Configuration — WAN Interfaces
Avaya Secure Router 2330/4134

Release 10.3.5
NN47263-500
Issue 04.02
July 2013

© 2013 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise,

any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Comments? infodev@avaya.com

Contents

Chapter 1: Introduction 13
- Purpose 13
- Related Resources 13
  - Documentation 13
  - Training 13
  - Avaya Mentor videos 13
  - Support 14

Chapter 2: New in this release 15
- Other changes 15
  - Interoperability with Silver Peak NX WAN optimization 15
  - ISDN BR voice bundles with point-to-multipoint 15

Chapter 3: WAN module fundamentals 17
- Silver Peak WAN optimization 17
- WAN modules 17
- T1/E1 modules 18
  - Voice support on T1/E1 small modules 18
  - Mixed mode E1 Support for 8 port T1/E1 modules 18
  - Standards compliance 19
  - PSTN connectivity with T1/E1 BRI 20
- CT3 module 20
  - DS3 module 20
  - Standards compliance 20
- Serial modules 21
- HSSI modules 21
- ISDN BRI modules 22
  - ISDN BRI S/T 23
  - Voice support on ISDN BRI modules 23
  - Standards compliance 23
- ADSL modules 23
  - ADSL Overview 23
  - ADSL small module 24
  - ATM 24
  - Multiplexing 25
  - How the Secure Router 2330/4134 connects to the Internet using ADSL 25
  - ADSL small module standards compliance 26
  - ADSL small module limitations 26
- Voice Carrier medium module 27

Chapter 4: WAN encapsulation fundamentals 29
- WAN bundle logical interface 29
- HDLC 29
- PPP 29
  - Link Control Protocol (LCP) 30
  - Authentication 32
  - Network Control Protocol (NCP) 33

MLPPP ... 34
Compressed RTP ... 35
Standards compliance ... 36
Frame Relay ... 36
PVC ... 37
Address resolution for PVCs ... 37
UNI interface ... 37
NNI interface ... 37
FRF.12 fragmentation ... 38
Local Management Interface (LMI) ... 38
IP Header compression over FR ... 39
Multi-protocol Encapsulation over FR ... 39
Inverse ARP ... 40
MFR ... 40
Jumbo Frames ... 41
Frame Relay congestion control ... 41
Frame Relay Traffic Management ... 41
Standards compliance ... 42
Configuration of PPP and Frame Relay interfaces as Layer 2 switched interfaces ... 42
Chapter 5: T1/E1 module configuration ... 45
Setting the carrier type on T1/E1 modules ... 45
Configuring T1 interface properties ... 45
Configuring T1 framing ... 45
Configuring T1 linecode ... 46
Configuring T1 yellow alarm detection and generation ... 46
Configuring T1 clock source ... 47
Configuring T1 alarm thresholds ... 48
Configuring hierarchy for T1 alarms ... 49
Configuring CSU line mode for T1 ... 49
Configuring DSX line mode for T1 ... 50
Configuring T1 circuit ID ... 50
Configuring contact information for T1 ... 51
Configuring description for T1 ... 51
Configuring a name for T1 ... 52
Configuring loopback framing for T1 ... 52
Enabling the T1 interface ... 53
Configuring E1 interface properties ... 53
Configuring E1 framing ... 53
Configuring E1 linecode ... 54
Configuring E1 yellow alarm detection and generation ... 54
Configuring E1 clock source ... 55
Configuring E1 alarms ... 56
Configuring hierarchy for E1 alarms ... 57
Configuring line mode for E1 ... 57
Configuring E1 circuit ID ... 58
Configuring contact information for E1 ... 58
Configuring description for E1 ... 59

Configuring a name for E1 ... 59
Enabling the E1 interface ... 60
Setting the carrier type to 4 channelized E1 and 4 unframed ports on an 8 port T1/E1 module ... 60
Setting the carrier type to 3 channelized E1 and 5 unframed ports on an 8 port T1/E1 module ... 61
Setting the carrier type to 2 channelized E1 and 6 unframed ports on an 8 port T1/E1 module ... 62
Setting the carrier type to 1 channelized E1 and 7 unframed ports on an 8 port T1/E1 module ... 62
Linking a bundle to a T1/E1 interface ... 63
Configuring the bundle to drop errored links ... 64
Configuring how dropped multilink T1/E1 links are restored ... 65
Manually restoring dropped multilink T1/E1 links ... 65
Chapter 6: CT3 module configuration ... 67
Configuring CT3 interface properties ... 67
Configuring alarms for CT3 ... 67
Configuring cable length for CT3 ... 69
Configuring clock source for CT3 ... 69
Configuring framing for CT3 ... 70
Configuring T1 properties within CT3 ... 70
Linking a bundle to the CT3 interface ... 72
Chapter 7: DS3 module configuration ... 73
Configuring DS3 interface properties ... 73
Setting the carrier type on CT3 modules ... 73
Configuring alarms for DS3 ... 74
Configuring cable length for DS3 ... 75
Configuring clock source for DS3 ... 75
Configuring framing for DS3 ... 76
Configuring a name for DS3 ... 77
Linking a bundle to a DS3 interface ... 77
Chapter 8: Serial module configuration ... 79
Configuring serial interface properties ... 79
Configure the serial mode ... 79
Configuring the serial clock source ... 80
Configuring the serial clock rate ... 80
Configuring CRC for the serial interface ... 81
Configuring serial data mode ... 81
Configuring serial operational mode ... 82
Configuring a name for the serial interface ... 83
Linking a bundle to the serial interface ... 83
Chapter 9: HSSI module configuration ... 85
Configuring HSSI interface properties ... 85
Configuring HSSI operational mode ... 85
Configuring clock rate for HSSI ... 86
Configuring clock source for HSSI ... 86
Configuring CRC for HSSI ... 86
Configuring HSSI data mode ... 87
Configuring a name for the HSSI interface ... 87
Linking a bundle to the HSSI interface ... 88
Chapter 10: WAN module information display ... 89

Displaying WAN module alarms ... 89
Displaying ANSI statistics for T1 or CT3 modules ... 89
Displaying WAN module configuration ... 90
Displaying IETF statistics for E1/T1 and CT3/DS3 modules ... 90
Displaying ITUT statistics for E1 ... 90
Displaying thresholds for E1/T1 and CT3/DS3 modules ... 91
Displaying user statistics for WAN modules ... 91
Clearing user statistics for WAN modules ... 91
Displaying AVC information ... 92
Displaying AVC information ... 92
Clearing counters for DTE-to-DTE MFR AVC interfaces ... 92
Displaying interface information ... 92
Displaying bundle interface status information ... 92
Clearing interface counters ... 93
Clearing counters for all interfaces ... 93
Clearing counters for bundles ... 93
Chapter 11: ISDN configuration on BRI modules and on T1/E1 modules ... 95
Linking a bundle to the BRI interface ... 95
Linking a bundle to the T1/E1 module for ISDN PRI ... 96
Configuring ISDN properties for BRI or PRI ... 96
Configuring the switch type ... 96
Configuring the caller number ... 98
Configuring the call-back ... 98
Configuring the called number ... 99
Configure the called party in the incoming setup message ... 99
Configuring the calling number ... 100
Configuring the connect delay ... 100
Configuring the disconnect cause ... 101
Configuring the idle timeout period ... 103
Configuring the ISDN plan and type ... 104
Configuring the ISDN Q921 timer values ... 108
Configuring the ISDN Q931 timer values ... 111
Configuring service profile ID for B1 or B2 channel ... 116
Configuring the TEI mode ... 117
Configuring the TEI value for point-to-point TEI mode ... 118
Activating ISDN ... 118
Displaying ISDN information ... 119
Displaying ISDN global configuration information ... 119
Displaying ISDN interface configuration information ... 119
Displaying ISDN BRI statistics ... 119
Displaying ISDN PRI statistics ... 120
Clearing ISDN statistics ... 120
Clearing ISDN BRI statistics ... 120
Clearing ISDN PRI statistics ... 120
Chapter 12: HDLC configuration ... 121
Configuring encapsulation for WAN modules ... 121
Configuring HDLC ... 121

Setting bundle encapsulation to HDLC ... 121
Configuring HDLC properties ... 121
Assigning an IP address to the WAN bundle ... 122
Chapter 13: PPP configuration ... 125
Configuring encapsulation for WAN modules ... 125
Configuring PPP ... 125
Setting bundle encapsulation to PPP or MLPPP ... 125
Configuring authentication ... 126
Configuring sent username and password for PAP or CHAP ... 126
Configuring peer name and password for PAP or CHAP ... 127
Configuring authentication method ... 127
Configuring echo-interval ... 128
Configuring interleaving ... 128
Configuring fragmentation delay for interleaving ... 129
Configuring MTU, MRU, and magic number for PPP ... 129
Configuring peer address ... 130
Configuring retry interval ... 130
Configuring the source address ... 131
Configuring RTP ... 131
Enabling RTP Header Compression ... 131
Configuring the maximum number of connections for RTP header compression ... 132
Enabling negotiation of RTP options ... 133
Configuring the timeout for the compressor and decompressor engines ... 133
Configuring port range and bandwidth for RTP traffic ... 134
Configuring MLPPP properties ... 134
Configuring BCP on PPP bundles ... 135
Configuring the Layer 2 interface mode ... 135
Configuring the hybrid interface properties ... 136
Configuring trunk interface properties ... 137
Setting the default VLAN ID for the interface ... 137
Assigning an IP address to the WAN bundle ... 138
Chapter 14: Frame Relay configuration ... 139
Configuring encapsulation for WAN modules ... 139
Configuring Frame relay ... 139
Setting bundle encapsulation to Frame Relay or MFR ... 139
Enabling Frame Relay ... 140
Enabling RFC 1490 fragmentation ... 140
Configuring maximum frame size ... 140
Configuring interleaving ... 141
Configuring interface type ... 142
Configuring local management interface ... 142
Configuring the LMI error threshold (DCE) ... 143
Configuring the LMI error threshold (DTE) ... 144
Configuring the LMI keepalive ... 145
Configuring LMI fast recovery ... 145
Configuring the inverse ARP polling timer ... 146
Configuring Frame Relay PVCs ... 147

Adding a PVC to a Frame Relay bundle ... 147
Configure the network type for the PVC ... 147
Configuring a description for the PVC ... 148
Enabling PVCs ... 148
Enabling and disabling a selected PVC ... 149
Provisioning FRF12 on the PVC ... 150
Configuring FRF.20 IP header compression properties ... 150
Enabling FRF.20 IP header compression ... 151
Configuring IP address for the PVC ... 152
Assigning a static route to a PVC ... 152
Configuring PVC policing ... 153
Configuring PVC shaping ... 154
Enable Layer 2 switching on the PVC ... 155
Configuring MFR ... 155
Configuring ack message timer and retries ... 155
Configuring number of links required to activate bundle ... 156
Configuring differential delay ... 157
Configuring fragment size ... 157
Configuring hello timer ... 158
Configuring segmentation threshold ... 158
Configuring AVCs ... 159
Configuring number of links required to activate the AVC ... 159
Enabling the AVC ... 160
Adding a PVC to the AVC ... 161
Enabling CVCs ... 161
Configuring MFR enhanced mode for a specified AVC ... 162
Configuring enhanced FRF.15 mode for all AVCs ... 162
Configuring differential delay ... 163
Configuring fragment size ... 164
Configuring segmentation threshold ... 164
Configuring AVC sequence ... 165
Configuring an IP address for the AVC ... 165
Enabling directed broadcasts on the AVC ... 166
Assigning a static route to an AVC ... 166
Assigning an IP address to the WAN bundle ... 167
Displaying Frame Relay information ... 167
Displaying the configured AVCs ... 167
Displaying the configured CVCs ... 168
Displaying the configured PVCs ... 168
Displaying virtual circuit statistics ... 168
Clearing virtual circuit statistics ... 169
Displaying inverse ARP statistics ... 169
Clearing inverse ARP statistics ... 169
Displaying inverse ARP time interval ... 169
Displaying LMI statistics ... 170
Clearing LMI statistics ... 170
Chapter 15: ADSL small module configuration ... 171

Navigation ... 171
Upgrading the ADSL small module software ... 171
Configuring the ADSL small module ... 172
Displaying the ADSL small module configuration ... 173
Displaying ADSL small module user statistics ... 174
Configuring ATM on an ADSL module ... 175
Configuring the maximum VC circuits ... 177
Chapter 16: WAN interface bundle optional parameter configuration ... 179
Configuring WAN interface bundle optional parameters ... 179
Chapter 17: Configuration examples ... 181
FR/MFR configuration ... 181
Frame relay configuration for SR 4134A and SR 4134C ... 181
MFR configuration between SR 4134A and SR 4134C ... 183
MFR configuration between SR 4134B and SR 4134C ... 184
Configuration of AVCs ... 186
Configure CVC1 ... 186
Configure CVC2 ... 187
Configure CVC3 ... 187
Configuring AVC ... 188
PPP/MLPPP and HDLC configuration ... 188
MLPPP Configuration ... 189
PPP and MLPPP Configuration ... 190
HDLC Configuration ... 190
BRI as backup interface using DDR with idle timeout ... 191
PRI as primary interface with no DDR ... 192
ADSL module configuration example ... 194
MPoA ... 194
IPoA ... 195
IPoE ... 195
Negotiated IPoE on an IPoE bundle ... 196
PPPoA ... 196
PPPoE ... 197

Chapter 1: Introduction

Purpose

This document describes the operation and configuration of the WAN module interfaces on the Avaya Secure Router 2330/4134 (Avaya SR 2330/4134).

Related Resources

Documentation

See the *Avaya Secure Router 2330/4134 Documentation Roadmap*, NN47263-103, for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com.

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

There are no new features in *Avaya Secure Router 2330/4134 Configuration — WAN Interfaces* (NN47263-500).

Important:

In this document, the term Secure Router 2330/4134 is used interchangeably to refer to the Secure Router 2330 and the Secure Router 4134.

Other changes

The following sections identify changes that are not feature related.

Interoperability with Silver Peak NX WAN optimization

Starting with Release 10.3.5, the Secure Router 2330/4134 interoperates with the Silver Peak NX-Series WAN optimization appliances.

For more information, see Silver Peak WAN optimization on page 17.

ISDN BR voice bundles with point-to-multipoint

ISDN BR voice bundles with a default TEI mode of point-to-multipoint will not come up until the bundle is manually updated to point-to-point.

For more information, see Configuring the TEI mode on page 117. This section has been updated based on information that was previously documented in the Secure Router 2330/4134 Release Notes.

Comments? infodev@avaya.com

Chapter 3: WAN module fundamentals

Silver Peak WAN optimization

The Secure Router 2330/4134 interoperates with the Silver Peak NX-Series WAN optimization appliances. The Secure Router serves as the branch office WAN router and a Silver Peak NX-Series appliance accelerates the LAN traffic. This solution provides an effective strategy for cost reduction towards the use of WAN technologies.

Note:

The Silver Peak appliance is a separate device; it does not run on the Secure Router. However, this solution underwent thorough interoperability testing in the Avaya Data Solutions Test Lab and is fully supported by Avaya. For more information on this testing and for a configuration example, see *Avaya Secure Router 4134 with Silver Peak NX-Series WAN Optimization Appliances Technical Configuration Guide* (NN48500-623).

WAN modules

The Avaya Secure Router 2330/4134 supports a number of different modules to provide WAN links. The following sections provide a description of the supported modules.

Important:

Slot 2 of the Secure Router 4134 supports only one port for any WAN data small module. Therefore, if you install any 2-port small module in this slot and use it for data connections, only one port is functional (port 1).

This limitation also applies to the 2-port T1/E1 and ISDN BRI small modules if they are configured for voice traffic: only port 2/1 is functional. However, this limitation does not apply to FXS or FXO voice modules.

