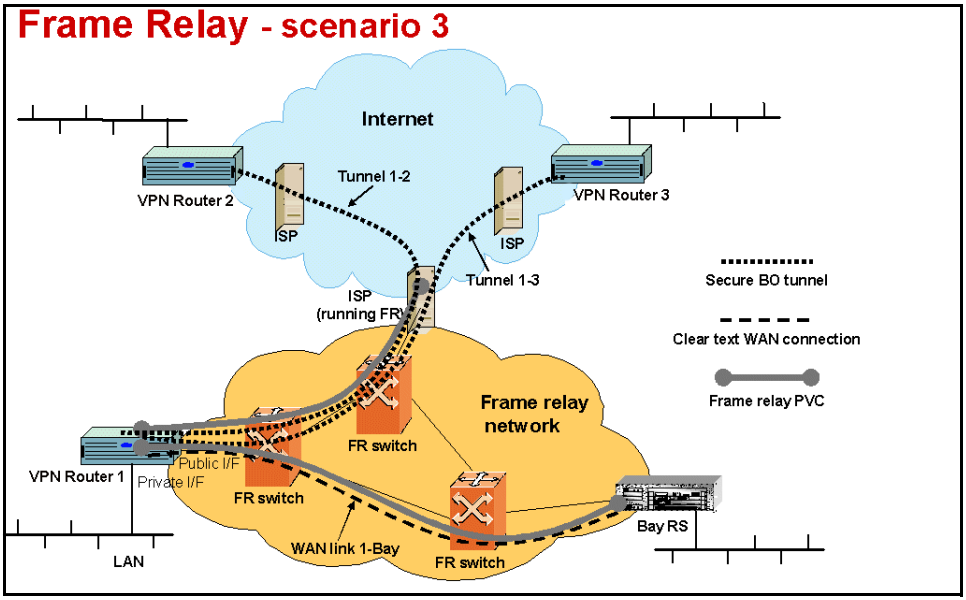
"Frame Relay multiple public interfaces" on page 77 shows three Frame Relay PVCs (logical connections) that run over a single interface on VPN Router 1. These logical connections are not possible using PPP. The connections in this example need not be branch office tunnels. The connections can also be unsecure, clear text connections over the secure Frame Relay private network.

Figure 13 Frame Relay multiple public interfaces



"Gateway between Frame Relay network and VPN network" on page 78 shows a gateway between an existing Frame Relay network and a new IP VPN network. VPN Router 1 acts as a gateway between the newer unsecure public network (Internet) and the older, secure Frame Relay private network. VPN Router 1 connects to VPN Router 2 and 3 using a branch office tunnel over a Frame Relay PVC. VPN Router 1 also connects 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 14 Gateway between Frame Relay network and VPN network



Permanent virtual circuits

A PVC is a dedicated logical path that connects two devices over a network. If you configure a PVC, it 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 disconnect after data travels across the network. 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 (CIR) enforcement and quality of service are the major components of Nortel traffic shaping. CCITT I.370 defines the traffic shaping parameters.

Committed information rate

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

If you configure 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, configure both the throughput (which is the CIR) and the committed burst (B_c) to 0, and configure the excess burst (B_e) to a value greater than 0. For more information about burst rates, see "Committed burst rate and excess burst rate".

• Maximum CIR: Make sure the maximum CIR is not greater than the speed of the access line on the slow end of a virtual circuit. In a big pipe and little pipe topology, likely CIRs at the remote sites are 32 Kb/s, 56 Kb/s, or 64 Kb/s. If you configure CIRs for these virtual circuits at the central site, 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 restricts the speed of outbound traffic to a rate no faster than the CIR. CIR 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 by shutting down the virtual circuit, or by limiting the traffic.

Committed burst rate and excess burst rate

American National Standards Institute (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 transmits over a specified time interval (T_c) when no congestion occurs. The excess burst size (B_e) defines the number of extra bits that the network attempts to send over the T_c when no congestion occurs. You configure both the B_c and the B_e values.

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

Traffic shaping configuration notes

Use traffic shaping at central offices to prevent the big pipe from sending too much data too quickly to remote sites with little pipes. Use this concept when you decide how to configure traffic shaping.

Consider the following when you configure traffic shaping:

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

  If, however, you send 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 the configuration of B_c is equal to 1/4 of the CIR yields a value lower than the packet size, configure the B_c to 1/3 to 1/2 of the CIR.

  For example, a typical Trivial File Transfer Protocol (TFTP) frame is 548 bytes. If the CIR is 16 000 bits, the B_c configured according to the 1/4 guideline is 4000 bits, or 500 bytes, which is not large enough to accommodate a TFTP frame.

  If you configure the B_c to 16 000/2, or 1/2 CIR, the result is 8000 bits, or a packet size of 1000 bytes, which works, but can result in excessive queuing because the T_c is 1/2 second. If you configure the B_c to 16 000/3, or 1/3 CIR, the result is a B_c of 5333 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 number increases constantly or dramatically, increase the value of B_c in small increments.

Overview of Frame Relay configuration

You can configure each physical WAN interface to run either PPP or Frame Relay as a link protocol, but not both simultaneously. However, in a VPN Router with multiple WAN interfaces, one interface can run PPP and another interface can run Frame Relay. PPP is the default link protocol.

Frame Relay on the VPN Router acts as a user to network interface (UNI) device; the router does not support network to network interface (NNI). You can configure each WAN link to run either PPP (the default) or Frame Relay. Each Frame Relay link can be a switched (default) or a direct connection.

Note: The WANic 700 HSSI does not support switched Frame Relay on the DigiLink, model DL3100.

Configure the gateway type for each link. The possible settings are ITU-T and ANSI, which determine the Local Management Interface (LMI) format and the Forward Explicit Congestion Notification (FECN) and Backward Explicit Congestion Notification (BECN) processing. You can configure the LMI poll interval timer and poll interval counter after you enable LMI.

Note: The VPN Router supports only approximately 1500-byte (Ethernet maximum) frames. The router discards larger frames as excessively long frames; this is an implementation limitation, not a protocol limitation.

Configuring Frame Relay settings

To configure Frame Relay settings

1 Choose **System**, **WAN**.

The WAN Interfaces window appears.

2 Select the interface that you want to configure, and then click **Configure**.

3 (Optional) Type a description of the interface in the **Description** box.

4 (Optional) Type a unique text name in the **Circuit ID** box. The circuit vendor specifies a character string, which you can use when you communicate with the vendor for troubleshooting.

Note: Although the T1/E1 MIB (RFC 1406) defines the circuit ID, it applies to most WAN connections; therefore, you configure it at the interface level.

5 Select an **Interface Filter** from the list.

6 Select **FR** from the **Protocol** list. The default is PPP.



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

7 Click **Configure**.

8 Enable **Debug** to log packet information in the Event Log.

9 Choose the connection type, either **switched** or **direct**.

To connect to a Frame Relay, configure the connection type to switched. In this mode, you can configure the gateway type. The gateway type determines both the LMI format and the FECN and BECN processing.

You can directly connect two VPN Routers without an intervening Frame Relay gateway through the interface connection type direct. After you select direct mode, you disable LMI messages and the router does not perform FECN and BECN processing. FRF 1.1 defines the UNI.

10 Select the gateway type: **ITU-T**, **ANSI**, or **ILMI**.

11 Type one of the following values for the LMI poll interval timer:

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

The gateway type parameter determines the LMI type when the physical interface is in the switched mode. This parameter also determines the FECN and BECN processing. LMI is disabled when the physical interface is in the direct mode.

12 Type one of the following values for the LMI poll interval counter.

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

13 Click **Configure Virtual Circuit**.

14 Type a **description**. This description is the same user-entered text description that existing physical interfaces use.

15 Select the state for the VC. This state is the same as the physical interface enable or disable. Four values exist:

- **TRUE**
- **TRUE_DEBUG**
- **FALSE**
- **FALSE_DEBUG**

The _DEBUG values cause the packet to appear in the event log.

16 Select the **VC protocol**, **IP MPoFR**.

17 Specify the Local IP address (static).

18 Select the interface. This interface is the same public or private (untrusted or trusted) parameter that existing physical interfaces use.

19 Specify the remote IP address (static).

20 Type a value for **DLCI**.

21 Type a value for **CIR**. The supported range is 0 to the maximum line speed. The default is 0.

The VPN Router supports traffic shaping and congestion control as defined in CCITT I.370. Configure the traffic shaping parameters, CIR, B_c, and B_e, for each VC. The router supports FECN and BECN processing as defined in ANSI T1.618 Annex A. The DE flag is not configured. The router does not support CLLM.

22 Type a value for $\mathbf{B_c}$. The supported range is 0 to the maximum line speed. The default is 0.

23 Type a value for $\mathbf{B_e}$. The supported range is 0 to the maximum line speed. The default is the maximum line speed.

24 Click **Statistics** to view collected statistics for the interface.

25 Click **Add** to create and define additional PVCs on the interface.

Configuring FRF.9

Frame Relay compression, as offered by FRF.9, provides Layer 2 type compression. If the router transports encrypted traffic over a Frame Relay link, you need not run FRF.9 compression because of the nature of encryption and compression. Compression finds patterns in data to remove 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 difficult for anyone eavesdropping to decipher the data.

The VPN Router Frame Relay software supports FR data compression as defined in FRF.9. Each FR virtual circuit can enable or disable FRF.9 compression, with disabled as the default. The VPN Router supports only the Lempel Ziv Stac (LZS) compression algorithm.

If you enable FRF.9, the VPN Router 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, the router does not perform data compression on the virtual circuit (VC). Three valid combinations of the FRF.9 compression and FRF.9 algorithm fields exist, as shown in "FRF.9 compression and algorithm fields" on page 85. 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. Choose **System, WAN Interfaces, Configure, FR, VC**.
2. Select **Use Compression** to enable FRF.9.
3. Click **OK**.

Configuring FRF.12

FRF.12 fragmentation sends (interleaves) high-priority packets of one VC between fragments of lower priorities of the same VC or other VCs "Interleave values" on page 87.

Note: For full functionality, you must enable FRF.12 for the PVC, and you must enable interleaving for the associated interface. Enabling or disabling interleaving does not cause a circuit restart.

FRF.12 fragmentation is a configurable, non-negotiable option for a PVC "Fragmentation value" on page 87. Enabling or disabling FRF.12 fragmentation causes a circuit restart. You must configure both sides of the circuit for FRF.12 fragmentation.

The router supports FRF.12 for speeds less than 1 MB.

Although FRF.12 does not explicitly define an interleaving scheme, this fragmentation sends (interleaves) high-priority packets of one VC between fragments of lower priorities of the same VC or other VCs.