T1/E1 modules

The Secure Router 2330/4134 provides support for T1/E1 connections using the following modules:

- 8-port T1/E1 medium module (supported on Secure Router 4134 only)
- 2-port T1/E1 small module
- 1-port T1/E1 small module

The T1/E1 interface operates at either 1.544 Mb/s (T1) or 2.048 Mb/s (E1). T1 provides support for 24 timeslots and E1 provides support for 31 timeslots.

The T1 connection is 100 ohms, and the E1 connection is 120 ohms.

With the T1/E1 modules 1-port and 2-port small modules only, you can also configure the modules to operate as Integrated Services Digital Network (ISDN) primary rate interface (PRI) connections, providing 23 (T1) or 30 (E1) bearer channels (B-channel) for data and 1 D-channel for signaling.

All of the T1/E1 modules provide support for the following encapsulations:

- PPP and MLPPP
- HDLC
- Frame Relay and MFR

Voice support on T1/E1 small modules

In T1 mode, the T1/E1 small modules can also provide the Secure Router 2330/4134 with voice connections to the PSTN using CAS signaling or ISDN PRI (voice is not supported in E1 mode). For more information on the voice subsystem, see *Avaya Secure Router 2330/4134 Configuration — SIP Media Gateway* (NN47263-508).

Mixed mode E1 Support for 8 port T1/E1 modules

The mixed mode E1 support allows for both E1 (31 channels per E1 port) and unframed E1 on the same 8 E1 port module. The 8 port module mixed E1 configurations are set through the carrier-type command like changing the module between E1 and T1. There are four new carrier types to support the mixed E1 configurations. In mixed mode, the channeled E1 ports are always first with the remaining ports set to unframed E1. There is no mixed mode for the small modules. The supported carrier types for 8 port T1/E1 modules mode settings are in the following table.

Comments? infodev@avaya.com

Carrier Type	Description
t1	8 T1 ports up to 16 channels per port
e1	8 E1 ports up to 16 channels per port
ue1	8 unframed E1 ports
c4u4	4 E1 ports up to 31 channels per port and 4 unframed E1 ports
c3u5	3 E1 ports up to 31 channels per port and 5 unframed E1 ports
c2u6	2 E1 ports up to 31 channels per port and 6 unframed E1 ports
c1u7	1 E1 ports up to 31 channels per port and 7 unframed E1 ports

PRI support has not changed and is only supported on the small modules.

To verify the carrier type currently active on a module the **`show system configuration`** command now shows the carrier type per module.

Standards compliance

The Secure Router 2330/4134 T1/E1 modules support the following standards:

T1

- ANSI T1.231, Telecommunications - Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring
- ANSI T1.403, Telecommunications - Network and Customer Installation Interfaces - DS1 Electrical Interface
- ANSI T1.408/T1.403.01, Telecommunications - Network and Customer Installation Interfaces - ISDN Primary Rate Layer 1 Electrical Interface Specification
- ATT TR-54016, Technical Reference Requirements For Interfacing Digital Terminal Equipment To Services Employing The Extended SuperFrame Format

E1

- ITU-T G.703, Series G: Transmission System And Media, Digital Systems And Networks; Digital Transmission Systems - Terminal Equipments - General; Physical/Electrical Characteristics Of Hierarchical Digital Interfaces
- ITU-T G.704, Series G: Transmission Systems And Media, Digital Systems And Networks; Digital Transmission Systems - Terminal Equipments- General; Synchronous Frame Structures And Used At 1544, 6312, 2048 and 44 736 Kbps Hierarchical Levels
- ITU-T G.826, Series G: Transmission And Media, Digital Systems And Networks; Digital Transmission Systems - Digital Networks - Quality And Availability Targets; Error Performance Parameters And Objectives For International, Constant Bit Rate Digital Paths

PSTN connectivity with T1/E1 BRI

PSTN connectivity with the ISDN BRI S/T interface is certified and is available for all countries and regions.

CT3 module

Note:

The CT3 module can operate in either CT3 mode or in DS3 clear channel mode. The default mode is CT3.

The Secure Router 4134 provides support for CT3 connections using the 1-port CT3 module. The CT3 interface operates at 44.736 Mhz, and can provide up to 28 T1 channels. The CT3 module provides support for the following encapsulations:

- PPP and MLPPP
- HDLC
- FR and MFR

The Secure Router 2330 does not support the CT3 module.

DS3 module

The Secure Router 4134 provides support for DS3 connections using the CT3 module in DS3 mode. The DS3 interface operates at 44.736 Mhz, with 44.210 Mhz available for data. The DS3 mode provides support for the following encapsulations:

- PPP
- HDLC
- Frame Relay and Multilink Frame Relay (bonding up to two CT3 modules in DS3 mode)

The Secure Router 2330 does not support the DS3 mode.

Standards compliance

The Secure Router 4134 CT3 module supports the following standards in both CT3 and DS3 modes:

- ANSI T1.101 – Synchronization Interface Standard
- ANSI T1.102 – Digital Hierarchy – Electrical Interfaces

- ANSI T1.107 – Digital Hierarchy – Formats Specifications
- ANSI T1.403 – Network and Customer Installation Interfaces – DS1 Electrical Interface
- ANSI T1.404 – Network and Customer Installation Interfaces – DS3 Metallic Interface Specification

Serial modules

The Secure Router 2330/4134 provides support for serial connections using the following modules:

- 1-port serial Small
- 2-port serial small

Each serial interfaces can operate at up to 2 Mb/s.

The Serial modules provide support for the following cable interfaces:

- V.35
- X.21
- RS-232
- RS-449
- EIA-530
- EIA-530A

The serial port can operate in either DTE or DCE mode. The default is DTE for all cable interface.

The Serial modules provide support for following encapsulations:

- PPP
- HDLC
- FR

No fractional channels are supported.

HSSI modules

The Secure Router 4134 provides support for high-speed serial connections using the 1-port HSSI medium module. The HSSI interface can operate at up to 52 Mb/s.

The HSSI module provides support for the following encapsulations:

- PPP
- FR
- HDLC

The HSSI interface can operate in either DTE or DCE mode. The default is DTE for all cable interface.

No fractional channels are supported.

The Secure Router 2330 does not support the HSSI module.

ISDN BRI modules

The ISDN BRI modules are designed for ISDN transmission of data over digital telephone networks. The basic rate interface (BRI), consists of two 64 kilobits per second (Kb/s) B channels for data and one 16 Kb/s D channel for control information.

The Secure Router 2330/4134 provides support for ISDN BRI using the 2-port S/T Small Module.

ISDN PRI is also supported on the 1-port and 2-port T1/E1 small modules, providing 23 (T1) or 30 (E1) B-channels for data and 1 D-channel for signaling.

ISDN BRI and PRI provide support for the following features:

- ISDN as primary/backup
- Dial-on-demand routing
- Idle timeout
- Connect delay
- CLIP
- P2P and P2MP (BRI only)
- Call back mechanism
- Support for the following switch types: dms100, ntt, 1tr6, vn3, ni2, euro, ccitt, 4ess, 5ess

The Secure Router 2330/4134 ISDN BRI and PRI provide support for the following encapsulations:

- PPP

You can use the ISDN BRI modules to provide backup network connectivity if the primary interface fails. The Dial-on-Demand Routing (DDR) feature on the ISDN BRI Small Modules enables you to configure the ISDN interface as a backup interface. Dial-on-demand enables you to establish a circuit on demand as opposed to having a leased-line connection, which is always available. By using a circuit on a demand basis, you can have a network connection only when you need it and significantly reduce your line costs.

ISDN BRI S/T

You can use the ISDN BRI S/T Small Module only at the user end (Terminal Equipment [TE]) of a point-to-point S/T, four-wire, interior S or T link. You cannot use the ISDN BRI S/T module as the NT end of an S/T link, or in passive bus or star applications. Terminating resistors are fixed on the module and cannot be removed.

The ISDN BRI S/T interface provides a data bandwidth of 128 Kbps (two 64 Kbps B-channels), and a 16 Kbps management channel (d-channel).

The ISDN BRI S/T module provides two ISDN BRI S/T interface ports, each supporting two data timeslots.

Voice support on ISDN BRI modules

The ISDN BRI modules can also provide the Secure Router 2330/4134 with voice connections to the PSTN. For more information on the voice subsystem, see *Avaya Secure Router 2330/4134 Configuration — SIP Media Gateway* (NN47263-508).

Standards compliance

The Secure Router 2330/4134 ISDN BRI modules comply with I.430 standards, and meet all other standard compliance of ISDN WAN interfaces.

ADSL modules

The Secure Router 2330/4134 supports Asymmetric Digital Subscriber Line (ADSL2+ g.992.5) functionality.

ADSL Overview

Digital Subscriber Line (DSL) technology enhances the data capacity of existing twisted-pair phone wire that runs between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000 Hz to filter noise off the voice line. To provide more bandwidth to improve access to the Internet, DSL operates in a frequency range above that of voice services, so the two systems can operate over the same cable.

There are seven types of DSL service, ranging in speeds from 16 Kbit/s to 52 Mbit/s. A DSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is

no dialing required. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity).

The Secure Router 2330/4134 supports ADSL2+ g.992.5, which is suitable for Internet users because more information is usually downloaded than uploaded. For example, a simple button click in a web browser can start an extended download that includes graphics and text.

ADSL small module

The ADSL small module is a hot swap capable interface module that installs onto the Secure Router 2330/4134 main board. With the hot swap feature, you can replace one module with another module of the same type while the system is operating, without affecting the system functionality. For information about the steps required to hot swap Secure Router 2330/4134 interface modules, see *Avaya Secure Router 2330/4134 Installation — Hardware Components,* (NN47263-301).

Important:

Avaya recommends that you shut down an operating interface module using the **`shutdown`** command before you remove it from the Secure Router 2330/4134 chassis.

The ADSL small module can be field-installed into an operating system at the rear panel of the Secure Router 2330/4134.

The Secure Router 2330/4134 supports a one-port ADSL Annex A WAN interface module.

You can use the ADSL small module for the following:

- as a backup replacement for an Integrated Services Digital Network (ISDN) interface

  When the ADSL small module is in backup mode, the routing protocol determines the best route based on routing parameters. Dial on demand functionality is not available in backup mode.

- as a primary interface

ATM

To allow traffic on an ADSL module, ADSL is used as the physical layer protocol and asynchronous transfer mode (ATM) is the link layer protocol. ATM on the ADSL module supports one virtual circuit (VC) that uses ATM Adaptation Layer 5 (AAL5) to format packets. AAL5 is a protocol that translates higher layer services into the size and format of an ATM cell. IP packets are encapsulated within AAL5 frames.

The Secure Router 2330/4134 supports the following AAL5 encapsulation types for encapsulating IP packets into ATM frames:

- Point to Point Protocol over ATM (PPPoA)
- Point to Point Protocol over Ethernet (PPPoE)

Comments? infodev@avaya.com

- IP over ATM (IPoA)
- IP over Ethernet (IPoE)
- Multi-Protocol Over ATM (MPoA)

Each ATM VC has a static or dynamic (DHCP or IPCP based) IP address and is identified by a virtual channel identifier (VCI) and a virtual path identifier (VPI). The VCI is a 16 bit field in the ATM cell header that identifies a virtual channel over which the cell is to travel. The VPI is an eight bit field in the ATM cell header which indicates the virtual path over which the cell is to be routed. The VCI in combination with the VPI constitute the ATM address, also called a VC address or just a VC.

Multiplexing

When configuring ATM VCs, you have two ways of carrying protocols over ATM and this is done by multiplexing. Be sure to use the multiplexing method required by your ISP.

VC-based multiplexing (AAL5MUX)

With VC-based multiplexing, each protocol is assigned to a specific virtual circuit (for example, VC1 carries IP only). In other words, the user defines one VC per protocol. This uses more VCs than LLC-based multiplexing, but reduces overhead, because a header is not necessary. VC-based multiplexing is dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based multiplexing (AAL5SNAP)

For LLC multiplexing, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In other words, the user multiplexes multiple protocols over a single ATM VC. Despite the extra bandwidth and processing overhead, this method can be advantageous if it is not practical to have a separate VC for each carried protocol.

How the Secure Router 2330/4134 connects to the Internet using ADSL

The following diagram shows how the Secure Router 2330/4134 connects to the Internet using ADSL. The physical connection is through a regular RJ-11 telephone cable plugged into a telephone port. This connection leads to a DSL Access multiplexer (DSLAM), which has an ATM connection to an Access Concentrator (ATM/IP Router) that connects to an IP network.

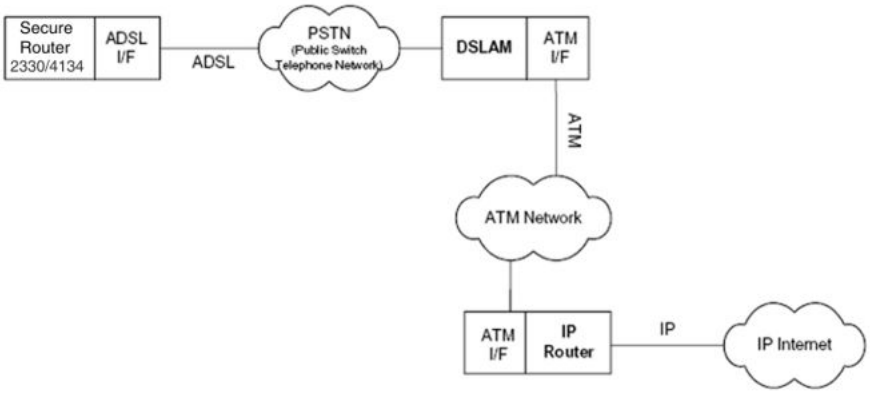


Figure 1: Secure Router 2330/4134 Internet connection using ADSL

ADSL small module standards compliance

The Secure Router 2330/4134 ADSL small module supports the following standards:

- PPP over AAL5
- PPP over Ethernet (PPPoE)
- multiprotocol encapsulation over Asynchronous Transfer Mode (ATM) adaptation Layer 5
- definitions of managed objects for the ADSL lines

ADSL small module limitations

The following ADSL small module limitations exist with the Secure Router 2330/4134 for Release 10.2.

- The ADSL small module does not support inverse address resolution protocol (ARP).
- The ADSL small module does not support definitions of extension managed objects for ADSL.
- The ADSL small module does not support the ADSL line extension MIB.
- The ADSL small module does not support ADSL2/2+ definition of managed objects for ADSL2/2+ lines.
- The ADSL small module supports only single PVC.
- The ADSL small module does not support protocols.
- The ADSL small module list of supported modulation modes must be configured as required by the ISP.

Voice Carrier medium module

The Voice Carrier medium module can house up to four small FXS or FXO modules. With this module, you can expand the number of available small slots on the SR 4134. You can install FXS or FXO modules only in the Voice Carrier module. With the Voice Carrier Medium module, the SR 4134 Media Gateway can accommodate a total of up to 64 FXS/FXO ports. However, only 16 total FXS/FXO ports are tested and qualified for this release.

For Voice Carrier medium module scaling information, see *Avaya Secure Router 2330/4134 Configuration- SIP Media Gateway* (NN47263-508).

Comments? infodev@avaya.com

Chapter 4: WAN encapsulation fundamentals

The following sections describe the encapsulations that are supported on the WAN interfaces. For a list of encapsulations supported on each module, refer to the appropriate module description in the preceding sections.

WAN bundle logical interface

In order to configure the encapsulation and IP address for a WAN interface, you must first associate the interface with a bundle. A bundle is a single, high speed virtual path consisting of one or more physical links. The Avaya Secure Router 2330 supports a maximum of 100 concurrent WAN bundles. The Avaya Secure Router 4134 supports a maximum of 500 concurrent WAN bundles.