You need fragmentation and interleaving to ensure high voice quality for Voice over IP (VoIP) packets when the router transmits voice and data over a WAN. You require fragmentation only over WANs that operate with speeds less than 1 Mb/s. Fragmentation and interleaving ensures that large data packets do not introduce variable delay (jitter) to the small 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, as shown in the following 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 router implements FRF.12 fragmentation within the Frame Relay stack, and implements the associated interleaving within Quality of Service (QoS) queues. Interleaving uses two classes of packets, voice and nonvoice, and no reordering of packets occurs 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 or disable interleaving
Interleaved Packets	False	UINT32	RW	0–4294967295	0	The number of interleaved packets

Table 12 Fragmentation value

OM member name	Index	Type	Access	Values	Default values	Description
Fragmentation	False	Enumeration	RW	0 or 1	0	Enable or disable fragmentation
FragSize	False	Integer	RW	40–800 (no fragmentation)	80	Fragment size in bytes

To configure FRF.12

1 Choose **System**, **WAN**.

The WAN Interfaces window appears.

2 Select the interface that you want to configure, and then click **Configure**.

3 (Optional) Type a description of the interface in the **Description** box.

4 (Optional) Type a unique text name in the **Circuit ID** box. The circuit vendor specifies this character string, which you can use when you communicate with the vendor for troubleshooting.

Note: Although the T1/E1 MIB (RFC 1406) defines the circuit ID, it applies to most WAN connections; therefore, configure it at the interface level.

5 Select an **Interface Filter** from the list.

6 Select **FR** from the **Protocol** list. The default is PPP.

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

7 Click **Configure**.

8 Enable **Debug** to log packet information in the event log.

9 Choose the connection type: **switched** or **direct**.

10 Select the gateway type: **ITU-T**, **ANSI**, or **ILMI**.

11 Type one of the following values for the LMI poll interval timer:

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

12 Type one of the following values for the LMI poll interval counter.

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

13 Enable **Use Interleaving**.

14 Click **OK**.

15 Click **Configure Virtual Circuit**.

16 Type a description. This description is the same user-entered text description that existing physical interfaces use.

17 Select the state for the VC. This state is the same as the physical interface enable or disable. Four values exist:

- **TRUE**
- **TRUE_DEBUG**
- **FALSE**
- **FALSE_DEBUG**

The _DEBUG values cause the packet to appear in the event log.

18 Select the **VC protocol**, **IP MPoFR**.

19 Specify the Local IP address (static).

20 Select the interface. This interface is the same public or private (untrusted or trusted) parameter that existing physical interfaces use.

21 Specify the remote IP address (static).

22 For **Use Fragmentation** select **True**.

23 In the **Fragmentation Size** box, type fragmentation size values "Fragmentation value" on page 87. Configure the fragment size the same as, or as close to, the size of the voice packet size to optimize voice performance.

24 Type a value for **DLCI**.

25 Type a value for **CIR**. The supported range is 0 to the maximum line speed. The default is 0.

26 Type a value for $\mathbf{B_c}$. The supported range is 0 to the maximum line speed. The default is 0.

27 Type a value for $\mathbf{B_e}$. The supported range is 0 to the maximum line speed. The default is the maximum line speed.

28 Click **Statistics** to view collected statistics for the interface.

29 Click **Add** to create and define additional PVCs on the interface.

30 Click **OK**.

Frame Relay Forwarding Priority to a VC

The FR Forwarding Priority to a VC provides a priority queuing scheme where prioritization is based on the destination of a permanent virtual circuit (PVC) rather than on the destination of the packet contents. For example, you can use FR Forwarding Priority to a VC to configure a PVC that transports voice traffic to have absolute priority over a PVC that transports signaling traffic, and a PVC that transports signaling traffic to have absolute priority over a PVC that transports data. FR Forwarding Priority to a VC provides three levels of priority: Low (1), Medium (2), and High (3).

The router examines the Frame Relay packet at the interface for the data link connection identifier (DLCI) value. The packet then transmits to the correct priority queue based on the priority level you configure for that DLCI.

Assigning priority to a PVC within a map class

You assign priority to a PVC within a Frame Relay map class. The router classifies all PVCs that use or inherit that map class according to the priority you configure.

To add a map class for a PVC

1 Choose **Profiles, Map Class**.

The Map Class window appears.

2 In the **New Map Class Name** box, type the name of the new map class.

3 Click **Add**.

To edit a Map Class associated with a PVC

1 Choose **Profiles, Map Class**.

The Map Class window appears.

2 Select a Map Class Name, and then click **Edit**.

3 Type a value for the following:

- **CIR**: The supported range is 0 to the maximum line speed. The default is 1.

- **Bc**: The supported range is 0 to the maximum line speed. The default is 0.
- **Be** The supported range is 0 to the maximum line speed. The default is the maximum line speed.



Note: If a PVC does not use an associated map class, or if the map class has no explicitly configured priority, the packets on that PVC queue on the default **none** priority forwarding.

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

4 Click **OK**.

To delete a Map Class

1 Choose **Profiles, Map Class**.

The Map Class window appears.

2 Select a Map Class name, and then click **Delete**.

A confirmation window appears.

3 Click **OK**.

Configuring VC with a map class

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

To use map class in VC

1 Choose **System, WAN, Configure, Frame Relay, Virtual Circuits**.

2 Perform the following steps:

a For a VC with fragmentation disabled

- **Virtual Circuits**: Select the virtual circuit you want to configure from the list.
- **Description**: Type an optional description.
- **State**: Select the state for the virtual circuit.
- **VC Protocol**: Select **MPoFR** (IETF RFC 2427).
- **Interface Type**: Select the interface type, either public or private.
- **Local IP Address**: Type the local IP address for the virtual circuit.
- **Subnet Mask**: Type a subnet address.
- **Remote IP Address Source**: Select the remote IP source.
- **Remote IP Address**: Type the remote IP address for the virtual circuit.
- **Map Class**: Select a Map Class.
- **Use Compression**: Select to use compressions.
- **Use Fragmentation**: Select **True** or **False**. Select True to initiate fragmentation.
- **DLCI**: Type a value for the DLCI parameter.

b For a VC using fragmentation

- **Local IP Address**: Type the local IP address for the virtual circuit.
- **Subnet Mask**: Type a subnet address.
- **Remote IP Address Source**: Select the remote IP source from the box.
- **Remote IP Address**: Type 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**: Select to use compressions.
- **Use Fragmentation**: Select TRUE.
- **Fragment Size**: The supported range is 40 to 800. The default is 80.
- **CIR**: The supported range is 0 to the maximum line speed. The default is 0.
- **Bc**: The supported range is 0 to the maximum line speed. The default is 0.
- **Be**: 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 replaces the first in, first out (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 the packets fragment.

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 you use different PVCs for the various traffic types.

To configure FRF.12 with FR Forwarding Priority

1. To configure the FRF.12, see "Configuring FRF.12" on page 86.
2. To configure the FRF.12 VC, see "Frame Relay Forwarding Priority to a VC" on page 90.

Frame Relay monitoring

The router collects statistics on both an individual link and an individual PVC basis and appear through Management Information Bases (MIB), the command line interface (CLI), and the Status, Health Check window. Statistics have two categories: generic statistics and frame-relay specific statistics. The generic statistics apply to a data link and report through the MIB-II ifTable (RFC 2233). All statistics are reported, even if the router does not collect them. A statistic that the router does not collect, reports as zero.

Frame Relay OM statistics

All Frame Relay-related statistics appear in the Status, Health Check window and in the CLI. A statistic that the router does not collect, reports as zero. Statistics initialize to 0 after you enable an object.

These statistics support the CLI `show interface` serial command.

IP statistics

The router collects the current individual WAN interface statistics for each PVC, not for each Frame Relay interface.

Chapter 7
Dial and Demand Services configuration

Support for asynchronous serial interfaces over the serial port and V.90 internal modem provides support for dial backup scenarios. With the serial port, use an external modem. You can use the modem as a backup service for a leased-line connection between the remote and central offices or between two branch offices. If the primary connection goes down, a circuit-switched connection establishes and traffic reroutes. After the primary link is restored, traffic redirects to the leased line, and the modem call releases.

In addition to backup services applications, you can use these interfaces to dial in to the VPN Router to manage it by using the browser-based management interface windows. You can use the serial ports to run the serial menu through a direct cable connection.

This chapter includes the following topics:

- "Dial interface configuration" on page 95
- "Demand Services" on page 102
- "Configuring Demand Services" on page 105
- "Configuring a remote network" on page 112
- "System log messages" on page 113
- "Healthcheck" on page 114

Dial interface configuration

The following procedure applies to the configuration of the VPN Router serial (COM) port as a dial interface; the procedure does not include the V.90 configuration. Except for the following issues, V.90 interface configuration is similar to the serial port configuration:

- For a V.90 interface, no port mode configuration parameter exists. Use V.90 only for the Point-to-Point Protocol (PPP).
- For a V.90 interface, no baud rate parameter exists. The V.90 interface autonegotiates baud rates down starting from 56 K 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 username and password parameters under the Demand Services configuration.

To configure dial interfaces

1 Choose **System, Dial Interface**.

The Dial Interfaces window appears.

2 Select an interface, and then click **Configure**.

The Dial Interface Configuration window appears. The port mode setting shows the current configuration.

3 Click **Modify System Settings** to change the port mode setting.

The Router Settings window appears.

4 Select one of the following port mode settings:

- PPP to support modem communications
- Serial Menu to support a direct connection through the VPN Router serial port
- Auto Detect
- AOT

5 Click **OK**.

6 Click **Return to Interface Configuration**.

7 The **Interface Filter Status** indicates if the Interface Filter is enabled and in use or disabled. Enable or disable the filter from the Services, Firewall NAT window.



Note: For the remainder of this procedure, the options that appear in this window depend on the port mode you select. For example, a serial port mode does not require a dial number.

8 Select the interface filter from the list of available filter options. If you want to create a new interface filter to apply to this dial interface, click **New Interface Filter** to access the Profiles, Filters window.

9 Type a description for the interface.

10 Provide an ID for the circuit.

11 Type the dial-out phone number.

12 Select whether the interface is **private** or **public**.

13 Click **Configure PPP** to access the Configure PPP window to configure IP addresses, if desired.

Configuring the modem

To configure the modem

1 Choose **Dial Interface, Interface Configuration**, and then click **Configure Modem**.

2 Select the desired baud rate from the list of available options.

3 Select the Auto Answer setting from the list of available options.

4 Type the initialization string that you want to use with the modem. The default is +++ATZ.

5 Type the termination string that you want to use with the modem. The default is +++ATH.

6 Type 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**.

Use this window to send commands and receive responses from the modem.

8 Enter the modem command.

9 Click **Apply**.

The modem response section shows the reply to the commands you enter.

Configuring PPP

To configure PPP

1 Click **Configure PPP**.

2 In the **Description** box, type a text description for the connection.

3 The IP local and remote address default to Accept Negotiated Address. To change the local or the remote IP addresses to specific values, select **Specify IP Address**.

4 If you select **Specify IP Address**, type the IP address and the subnet mask you want to apply to the local end of the connection.

5 Click **Authentication Settings** 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 VPN Router uses the authentication client information to dial and log on to a Dial-In Server. The VPN Router uses the authentication server settings only when a user dials into that VPN Router (the VPN Router is the dial-in server). To prevent users from dialing into a VPN Router and gaining access to the network, incoming authentication is always enabled and the default user name and password are the same as that stored in memory. You can override the default user name and password through the Authentication Server user name and password fields. Use Authentication Server less often for dial-out calls. You can use it to effect bidirectional authentication.

6 Click **Advanced Settings** to access the Advanced Settings window, which provides additional, advanced parameters for PPP.

Configuring ISDN BRI

To configure Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI)

1. Type a description for the connection in the **Description** box.
2. Provide an ID for the circuit. Specify an alphanumeric description of the circuit. You can enter up to 31 characters. If you enter a string with spaces, enclose the string in quotation marks.
3. Select the interface filter from the list of available filter options. If you want to create a new interface filter to apply to this dial interface, click **New Interface Filter** to access the Profiles, Filters window.
4. Type 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. For more information, see "Configuring PPP" on page 98.

7. Click **Configure ISDN BRI** to configure ISDN device parameters.
8. Select the Country Code for the country or continent in which this VPN Router operates. After you select this command, the VPN Router automatically loads country-specific information. Each country or continent uses a set of valid ISDN switch types.



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

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

- Auto—specifies automatic ISDN switch type detection
- Disable—disables automatic ISDN switch type detection
- On-reset—specifies automatic ISDN switch type detection after a switch reset

10 Select the switch type based on your location. The following table shows the switch types for each location.

Table 13 Switch types and locations

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

11 Enable **DOVBS** to implement data over voice bearer services (DOVBS). Use an adaptation rate of 56 Kb/s 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 Select **Auto SPID Detect** 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). The default is disabled.

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

14 Configure SPID 1 and SPID 2 to configure the service profile IDs (SPID) to register the B channel with the ISDN switch of the service provider. If you do

not use a SPID number (used mostly in North America), select **none** as the SPID number.

15 Configure Manual TEI to specify that you manually enter the terminal end-point identifier (TEI). Some switches do not support automatic TEI. The local ISDN provider issues the TEI number.

16 In the Call per TE1 box, type 1 to permit only one bearer call for each TEI or enter 2 to permit two bearer calls on a single TEI. Two bearer calls for each TEI is the default.

Configure the calls for each TEI with the CLI:

```
interfaces bri isdn calls-per-tei <1|2>
```

where

- 1 permits only one bearer call for each TEI.
- 2 permits two bearer calls on a single TEI. 2 is the default value.

17 Select **Dial Out MultiLink** to enable multilink for outgoing calls. If you enable this option, outgoing calls are a bundle of two B-channels into a 128 Kbps pipe to provide higher bandwidth on an as needed basis.

18 Select **Dial In MultiLink** to enable multilink for an incoming call. If you enable this option, an incoming call negotiates for multilink if the other side can perform multilink. If the other side cannot perform multilink, the call falls back to plain PPP, and the incoming call negotiates for no multilink.

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

20 Click **OK** to save the ISDN device settings and return to the System, Dial Interfaces, Interface Configuration window.

21 Click **Connect** to make the defined ISDN connection.

Demand Services

Demand Services starts a backup interface based on one of the following triggers: traffic, interface group, hour, unreachable route, or ping. Demand Services provides two functions: backup interfaces, formerly known as BIS, and Dial on Demand (DoD). Backup interfaces provide an automated mechanism to enable a backup interface after a designated primary connection fails. DoD activates the dial interface when traffic must route over a dial interface route, and then deactivates the dial interface when no traffic needs to route.

You can use the V.90 modem, Ethernet interface, WAN interface, or ISDN interface for backup services.



Note: The router supports only nailed-up circuits 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 after one of the following triggers occurs:

- interface group failure
- route unreachability
- ping failure
- hour

You configure Demand Services to activate an interface after the traffic trigger occurs.



Note: Configure both backup interfaces and DoD interfaces in the same demand windows. Backup interfaces and DoD interfaces work in the background, depending on the trigger that causes an event.

You assign each demand interface a priority. The router uses the priority after it encounters a contention for the dial interface. The following list identifies the demand interface status:

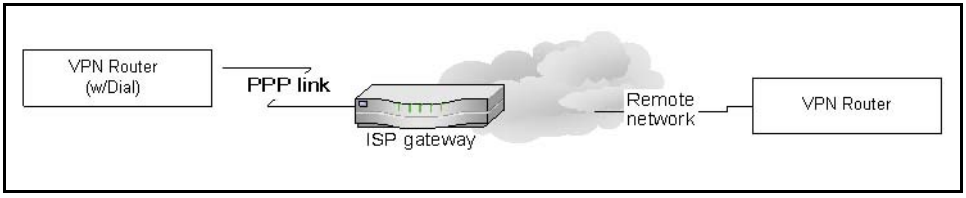
- Idle—trigger event did not occur
- Active—trigger event occurs
- Connecting—connection attempts are in progress
- Connected—connection completed, traffic flowing

Note: You can activate many demand interfaces at one time, but only the interface with the highest priority connects. The demand interface with the lowest number has the highest priority.

Demand Services runs on all VPN Router platforms that can run software Release 6.0. Demand Services is a basic feature and does not require a key.

The following figure shows a typical demand setup.

Figure 15 Typical demand setup



Dialing functionality

You can configure a maximum of three numbers to dial from the dial interface. You configure the number of times the interface retries each number before it dials the next number. You can also configure the delay between each redial.

Backup interfaces

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

After the primary connection goes down, Demand Services activates the backup interface using parameters you configure in the demand profile. The demand profile specifies the primary connection to back up, the backup interface, and other failover parameters.

You can use the V.90 modem, Ethernet interface, WAN interface, or ISDN interface for backup services. For example, you can designate one of the following interfaces as a backup interface for a primary T1 circuit on your VPN Router:

- ISDN interface
- Ethernet interface
- dial interface (V.90 modem)
- another WAN interface

You must install and configure the interface before you can use it in a backup interface configuration.



Note: The ping default route feature pings an address to ensure that the route is valid before the router adds that route to the routing table. If you turn the ping default route feature on, you can use it to validate a backup route. For more information about the ping default route feature, see *Nortel VPN Router Configuration — Routing* (NN46110-504).

Configuring subinterfaces as backup interfaces

You cannot configure the following VPN Router subinterfaces and virtual circuits (VC) as backup interfaces:

- 802.1Q VLAN subinterfaces
- Interfaces with virtual circuits such as Frame Relay, Asymmetric Digital Subscriber Line (ADSL), and Asynchronous Transfer Mode (ATM)

ABOT configuration for backup interfaces

If you configure 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 below the IPsec parameters if you use the Profiles, Branch Office, Groups, Configure menu path.

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) fails for a period of time equal to the ABOT idle timeout on the responder side. To work around this issue, lower the idle timeout value until the outcome is satisfactory. You can fine-tune the idle timeout value; if you set the idle timeout too low, it can cause unnecessary tunnel teardowns if a break in traffic occurs.

Dial on Demand

Use DoD in situations where you must connect a LAN to the Internet or to a corporate remote access service (RAS), and the only available technology occurs infrequently or is dial-up. The typical use for DoD is for remote offices that cannot access a high speed WAN technology, because of availability or cost.

The normal state of a DoD connection is down. DoD activates the dial interface after 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. Choose **Services, Demand**.

   The Demand Settings window appears.

2. Select **Enable** to globally enable Demand Services on the VPN Router.
3. Click **Add** to add a backup interface.

   The Demand Interface > Add Interface window appears.

4. Type a descriptive name for the Demand Interface profile configuration.
5. Click **OK**.
6. Select **Enabled** to enable this specific Demand profile.
7. Assign a priority for the interface.

8 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 refreshes to include parameters that you must configure for that specific type of trigger. See the following sections for information about how to configure 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. After 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 the following factors:

- Tunnels: The VPN Router detects the loss of IPsec keepalives on the tunnels included in an interface group. By default, IPsec keepalive messages send every 15 minutes, so 15 minutes can elapse before the backup interface triggers. You can reduce the IPsec keepalive interval; however, more frequent keepalive messages can burden the central site VPN Router.
- Physical interfaces: The VPN Router 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 elapses before the VPN Router discovers the failure and activates the backup interface.

To configure an Interface Group as the trigger

1. Select **Interface Group** as the trigger.
2. Select **Enabled** to enable the interface.
3. Assign a priority for the interface.
4. From the **Interface Group** list, select the interface group you want to back up.

   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.

5. From the **Physical Interface** list, select the backup interface for this Demand profile.

   Assign demand interfaces a priority level, which allows the system to create multiple definitions for a single physical interface.

6. From the **Hours** list, select a time specification to configure the Demand profile to activate only during certain days and hours. To create a new time specification, click **Add an Access Hour**.
7. Configure the dialout parameters for the backup interface. To configure dialout parameters, see "Configuring Demand dialout parameters" on page 112.
8. 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, run the **`access-hours`** command in Global Configuration mode or go to the Profiles, Hours window.

You can also use a time-of-day specification with one of the other trigger types: ping, interface group, traffic, or route unreachable. For example, you can configure Demand Services to activate after 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

1. Select **Hour** as the trigger.
2. Select **Enabled** to enable the interface.
3. Assign a priority to the interface.
4. From the **Physical Interface** list, select the backup interface for this Demand profile.
5. From the **Hours** list, select a time specification to activate this Demand profile. Click **Add an Access Hour** to create a new time specification.

   If a Demand backup connection occurs after the endpoint specified in the time specification arrives, the connection tears down.

6. Configure the dialout parameters for the backup interface, see "Configuring Demand dialout parameters" on page 112.
7. Click **OK** or **Apply**.

Configuring Demand Services with a route unreachable trigger

You can configure Demand Services to become active after a specific route times out in the routing table. To configure a route, run 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 the Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) and if alternative routes exist between endpoints. If you do not configure redundant routing paths into your network, route timeout and, therefore, Demand activation, can take several minutes to failover as the VPN Router waits for the routing protocol to determine that the route no longer exists.

For example, if you use 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 lost, the route times out in the routing table and triggers Demand Services. Several minutes can elapse, however, before Demand Services trigger.

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

To configure Demand Services with a Route Unreachable trigger

1. Select **Route Unreachable** as the trigger.
2. Select **Enabled** to enable the interface.
3. Assign a priority for the interface.
4. From the **Route** list, select the network route connection to monitor. Click **Add a Network** to define a network route and add it to the list.
5. From the **Physical Interface** list, select the backup interface for this Demand profile.
6. From the **Hours** list., select a time specification to configure the Demand profile to activate only during certain days and hours. To create a new time specification, click **Add an Access Hour**.
7. Configure the dialout parameters for the backup interface. To configure dialout parameters, see “Configuring Demand dialout parameters” on page 112.
8. Click **OK** or **Apply**.

Configuring Demand Services with a ping trigger

You can configure Demand Services to trigger when a ping to a specified destination fails. The main application for the ping trigger is DSL with attached Ethernet DSL modem. The VPN Router pings the device on the other end of the local loop, for example, a Digital Subscriber Line Access Multiplexer (DSLAM). In this way, the VPN Router determines whether a local loop failure or a failed connection exists to the Internet service provider (ISP).



Note: To successfully use the **test** button on a ping trigger demand interface, the ping destination must be unreachable during the test. Use a temporary fake ping destination address when you perform 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 VPN Router can reach the tunnel end point through the backup interface.