All interfaces other than Ethernet ports must be associated with a bundle.

HDLC

HDLC is a WAN protocol that supports full-duplex transmission over a point-to-point communication link. The integrity of the link is checked periodically using keep alive messages.

PPP

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. These links provide full-duplex simultaneous bi-directional operation and deliver packets in order.

PPP is a set of layered protocols. The basic link is established using the Link Control Protocol (LCP). The use of an Authentication Protocol is optional, and if activated, it is negotiated during the LCP phase. Once the basic link is established, a set of Network Control Protocols (NCP) can then negotiate over the link.

Therefore, PPP as a whole is a Link Layer protocol, formed by three sub-layers of operation (LCP, Authentication and NCP). The LCP layer configures the physical interface to conform to certain parameters, authentication provides security and NCP interfaces with the network layer.

The following figure shows the relationship of the PPP Layers within the OSI model:

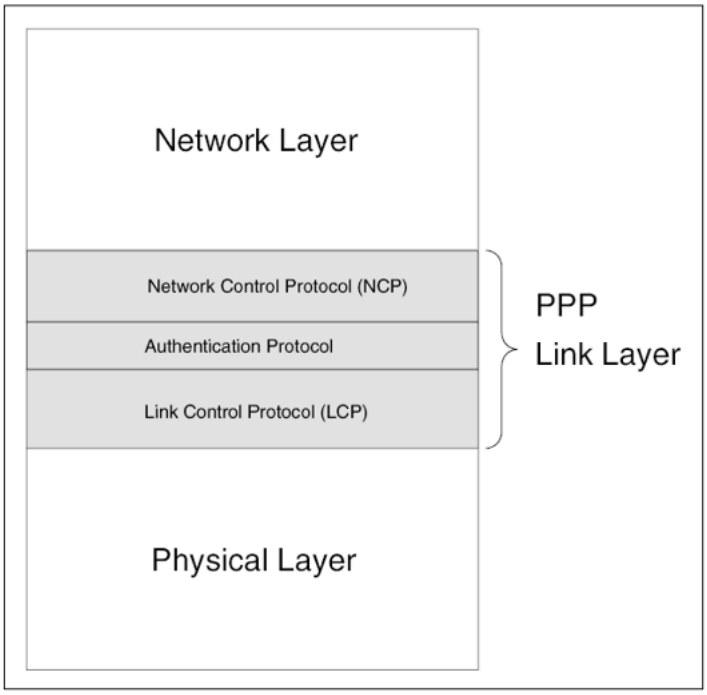


Figure 2: PPP layers within OSI model

At the lowest level, PPP sessions can be enabled on each DS0.

Link Control Protocol (LCP)

To allow two PPP nodes to agree on a set of parameters for the creation of a link, PPP uses the Link Control Protocol (LCP). Link Control Protocol implements procedures to establish the link, negotiate various options for the link, and finally to terminate the link to tear down the session. LCP is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, and detect a looped-back link and other common configuration errors

LCP generates three types of packets:

- Link configuration packets, including configure-request, configure-ACK, configure-NAK, and configure-reject packets
- Link termination packets, including terminate-request and terminate-ACK packets
- Link maintenance packets, including code-reject, protocol-reject, echo-request, and echo-reply packets

Link negotiation with LCP

When two devices initialize a PPP dialog, each sends a configure-request packet to the other. Each configure-request packet contains a list of LCP options and corresponding values that the sending device uses to define its end of the link.

For example, a configure-request packet can specify the maximum receive unit (MRU) size for the link. The configure-request packet contains the user-configured values, which the sender and the peer router need to negotiate.

Each router receives a configure-request packet from its peer. Each router responds with one of three types of packets:

- Configure-Reject

  If the configure-request packet contains options that the peer router is not willing to negotiate, the peer router sends back a configure-reject packet specifying the nonnegotiable options. From that point on, configure-request packets that the originating router sends should eliminate the unacceptable options.

- Configure-NAK

  If the negotiating end point disagrees with some or all of the values of the proposed options in the configure-request packet, it responds with a Configure Negative Acknowledgment (NAK) packet. The Configure-NAK packet notes the values that the end point disagrees with, and it includes the corresponding values that the end point would like to see in subsequent Configure-Request packets.

- Configure-ACK

  If a router accepts the proposed LCP options, it responds with a Configure Acknowledgment (ACK) packet.

  When the routers on each side of the link send and receive configure-ACK packets, the LCP advances to an open state, which means that the PPP interface can advance to the next phase.

LCP negotiations between sending and receiving devices continue until either:

- Both devices converge (reach an agreement regarding the configure-request).
- The receiving device transmits a specified number of configure-NAK packets before sending a configure-reject packet.
- The convergence timer expires.

Authentication

Authentication protocols are intended for use primarily by hosts and routers that connect to a PPP network server via switched circuits or dial-up lines, but might also be applied to dedicated links as well. The authentication phase operates in between the LCP and NCP negotiation phases. Authentication is optional and if the entity negotiating PPP desires the peer to authenticate, it specifies the authentication protocol it wishes its peer to negotiate during the LCP negotiation phase. Any failure during the authentication phase results in the termination of the links.

In the authentication phase of PPP initialization, one or both peer routers can enable either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). PPP can also interface with AAA (RADIUS) for username and password validations.

Password Authentication Protocol

PAP imposes network security by requiring the peer router to send a PAP packet that contains a plain text user identifier and password to the originating router before the interface can advance to the network layer protocol phase.

If PAP fails, the network administrator must change the identifier and password on both peer routers and disable and re-enable LCP to re-initialize the line.

Challenge Handshake Authentication Protocol

CHAP imposes network security by requiring that the peers share a plain-text secret. The originating peer sends a challenge message to its receiving peer. The receiving peer responds with a value it calculates on the basis of knowing the secret. The first peer then matches the response against its own calculation of what the response should be. If the values match, it sends a success message, and the LCP establishes the link.

CHAP uses an incrementally changing identifier and a variable challenge value to provide network security. It also allows for repeated challenges at intervals that either router on a link can specify. A router can transmit challenge packets not only during the link establishment phase, but also at any time during the network layer protocol phase to ensure that the connection retains its integrity.

If CHAP fails, the network administrator must change the identifiers and secret on both peer routers and disable and re-enable LCP to re-initialize the line.

RADIUS

With the Secure Router 2330/4134, you can also implement PAP or CHAP authentication in conjunction with a RADIUS server. The username and password can reside locally on the system or on the RADIUS server.

One-way authentication

One-way authentication uses an authentication protocol on only one side of a dial-up connection. The router placing the call disables the authentication protocol for a circuit, while the router on the receiving side enables authentication. Disabling the outbound authentication lets the router interoperate with other devices that may not allow two-way authentication or support CHAP.

The receiving router does not allow a change in the authentication method. When the router receives a call, it authenticates using the user-configured protocol. If the calling router rejects the authentication protocol, for example CHAP, the receiving router cannot automatically switch to PAP, and so the link cannot converge.

Network Control Protocol (NCP)

The Network Layer Protocol is the link between PPP and the network layer protocols such as IP. PPP uses various network control protocols to determine the values of parameters during network layer negotiations, which is the final phase of PPP initialization. Similar to the LCP, each network control protocol allows the devices to negotiate various network options over the data link by transmitting configure-request, configure-ACK, configure-NAK, and configure-reject packets.

Networks options include which network addresses to use and which media types to bridge. Once both devices agree upon networks options, the network control protocol reaches the open state. The devices then begin transmitting user data packets for upper-layer protocols over the link.

NCP has a set of procedures to establish the NCP layer, negotiate various options and to tear down the NCP session. There is a NCP for each network protocol for example, IPCP for IP networks, IPv6CP for IPv6 networks, and so on.

The Secure Router 2330/4134 supports the following NCPs:

- Internet Protocol Control Protocol (IPCP)
- IPv6 Control Protocol (IPv6CP)

- Bridging Control Protocol (BCP)
- MPLS Control Protocol (MPLSCP)

IPCP

IP Control Protocol (IPCP) establishes and configures IP over PPP by enabling PPP to negotiate IP addresses. IPCP also enables and disables IP interfaces on a point-to-point link. IPCP uses the same packet exchange mechanism as LCP.

IPv6CP

IPv6 Control Protocol (Iv6PCP) establishes and configures IPv6 over PPP and MLPPP interfaces. Multiple IPv6 addresses can be configured on one interface.

Bridge Control Protocol (BCP)

Bridge Control Protocol (BCP) is a type of NCP used for forwarding messages from one network to another without reference to their network layer information. BCP can provide methods of carrying Ethernet frames over PPP.

The Secure Router 2330/4134 supports two implementations of BCP, one to support LAN traffic, and the other to support VLAN traffic. In the LAN setting, if the PPP interface receives untagged packets, it forwards them; in the VLAN setting, if the PPP interface receives VLAN-tagged packets, it forwards them.

MPLSCP

The Secure Router 2330/4134 also supports MPLSCP which allows MPLS traffic to travel over PPP encapsulated links. For more information on MPLS, refer to Configuration – MPLS (NN47263-505).

MLPPP

The Secure Router 2330/4134 also provides support for Multilink PPP (MLPPP), which is the capability of splitting and recombining sequenced PPP packets across multiple logical or physical interfaces.

When the bandwidth requirements go beyond the bandwidth available on a single link, Multilink PPP can be used to provide more bandwidth. MLPPP is based on an LCP option negotiation that permits a system to indicate to its peer that it is capable of combining multiple physical links into a logical bundle. Multilink preserves ordering by introducing a sequence number for each fragment that goes out on the individual links. MLPPP can also provide load balancing of traffic between the bundled links.

Comments? infodev@avaya.com

Link Fragmentation and Interleaving

Secure Router 2330/4134 PPP supports link fragmentation and interleaving (LFI).

With fragmentation, the sending nodes fragment IP packets into smaller packets with sequence numbering so that latency through the PPP network is minimal.

With interleaving, the router sends high-priority packets (such as voice) in between fragments of large packets that have been fragmented due to their size. This minimizes the serialization delay of voice packets across low-speed interfaces such as T1/E1.

Compressed RTP

Compressed RTP (cRTP) is a QoS feature that is required for bandwidth-limited wide area connections. Bandwidth limited connections are wide area links with less than T1 (1.54Mbps) speeds. Compressed RTP reduces the number of times the complete VoIP header needs to be sent, thereby reducing the volume of traffic on the network.

The cRTP compression method sends a complete IP/UDP/RTP header over the PPP connection at the beginning of every flow to provide all the header information for the egress end of the PPP connection. This is followed by sending only the information that changes in the header encoded into 2-4 bytes.

cRTP can be used on MLPPP bundles as well as PPP bundles. Currently, cRTP is supported only on IPv4. The interface must be configured with an IPv4 address before cRTP can be enabled on the interface.

Some of the configuration considerations with cRTP are as follows:

- Max-header size that can be compressed/decompressed is 40 bytes. This value is not configurable.
- Only RTP packets can be compressed.
- Packets with IP options are not compressed.
- TCP header compression is not supported.
- If the Secure Router using cRTP is in networks with existing Secure Routers running code earlier than 9.2 for 3120 and SR1000, use the CLI command ‘no negotiation’ for the backward compatibility mode.

Standards compliance

The Secure Router 2330/4134 implementation of PPP supports the following standards:

- RFC 1661 – Point-to-Point Protocol
- RFC 1662 – PPP in HDLC-like Framing
- RFC 1334 – PAP Authentication Protocol
- RFC 1994 – CHAP Authentication Protocol
- RFC 1332 – PPP Internet Protocol Control Protocol (IPCP)
- RFC 1990 – MultiLink PPP protocol (MLPPP)
- RFC 2472 – IPv6 over PPP
- RFC 3518 – PPP Bridging Control Protocol (BCP)
- RFC 3032 – MPLSCP
- RFC 1471 -- The Definitions of Managed Objects for the LCP of the PPP.
- RFC 1473 -- The Definitions of Managed Objects for the IPCP of the PPP.

Frame Relay

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

Frame relay is a synchronous HDLC protocol based network. Data is sent in HDLC packets, referred to as frames.

Frame relay is a Layer 2 connection-oriented protocol, which means that it relies on existing end-to-end paths between devices connected across the network. It implements these connections using permanent virtual circuits (PVCs).

Frame relay assumes that networks use transmission lines with low error rates, such as digital transmission media. Consequently, frame relay provides only basic error detection with no error recovery. This minimizes the processing required for each packet, allowing frame relay networks to operate at higher speeds with fewer network delays.

Because frame relay performs only basic error checking, end stations running upper-layer protocols such as Internet Protocol (IP) are responsible for resending packets that did not transmit correctly the first time.

PVC

A permanent virtual circuit (PVC) is a dedicated logical path within a Frame Relay connection that connects two devices over a network. This path between the source and destination point is a dedicated connection, so the PVC is always available to the connected devices. Because many PVCs can coexist on one physical line, devices can share the bandwidth of the same transmission line.

The permanent virtual circuit (PVC) is identified by the DLCI identification number. The frame relay network uses the DLCI to direct basic data flow.

Address resolution for PVCs

Within the frame relay network, frames travel through a series of switches to arrive at their destination. Each frame has an address that the network uses to determine the destination of the frame.

Address resolution for PVCs maps a remote network address such as an IP address to a local DLCI number. To perform this mapping, IP uses the Address Resolution Protocol (ARP). ARP dynamically generates an ARP table of addresses and DLCI numbers by sending messages back and forth to each network node to gather address information. This process increases broadcast traffic across the network.

UNI interface

The Secure Router 2330/4134 supports FRF.1.2, which describes the User to Network Interface (UNI) features for PVC creation and maintenance. This is the connectivity from the DTE (data terminating Equipment) at the subscriber end to the Frame Relay edge device at the service provider end (data circuit-terminating equipment [DCE]).

The frame relay frames follow the Q.922 Annex A format as defined by ITU-T.

NNI interface

The Secure Router 2330/4134 supports FRF.2.2, which describes the Frame Relay Network to Network interface (NNI) features, which include directly connecting Frame Relay devices between two Frame Relay networks, rather than connecting to a Frame Relay DCE device at the service provider edge. An NNI interface can only connect with another NNI interface.

FRF.12 fragmentation

The Secure Router 2330/4134 supports FRF.12, which is a backward compatible, lightweight fragmentation protocol and is configurable on one or more PVCs of a Frame Relay bundle. With FRF.12, Frame Relay DTEs and DCEs fragment long frames into sequences of shorter frames. Upon arrival, the fragments are reassembled into the original frame by the receiving peer DTE or DCE.

When used in combination with interleaving, serialization delay of voice packets over low speed frame links can be reduced resulting in performance enhancements. Interleaving is configurable on a Frame Relay bundle basis. On low speed links, FRF.12 can be used to fragment low priority data of large size (approximately 1500 bytes) into smaller fragments and then interleave with high priority voice traffic.

FRF.12 can be helpful when a single PVC in a branch office location is needed to transport both voice and data over a FR WAN or for separate PVCs in a FR interface used in carrying voice or data.

The following are some FRF.12 design considerations:

- On AVCs (FRF.15 End-to-end MFR), the FRF.12 feature is supported, but interleaving is not supported.
- Oversubscription of bandwidth on the Frame Relay bundle is not allowed when interleaving is enabled.
- Class Based Queuing (CBQ) over Frame Relay feature is not recommended on Frame Relay bundles with interleaving enabled.
- 0 –CIR PVCs can not be supported on the FR bundles with interleaving enabled.
- FRF.12 fragmentation is not currently supported on the bridged PVCs.
- Interleaving can only be enabled when FRF.12 fragmentation is configured on at least one PVC in a Frame Relay bundle.
- Interleaving on a bundle is automatically disabled when FRF.12 is disabled on all the PVCs of the bundle. It has to be re-enabled manually when FRF.12 is re-provisioned on the PVC.
- Assumes that IP packets are marked with proper DSCP value before reaching the outgoing Frame Relay PVC.