To configure Demand Services with Ping as the trigger

1. Select **Ping** as the trigger.
1. Select **Enabled** to enable the interface.
2. Assign a priority for the interface.
3. In the **Ping Destination Address** box, type the IP address that you want to regularly ping. This connection is the entity to back up.
4. From the **Ping Source Interface** list, select the interface on this VPN Router to use as the source of the ping.
5. In the **Ping Delay** box, type the maximum number of seconds that the VPN Router waits to receive an Internet Control Message Protocol (ICMP) reply before it determines that the connection fails and triggers the backup interface. Type an integer from 1 to 900. The default value is 5.
6. In the **Ping Retries** box, type the maximum number of ping retries allowed before the VPN Router assumes that the connection fails and triggers the backup interface. Type an integer from 1 to 6. The default value is 3.
7. From the **Physical Interface** list, select the backup interface for this Demand profile.

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

9 Configure the dialout parameters for the backup interface. To configure dialout parameters, see "Configuring Demand dialout parameters" on page 112.

10 Click **OK** or **Apply**.

Configuring Demand Services with a Traffic trigger

An inactivity timer polices the dial session to prevent up time when no traffic flows. Sometimes the line is billed for each minute of operation, so do not keep the session active unnecessarily.

The inactivity threshold timer default is 120 seconds. The timer starts after no traffic arrives for 1 second. After the timer expires, tunnels that you configure over the dial interface tear down, clear of state information, and the session terminates.

Each Demand interface remembers the 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.

Use this option to activate a line only when traffic flows.

1 Select **Traffic** as the trigger.

2 Select **Enabled** to enable the interface.

3 Assign a priority for the interface.

4 From the **Physical Interface** list, select the backup interface for this Demand profile.

5 In the **Idle Timeout** box, define the length of time the line remains idle before it shuts down. The range is 30 to 3600 seconds, with a default of 120.

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

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

8 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 user name.

5 You can assign three separate user names and passwords to each of the three phone numbers, for dialing 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 using the next number. Select a value from 1 to 10; the default is 3.

If the number of redial attempts is three, the system dials the primary number three times before it moves 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 from 1 to 500; the default is 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 window.



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

To configure a remote network

1. Choose **Services**, **Demand,** and then click **Configure** for a demand interface**.**
2. In the Remote Networks section, click **Add**.

   The Demand > Interface > Add Remote Network window appears.

3. Type the IP address.
4. Type the IP mask.
5. Type the cost. Configure the cost the same as other static routes. To configure a Demand interface, configure the cost appropriately to ensure that the connected Demand route uses a lower cost than the primary routes. The default is 10.
6. Select **Enabled** to enable the Remote Network.
7. Click **OK**.

System log messages

The system generates event log for the following situations:

- Demand line connects—identifies the connection that brought up the line.
- Demand line disconnects—indicates the reason for the disconnect:
  - — inactivity
  - — line error
  - — line drop
- other miscellaneous messages regarding Demand status.

Healthcheck

Table 14 describes the healthcheck status of each Demand interface.

Table 14 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
VPN Router Data Link Switching

Data Link Switching (DLSw) provides support for IBM System Network Architecture (SNA) protocol networking in IP networks. This includes IP encapsulation and session-oriented IP networking and support for synchronous data link control (SDLC) and logical link control (LLC) Type 2 interfaces to integrate native SNA traffic. DLSw deploys VPN Routers to support future application migration from SNA to IP in a secure IP environment.

This chapter includes the following topics:

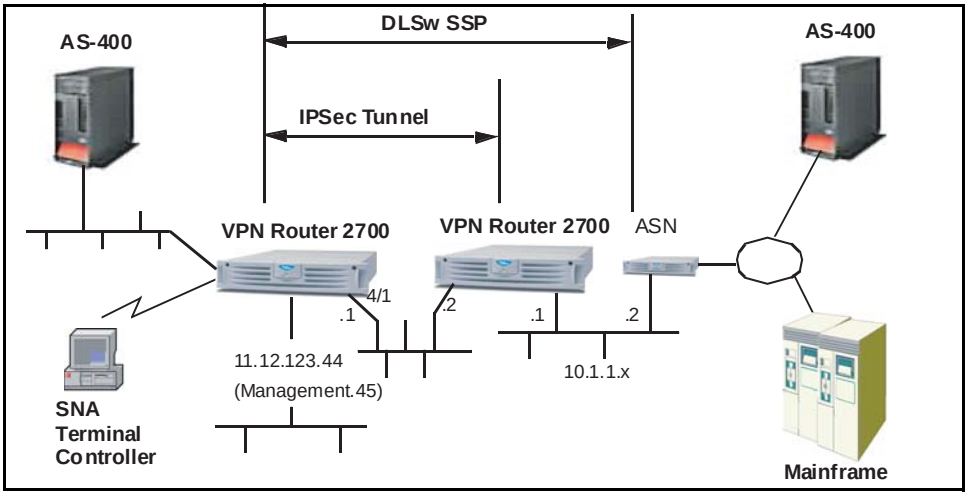
- "Introduction" on page 115
- "Supported functionality" on page 120
- "Configuring DLSw" on page 122

Introduction

DLSw is a forwarding mechanism for the IBM SNA and IBM Network Basic Input Output System (NetBIOS) protocols. DLSw does not provide full routing but provides switching at the Data Link layer and encapsulation in TCP/IP for transport over the Internet.

Because SNA and NetBios are connection-oriented protocols, the data link control procedure used on the LAN is Institute of Electrical and Electronics Engineers (IEEE) 802.2 LLC Type 2. Data link switching also accommodates SNA protocols over WAN links through the SDLC protocol, as shown in "VPN Router DLSw configuration" on page 116.

Figure 16 VPN Router DLSw configuration



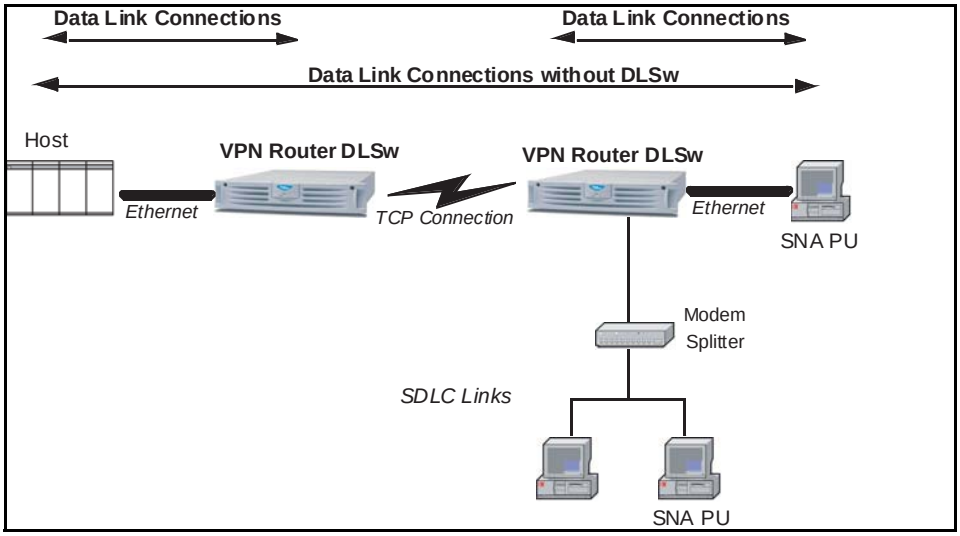
The VPN Router implementation of Data Link Switching supports the following

- 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, PU 2, PU 2.1 (primary or secondary), and PU 4 systems attached to IBM SDLC links (A data link switch provides the SDLC attached systems with a LAN appearance within the Data Link Switch. Data Link Switching presents each SDLC PU to the Switch to Switch Protocol (SSP) as a unique MAC/SAP address pair.)
- all PUs transparently

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

"Data Link Connections without DLSw" on page 117 shows data link connections without DLSw.

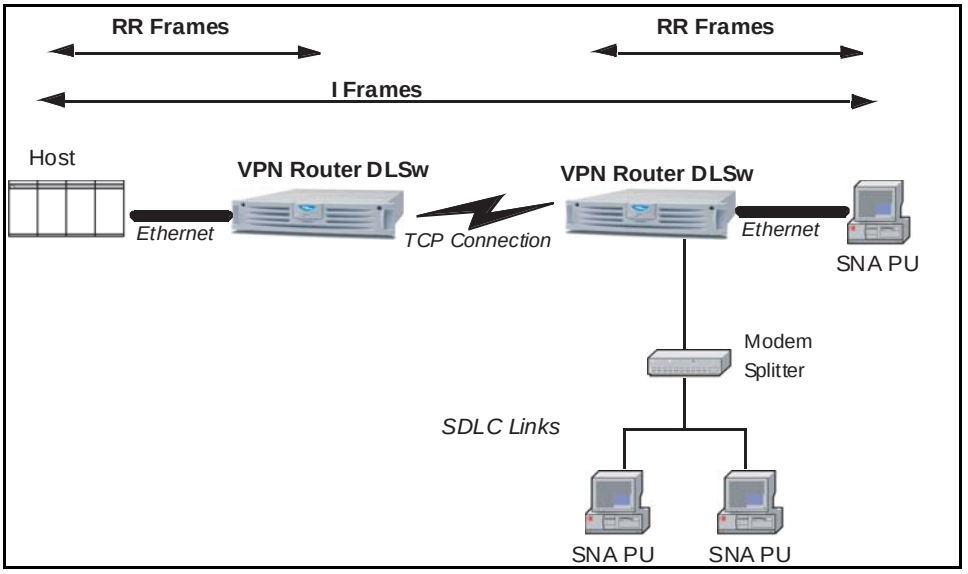
Figure 17 Data Link Connections without DLSw



The DLS multiplexes LLC connections onto a TCP connection to another DLS. The LLC connections at each end are independent of each other. The data link switch delivers frames that it receives from an LLC connection to the other end. This design limits LLC time-outs to the local LAN (they do not traverse the wide area). Also, the LLC Type 2 acknowledgments (RR) do not traverse the WAN, which reduces traffic across the wide area links. For SDLC links, polling and poll response occur locally, not over the WAN.

"Data Link with DLSw" on page 118 shows the data link connections with DLSw.