Local Management Interface (LMI)

Frame relay uses the Local Management Interface signaling standard to exchange information about the interface and the status of each virtual circuit.

Comments? infodev@avaya.com

The Secure Router 2330/4134 supports the following LMI types in both UNI and NNI type interfaces:

- ITU-T Q933 Annex A (Q933A)
- ANSI T1.617 Annex D (ansi)
- Cisco (Stratacom)
- None (no LMI option)

  None provides no management interface between the router and the frame relay network. In the absence of management support, you must configure all PVCs manually.

Be sure to configure the frame relay interface on the Secure Router 2330/4134 to use the same management protocol as the switched network to which it is connected.

SR 4134 currently supports ASYNC status update as default. For customer-premises equipment (CPE) or access router devices like the Secure Router 2330/4134, Avaya recommends that this configuration be always ON to avoid CPE status UP delay and to improve system up time and performance.

IP Header compression over FR

The Secure Router 2330/4134 supports FRF.20, which provides IP header compression over Frame Relay.

Multi-protocol Encapsulation over FR

The Secure Router 2330/4134 supports RFC 2427, FRF.3 (obsoletes RFC1490), which defines the method to encapsulate IP, LAN, VLAN and any other layer 2/3 packets over the frame relay DTE PVC circuits.

This includes both fragmentation and multi-protocol encapsulation.

The Secure Router 2330/4134 supports, on both FR and MFR interfaces, the following layer 2/3 traffic:

- IPv4

  One IP address (and subnet) per PVC can be configured
- bridging of IEEE 802.3 Ethernet traffic
- bridging of IEEE 802.1Q VLAN traffic

  Many VLAN IDs (flows) can be transmitted over a single PVC.
- bridging of virtual LAN domains (VLDs)

Many VLD ids (flows) can be transmitted over a single PVC.

- IPv6

  One or more IPv6 address per PVC can be configured

Inverse ARP

The Secure Router 2330/4134 supports inverse ARP, where the PVC dynamically learns the IP address of the remote peer.

MFR

Multilink Frame Relay (MFR) is composed of two standards: FRF.15 and FRF.16.1. The latter is more common and defines UNI/NNI interfaces for implementing MFR. FRF.16.1 is used for multiplexing dedicated T1s in the local loop and requires compatible equipment at the carrier point of presence (POP). With FRF.15 or DTE-to-DTE MFR, the router multiplexes frame relay T1s between end points without impacting POP equipment. As a result, FRF.15 can be implemented across multiple frame relay carriers to provide additional redundancy. The Secure Router 2330/4134 supports FRF.15 and FRF.16, allowing for link aggregation as follows:

- Full T1s can be bonded
- Full E1s can be bonded
- T1s within a CT3 can be bonded
- T1/E1s from different WAN modules within the same system can be bonded
- Up to 2 clear channel DS3s can be bonded
- Same set of DS0s can be bonded. For example, DS0 1 to 10 of T1#1 can be bonded with DS0 11 to 20 of T1#2.

FRF.15 uses an aggregated virtual circuit (AVC) for the combined interface. The AVC is composed of constituent virtual circuits (CVC) that represent the frame relay T1s ordered from the carrier.

In Secure Routers, CVCs are configured using bundles. After the CVCs are configured, they can be assigned to the AVC. The AVC names and DLCI numbers can be different on each end if necessary.

Avaya recommends that when you use End-to-End MFR to aggregate PVCs, the PVCs have the same shaping and policing parameters.

Jumbo Frames

The Secure Router 2330/4134 Frame Relay supports Jumbo frames up to 9216 bytes.

Frame Relay congestion control

Network congestion can degrade network performance. Congestion occurs when a node receives more frames than it can process, or sends more frames than the transmission line can handle. When congestion occurs in the network, the Frame Relay devices can inform the nodes of congestion, so that they can reduce the amount of traffic across the network.

In the Frame Relay packet header, there are two bits that the devices can set to alert nodes of network congestion. These bits are the FECN (forward explicit congestion notation) bit and the BECN (backward explicit congestion notation) bit.

If the network detects congestion, it alerts the router in the same direction as the received frame by changing the frame's FECN bit from 0 to 1. For nodes in the opposite direction of the received frame, it changes the frame's BECN bit from 0 to 1.

If you enable the congestion control feature, you can specify the number of FECN/BECN bits the router receives in a given time period before it stops transmitting frames. While frames are going across the network, the frame relay interface checks received packets for FECN and BECN bits set to 1. If the interface receives the specified number of bits during the designated time period, frame relay drops all traffic destined for the PVC where there is congestion. When the interface no longer receives these congestion notifications, the router resumes transmission.

For example, suppose you set the congestion timer to 0.5 seconds and the congestion count to 3. In this case, if an interface receives 3 FECNs or BECNs within 0.5 seconds, the node stops sending frames (although it continues to receive frames for this PVC). If the interface receives no FECNs or BECNs during the next 0.5 seconds, the router resumes transmission.

If you enable congestion control and also enable traffic shaping, you can queue or throttle congested traffic rather than drop it by choosing that value in the Congestion Method parameter.

Frame Relay Traffic Management

The Secure Router 2330/4134 supports per-PVC shaping based on the Committed Information Rate (CIR), Committed Burst (BC) and Excess Burst (BE) parameters. The Secure Router 2330/4134 can also support policing, based on the CIR, BC, BE, and Discard Eligible (DE) parameters. With policing, the system responds to Discard Eligible (DE) frames. Upon transmitting a frame, if the system is congested, the router marks the DE bit.

Alternatively, the system can support Class Based Queueing (CBQ) on a per bundle basis. Using user-specified hierarchical classifications, the CBQ feature can shape multiple packet flows and can support up to 8 priorities. RED can also be configured on each packet queue. For details, see Performance Management – Quality of Service (NN47263-601).

When CBQ is enabled, Frame Relay policing can be enabled, but Frame Relay traffic shaping is bypassed since the shaping happens at Layer 3. (CBQ and QoS policing are mutually-exclusive.)

Standards compliance

The Secure Router 2330/4134 implementation of Frame Relay supports the following standards:

MIBs

- RFC1315

RFCs

- RFC1490
- RFC2390
- RFC2427

Frame Relay Forum implementation agreements

- FRF1.2
- FRF 2.2
- FRF3
- FRF12
- FRF15
- FRF16
- FRF20

Configuration of PPP and Frame Relay interfaces as Layer 2 switched interfaces

Any bundle interface that is configured with PPP or Frame Relay encapsulation can be configured as an Ethernet Layer 2 switched interface. All Ethernet Layer 2 features (including VLANs, MSTP, GVRP, and IGMP snooping) are supported on these interfaces, with the exception of LACP and port mirroring. The commands used to configure the bundles are the

same as those used to configure Ethernet ports. For detailed information on these commands, refer to *Avaya Secure Router 2330/4134 Configuration—Layer 2 Ethernet* (NN47263-501).

Comments? infodev@avaya.com

Chapter 5: T1/E1 module configuration

1. Configure the carrier type.
2. Configure properties

   If desired, you can enable a T1/E1 link using the default properties.
3. Assign one or more T1/E1 links to a WAN bundle.
4. Configure encapsulation for the bundle.
5. Assign IP address to the bundle.

Setting the carrier type on T1/E1 modules

Configure the carrier type for the T1/E1 module to support T1 or E1 links. You must reboot the router in order for the configuration to take effect.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```
2. To select the module and carrier type, enter:

   ```
   system carrier-type <slot> {t1 | e1}
   ```
3. To exit the configuration mode, enter:

   ```
   exit
   ```
4. To reboot the Avaya Secure Router 2330/4134, enter:

   ```
   reboot
   ```

Configuring T1 interface properties

Configuring T1 framing

Set the framing mode for a T1 link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T1 module port to configure, enter:

   ```
   module t1 <slot/port>
   ```

3. To configure framing, enter:

   ```
   framing {esf | d4}
   ```

Table 1: Variable definitions

Variable	Value
esf	Extended Super Frame framing format for T1 (default)
d4	Super Frame framing format for T1

Configuring T1 linecode

Set the type of line coding for a T1 link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T1 module port to configure, enter:

   ```
   module t1 <slot/port>
   ```

3. To configure the linecode, enter:

   ```
   linecode {b8zs | ami}
   ```

Table 2: Variable definitions

Variable	Value
ami	AMI linecode for T1
b8zs	B8Zs linecode for T1 (default).

Configuring T1 yellow alarm detection and generation

Set the yellow alarm operation on a T1 link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T1 module port to configure, enter:

   ```
   module t1 <slot/port>
   ```

3. To configure yellow alarm, enter:

   ```
   yellow_alarm {generate | detect | gen_det | disable}
   ```

Table 3: Variable definitions

Variable	Value
detect	Detect incoming yellow alarms from the network.
disable	Disable yellow alarm generator.
gen_det	Generate and detect yellow alarms (default state).
generate	Generate and send yellow alarms to the network.

Configuring T1 clock source

Configure the clock source to set the network timing source for a T1 link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T1 module port to configure, enter:

   ```
   module t1 <slot/port>
   ```

3. To configure the clock source, enter:

   ```
   clock_source {network | internal | line}
   ```

Table 4: Variable definitions

Variable	Value
backplane	Sets the clock source to the backplane of the Secure Router 2330/4134.
internal	Sets the clock source to the internal clock of the Secure Router 2330/4134 (default).
line	Sets the clock source to be recovered from the incoming T1 signal (loop timing).

Configuring T1 alarm thresholds

Set the T1 user statistic alarm thresholds.

When user-configurable thresholds are exceeded, the Secure Router 2330/4134 generates alarms that indicate the possible deterioration of a T1 link. Refer to the following parameters to determine the specific T1 data type that needs to be configured. You can define one alarm threshold for each parameter.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T1 module port to configure, enter:

   ```
   module t1 <slot/port>
   ```

3. To configure the alarm for user statistics, enter:

   ```
   alarms thresholds user <1 - 10>
   [ ses | es | uas | eev | css | oof | crc | bpv ]
   <sampling-interval> <rising-threshold> <falling-threshold>
   sample_type [ absolute | delta ]
   ```

Table 5: Variable definitions

Variable	Value
1-10	Alarm threshold number.
absolute | delta	absolute: The errored second or event count is compared directly to the specified threshold values, and the appropriate alarm type (rising or falling) is reported. delta: The errored second or event count is compared to the difference between the rising and falling thresholds, and a rising alarm is reported if the actual error count exceeds that difference. This is the default setting if you do not specify a sampling type.
ses | es | uas | eev | css | oof | crc | bpv	Specifies the threshold type: bpv: Threshold for bipolar violation crc: Threshold for cyclic redundancy check css: Threshold for controlled slip second eev: Threshold for esf error events es: Threshold for errored seconds oof: Threshold for out of frame ses: Threshold for severely errored seconds uas: Threshold for unavailable seconds
falling-threshold	Minimum number of errored seconds or events below which a falling alarm is reported. This alarm is reported if a rising alarm was previously reported and the number of errored seconds or events subsequently dropped below this

Comments? infodev@avaya.com

Variable	Value
	minimum threshold. The falling threshold value must be less than the rising threshold value above. The range is 0 - 2147483647.
rising-threshold	Number of errored seconds or events which, if exceeded during any sampling interval, results in a rising alarm. The range is 0 - 2147483647
sampling-interval	Sampling interval, in seconds. The range is 1 - 65535.

Configuring hierarchy for T1 alarms

Enable or disable the hierarchy for displaying Receive Loss of Signal (RLOS) and Receive Loss of Frame (RLOF) on a T1 link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T1 module port to configure, enter:

   ```
   module t1 <slot/port>
   ```

3. To configure hierarchy, enter:

   ```
   [no] alarms hierarchy
   ```

Table 6: Variable definitions

Variable	Value
no	Disables hierarchy.

Configuring CSU line mode for T1

Set the amount of T1 line build out (LBO) for the Channel Service Unit (CSU) interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T1 module port to configure, enter:

   ```
   module t1 <slot/port>
   ```

3. To configure CSU line mode, enter:

```
linemode csu lbo {db_zero | db7_5 | db15 | db22_5}
```

Table 7: Variable definitions

Variable	Value
db7_5	Configure LBO for zero db (default)
db15	Configure LBO for 7.5 db
db22_5	Configure LBO for 15 db
db_zero	Configure LBO for 22.5 db

Configuring DSX line mode for T1

Set the amount of T1 signal equalization based on the cabling distance to the DSX cross-connect.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T1 module port to configure, enter:

   ```
   module t1 <slot/port>
   ```

3. To configure DSX line mode, enter:

   ```
   linemode dsx cable-length <length>
   ```

Table 8: Variable definitions

Variable	Value
<length>	1: specifies cable length of 0-110 2: specifies cable length of 110-220 3: specifies cable length of 220-330 4: specifies cable length of 330-440 5: specifies cable length of 440-550 6: specifies cable length of 550-660

Configuring T1 circuit ID

Specify an optional circuit ID to a T1 interface.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the T1 module port to configure, enter:

```
module t1 <slot/port>
```

3. To configure the T1 circuit ID, enter:

```
circuitId [cktID] <circuit-id>
```

Table 9: Variable definitions

Variable	Value
circuit-id	Optional circuit ID for the T1 channel.

Configuring contact information for T1

Specify contact information for a person who can provide information regarding the T1 link.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the T1 module port to configure, enter:

```
module t1 <slot/port>
```

3. To configure the contact information, enter:

```
contactInfo <contact-info>
```

Table 10: Variable definitions

Variable	Value
contact-info	Person to contact for information regarding the T1 link.

Configuring description for T1

Enter a description for the T1 interface.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the T1 module port to configure, enter:

```
module t1 <slot/port>
```

3. To enter the description, enter:

```
description <port-description>
```

Table 11: Variable definitions

Variable	Value
port-description	Describes the T1 interface.

Configuring a name for T1

Assign a name to the T1 link.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the T1 module port to configure, enter:

```
module t1 <slot/port>
```

3. To assign a name to the T1 link, enter:

```
name <name>
```

Table 12: Variable definitions

Variable	Value
name	Assigns a name to the T1 link (max 15 bytes).

Configuring loopback framing for T1

Set overwriting or insertion of framing for in-band loopcode.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the T1 module port to configure, enter:

```
module t1 <slot/port>
```

3. To configure loopback framing, enter:

```
loopback_framing {overwrite | insert}
```

Table 13: Variable definitions

Variable	Value
overwrite	Overwriting of framing for in-band loopcode for T1 (default).
insert	Insertion of framing for in-band loopcode for T1.

Enabling the T1 interface

Enable the T1 interface to allow the link to transmit and receive data.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T1 module port to configure, enter:

   ```
   module t1 <slot/port>
   ```

3. To enable the selected T1 module port, enter:

   ```
   [no] enable
   ```

Table 14: Variable definitions

Variable	Value
[no]	Takes the T1 link out of service. This action sends an all-ones Alarm Indication Signal (AIS) to the far end and places the link out of service.

Configuring E1 interface properties

Configuring E1 framing

Set the framing mode for the E1 link.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the E1 module port to configure, enter:

```
module e1 <slot/port>
```

3. To configure framing, enter:

```
framing {crc | non_crc | disable}
```

Table 15: Variable definitions

Variable	Value
crc	Specifies CRC framing format for E1 (default).
non_crc	Specifies non-CRC framing format for E1
disable	Disables the E1 framer.

Configuring E1 linecode

Set the type of line coding for the E1 link.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the E1 module port to configure, enter:

```
module e1 <slot/port>
```

3. To configure the linecode, enter:

```
linecode {hdb3 | ami}
```

Table 16: Variable definitions

Variable	Value
ami	AMI linecode for E1
hdb3	HDB3 linecode for E1 (default).

Configuring E1 yellow alarm detection and generation

Configure the yellow alarm operation on the E1 link.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the E1 module port to configure, enter:

```
module e1 <slot/port>
```

3. To configure yellow alarm, enter:

```
yellow_alarm {generate | detect | gen_det | disable}
```

Table 17: Variable definitions

Variable	Value
detect	Detect incoming yellow alarms from the network.
disable	Disable yellow alarm generator.
gen_det	Generate and detect yellow alarms (default state).
generate	Generate and send yellow alarms to the network.

Configuring E1 clock source

Configure the clock source to set the network timing source for an E1 link.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the E1 module port to configure, enter:

```
module e1 <slot/port>
```

3. To configure the clock source, enter:

```
clock_source {internal | line}
```

Table 18: Variable definitions

Variable	Value
internal	Sets the clock source to the internal clock of the Secure Router 2330/4134 (default).
line	Sets the clock source to be recovered from the incoming E1 signal (loop timing).

Configuring E1 alarms

When thresholds are exceeded, the system generates alarms that indicate the possible deterioration of an E1 link. You can define one alarm threshold for each available parameter.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the E1 module port to configure, enter:

   ```
   module e1 <slot/port>
   ```

3. To configure the alarm for user statistics, enter:

   ```
   alarms thresholds user <1 - 10>
   [ ses | es | uas | css | oof | crc | bpv ]
   <sampling-interval> <rising-threshold> <falling-threshold>
   sample_type [absolute | delta]
   ```

Table 19: Variable definitions

Variable	Value
1-10	Alarm threshold number.
absolute	The errored second or event count is compared directly to the specified threshold values, and the appropriate alarm type (rising or falling) is reported.
ses | es | uas | css | oof | crc | bpv	bpv: Threshold for bipolar violation crc: Threshold for cyclic redundancy check css: Threshold for controlled slip second es: Threshold for errored seconds oof: Threshold for out of frame ses: Threshold for severely errored seconds uas: Threshold for unavailable seconds
delta	The errored second or event count is compared to the difference between the rising and falling thresholds, and a rising alarm is reported if the actual error count exceeds that difference. This is the default setting if you do not specify a sampling type.
falling-threshold	Minimum number of errored seconds or events below which a falling alarm is reported. This alarm is reported if a rising alarm was previously reported and the number of errored seconds or events subsequently dropped below this minimum threshold. The falling threshold value must be less

Variable	Value
	than the rising threshold value above. The range is 0 - 2147483647.
rising-threshold	Number of errored seconds or events which, if exceeded during any sampling interval, results in a rising alarm. The range is 0 - 2147483647
sampling-interval	Sampling interval, in seconds. The range is 1 - 65535.

Configuring hierarchy for E1 alarms

Enable or disable the hierarchy for displaying Receive Loss of Signal (RLOS) and Receive Loss of Frame (RLOF) on an E1 link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the E1 module port to configure, enter:

   ```
   module e1 <slot/port>
   ```

3. To configure hierarchy, enter:

   ```
   [no] alarms hierarchy
   ```

Table 20: Variable definitions

Variable	Value
no	Disables hierarchy.

Configuring line mode for E1

Configure the line mode for the E1 interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the E1 module port to configure, enter:

   ```
   module e1 <slot/port>
   ```

3. To configure line mode, enter:

```
linemode {long_haul | short_haul}
```

Table 21: Variable definitions

Variable	Value
long_haul	Long haul type for linemode configuration. Operations up to 6 dB. (default).
short_haul	Short haul type for linemode configuration. Operations up to 43 dB.

Configuring E1 circuit ID

Specify an optional circuit ID for the E1 interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the E1 module port to configure, enter:

   ```
   module e1 <slot/port>
   ```

3. To configure the E1 circuit ID, enter:

   ```
   circuitId <circuit-id>
   ```

Table 22: Variable definitions

Variable	Value
circuit-id	Optional circuit ID for the E1 channel.

Configuring contact information for E1

Specify contact information for a person who can provide details regarding the E1 link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the E1 module port to configure, enter:

   ```
   module e1 <slot/port>
   ```

3. To configure the contact information, enter:

   ```
   contactInfo <contact-info>
   ```

Table 23: Variable definitions

Variable	Value
contact-info	Person to contact for information regarding the E1 link.

Configuring description for E1

Enter a description for the E1 interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the E1 module port to configure, enter:

   ```
   module e1 <slot/port>
   ```

3. To enter the description, enter:

   ```
   description <port-description>
   ```

Table 24: Variable definitions

Variable	Value
port-description	Describes the E1 interface.

Configuring a name for E1

Assign a name to the E1 link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the E1 module port to configure, enter:

   ```
   module e1 <slot/port>
   ```

3. To assign a name to the E1 link, enter:

   ```
   name <name>
   ```

Table 25: Variable definitions

Variable	Value
<name>	Assigns a name to the E1 link (max 16 bytes).

Enabling the E1 interface

Enable the E1 interface to allow the link to transmit and receive data.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the E1 module port to configure, enter:

   ```
   module e1 <slot/port>
   ```

3. To enable the selected E1 module port, enter:

   ```
   [no] enable
   ```

Table 26: Variable definitions

Variable	Value
[no]	Takes the E1 link out of service. This action sends an all-ones Alarm Indication Signal (AIS) to the far end and places the link out of service.

Setting the carrier type to 4 channelized E1 and 4 unframed ports on an 8 port T1/E1 module

Configure the carrier type for mixed E1 mode with 4 channelized E1 and 4 unframed ports. You must reboot the router in order for the configuration to take effect. For this mode, the parameter on the **`carrier-type`** command is **`c4u4`**.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the module and carrier type, enter:

Comments? infodev@avaya.com

```
system carrier-type <slot> c4u4
```

3. To exit the configuration mode, enter:

```
exit
```

4. To reboot the SR4134, enter:

```
reboot
```

Table 27: Variable definitions

Variable	Value
<slot>	Specifies the chassis slot number for the module.

Setting the carrier type to 3 channelized E1 and 5 unframed ports on an 8 port T1/E1 module

Configure the carrier type for mixed E1 mode with 3 channelized E1 and 5unframed ports. You must reboot the router in order for the configuration to take effect. For this mode, the parameter on the **`carrier-type`** command is **`c3u5`**.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the module and carrier type, enter:

```
system carrier-type <slot> c3u5
```

3. To exit the configuration mode, enter:

```
exit
```

4. To reboot the SR4134, enter:

```
reboot
```

Table 28: Variable definitions

Variable	Value
<slot>	Specifies the chassis slot for the module.

Setting the carrier type to 2 channelized E1 and 6 unframed ports on an 8 port T1/E1 module

Configure the carrier type for mixed E1 mode with 2 channelized E1 and 6 unframed ports. You must reboot the router in order for the configuration to take effect. For this mode, the parameter on the **carrier-type** command is **c2u6**.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the module and carrier type, enter:

   ```
   system carrier-type <slot> c2u6
   ```

3. To exit the configuration mode, enter:

   ```
   exit
   ```

4. To reboot the SR4134, enter:

   ```
   reboot
   ```

Table 29: Variable definitions

Variable	Value
<slot>	Specifies the chassis slot position for the module.

Setting the carrier type to 1 channelized E1 and 7 unframed ports on an 8 port T1/E1 module

Configure the carrier type for mixed E1 mode with 1 channelized E1 and 7 unframed ports. You must reboot the router in order for the configuration to take effect. For this mode, the parameter on the **carrier-type** command is **c1u7**.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the module and carrier type, enter:

Comments? infodev@avaya.com

```
system carrier-type <slot> c1u7
```

3. To exit the configuration mode, enter:

   ```
   exit
   ```

4. To reboot the SR4134, enter:

   ```
   reboot
   ```

Table 30: Variable definitions

Variable	Value
<slot>	Specifies the chassis slot position for the module.

Linking a bundle to a T1/E1 interface

Link a bundle to the T1/E1 interface to group DS0's into one configurable interface, and to configure the encapsulation.

Procedure steps

1. To enter configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link the bundle to the module, enter:

   ```
   link [t1 | e1] <slot/port>[:<DS0>] [speed {56 | 64}]
   [invert_data {inverted_data}]
   ```

Table 31: Variable definitions

Variable	Value
<slot/port>	Specifies the slot and port of the T1 or E1 interface to configure.
[:<DS0>]	Optional DS0 channels to be assigned to a fractional T1 bundle (1 - 24) or fractional E1 bundle (1-31).
speed	Transmission speed of all DS0 channels in the bundle (56 or 64 kbps). If this parameter is not entered, all DS0 channels will operate at 64 kbps.
inverted_data	Whether or not to invert the data on all DS0 channels (optional entry). If inverted_data is not entered, the data will not be inverted on any DS0 channels.

Configuring the bundle to drop errored links

Use this command to allow the router system to drop an errored T1 or E1 link from the bundle. A bundle is dropped if excessive errors of a user-specified type occur for a user-defined time interval.

This parameter does not apply for single-T1 or E1 link and N x DS0 (fractional T1 or E1) bundles.

Procedure steps

1. To enter configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure the link dropping method for the bundle, enter:

   ```
   drop error_type {es | ses | uas | eev | bpv | css | oof | crc }
   <drop-value>
   ```

Table 32: Variable definitions

Variable	Value
error_type	Error condition that will cause droppage of a T1 or E1 link from the bundle.
es	Errored Seconds
ses	Severely Errored Seconds
uas	Unavailable Seconds
eev	Excessive Error Violations Seconds
bpv	Bipolar Violations
css	Controlled Slip Seconds
oof	Out of Frame Seconds
crc	CRC-6 Errors
<drop-value>	Drop time in consecutive seconds (1-10 for es, ses, uas) or drop counts.

Comments? infodev@avaya.com

Configuring how dropped multilink T1/E1 links are restored

Configure how a dropped link of a multilink T1 or E1 bundle is restored. You can configure the system to restore dropped links automatically (the default setting) or manually.

If link restore is set to manual and a T1 or E1 link is dropped from a bundle, re-configuring link restore to automatic does not bring the link back into bundle. You must restore any dropped links manually before re-configuring automatic link restore.

Procedure steps

1. To enter configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link the bundle to the module, enter:

   ```
   restore {automatic | manual}
   ```

Table 33: Variable definitions

Variable	Value
automatic	Automatically restores a link to a bundle if that link is free of the specified type of error for <interval> seconds. This is the default restore mode.
<interval>	Error-free time interval (seconds) that must pass before a link is automatically restored. The default is 120 seconds.
manual	Requires you to restore the link manually using the **`configure interface bundle link_restore`** command.

Manually restoring dropped multilink T1/E1 links

Manually restore a link that was previously dropped from a multilink T1 or E1 bundle.

This procedure is not needed if the bundle is configured for automatic link restore (the default state).

Procedure steps

1. To enter configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link the bundle to the module, enter:

   ```
   link_restore <slot/port>[:<DS0>]
   ```

Table 34: Variable definitions

Variable	Value
<slot/port>	Specifies the slot and port of the T1 or E1 interface to configure.
[:<DS0>]	Optional DS0 channels to be assigned to a fractional T1 bundle (1 - 24) or fractional E1 bundle (1-31).

Chapter 6: CT3 module configuration

Note:

The CT3 module can operate in either CT3 mode or in DS3 clear channel mode. The default mode is CT3.

To change the mode to DS3, see Setting the carrier type on CT3 modules on page 73.

Important:

Only the Secure Router 4134 supports the CT3 module. The Avaya Secure Router 2330 does not support CT3 module configuration.

1. Configure properties

   You can enable a link with all default properties if desired.
2. Link a bundle to the desired interface.
3. Configure encapsulation for the bundle.
4. Assign IP address to the bundle.

Configuring CT3 interface properties

Configuring alarms for CT3

Set the alarm thresholds for the CT3 and CT3 T1 user statistics gathered by the Avaya Secure Router 4134.

Each router gathers seven types of user statistics for a CT3 WAN link, and you can set a separate alarm threshold for each type of statistic. Each router also gathers 10 types of user statistics for every T1 channel of a CT3 link.

- To show the current user statistic alarm threshold settings, use the **`show module thresholds ct3`** command.
- To view the user statistic alarms in progress, use the **`show module alarms ct3`** command.
- To view the actual user statistics, use the **`show module userstats ct3`** command.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the CT3 port to configure, enter:

   ```
   module ct3 <slot/port>
   ```

3. To configure the alarm for user statistics, enter:

   ```
   alarms thresholds user <1 - 10>

   [ lcv | fbe | pbe | cpbe| febe| cofa | ses | es | bes | uas |
   eev | lofc | css | oof | crc | bpv ]

   <sampling-interval> <rising-threshold> <falling-threshold>

   sample_type [absolute | delta]

   [t1 <1-28>]
   ```

Table 35: Variable definitions

Variable	Value
1-10	Alarm threshold number.
1-28	T1 number.
absolute	The errored second or event count is compared directly to the specified threshold values, and the appropriate alarm type (rising or falling) is reported.
lcv | fbe | pbe | cpbe| febe| cofa | ses | es | bes | uas | eev | lofc | css | oof | crc | bpv	bes: Threshold for BES (configurable at T1 level) bpv: Threshold for bipolar violation (configurable at T1 level). crc: Threshold for cyclic redundancy check (configurable at T1 level). css: Threshold for controlled slip second (configurable at T1 level). eev: Threshold for EEV (configurable at T1 level). es: Threshold for errored seconds (configurable at T1 level). lofc: Threshold for LOFC (configurable at T1 level). oof: Threshold for out of frame (configurable at T1 level). ses: Threshold for severely errored seconds (configurable at T1 level). uas: Threshold for unavailable seconds (configurable at T1 level). cofa: Threshold for COFA (configurable at T3 level). cpbe: Threshold for CPBE (configurable at T3 level). fbe: Threshold for FBE (configurable at T3 level). febe: Threshold for FEBE (configurable at T3 level). lcv: Threshold for LCV (configurable at T3 level). pbe: Threshold for PBE (configurable at T3 level).
delta	The errored second or event count is compared to the difference between the rising and falling thresholds, and a rising alarm is reported if the actual error count exceeds that difference. This is the default setting if you do not specify a sampling type.

Comments? infodev@avaya.com

Variable	Value
falling-threshold	Minimum number of errored seconds or events below which a falling alarm is reported. This alarm is reported if a rising alarm was previously reported and the number of errored seconds or events subsequently dropped below this minimum threshold. The falling threshold value must be less than the rising threshold value above. The range is 0 - 2147483647.
rising-threshold	Number of errored seconds or events which, if exceeded during any sampling interval, results in a rising alarm. The range is 0 - 2147483647
sampling-interval	Sampling interval, in seconds. The range is 1 - 65535.

Configuring cable length for CT3

Set the CT3 link transmit signal build-out to condition the outgoing signal according to the cabling distance to the external CT3 device.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the CT3 port to configure, enter:

   ```
   module ct3 <slot/port>
   ```

3. To configure cable length, enter:

   ```
   cable_length [ 1 | 2 ]
   ```

Table 36: Variable definitions

Variable	Value
1	0-225 feet (default)
2	226 - 450 feet

Configuring clock source for CT3

Specify the network timing source for a CT3 WAN link.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the CT3 port to configure, enter:

```
module ct3 <slot/port>
```

3. To configure clock source, enter:

```
clock_source [internal | line]
```

Table 37: Variable definitions

Variable	Value
internal	Local clock generated by the Secure Router 4134 (default).
line	Clock signal recovered from the incoming CT3 signal. Use this setting if the system is loop-timed from the far-end CT3 system.

Configuring framing for CT3

Configure either C-bit or M13 framing for the CT3 link.