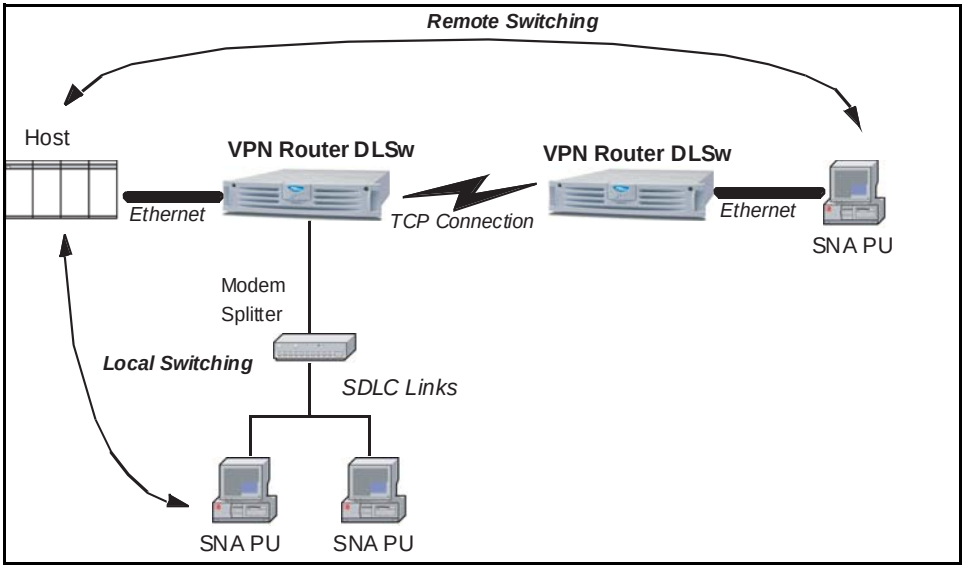
Figure 18 Data Link with DLSw



You can use Data Link Switches 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 by 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.

"Local and Remote Switching" on page 119 shows local and remote switching.

Figure 19 Local and Remote Switching



Before Data Link Switching can occur between two routers, they must establish a TCP connection between them. After this connection exists, 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 the statuses (active or inactive).

VPN Router DLSw fully supports RFC 1434 and RFC 1795. VPN Router partially supports RFC 2166. VPN Router DLSw does not support User Datagram Protocol (UDP) services; it supports TCP services only.

When the router initiates a connection, DLSW first tries to connect using RFC 2166. If this fails, VPN Router DLSW then tries to connect according to RFC 1795. If this also fails, it connects as RFC 1434.

Supported functionality

The following list identifies functions that the VPN Router DLSw implementation supports:

- configure VPN Router DLSw only through the CLI
- requires a feature license key
- local peer configurable on private or circuitless IP (CLIP) addresses
- full back-level interoperability with RFC 1434
- 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 though an assigned cost
- unconfigured peers that allow VPN Router to accept DLSw peering where you do not preconfigure the remote peer
- global command to enable or disable DLSw without loss of the DLSw configuration
- local and Remote switching for both Ethernet LANs for SNA traffic and SDLC stations
- SDLC and LLC Type 2 support on private interfaces
- marking of the VPN Router-generated DLSw IP packets with a fixed Differentiated Services Code Point (DSCP) value equal to Assured Forwarding (AF) 21
- clear circuit: the ability to delete a specific circuit or group of circuits (A cleared circuit can automatically reestablish itself.)

VPN Router DLSw does not support the following functionality:

- DLSw Management Information Bases (MIB)
- NetBios traffic
- UDP and IP multicast between DLSw peers

Ethernet LLC Type 2 functionality

Ethernet LLC Type 2 functionality supports the following

- SNA LLC Type 2 traffic on all private Ethernet interfaces

- type 1 and 2 LLC communications
- simultaneous SNA and non-SNA traffic
- Ethernet MAC including autosensing of 802.3/DIX2 Ethernet formats by Link Station
- Dynamic Window Algorithm from IBM for controlled restart of I-frame traffic after LAN congestion

Ethernet LLC Type 2 MAC address translation functionality supports the following:

- Provides the optional ability to translate the LLC Type 2 MAC Addresses for traffic transiting the VPN Router LLC Type 2 interfaces.
- Addresses the occasional need to change the mainframe or data center without the reconfiguration of the host MACs across many branch 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 multidrop 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 (the primary station sends XID and VPN Router DLSw uses it to poll the secondary station)

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) and V.35, X.21 interfaces
- Data Communications Equipment (DCE) (internal clock) mode on the single port V.35/X.21 to provide clocking to locally connected SDLC devices

- non-return-to-zero inverted (NRZI) and non-return-to-zero (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. From the Serial Port menu, enter **L** to access the command line interface.
   - Establish a Telnet session with the management IP address.
2. At the Login prompt, log on to the VPN Router 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 go to Global Configuration mode.

   ```
   CES> enable
   Password:<password>
   CES# configure terminal
   Enter configuration commands, one per line. End with
   Ctrl/z.
   CES(config)#
   ```

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

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

5. Start a 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 an LLC Type 2 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 Exit the interface configuration mode for the private interface.

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

10 Create an SDLC port. Configure SDLC parameters. In this example, you use an external modem eliminator or equipment that provides clocking.

```
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 use a minimum serial board firmware revision level of 7. You can determine the revision level by using the CLI command **show interface serial** *x/x* **statistics**. The revision level appears in the last line of the following example 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
```

11 Reboot the VPN Router after you configure SDLC on the serial interface card. (You need not reboot before you complete the configuration; however, you cannot enable or start the link station until after the reboot.)

12 After you restart the VPN Router, configure the SDLC port role, if required. The default is primary.

```
CES(config-if)#sdlc role {pri|neg|sec}
```

13 Enable the SDLC port.

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

14 Create and configure an 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 configure the local mac–sap and remote mac–sap pairs. Enable and start the SDLC link station. In this example, the poll frame is the default, SNRM. You can create the remote peer after you create the llc2 port or sdlc port.

VPN Router configuration commands example

Use the following CLI commands to configure the VPN Router DLSw in the example configuration.

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

DLSw local peer configuration

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

1. Create a DLSw local peer on a specific private or CLIP address. This DLSw local peer listens for and accepts incoming connections. VPN Router DLSw currently supports one local peer.
2. Enable or disable MAC address translation. The default value is disabled.
3. Configure MAC cache limit. The default is 0.
4. Enable or disable backlevel flow control. The default value is disabled. Nortel recommends that you enable this option for RFC 1434 type peers.
5. Enable or disable the local peer. You can change the IP address used by the local peer only if you administratively disable the local peer.
6. Enable or disable unconfigured peer support. The default is disabled.

DLSw remote peer configuration

To configure DLSw remote peer, use the following basic steps and related commands. Many 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. You use this parameter when two peers negotiate connection capability. The default is 1.



Note: Nortel recommends that you use the defaults for the llc2 timers, counters, lan-type, and window parameters unless you require changes to resolve specific issues.

3. Configure circuit inactivity timeout. For RFC 2166 peers you can configure the time after which a connection without circuits changes to a standby state. The default is 0.
4. Configure the remote peer cost. Use peer cost in the preferred peer feature (all peers with the same cost are broadcast at the same time). The default is 5 (minimum).
5. Enable or disable the remote peer.
6. Create the DLSw remote peer as backup peer.
7. Configure a backup peer for a specific connection.

LLC Type 2 port configuration

To configure the LLC Type 2 port, use the following basic steps and related commands. Many steps are optional; the default values are typically sufficient for proper operation.

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

4 Configure the lan-type. Supported LAN types are 802.3 and DIX. The default is 802.3 and DIX.

5 Configure the port maximum received window. The default is 7 (modulo 8).

SDLC port configuration

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

1 Create an SDLC port.

2 Configure the activation sequence that a primary port uses to become active (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 occurs if you do not power on the local device. Use Peer-first if you want the VPN Router to establish the host connection before it polls the local device.

Troubleshooting hint: Use this parameter to test local or remote communications when you cannot normally test a connection.

3 Configure values for port timers.



Note: Configure 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 or disable debug. You must enable debug to display all in and out SDLC packets in the event log. The default is disabled.

6 Enable or disable interframe-fill. The default is disabled.

7 Configure the port maximum received window. The default is 7 (modulo 8).

8 Configure an SDLC port poll address.

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



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

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

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

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

SDLC link station configuration

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

1 Create an SDLC link station. Assign a poll address to the link station. In the CLI, create a new link station configuration mode.

2 Configure the local MAC or SAP used for outgoing or incoming circuits.

3 Configure the remote MAC or SAP used for outgoing or incoming circuits.

4 Configure the SDLC link station counters.



Note: Nortel recommends that you do not change these settings unless you must address a specific configuration issue.

5 Configure values for the 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 router polls the device at a 400-millisecond (ms) interval for 16 tries, and thereafter at 1-second intervals until it receives a productive response (an I-Frame) to a poll. This action 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 an SDLC link station received window. The default is 7 (modulo 8).



Note: Nortel recommends that you do not change these settings unless you must address a specific configuration issue.

7 Configure an SDLC link station send window. The default is 7 (modulo 8).



Note: Nortel recommends that you do not change these settings unless you must address a specific configuration issue.

8 (Optional) Configure a group poll address. Use this option only if you use an IBM 3174 controller as a LAN gateway.

9 Configure a proxy XID. Only PU Type 2 devices requires proxy XID. 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 is SNRM. The poll frame default works in many cases, and you need to modify it only if required for the particular attached device.



Note: Nortel recommends that you not change this setting unless the device does not respond to normal reactivation polling.

11 Enable or disable the SDLC link station. The default is disabled.

12 Start or stop the SDLC link station to activate or deactivate it.

DLSw timers configuration

Configure global timer values at the local peer level:

```
CES(config)#dlsw timer tcp-connect-retry <0-65535>
CES(config)#dlsw timer test-timeout <0-65535>
CES(config)#dlsw timer explorer-timeout <0-65535>
CES(config)#dlsw timer explorer-wait-timeout <0-65535>
CES(config)#dlsw timer explorer-delay <0-65535>
CES(config)#dlsw timer circuit-ack-timeout <0-65535>
CES(config)#dlsw timer idle-timeout <0-65535>
```

DLSw miscellaneous configuration

Miscellaneous DLSw configuration includes the following:

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

Single port V.35/X.21 configuration

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

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

Chapter 9
IPX configuration

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

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

This chapter includes the following topics:

- "Introduction" on page 131
- "IPX client" on page 132
- "Enabling IPX for group users" on page 133
- "Sample IPX VPN gateway topology" on page 133

Introduction

The VPN Router supports IPX by encapsulating IPX traffic within Point-to-Point Tunneling Protocol (PPTP) client connections.



Note: The VPN Router 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 VPN Router provides the network node addressing.

Network addresses form the basis of the IPX internetwork addressing scheme to send packets between network segments. Assign every network segment of an internetwork a unique network address by which routers forward packets to their final destination network. The VPN Router treats all public interfaces 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's are hexadecimal characters.

```
0xnnnnnnnn
```

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

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

The VPN Router 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 (MS-DUN), you must enable the dial-up networking IPX option. After you enable IPX, you can tunnel using IPX, IP, or IPX and IP according to the dial-up networking selections.

Windows 95 and Windows 98

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

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 you use IPX with PPTP.

Windows NT

The NetWare client exists on Windows NT systems. You can use the NetWare client or the Novell intraNetWare client, which you can access from the Novell Web site.

Enabling IPX for group users

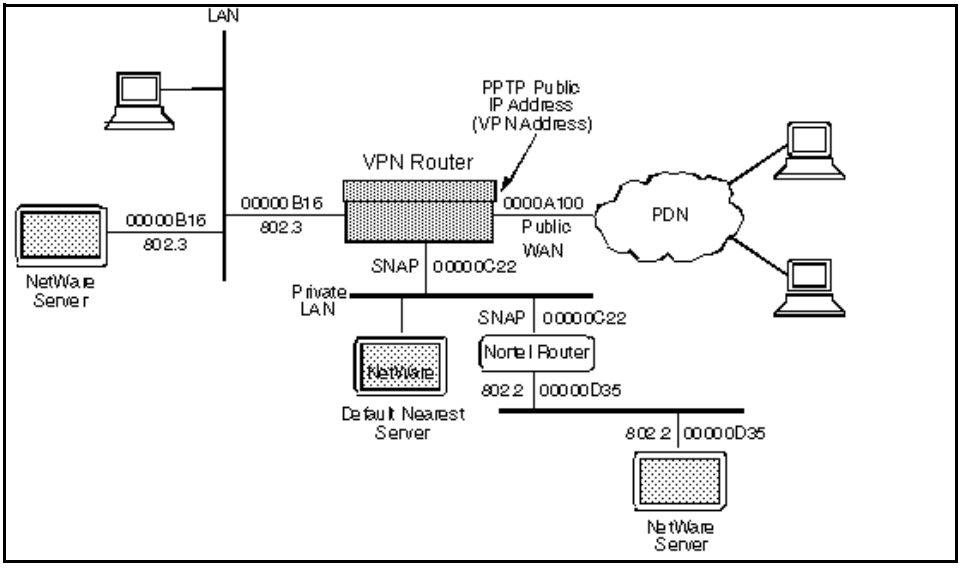
By default, IPX is disabled for individual groups. Therefore, you must enable IPX for group users to access IPX. Enable IPX for group users from the Profiles, Groups, Edit, Connectivity window.

Sample IPX VPN gateway topology

Regardless of the number of IPX public interfaces that you configure on the VPN Router, 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 VPN Router provides is 0000A100.

In "IPX topology" on page 134, 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 20 IPX topology



Note: The private LAN can simultaneously carry IP and IPX traffic. This preceding figure does not show IP addresses.

Chapter 10
Interoperability configuration

This chapter explains the requirements and procedures to set up various vendor hardware or software to interoperate with the VPN Router. You can use these instructions to establish encrypted tunnels to and from the VPN Router with the noted vendors. These requirements and procedures are subject to change based on hardware and software changes by the vendors.

Branch office Network Address Translation (NAT) Traversal works with vendors that support the following modes:

- draft mode—based on IETF draft draft-ietf-ipsec-nat-t-ike-00
- RFC mode—based on IETF RFC 3947

For information about Internetwork Packet Exchange (IPX), see Chapter 9, "IPX configuration," on page 131. This chapter includes procedures for the following products:

- Cisco 2514 router, Version 11.3
- SafeNet, Inc. (IRE), SafeNet/Soft-PK Security Policy Database Editor, Version 1.0
- Third-party clients

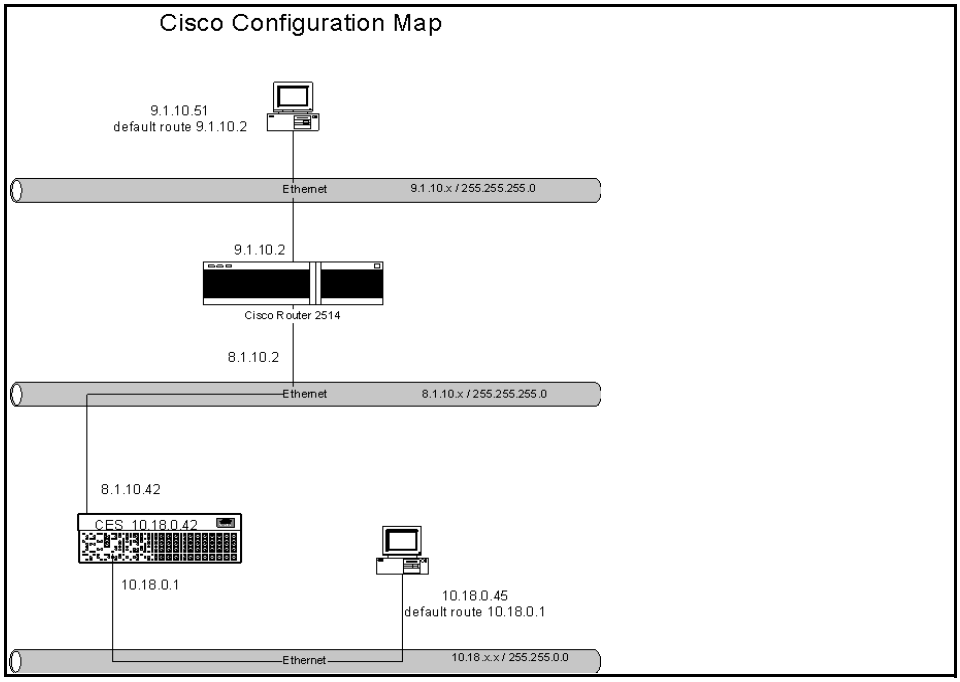
This chapter includes the following topics:

- "Configuring the Cisco 2514 router Version 11.3" on page 136
- "Configuring the VPN Router for Cisco interoperability" on page 138
- "Configuring the SafeNet/Soft-PK Security Policy Database Editor Version 1.0s" on page 139
- "Configuring the VPN Router for IRE interoperability" on page 143
- "Third-party client installation" on page 144

Configuring the Cisco 2514 router Version 11.3

To set up the VPN Router to establish encrypted tunnel connections with the Cisco 2514 router, as shown in the following figure, configure the Cisco 2514 with the **`show configuration`** command.

Figure 21 VPN Router and Cisco 2514 network topology



The following is the **show config** command:

```
Cisco2514# show config
Using 1088 out of 32762 bytes
version 11.3
no service password-encryption
hostname Cisco2514
enable secret 5 $1$aSJB$Xz/o4I4IqCY.FT2RH372/1
enable password password
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 3000
crypto isakmp key test address 8.1.10.42
!
crypto ipsec transform-set esp1 esp-des esp-md5-hmac
!
crypto map bay 11 ipsec-isakmp
 set peer 8.1.10.42
 set session-key lifetime seconds 3000
 set transform-set esp1
 match address 132
!
!
interface Ethernet0
 ip address 9.1.10.2 255.255.255.0
 no mop enabled
!
interface Ethernet1
 ip address 8.1.10.2 255.255.255.0
 no mop enabled
 crypto map bay
!
interface Serial0
 no ip address
 no ip mroute-cache
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
ip classless
ip route 10.18.0.45 255.255.255.255 8.1.10.42
access-list 132 permit ip host 9.1.10.51 host 10.18.0.45
access-list 132 permit ip host 10.18.0.45 host 9.1.10.51
dialer-list 1 protocol ip permit
```

```
dialer-list 1 protocol ipx permit
snmp-server community public RO
line con 0
line aux 0
line vty 0 4
password terminal
login
end
```

Configuring the VPN Router for Cisco interoperability

To configure the VPN Router for Cisco interoperability

1. Choose **Profiles**, **Networks,** and then click **Edit** for a network.
2. Create local accessible networks that you want available.
3. Type the IP address for the new subnet; for example, 10.18.0.45.
4. Type the subnet mask for the new network.
5. Click **Add**.

   The Networks > Edit window appears and shows the newly created subnet in the Current Subnets list for the named network.

6. Add each local subnet to a Network profile for which you want tunneled connections going to or coming from.
7. On the Branch Office > Edit GROUP window, verify that your settings synchronize with the Cisco router.

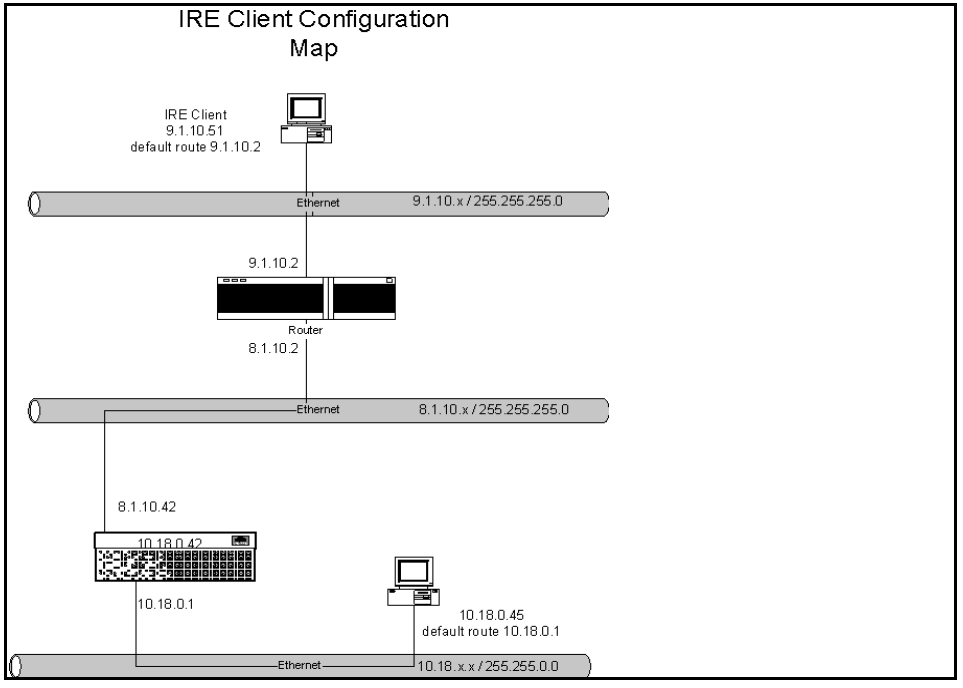
   For Cisco, to turn off Vendor ID and Perfect Forward Secrecy (PFS), choose **Profiles**, **Groups, Configure, IPsec, Configure**.

8. Create and configure the IPsec branch office connection on the VPN Router, using the network profile that you create for the local accessible network.
9. On the Profiles, Branch Office window, enable **IPsec Authentication: Text Pre-Shared Key**.

Configuring the SafeNet/Soft-PK Security Policy Database Editor Version 1.0s

To configure the VPN Router to establish encrypted tunnel connections with the IRE Soft-PK Security Policy Client as illustrated in the following figure, configure the windows as described in this section.