Contact your carrier to determine the appropriate setting.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the CT3 port to configure, enter:

```
module ct3 <slot/port>
```

3. To configure framing, enter:

```
framing [c_bit | m13 ]
```

Table 38: Variable definitions

Variable	Value
c_bit	C-bit framing format for CT3 (default)
m13	M13 framing format for CT3

Configuring T1 properties within CT3

Configure the properties for the T1 connections in the CT3 interface:

Comments? infodev@avaya.com

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the CT3 port to configure, enter:

   ```
   module ct3 <slot/port>
   ```

3. To select the T1 link and configure the desired properties, enter:

   ```
   t1 <t1-no>
   [framing {esf | d4}]
   [yellowalarm {generate | detect | gen_det | disable}]
   [clock_source {backplane | internal | line}]
   [name <name>]
   [description <t1-description>]
   [cicuitId <circuit-id>]
   [contactInfo <contact-info>]
   ```

Table 39: Variable definitions

Variable	Value
<t1-no>	T1 number or range of T1s (1-28).
[framing {esf | d4}]	esf: Extended Super Frame framing format for T1 (default) d4: Super Frame framing format for T1
[yellowalarm {generate | detect | gen_det | disable}]	generate: Generate and send yellow alarms to the network. detect: Detect incoming yellow alarms from the network. gen_det: Generate and detect yellow alarms. disable: Disable yellow alarm generator (default state).
[clock_source {backplane | internal | line}]	backplane: Sets the clock source to the backplane of the Secure Router 4134. internal: Sets the clock source to the internal clock of the Secure Router 4134. line: Sets the clock source to be recovered from the incoming T1 signal (loop timing).
[name <name>]	Assigns a name to the T1 link (max 15 bytes).
[description <t1-description>]	Describes the T1 interface.
[cicuitId <circuit-id>]	Optional circuit ID for the T1 channel.
[contactInfo <contact-info>]	Person to contact for information regarding the T1 link.

Linking a bundle to the CT3 interface

Link a bundle to the CT3 interface in order to configure the encapsulation for the interface.

Procedure steps

1. To enter configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link a bundle to the module, enter:

   ```
   link ct3 <slot/port/t1no>[:<DS0>] [speed {56 | 64}]
   [invert_data {inverted_data}]
   ```

Table 40: Variable definitions

Variable	Value
<slot/port/t1no>	Specifies the slot and port of the CT3 interface, as well as the T1 channels to configure from the CT3 link.
[:<DS0>]	Optional DS0 channels to be assigned to a fractional T1 bundle (1 - 24).
[speed {56 | 64}]	Transmission speed of all DS0 channels in the bundle (56 or 64 kbps). If this parameter is not entered, all DS0 channels will operate at 64 kbps.
[invert_data {inverted_data}]	Whether or not to invert the data on all DS0 channels (optional entry). If inverted_data is not entered, the data will not be inverted on any DS0 channels.

Comments? infodev@avaya.com

Chapter 7: DS3 module configuration

Note:

The CT3 module can operate in either CT3 mode or in DS3 clear channel mode. The default mode is CT3.

To change the mode to DS3, see Setting the carrier type on CT3 modules on page 73.

Important:

Only the Secure Router 4134 supports the CT3 module. The Avaya Secure Router 2330 does not support CT3 module configuration.

1. Configure DS3 properties

   You can enable a link with all default properties.
2. Link a bundle to the interface.
3. Configure encapsulation for the bundle.
4. Assign IP address to the bundle.

Important:

DS3 scrambling is not supported.

Configuring DS3 interface properties

Setting the carrier type on CT3 modules

You can configure the carrier type for the CT3 module to support DS3 links. In this case, you must use the DS3 module commands to configure the interface.

You must reboot the router in order for the configuration to take effect.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```
2. To select the module and carrier type, enter:

```
system carrier-type <slot> {ct3 | ds3}
```

3. To exit the configuration mode, enter:

   ```
   exit
   ```

4. To reboot the Secure Router 4134, enter:

   ```
   reboot
   ```

Configuring alarms for DS3

Set the alarm thresholds for the DS3 user statistics gathered by the Avaya Secure Router 4134.

Each router gathers seven types of user statistics for a T3 WAN link, and you can set a separate alarm threshold for each type of statistic.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T3 port to configure, enter:

   ```
   module t3 <slot/port>
   ```

3. To configure the alarm for user statistics, enter:

   ```
   alarms thresholds user <1 - 10> [ lcv | fbe | pbe | cpbe|
   febe| |exz | cofa ] <sampling-interval> <rising-threshold>
   <falling-threshold> sample_type [absolute | delta] [t1
   <1-28>]
   ```

Table 41: Variable definitions

Variable	Value
1-10	Alarm threshold number.
absolute	The errored second or event count is compared directly to the specified threshold values, and the appropriate alarm type (rising or falling) is reported.
lcv | fbe | pbe | cpbe| febe| | exz | cofa	cofa: Threshold for COFA cpbe: Threshold for CPBE exz: Threshold for EXZ fbe: Threshold for FBE febe: Threshold for FEBE lcv: Threshold for LCV pbe: Threshold for PBE
falling-threshold	Minimum number of errored seconds or events below which a falling alarm is reported. This alarm is reported if a rising alarm was previously reported and the number of errored seconds or events subsequently dropped below this minimum threshold. The falling threshold value must be less

Comments? infodev@avaya.com

Variable	Value
	than the rising threshold value above. The range is 0 - 2147483647.
rising-threshold	Number of errored seconds or events which, if exceeded during any sampling interval, results in a rising alarm. The range is 0 - 2147483647
sampling-interval	Sampling interval, in seconds. The range is 1 - 65535.

Configuring cable length for DS3

Set the DS3 link transmit signal build-out to condition the outgoing signal according to the cabling distance to the external DS3 device.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the T3 port to configure, enter:

   ```
   module t3 <slot/port>
   ```

3. To configure cable length, enter:

   ```
   cable_length <1-2>
   ```

Table 42: Variable definitions

Variable	Value
1	0-225 feet (default)
2	226 - 450 feet

Configuring clock source for DS3

Specify the network timing source for a DS3 WAN link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the CT3 port to configure, enter:

   ```
   module t3 <slot/port>
   ```

3. To configure clock source, enter:

```
clock_source {internal | line}
```

Table 43: Variable definitions

Variable	Value
internal	Specifies the local clock (default).
line	Specifies the network clock.

Configuring framing for DS3

Configure framing for the DS3 link.

Important:

The Clear Channel DS3 interface module does not currently support the use of the M13 framing format. Only the default framing format of C-BIT can be used on Clear Channel DS3 interface modules.

Important:

Jumbo frames must be enabled in the system setting to allow DS3 module to connect with other vendors.

```
SR 4134/configure# system jumbo-mtu-limit >? WORD Enter MTU Limit
1500 or 9216 (default =1500)
```

Enter 9216 to enable jumbo frames, save configuration and reboot.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the DS3 port to configure, enter:

   ```
   module t3 <slot/port>
   ```

3. To configure framing, enter:

   ```
   framing {c_bit}
   ```

Table 44: Variable definitions

Variable	Value
c_bit	C_BIT framing format for T3 (default)

Comments? infodev@avaya.com

Configuring a name for DS3

Assign a name to the DS3 link.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the DS3 port to configure, enter:

   ```
   module t3 <slot/port>
   ```

3. To configure framing, enter:

   ```
   name <name>
   ```

Table 45: Variable definitions

Variable	Value
name	Assigns a name to the T3 link (max 16 bytes).

Linking a bundle to a DS3 interface

Link a bundle to a DS3 interface to configure the encapsulation for the interface.

Procedure steps

1. To enter configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link a bundle to the module, enter:

   ```
   link t3 <slot/port>
   ```

Comments? infodev@avaya.com

Chapter 8: Serial module configuration

1. Configure properties

   At minimum, you must configure the serial operating mode (such as V.35).
2. Link a bundle to the interface.
3. Configure encapsulation for the bundle.
4. Assign IP address to the bundle.

Configuring serial interface properties

Configure the serial mode

Configure the serial module mode.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```
2. To select the serial port to configure, enter:

   ```
   module serial <slot/port>
   ```
3. To configure the serial mode, enter:

   ```
   mode {X.21 | V.35 | S232 | S449 | S530 | S530A }
   ```

Table 46: Variable definitions

Variable	Value
X.21	X.21 mode.
V.35	V.35 mode.
S232	RS-232 mode.
S449	RS-449 mode.
S530	EIA-530 mode.

Variable	Value
S530A	EIA-530A mode.

Configuring the serial clock source

Configure the clock source for the serial interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the serial port to configure, enter:

   ```
   module serial <slot/port>
   ```

3. To select the active serial mode, enter:

   ```
   { x21 | v35 | S232 | S449 | S530 | S530A }
   ```

4. To configure the clock source, enter:

   ```
   clock_source {internal | line}
   ```

Table 47: Variable definitions

Variable	Value
internal	Specifies the clock source is received from the router.
line	Specifies the clock source is received from an external network clock.

Important:

When you specify the serial port clock source as an external network clock (**`clock_source line`**), use the **`clock_rate`** command to specify a clock rate that is equal to the speed of the clock provided by the far-end equipment.

Configuring the serial clock rate

Configure the clock rate for the serial interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the serial port to configure, enter:

Comments? infodev@avaya.com

```
module serial <slot/port>
```

3. To select the active serial mode, enter:

```
{ x21 | v35 | S232 | S449 | S530 | S530A }
```

4. To configure the clock rate, enter:

```
clock_rate <clock-rate>
```

Table 48: Variable definitions

Variable	Value
<clock-rate>	Valid range for X.21, V.35, S449, S530, and S530A: 56000 - 2000000 Valid range for S232: 1200 - 115000

Configuring CRC for the serial interface

Configure the CRC check sum for the serial interface.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the serial port to configure, enter:

```
module serial <slot/port>
```

3. To select the active serial mode, enter:

```
{ x21 | v35 | S232 | S449 | S530 | S530A }
```

4. To configure the CRC value, enter:

```
crc {16 | 32}
```

Table 49: Variable definitions

Variable	Value
16	Specifies 16 bits in the check sum.
32	Specifies 32 bits in the check sum.

Configuring serial data mode

Configure the data mode for the serial interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the serial port to configure, enter:

   ```
   module serial <slot/port>
   ```

3. To select the active serial mode, enter:

   ```
   { x21 | v35 | S232 | S449 | S530 | S530A }
   ```

4. To configure the data mode, enter:

   ```
   data_mode {normal | inverted}
   ```

Table 50: Variable definitions

Variable	Value
inverted	Specifies that data is sent inverted.
normal	Specifies that data is sent without modification.

Configuring serial operational mode

Configure the operational mode for the serial interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the serial port to configure, enter:

   ```
   module serial <slot/port>
   ```

3. To select the active serial mode, enter:

   ```
   { x21 | v35 | S232 | S449 | S530 | S530A }
   ```

4. To configure the operational mode, enter:

   ```
   mode {dte | dce}
   ```

Table 51: Variable definitions

Variable	Value
dte	Specifies that the port is operating as a Data Terminal Equipment. This is the default for all serial port modes.
dce	Specifies that the port is operating as a Data Communications Equipment

Configuring a name for the serial interface

Configure the name for the serial interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the serial port to configure, enter:

   ```
   module serial <slot/port>
   ```

3. To select the active serial mode, enter:

   ```
   { x21 | v35 | S232 | S449 | S530 | S530A }
   ```

4. To configure the name, enter:

   ```
   name <name>
   ```

Table 52: Variable definitions

Variable	Value
<name>	Specifies the name of the interface (max 16 bytes)

Linking a bundle to the serial interface

Link a bundle to the serial interface in order to configure the encapsulation for the interface.

Procedure steps

1. To enter configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link the bundle to the module, enter:

   ```
   link serial <slot/port>
   ```

Comments? infodev@avaya.com

Chapter 9: HSSI module configuration

Important:

The Avaya Secure Router 2330 does not support HSSI module configuration.

1. Configure properties
2. Link a bundle to the interface.
3. Configure encapsulation for the bundle.
4. Assign IP address to the bundle.

Configuring HSSI interface properties

Configuring HSSI operational mode

Configure the operational mode for the HSSI interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the HSSI port to configure, enter:

   ```
   module hssi <slot/port>
   ```

3. To configure the HSSI mode, enter:

   ```
   mode {dte | dce}
   ```

Table 53: Variable definitions

Variable	Value
dte	DTE mode.
dce	DCE mode.

Configuring clock rate for HSSI

Configure the clock rate for the HSSI interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the HSSI port to configure, enter:

   ```
   module hssi <slot/port>
   ```

3. To configure the clock rate, enter:

   ```
   clock_rate <1000000 - 52000000>
   ```

Configuring clock source for HSSI

Configure the clock source for the HSSI interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the HSSI port to configure, enter:

   ```
   module hssi <slot/port>
   ```

3. To configure the clock source, enter:

   ```
   clock_source {internal | line}
   ```

Table 54: Variable definitions

Variable	Value
internal	Specifies the clock source is received from the router.
line	Specifies the clock source is received from an external network clock.

Configuring CRC for HSSI

Configure the CRC check sum for the HSSI interface.

Comments? infodev@avaya.com

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the HSSI port to configure, enter:

   ```
   module hssi <slot/port>
   ```

3. To configure crc, enter:

   ```
   crc {16 | 32}
   ```

Table 55: Variable definitions

Variable	Value
16	Specifies 16 bits in the check sum.
32	Specifies 32 bits in the check sum.

Configuring HSSI data mode

Configure the data mode for the HSSI interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the HSSI port to configure, enter:

   ```
   module hssi <slot/port>
   ```

3. To configure the data mode, enter:

   ```
   data_mode {normal | inverted}
   ```

Table 56: Variable definitions

Variable	Value
inverted	Specifies that data is sent inverted.
normal	Specifies that data is sent without modification.

Configuring a name for the HSSI interface

Configure the name for the HSSI interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the HSSI port to configure, enter:

   ```
   module hssi <slot/port>
   ```

3. To configure the name, enter:

   ```
   name <name>
   ```

Table 57: Variable definitions

Variable	Value
<name>	Name for the HSSI interface (max 16 bytes).

Linking a bundle to the HSSI interface

Link a bundle to the HSSI interface in order to configure the encapsulation for the interface.

Procedure steps

1. To enter configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link the bundle to the module, enter:

   ```
   link hssi <slot/port>
   ```

Chapter 10: WAN module information display

Displaying WAN module alarms

Display the alarms detected on a WAN module interface.

This command also shows individual user threshold alarms for all user statistics currently configured with alarm thresholds (for T1/E1 and CT3/DS3 modules only). To view the current user alarm threshold settings, use the **show module thresholds** command.

To display the alarms in real-time, specify the desired refresh interval in minutes when entering this command. To return to the system command prompt, type **q**.

Procedure steps

To display WAN module alarms, enter:

```
show module alarms {ct3|t3|e1|t1|hssi|serial} <slot/port>[:t1-no] [refresh_interval <1-65535>]
```

Table 58: Variable definitions

Variable	Value
[refresh_interval <1-65535>]	Specifies how often, in minutes, the alarm display is updated (optional entry; minimum is 1 minute). If you do not specify an interval, you must repeat the command to update the alarm display.
[:t1-no]	Specifies a T1 channel for viewing T1 alarms on CT3 modules. The range is 1 - 28. You can view only one channel at a time.

Displaying ANSI statistics for T1 or CT3 modules

Display ANSI statistics for a T1 or CT3 module interface.

The command shows the current 15-minute interval statistics, the elapsed time in the current sampling interval, and the total counts for the past 8 hours. These statistics can be cleared only by the carrier by FDL requests from the remote end.

You can view statistics for multiple 15-minute intervals by specifying the number of intervals you wish to view (from 1 to 96).