Figure 22 VPN Router and IRE SafeNet network topology



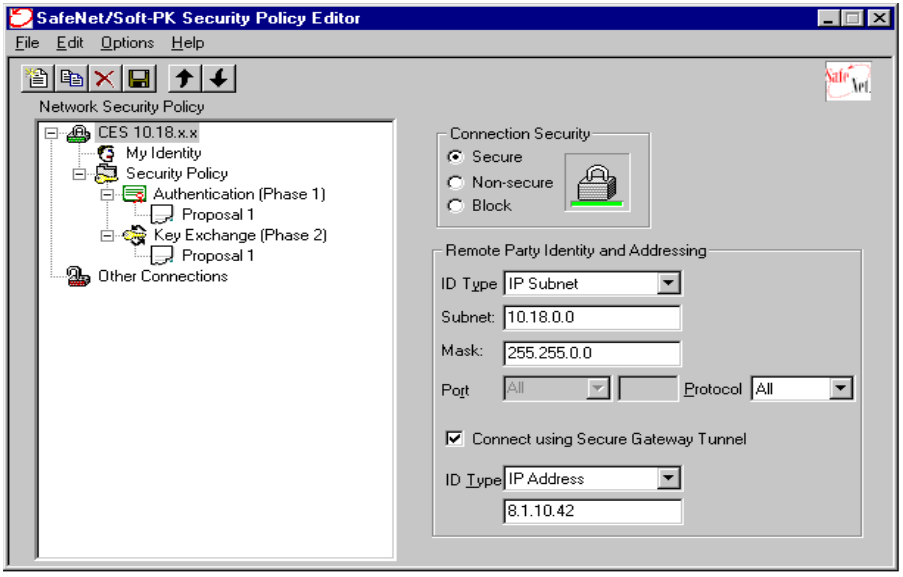
Connecting to IRE SafeNET/Soft-PK Security Policy Client

To configure the VPN Router to establish encrypted tunnel connections with the IRE SafeNet/Soft-PK Security Policy Client, perform the following steps:

1 Open the SafeNet/Soft-PK Security Policy Client, and then choose **File, New**.

Use the following window to configure the network so that packets going to the 10.18.0.0 subnet go through the 8.1.10.42 interface to establish a tunnel.

Figure 23 Security Policy Editor dialog box



2 Select the switch **CES 10.18.x.x**.

3 For **Connection Security**, select **Secure**.

4 Under Remote Party Identity and Addressing, select the following:

- ID Type: **IP Subnet**
- Subnet: **10.18.0.0**.
- Mask: **255.255.0.0**
- Protocol: **All**

5 Select **Connect using Secure Gateway Tunnel** and select the following:

- ID Type: **IP Address**

- **8.1.10.42**

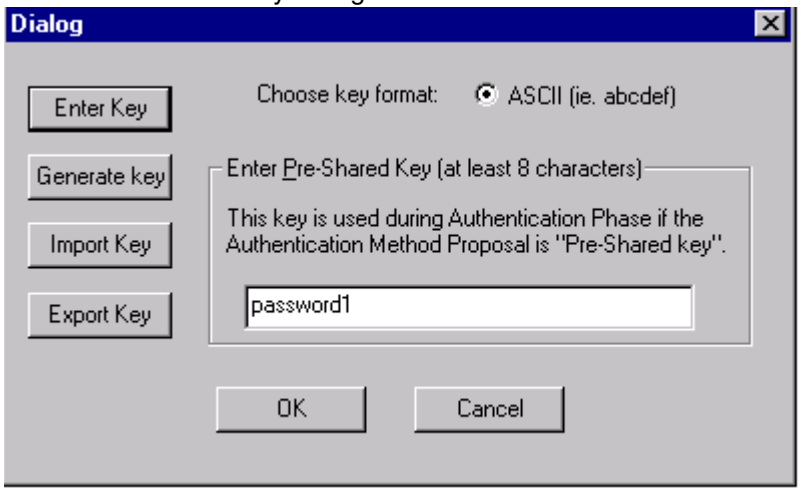
The SafeNet/Soft PX Security Policy Editor dialog box appears.

6 Click **My Identity** to configure the SafeNet client, and select the following:

- Select Certificate: **None**
- ID Type: **IP Address**
- Port: **All**

7 Click **Pre-Shared Key**.

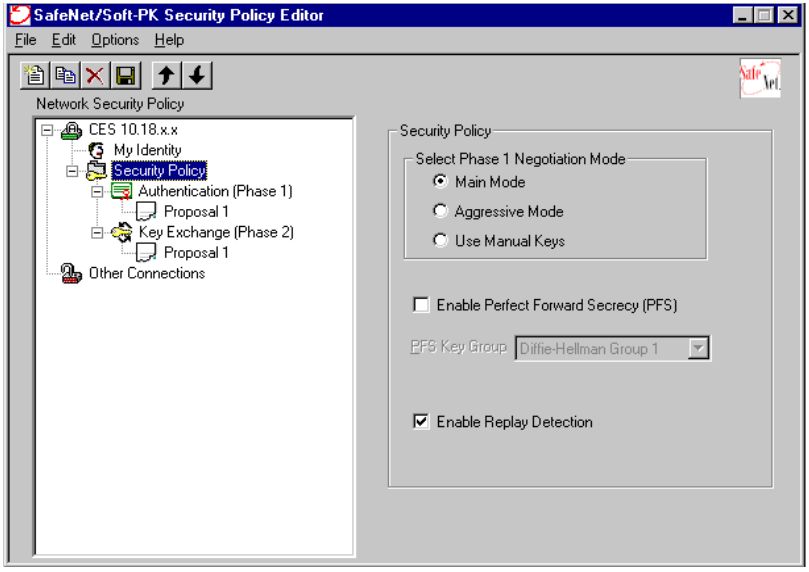
Figure 24 Pre-Shared Key dialog box



8 In the Pre-Shared Key dialog box, click **Enter Key**, and then enter the preshared key.

9 Click **OK**.

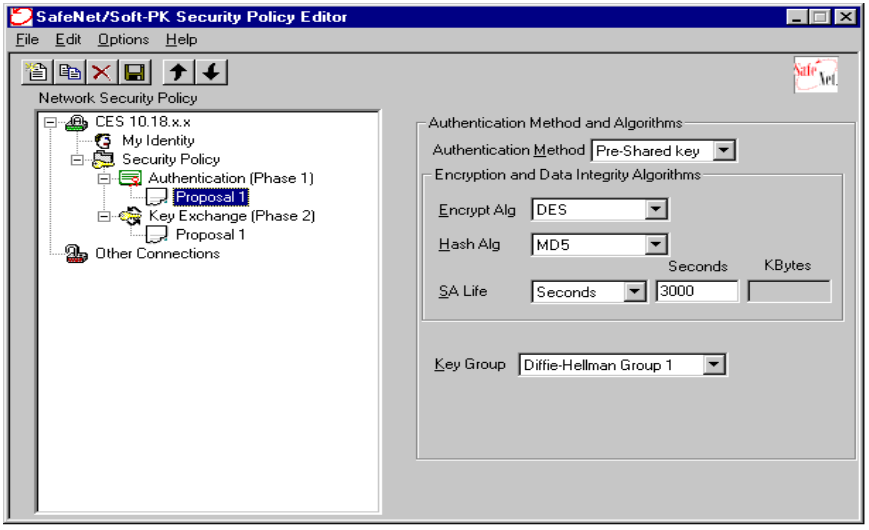
Figure 25 Security Policy Editor dialog box 2



10 From Security Policy: Select Phase 1 Negotiation Mode, select **Main Mode**.

11 Select **Enable Replay Detection**.

Figure 26 Security Policy Editor dialog box 3



12 On the Authentication (Phase 1), Proposal 1, Authentication window, enable the following:

- Authentication Method: **Pre-Shared key**
- Encrypt Alg: **DES**
- Hash Alg: **MD5**
- SA Life: **Seconds and 3000 (Seconds)**
- Key Group: **Diffie-Hellman Group 1**

13 On the Key Exchange (Phase 2), Proposal 1 window, enable the following:

- **Encapsulation Protocol (ESP)**
- Encrypt Alg: **DES**
- Hash Alg: **MD5**
- Encapsulation: **Tunnel**
- SA Life: **Seconds and 3000 (Seconds)**

Configuring the VPN Router for IRE interoperability

To configure the VPN Router for IRE interoperability

1 Choose **Profiles**, **Networks,** and then click **Edit**.

2 Create the network object used for local accessible networks.

3 In the Networks Edit window, type the IP address for the new subnet; for example, 10.18.0.45.

4 Type the subnet mask for the new network: **255.255.0.0**.

5 Click **Add**.

The Networks > Edit window appears and shows the newly created subnet in the Current Subnets list for the named network.

6 Add each local subnet for which you want tunneled connections going to or coming from the VPN Router to a network profile.

7 On the Branch Office > Edit GROUP window, verify that your settings synchronize with the SafeNet client.

8 Create and configure the IPsec Branch Office connection on the VPN Router by using the network profile you just created for the local accessible network. On the Branch Office window, select the IPsec Authentication: **Text Pre-Shared Key** option.

9 For some vendors, if you want to turn off Vendor ID or Perfect Forward Secrecy (PFS), choose **Profiles**, **Groups**, **Configure**, **IPsec**, **Configure**.

Third-party client installation

The VPN Router supports third-party IPsec clients and includes support for the following functions:

- Authentication using either preshared authentication using Internet Key Exchange (IKE) Aggressive mode or digital signature certificate authentication using IKE Main mode into the IPsec account of the remote user for third-party IPsec clients.
- Client address assignment used within the IPsec tunnel formed through Quick Mode negotiation. The IKE Quick Mode exchange uses the external client IP address or a prearranged internal IP address as the address to negotiate.
- Split tunneling with third-party IPsec clients. If you enable split tunneling on the VPN Router, you must list the subnet that the client specifies as the VPN Router identity within the tunnel during IKE Quick Mode as one of the split tunnel networks for the client to accept the Quick Mode proposal. If you do not enable split tunneling, the client can specify a value for the VPN Router identity in Quick Mode.

Depending on the third-party client that you use, you must configure either a branch office tunnel or a user tunnel. For example, Nortel configured and tested the VPN Router with the LINUX FreeS/WAN client. If you use the FreeS/WAN LINUX client, you must configure your user and the VPN Router as a branch office tunnel. If you use another client that supports IPsec Aggressive mode, you can configure your VPN Router as a user tunnel.

Considerations for using third-party clients

The following considerations exist regarding the use of third-party clients with VPN Router:

- Client dynamic addressing—Many third-party clients now support the Aggressive mode method of establishing a security association (SA). The advantage of Aggressive mode for remote user access is that, unlike Main mode, the VPN server does not authenticate the security association based on prior knowledge of the IP address of the user. Therefore, the ISP can dynamically assign an address to the remote user.
- Client address advertisement—After the router connects to the Nortel VPN client, the VPN Router assigns the client-side inner address of the IPsec tunnel from the enterprise address space. This address is the address that devices on the private network send data to in response to requests from the client. The VPN Router captures packets destined for those addresses and sends them through the public interface encapsulated within IPsec, addressed to the ISP-assigned outer address of the client.

  In the case of third-party clients, the VPN Router does not assign the inner address of the client. The inner address of the client tunnel is normally set the same as the ISP-assigned outer address. Servers in the enterprise need to find a route back to these clients. You must configure the VPN Router as the default VPN Router on the network. The VPN Router can then forward tunneled traffic to served clients and forward other traffic to the Internet or other default VPN Routers. This option is not always desirable because of the impact on the customer network infrastructure.
- Authentication—Third-party clients does not support all authentication services that the Nortel VPN Client supports. Remote Authentication Dial In User Service (RADIUS), RSA SecurID, PassGo, and other RADIUS-based services do not work with the VPN Router, even if the third-party client supports these services. The only authentication services that the VPN Router supports with third-party clients is LDAP with a preshared key and unmanaged certificates.
- Client customization—If you are a service provider, use this option to customize the look of the client with your branding. In addition, you can preconfigure the service profiles (VPN Router destination and authentication options) and lock down the client configuration for the end-user so that they cannot modify or change these attributes.