Procedure steps

To display ANSI statistics for a T1 or CT3 module, enter:

```
show module ansistats {t1 <slot/port> | ct3 <slot/port> [t1_no
<t1-no>]} [interval_range <1-96>]
```

Displaying WAN module configuration

Display the configuration for a specified WAN module interface or all WAN interfaces.

To display WAN module configuration, enter:

```
show module configuration {all|ct3|t3|e1|t1|hssi|serial} <slot/
port>[:t1-no]
```

Displaying IETF statistics for E1/T1 and CT3/DS3 modules

Display IETF performance statistics for E1/T1 and CT3/DS3 module interfaces. You can view statistics for multiple 15-minute intervals by specifying the number of intervals you wish to view (from 1 to 96).

Procedure steps

To display IETF statistics for E1/T1 or CT3/DS3 WAN modules, enter:

```
show module ietfstats {ct3|t3|e1|t1} <slot/port> [t1_no <t1-
no>] [interval_range <1-96>]
```

Displaying ITUT statistics for E1

Display ITUT performance statistics for an E1 interface. You can view statistics for multiple 15-minute intervals by specifying the number of intervals you wish to view (from 1 to 96).

Procedure steps

To display ITUT statistics for E1 WAN modules, enter:

```
show module itutstats e1 <slot/port> [interval_range <1-96>]
```

Displaying thresholds for E1/T1 and CT3/DS3 modules

This command shows the alarm threshold settings for a module interface. Alarm thresholds are configured on a per-module basis.

Procedure steps

To display WAN module thresholds, enter:

```
show module thresholds {ct3|t3|e1|t1} <slot/port> [t1_no <t1-
no>]
```

Displaying user statistics for WAN modules

Display performance statistics for a WAN module interface.

You can view statistics for multiple 15-minute intervals by specifying the number of intervals you wish to view (from 1 to 96). To clear these statistics after viewing them, use the **clear module** command.

Procedure steps

To display user statistics for WAN modules, enter:

```
show module userstats {ct3|t3|e1|t1|serial|hssi} <slot/port>
[t1_no <t1-no>] [interval_range <1-96>]
```

Clearing user statistics for WAN modules

Clear user statistics for a WAN module interface.

Procedure steps

To clear user statistics for WAN modules, enter:

```
clear module {ct3_userstats | t3_userstats | e1_userstats |
serial_userstats | t1_userstats | hssi_userstats} <slot/port>
```

```
[t1_no <t1-no>]
```

Displaying AVC information

Displaying AVC information

Display information about a DTE-to-DTE MFR AVC, including the status of the AVC and the status of each CVC in the AVC.

Procedure steps

To clear the counters for all interfaces, enter:

```
show interface avc <avc-name> <dlci>
```

Clearing counters for DTE-to-DTE MFR AVC interfaces

Clear the counters for AVC interfaces.

Procedure steps

To clear the counters for AVC interfaces, enter:

```
clear interface {avc <avc-name> | avcs}
```

Displaying interface information

Displaying bundle interface status information

Display the configuration and status for a specified bundle or all bundles.

Procedure steps

To clear the counters for all interfaces, enter:

Comments? infodev@avaya.com

```
show interface {bundles | bundle <bundle-name>}
```

Clearing interface counters

Clearing counters for all interfaces

Clear the counters for all interfaces.

Procedure steps

To clear the counters for all interfaces, enter:

```
clear interface all
```

Clearing counters for bundles

Clear the counters for a specified bundle or all bundles.

Procedure steps

To clear the counters for AVC interfaces, enter:

```
clear interface { bundles | bundle <bundle-name> [dlci
<dlci>] }
```

Comments? infodev@avaya.com

Chapter 11: ISDN configuration on BRI modules and on T1/E1 modules

1. Create a bundle.
2. Link the ISDN BRI interface or ISDN PRI (for T1/E1) interface to the bundle.
3. Configure encapsulation (PPP) for the bundle.
4. Assign an IP address to the bundle.
5. Configure the ISDN parameters. Called-num and switch-type parameters are mandatory.

Linking a bundle to the BRI interface

Link a bundle to the BRI interface in order to configure the ISDN properties and encapsulation for the interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To create the bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link the bundle to a BRI port and channel, enter:

   ```
   link bri <slot/port:links>
   ```

4. To set the bundle encapsulation, enter:

   ```
   encapsulation ppp
   ```

5. To set the bundle ip address, enter:

   ```
   ip address <ip-address/netmask>
   ```

Table 59: Variable definitions

Variable	Value
slot/port	slot and port of the BRI module.
links	1 (64Kb/s) or 2 (128 Kb/s)

Linking a bundle to the T1/E1 module for ISDN PRI

Link a bundle to the T1/E1 module interface in order to configure the ISDN properties and encapsulation for the interface.

ISDN PRI is only supported on the 1-port and 2-port T1/E1 small modules.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To create the bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link the bundle to a T1/E1 port and channel, enter:

   ```
   link {pri_e1 | pri_t1} <slot/port:links>
   ```

4. To set the bundle encapsulation, enter:

   ```
   encapsulation ppp
   ```

5. To set the bundle ip address, enter:

   ```
   ip address <ip-address/netmask>
   ```

Table 60: Variable definitions

Variable	Value
pri_e1	Configure a PRI link on E1 module.
pri_t1	Configure a PRI link on T1 module.
slot/port	slot and port of the PRI module.
links	Range for E1: 1 - 30 Range for T1: 1 - 23

Configuring ISDN properties for BRI or PRI

Configuring the switch type

Configure the switch type to specify the ISDN protocol variant supported on the interface.

Comments? infodev@avaya.com

Shut down the bundle before changing the interface type.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To configure the switch type, enter:

   ```
   [no] switch-type <switch-type>
   ```

Table 61: Variable definitions

Variable	Value
basic-ni	National ISDN Switch type
basic-dms	NT DMS-100 switch type
basic-5ess	AT&T basic rate switch type (default)
basicntt	ntt switch type
basic-euro	Euro basic switch type
basic-ccitt	CCITT basic switch type
basic1tr6	German 1tr6 basic switch type
basicvn3	French basic switch type
primary-dms100	DMS100 primary rate switch type
primary-ntt	NTT primary rate switch type
primary-ni2	National ISDN 2 primary rate switch type
primary-euro	Euro ISDN primary rate switch type
primary-ccitt	CCITT/ITU-T primary rate switch type
primary-4ess	AT&T primary rate switch type
primary-5ess	AT&T primary switch type (default)
primary-vn3	French primary rate switch type

Configuring the caller number

Configure the caller number to specify the expected origin of the call. This configuration enables the router to screen the incoming call. If the incoming call matches with the caller configured then the call is put through

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To configure the caller number, enter:

   ```
   caller <caller>
   ```

Table 62: Variable definitions

Variable	Value
<caller>	Caller number (maximum of 20 digits).

Configuring the call-back

Enable or disable call-back for the interface. (The interface uses the caller value to place the call.)

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To enable or disable call back, enter:

   ```
   [no] call-back
   ```

Table 63: Variable definitions

Variable	Value
no	Disables call back.

Configuring the called number

Configure the called number to specify the called party number for the interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To configure the caller number, enter:

   ```
   callednum <called-num> sub-address <sub-address>
   ```

Table 64: Variable definitions

Variable	Value
callednum	Called number (maximum of 20 digits).
sub-address	Sub address (maximum of 10 digits).

Configure the called party in the incoming setup message

Configure the called party in the incoming setup message.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

```
isdn
```

4. To configure the called party, enter:

```
[answer1 | answer2] <callednum> [sub-address <sub-address>]
```

Table 65: Variable definitions

Variable	Value
<callednum>	Caller party number (maximum of 20 digits).
[sub-address <sub-address>]	Sub address (maximum of 10 digits).

Configuring the calling number

Configure the calling number to specify the calling party number for the interface.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To specify the ISDN WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify ISDN configuration, enter:

```
isdn
```

4. To configure the calling number

```
callingnum <callingnum> [sub-address <sub-address>]
```

Table 66: Variable definitions

Variable	Value
<callingnum>	Calling number (maximum of 20 digits).
[sub-address <sub-address>]	Sub address (maximum of 10 digits).

Configuring the connect delay

Configure the connected delay period for the ISDN calls.

Procedure steps

1. To enter the configuration mode, enter:

Comments? infodev@avaya.com

```
configure terminal
```

2. To specify the ISDN WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify ISDN configuration, enter:

```
isdn
```

4. To configure the connect delay, enter:

```
connect-delay <1-60>
```

Table 67: Variable definitions

Variable	Value
<1-60>	Connect delay in seconds. Valid range is 1-60. The default is 15.

Configuring the disconnect cause

Configure the disconnect cause code.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To specify the ISDN WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify ISDN configuration, enter:

```
isdn
```

4. To configure the disconnect cause, enter:

```
disconnect-cause <disconnect-cause>
```

Table 68: Variable definitions

Variable	Value
<disconnect-cause>	• 1 unassigned number • 2 no route to transit network • 3 no route to destination • 6 channel unacceptable • 7 call awarded and being delivered • 9 prefix 1 dialed in error

Variable	Value
	• 16 normal call clearing • 17 user busy (default) • 18 no user response • 19 no answer (user alerted) • 21 call rejected • 22 number changed • 24 number unassigned • 26 non selected User clearing • 27 destination out of order • 28 invalid number format • 29 facility rejected • 30 response to satus enquiry • 31 normal unspecified • 34 no circuit/channel available • 35 call queued • 38 network out of order • 41 temporary failure 4 • 42 switch equipment congestion • 43 access info discarded • 44 requested circuit/channel unavailable • 47 resources unavailable, unspecified • 49 quality of Service unavailable • 50 requested facility not subscribed • 52 outgoing calls barred • 57 bearer capability not authorized • 58 bearer capability not available • 59 call restriction • 60 terminal call redirection rejected • 62 unauthorized service • 63 service or option unavailable • 65 bearer capability not implemented • 66 channel type not implemented • 69 requested facility not implemented

Comments? infodev@avaya.com

Variable	Value
	• 70 only restricted digital bear cap is avail • 79 service or option not implemented • 81 invalid call reference • 82 channel does not exist • 83 susp. call exists, call id is invalid • 84 call identity is in use • 85 no call suspended • 86 call id has been cleared • 88 incompatible destination • 91 invalid transit network selection • 92 invalid facility parameter • 95 invalid message, unspecified • 96 mandatory info element is missing • 97 message type is non-existent or not implemented • 98 message type invalid in call state or not implemented • 99 info element non-existent or not implemented • 100 invalid info element • 101 message type not compatible with call state • 102 recovery on timer expiry • 103 message received with mandatory info element of incorrect length • 111 protocol error, unspecified • 112 protocol discriminator error • 113 bearer service not available • 114 end-to-end info transfer impossible • 126 entering conversation mode • 127 interworking specified

Configuring the idle timeout period

Configure the idle timeout period that must pass before the ISDN call is disconnected.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To configure the idle timeout period, enter:

   ```
   idle-timeout <0-60>
   ```

Table 69: Variable definitions

Variable	Value
<0-60>	Idle timeout in minutes (default is 5). A value of 0 disables the timeout feature.

Configuring the ISDN plan and type

Use this procedure to configure the ISDN type and plan used on a bundle for outgoing traffic by the router.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To configure the plan and type, enter:

   ```
   [no] map addr <string> plan <numbering_plan> type
   <number_type>
   ```

Table 70: Variable definitions

Variable	Value
addr <string>	Specifies the calling number or the called number. It can be a regular expression also for pattern matching. If the called

Comments? infodev@avaya.com

Variable	Value
	number matches the argument then the specified ISDN type and plan are used.
[no]	Disables the ISDN numbering plan and type.
plan <numbering_plan>	Specifies the ISDN numbering plan. Values include: • unknown • isdn—ISDN/telephony numbering - E.164/E.163 • tel—telephony numbering - E.163 • data—data numbering - X.121 • telex—telex numbering - Recommendation F.69 • national—national standard numbering • private—private numbering Default values for the called party are: • Data—isdn • Voice—unknown Default values for the calling party are: • Data—unknown • Voice—unknown
type <number_type>	Specifies the ISDN numbering type. Values include: • unknown • international—international number • national—national number • network—network specific number • subscriber—subscriber number • overlap—overlap sending • abbreviated—abbreviated number Default values for the calling party are: • Data—national • Voice—unknown Default values for the calling party are: • Data—unknown • Voice—unknown

Job aid: sample configuration

The following example sets the numbering plan and number type as unknown for all the calls.

```
SR4134/configure#interface bundle wan

SR4134/configure/interface/bundle/wan#isdn map .% unknown unknown
```

Supported Number Plan and Type for each Switch Type

Switch-Type: Euro

Number Plan
unknown - unknown
isdn - ISDN/telephony numbering - E.164/E.163
data - data numbering - X.121
telex - telex numbering - Recommendation F.69
national - national standard numbering
private - private numbering
extension - reserved for extension

Number Type
unknown
international
national
network
subscriber
extension

Switch-Type: DMS100

Number Plan
unknown - unknown
isdn - ISDN/telephony numbering - E.164/E.163
private - private numbering

Number Type
unknown

Comments? infodev@avaya.com

international
national
subscriber

Switch-Type: QSIG

Number Plan
unknown - unknown
isdn - ISDN/telephony numbering - E.164/E.163
private - private numbering

Number Type
unknown
international
national
subscriber

Switch-Type: CCITT

Number Plan
unknown - unknown
isdn - ISDN/telephony numbering - E.164/E.163
tel - telephony numbering - E.163
data - data numbering - X.121
telex - telex numbering - Recommendation F.69
national - national standard numbering
private - private numbering
extension - reserved for extension

Number Type
unknown
international
national
network

subscriber
abbreviated
extension

Switch-Type: 5ESS

Number Plan
unknown - unknown
isdn - ISDN/telephony numbering - E.164/E.163
national - national standard numbering
private - private numbering

Number Type
unknown
international
national
subscriber

Configuring the ISDN Q921 timer values

The following sections describe the configuration for ISDN Q921 timers, which are used to configure Layer 2 timers for the ISDN interface.

Configuring Outstanding I frames

Configure outstanding I frames.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To select Q921 timers, enter:

Comments? infodev@avaya.com

```
q921-timers
```

5. To configure Outstanding I frames, enter:

```
k <1-10>
```

Table 71: Variable definitions

Variable	Value
<1-10>	Value (default: 7)

Configuring n200 max number of retransmit value

Configure the n200 value.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To specify the ISDN WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify ISDN configuration, enter:

```
isdn
```

4. To select Q921 timers, enter:

```
q921-timers
```

5. To configure n200 value, enter:

```
n200 <1-10>
```

Table 72: Variable definitions

Variable	Value
<1-10>	Value (default: 3)

Configuring n201 max number of TEI

Configure the n201 value.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To specify the ISDN WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To select Q921 timers, enter:

   ```
   q921-timers
   ```

5. To configure n201 value, enter:

   ```
   n201 <500-2000>
   ```

Table 73: Variable definitions

Variable	Value
<500-2000>	Value (default: 1028)

Configuring t200 timer

Configure the t200 timer.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To select Q921 timers, enter:

   ```
   q921-timers
   ```

5. To configure t200 timer, enter:

   ```
   t200 <1-10>
   ```

Table 74: Variable definitions

Variable	Value
<1-10>	Time in seconds (default: 2)

Configuring t203 timer

Configure the t203 timer.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To select Q921 timers, enter:

   ```
   q921-timers
   ```

5. To configure t203 timer, enter:

   ```
   t203 <5-15>
   ```

Table 75: Variable definitions

Variable	Value
<5-15>	Time in seconds (default: 5)

Configuring the ISDN Q931 timer values

The following sections describe the configuration for ISDN Q931 timers, which are used to configure Layer 3 timers for the ISDN interface.