- Load balancing—Traditional load balancers often do not work with the IPsec protocol because of the security features on individual packets and separate key management and data channels. The VPN Router uses built-in load balancing features for IPsec client terminations that allow two VPN Routers to load balance and failover connections. This feature works with third-party clients.
- Quality of Service (QoS)—The Nortel VPN Client is subject to manager-defined QoS policies. You can reserve connection slots for various classes of user, and you can assign different forwarding priorities for their traffic. The VPN Router preserves Diff-Serv markings for dial tunnels, copying the Diff-Serv Code Point (DSCP) from the inside packet to the tunnel header.
- Advanced attribute definition from the server—On a group-by-group basis, you can load the client with the tunneled IP address and subnet mask, a Microsoft domain name, both Windows Internet Naming Service (WINS) and Domain Name System (DNS) servers, a message of the day, and the VPN Router banner. The network manager can also determine access days and hours, crypto strength, how often the client rekeys, and whether the client can store a password for the group. The network manager can initiate a password-protected screen saver if the user leaves the PC, and can log off idle connections. You can filter traffic in the tunnel based on IP address or port number and can configure to close the tunnel if certain network applications run. You can set the tunnel to automatically start after users access predefined applications or destinations, and close after these application are complete. These features are not available with third-party clients.
- Address assignment—A Dynamic Host Configuration Protocol (DHCP) server assigns client-tunneled IP addresses, for each group from a named pool, through RADIUS attribute or statically. The client receives the inner IP address from the enterprise address space. Third-party remote access clients have the inner address assigned the same as the outer, which is normally what the ISP assigns, and is not part of the enterprise address space.
- Split Tunneling—On a group-by-group basis, a service provider determines which IP addresses go into the tunnel and which use the local adapter (for general Internet access, or local printing or server use). With third-party clients, enable split tunneling. If you disable Split Tunneling, add the client to a group that permits undefined networks.

- Advanced security features—The Nortel VPN Client tunnel accepts only packets that originate from the machine on which the client runs. If an entity attempts to route packets through a VPN Client, the tunnel closes. After you enable non-split tunneling, the client accepts only packets that pass through the VPN (correctly decrypt and authenticate); the client drops other packets. If an attempt is made to change the station address of the client, the tunnel automatically closes. Third-party clients do not necessarily use this security.
- Tight integration with Microsoft Dial-Up Networking (MS-DUN) and iPass—This option provides one-click access that dials and authorizes the ISP connection and then automatically creates the VPN connection. Third-party clients typically do not use this feature.
- High end Public Key Infrastructure (PKI) integration—The VPN Router integrates software from the leading certificate vendors, for a high-end managed PKI implementation. Managed PKI features like automated enrollment and automatic renewal are critical for large-scale rollouts. Other clients use loose or no integration for managed PKI and rely on the features of a browser or simple cut-and-paste methods. This option is not available with third-party clients, even if the client supports it.

Configuring the VPN Router as a branch office tunnel

To configure the VPN Router as a branch office tunnel

1. Choose **Profiles**, **Branch Office,** and then under Connections, click **Add**.

   The Add Connection window appears.

2. Type a name for the connection.
3. Configure the tunnel type to **IPsec**.
4. Click OK.
5. For the local endpoint address, select the address of the local VPN Router from the list.
6. For the remote endpoint address, type the address of the remote VPN Router that forms the opposite end of the branch office connection.
7. Depending on your third-party client support, you can use either preshared key or digital certificate authentication. Click to enable the user name and password to authenticate user identity. The user name is the IP address and the

password is any password. Match the preshared secret with the client shared secret.

8. Click **RSA Digital Signature** to enable certificate authentication if your third-party client supports RSA Digital Signature authentication. You must then select a default server certificate from the list. You configure servers from the System, Certificates window.
9. Select **Profiles**, **Branch Office**, click **Configure** for the group, scroll down to the IPsec section, and then click **Configure**.
10. Select the encryption type supported by your third-party client.
11. Select **Enabled** or **Disabled** for the **VendorID**.
12. Configure **Perfect Forward Secrecy (PFS)** to match the client side.
13. In the **Rekey Time-out** box, type the amount of time you want to limit the lifetime of a single key used to encrypt data. The default is 08:00:00 (8 hours).
14. In the **Rekey Data Count** box, you can choose to configure a rekey data count depending on how much data you expect to transmit through the tunnel with a single key. The default is 0 KB; a value of 0 disables this count.

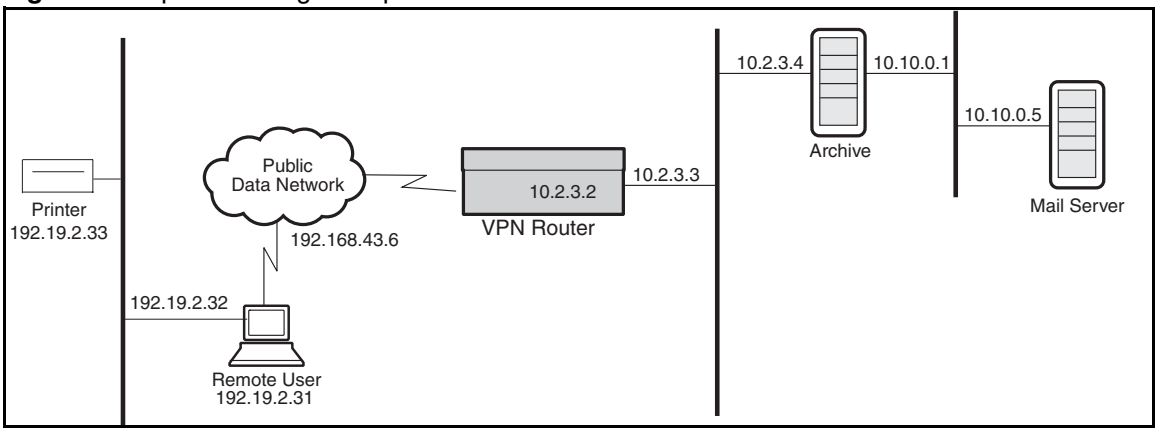
Configuring the VPN Router as a user tunnel

If you use third-party client software that supports Aggressive mode IPsec, you can configure the VPN Router as a user tunnel. You must use either the LDAP database or the certificate authentication. The VPN Router supports both preshared key and RSA digital signature authentication methods and you must specify one or both of these methods.

Nortel recommends that you enable split tunnels for all groups that support third-party clients. If you disable split tunneling, third-party clients can connect only if you configure the group to allow undefined networks. This means that the client can establish IPsec security associations for all networks. If you do not enable split tunneling, you must enable the Allow undefined networks option.

"Split tunneling example" on page 149 shows a network with a split tunneling environment.

Figure 27 Split tunneling example



To configure the VPN Router as a user tunnel

1. Choose **Profiles**, **Groups,** and then click **Add**. Type a group name of up to 64 characters (you can use spaces); for example, Research and Development.
2. Click **OK**.
3. Click **Edit** next to the name of the new group, scroll down to the IPsec section, and then click **Configure**.
4. Enable Split tunneling if you want your VPN Router to control the networks that the third-party client can access. If you disable split tunneling and enable Allow undefined networks for non-Nortel VPN Clients, the clients can connect to all internal networks. If you select both Split Tunneling and Allow undefined networks for non-Nortel VPN Clients, the VPN Router uses the split tunneling feature and ignores the Allow undefined networks selection.
5. Under Client Selection, click Configure, and select **Non-VPN Router Clients (LINUX/Windows 2000)** or **Both VPN Router and Non-VPN Router Clients** from the list.
6. Third-party clients can use either preshared key or digital certificate authentication. Under Authentication, click **Configure**. Enable the user name and password to authenticate user identity. If you use Main mode, the user name is the IP address and the password is any password.
7. Select **RSA Digital Signature** to enable certificate authentication if your client supports this. You must then select a default server certificate from the list. You configure servers from the System, Certificates window.

8. Selections in the Encryption section depend on the type of encryption that your third-party client supports.
9. Enable **Perfect Forward Secrecy (PFS)**. PFS ensures that if one key is compromised, subsequent keys are not compromised.
10. Enable compression for IPsec tunneling.
11. In the **Rekey Time-out** section, click **Configure**, and then type the time you want to limit the lifetime of a single key used to encrypt data. The default is 08:00:00 (8 hours).
12. In the **Rekey Data Count** section, click **Configure**, and then type a rekey data count depending on how much data you expect to transmit through the tunnel with a single key. The default is 0 KB; a value of 0 disables this count.
13. Click **OK**.
14. From the Connectivity section, click **Configure**.
15. In the **Forced Logoff** section, click **Configure**, and then specify a time after which all active users automatically log off. The default is 0, which means the option is turned off. The possible range is 000:00:00 to 119:59:59.
16. Click **OK**.

Index

Numbers

56/64K CSU/DSU
connector 54
802.1Q
configuring 27
tagging 26

A

accelerator cards, hardware encryption
described 45
address control field compression 68
ADSL 59
asynchronous serial interfaces 95
ATM 60
ATM virtual circuit 61
Auto Answer 101
Auto SPID 100

B

backup interface services (BIS) 95
BIS
configuring 105
configuring ABOT 104
BIS trigger
interface group failure 106
ping failure 110
route unreachable 108
time of day 108

C

circuitless IP (CLIP) 41
committed burst rate 80
committed information rate
CIR 79
Country Code 99

D

data link switching (DLSw) 115
demand services 102
Dial In 101
dial interfaces 95
Dial Out 101
DLSw
local peer configuration 125
operational overview 116
remote peer configuration 126
RFCs 119
supported functions 120
supports 116
DOVBS 100

E

echo
fault threshold 68
interval 69
encryption accelerator cards, hardware
described 45
ESF 51

F

Frame Relay 75

Frame Relay Forwarding Priority 90

FRF.12 86

FRF.9 85

H

hardware encryption accelerator cards
described 45

I

interface
debug 69

Internetwork Packet Exchange 131

IPCP
settings 69

IPX 131

IPX client 132

ISDN 99

ISDN BRI 99

ISP 33, 68

L

LCP 64, 68

LLC2 port
configuration 126

LLC2 support 120

M

Manual TEI 101

map class 90

MultiLink 101

N

NetWare client 133

NI-2 ISDN 100

Novell intraNetWare client 133

P

permanent virtual circuit
PVC 75, 78

Point to Point Protocol over Ethernet (PPPoE) 71

PPP 67, 98

protocol
field compression 68

publications
hard copy 15

Q

Quad T1/E1 51

R

RFC 2233 93

S

SCLC functions 121

SDLC
link station configuration 128

SDLC port
configuration 127

SF 51

single port V.35/X,21 serial card 121

SPID 100

subinterface statistics 29

switched virtual circuit
SVC 75

T

T1 CSU/DSU 51

TCP MSS clamping 31

technical publications 15

TEI 101
traffic shaping 79

V

Van Jacobson compression 69
VJ
  compression 69
  max slots 69
VLAN subinterfaces
  configuring 28

W

WAN interfaces
  configuration 33
  currently installed 34