Configuring t303 setup sent timer

Configure the t303 timer.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To select Q931 timers, enter:

```
q931-timers
```

5. To configure t303 setup sent timer, enter:

```
t303 <2-10>
```

Table 76: Variable definitions

Variable	Value
<2-10>	Time in seconds (default: 4)

Configuring t304 setup ack received timer

Configure the t304 timer.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To specify the ISDN WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify ISDN configuration, enter:

```
isdn
```

4. To select Q931 timers, enter:

```
q931-timers
```

5. To configure t304 setup ack received timer, enter:

```
t304 <20-50>
```

Table 77: Variable definitions

Variable	Value
<20-50>	Time in seconds (default: 30)

Configuring t305 disconnect sent timer (user)

Configure the t305 disconnect sent timer (user).

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To specify the ISDN WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To select Q931 timers, enter:

   ```
   q931-timers
   ```

5. To configure t305 timer, enter:

   ```
   t305 <20-50>
   ```

Table 78: Variable definitions

Variable	Value
<20-50>	Time in seconds (default: 30)

Configuring t308 Release sent timer

Configure the t308 timer.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To select Q931 timers, enter:

   ```
   q931-timers
   ```

5. To configure t308 Release sent timer, enter:

   ```
   t308 <2-10>
   ```

Table 79: Variable definitions

Variable	Value
<2-10>	Time in seconds (default: 4)

Configuring t310 call proceeding received timer

Configure the t310 timer.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To select Q931 timers, enter:

   ```
   q931-timers
   ```

5. To configure t310 call proceeding received timer, enter:

   ```
   t310 <20-50>
   ```

Table 80: Variable definitions

Variable	Value
<20-50>	Time in seconds (default: 30).

Configuring t313 connect sent, waiting for connect ack timer

Configure the t313 timer.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To select Q931 timers, enter:

   ```
   q931-timers
   ```

5. To configure the t313 timer, enter:

   ```
   t313 <2-10>
   ```


Comments? infodev@avaya.com

Table 81: Variable definitions

Variable	Value
<2-10>	Time in seconds (default: 4)

Configuring t316 restart sent, wait for restart ack timer

Configure the t316 timer.

Procedure steps

1. To enter the configuration mode, enter:
   ```
   configure terminal
   ```
2. To specify the ISDN WAN bundle, enter:
   ```
   interface bundle <bundle-name>
   ```
3. To specify ISDN configuration, enter:
   ```
   isdn
   ```
4. To select Q931 timers, enter:
   ```
   q931-timers
   ```
5. To configure t316 timer, enter:
   ```
   t316 <110-140>
   ```

Table 82: Variable definitions

Variable	Value
<110-140>	Time in seconds (default: 120)

Configuring t319 timer

Configure the t319 timer.

Procedure steps

1. To enter the configuration mode, enter:
   ```
   configure terminal
   ```
2. To specify the ISDN WAN bundle, enter:
   ```
   interface bundle <bundle-name>
   ```
3. To specify ISDN configuration, enter:

```
isdn
```

4. To select Q931 timers, enter:

```
q931-timers
```

5. To configure t319 timer, enter:

```
t319 <2-10>
```

Table 83: Variable definitions

Variable	Value
<2-10>	Time in seconds (default: 4).

Configuring t322 status enquiry sent timer

Configure the t322 timer.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To specify the ISDN WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify ISDN configuration, enter:

```
isdn
```

4. To select Q931 timers, enter:

```
q931-timers
```

5. To configure t322 timer, enter:

```
t322 <2-10>
```

Table 84: Variable definitions

Variable	Value
<2-10>	Time in seconds (default: 4)

Configuring service profile ID for B1 or B2 channel

Configure the service profile ID for B1 or B2 channel. The service profile is applicable for ISDN BRI only.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To configure the service profile ID, enter:

   ```
   [spid1 | spid2] <spid>
   ```

Table 85: Variable definitions

Variable	Value
spid1	Configures the service profile ID for B1 channel
spid2	Configures the service profile ID for B2 channel
<spid>	Service profile ID (maximum 20 digits)

Configuring the TEI mode

Configure the TEI mode to provision ISDN BRI as point-to-point or point-to-multipoint. The TEI mode is applicable for ISDN BRI only.

Note:

ISDN BR voice bundles with a default TEI mode of point-to-multipoint will not come up until the bundle is manually changed to point-to-point.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To configure the TEI mode, enter:

   ```
   tei-mode {point-to-point | point-to-multipoint}
   ```

Table 86: Variable definitions

Variable	Value
point-to-point	Point to point
point-to-multipoint	Point to multipoint

Configuring the TEI value for point-to-point TEI mode

Configure the TEI value to provision a static TEI value for the interface. The TEI value is applicable only for ISDN BRI in point-to-point mode.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To configure the TEI value, enter:

   ```
   tei-value <0-63>
   ```

Table 87: Variable definitions

Variable	Value
<0-63>	TEI value (default: 0)

Activating ISDN

Activate ISDN.

If you change any of the ISDN properties (except callingnum, callednum, idle-timeout, call-back, and connect-delay), you must deactivate ISDN (using the **`no activate`** command) and then reactivate ISDN for the changes to be applied.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the ISDN WAN bundle, enter:

Comments? infodev@avaya.com

```
interface bundle <bundle-name>
```

3. To specify ISDN configuration, enter:

   ```
   isdn
   ```

4. To activate ISDN, enter:

   ```
   activate
   ```

Displaying ISDN information

Displaying ISDN global configuration information

Display ISDN global configuration information.

Procedure steps

To display ISDN global configuration information, enter:

```
show isdn global
```

Displaying ISDN interface configuration information

Display ISDN interface configuration information.

Procedure steps

To display ISDN interface configuration information, enter:

```
show isdn {interfaces | interface <bundle-name>}
```

Displaying ISDN BRI statistics

Display ISDN BRI statistics.

Procedure steps

To display ISDN BRI statistics, enter:

```
show isdn bri-statistics <slot/port>
```

Displaying ISDN PRI statistics

Display ISDN PRI statistics.

Procedure steps

To display ISDN PRI statistics, enter:

```
show isdn pri-statistics <slot/port>
```

Clearing ISDN statistics

Clearing ISDN BRI statistics

Clear ISDN BRI statistics.

Procedure steps

To clear ISDN BRI statistics, enter:

```
clear isdn pri-statistics <slot/port>
```

Clearing ISDN PRI statistics

Clear ISDN PRI statistics.

Procedure steps

To clear ISDN PRI statistics, enter:

```
clear isdn pri-statistics <slot/port>
```

Chapter 12: HDLC configuration

Configuring encapsulation for WAN modules

In order to configure the encapsulation and IP address for a WAN interface, you must first associate the interface with a bundle. A bundle is a single, high speed virtual path consisting of one or more physical links. For instructions on configuring a bundle for an interface, see the preceding module-specific section.

All of the following procedures assume that you have already created a WAN interface bundle that is linked to a physical WAN port.

Configuring HDLC

Setting bundle encapsulation to HDLC

Set the bundle encapsulation to HDLC

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To set the encapsulation, enter:

   ```
   encapsulation hdlc
   ```

Configuring HDLC properties

Configure HDLC properties on the bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure HDLC, enter:

   ```
   hdlc [keepalive <0-120>] [packet_type {unicast|broadcast}]
   [mtu <64-9216>]
   ```

Table 88: Variable definitions

Variable	Value
[keepalive <0-120>]	Specifies the keep-alive interval for the link, in seconds. Default is 10 seconds. The Avaya Secure Router 2330/4134 sends a message once every configured interval to check the status of the bundle. To turn off the keepalive, enter 0.
[packet_type {unicast| broadcast}]	Specifies the keep-alive packet type, either unicast or broadcast. Default is unicast.
[mtu <64-9216>]	Specifies the maximum transmission unit. This is the maximum packet size that can be transmitted, in bytes. Default is 1500.

Assigning an IP address to the WAN bundle

Once the bundle is configured with an encapsulation, assign an IP address and subnet mask to the bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To set the IP address for the bundle, enter:

   ```
   ip address <A.B.C.D> <netmask>
   ```

Table 89: Variable definitions

Variable	Value
<A.B.C.D> <netmask>	Specifies the IP address and subnet mask of the bundle.

Comments? infodev@avaya.com

Chapter 13: PPP configuration

Configuring encapsulation for WAN modules

In order to configure the encapsulation and IP address for a WAN interface, you must first associate the interface with a bundle. A bundle is a single, high speed virtual path consisting of one or more physical links. For instructions on configuring a bundle for an interface, see the preceding module-specific section.

All of the following procedures assume that you have already created a WAN interface bundle that is linked to a physical WAN port.

Configuring PPP

Configure the PPP properties.

Setting bundle encapsulation to PPP or MLPPP

Set the bundle encapsulation to PPP or MLPPP. If you choose PPP in a multilink bundle, the router automatically activates MLPPP. Further, you can enable MLPPP on a bundle containing a single link by specifying the encapsulation as MLPPP.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To set the encapsulation, enter:

   ```
   encapsulation {ppp | mlppp}
   ```

Configuring authentication

Configure the user authentication

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure PPP, enter:

   ```
   ppp authentication {pap | chap}
   ```

Table 90: Variable definitions

Variable	Value
chap	Specifies CHAP authentication.
pap	Specifies PAP authentication.

Configuring sent username and password for PAP or CHAP

Configure the sent username and password for PAP or CHAP.

This command causes the bundle to flap in order to re-trigger negotiation. Therefore, before you modify the PPP PAP or CHAP sent username (or peername) parameters, shutdown the bundle (using the **shutdown** command) and reenable it (using the **no shutdown** command) after you complete the configuration .

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure sent username for PAP or CHAP, enter:

   ```
   ppp {pap | chap} sent-username <username> <password>
   ```


Comments? infodev@avaya.com

Table 91: Variable definitions

Variable	Value
chap	Configure properties for CHAP.
pap	Configure properties for PAP.
<username>	PAP or CHAP username for PPP/MLPPP bundle.
<password>	PAP or CHAP password for PPP/MLPPP bundle.

Configuring peer name and password for PAP or CHAP

Configure the peer name and password for PAP or CHAP authentication.

This command causes the bundle to flap in order to re-trigger negotiation. Therefore, before you modify the PPP PAP or CHAP peer name (or sent username) parameters, shutdown the bundle (using the **shutdown** command) and reenable it (using the **no shutdown** command) after you complete the configuration .

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure the peer name for PAP or CHAP, enter:

   ```
   ppp {pap | chap} peer-name <peername> <password>
   ```

Table 92: Variable definitions

Variable	Value
chap	Configure properties for CHAP
pap	Configure properties for PAP
<peername>	PAP or CHAP username expected from the peer.
<password>	PAP or CHAP password for peer.

Configuring authentication method

Configure the method to use for user authentication.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure the PPP authentication method, enter:

   ```
   ppp authentication-database { local | radius }
   ```

Table 93: Variable definitions

Variable	Value
local	Specifies local authentication.
radius	Specifies RADIUS authentication.

Configuring echo-interval

Configure the echo interval for the interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure the PPP echo interval, enter:

   ```
   ppp echo-interval <3-60>
   ```

Table 94: Variable definitions

Variable	Value
<3-60>	Specifies the interval in seconds (default is 5).

Configuring interleaving

Enable or disable interleaving on the interface.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To configure PPP interleaving, enter:

```
[no] ppp interleave
```

Configuring fragmentation delay for interleaving

Configure the fragmentation delay for interleaving.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To configure fragmentation delay, enter:

```
ppp lfi-fragment-delay <10-50>
```

Table 95: Variable definitions

Variable	Value
<10-50>	Specifies the delay in milliseconds (default is 10).

Configuring MTU, MRU, and magic number for PPP

Configure the MTU, MRU, and magic number parameters for the PPP or MLPPP bundle.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To configure MTU, MRU, and magic number for PPP, enter:

```
ppp mtu-mru-magic <mtu-range> [mru <mru-range>] [magic_check
{enable|disable}]
```

Table 96: Variable definitions

Variable	Value
<mtu-range>	Maximum transmission unit range, specified as <minimum-default-maxiumum>. Default value is 64-1500-9216. The Maximum Transmit Unit (MTU) is the maximum size of the PPP information field that the interface can transmit.
<mru-range>	Maximum receive unit range, specified as <minimum-default-maximum>. Default value is 64-1500-9216. The Maximum Receive Unit (MRU) is the maximum size of the PPP information field that the interface can receive. **Important:** The MRU value must be within the configured system jumbo-limit.
enable	Enables magic number, which is a random number chosen to distinguish the two ends of a link and to detect loopback error conditions.
disable	Disables magic number.

Configuring peer address

Configure the peer IP address for the PPP bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure peer address, enter:

   ```
   ppp peer-addr <A.B.C.D>
   ```

Configuring retry interval

Configure the retry timer for the PPP bundle.

Procedure steps

1. To enter the configuration mode, enter:

Comments? infodev@avaya.com

```
configure terminal
```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To configure retry interval, enter:

```
ppp retry-interval <3-60>
```

Table 97: Variable definitions

Variable	Value
3-60	Specifies the interval in seconds. Default value is 3.

Configuring the source address

Configure the negotiating IP address of the bundle.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To configure source address, enter:

```
ppp src-addr <A.B.C.D>
```

Table 98: Variable definitions

Variable	Value
<A.B.C.D>	Specifies the negotiating IP address of the bundle (default is source forwarding address of the bundle).

Configuring RTP

Enabling RTP Header Compression

Enable or disable the RTP Header Compression feature. Before enabling RTP Header Compression, the bundle must be configured with a link, encapsulated with PPP protocol, and

assigned an IPv4 address. When this command is enabled, the RTP options are negotiated with the peer during the IPCP phase.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure the RTP Header Compression feature, enter:

   ```
   [no] rtp
   ```

Table 99: Variable definitions

Variable	Value
[no]	Disables RTP

Configuring the maximum number of connections for RTP header compression

Configure the maximum number of connections for which RTP header compression is applicable on transmit or receive side.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify RTP Header Compression configuration, enter:

   ```
   [no] rtp
   ```

4. To configure the maximum number of connections for RTP Header Compression, enter:

   ```
   [no] connections <1-1000>
   ```

Table 100: Variable definitions

Variable	Value
[no]	Resets the number of connections to the default value (1000).

Comments? infodev@avaya.com

Enabling negotiation of RTP options

Enable negotiation of RTP options with the peer. This command allows interoperability with legacy Tasman products. Since the default behaviour of RTP is to enable negotiation, use the no form of this command in order to interoperate with legacy Tasman products that do not support negotiation.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify RTP Header Compression configuration, enter:

   ```
   [no] rtp
   ```

4. To configure the maximum number of connections for RTP Header Compression, enter:

   ```
   [no] negotiation ipcp
   ```

Table 101: Variable definitions

Variable	Value
[no]	Disables negotiation of RTP options during the IPCP phase

Configuring the timeout for the compressor and decompressor engines

Configure the timeout (flushing time) in seconds for the context table entries for both compressor and decompressor engines. The flushing for any particular context entry will happen only if for this (timeout) duration no packets are received with that particular context-identifier (CID).

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify RTP Header Compression configuration, enter:

   ```
   [no] rtp
   ```

4. To configure the timeout, enter:

   ```
   [no] timeout <3-1000>
   ```

Table 102: Variable definitions

Variable	Value
[no]	Sets the timeout value to the default (5 seconds).

Configuring port range and bandwidth for RTP traffic

Configure the UDP port range for LFI treatment along with maximum bandwidth reserved for voice traffic.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure port range and bandwidth for RTP traffic, enter:

   ```
   ppp ip-rtp-reserve <start-port> <end-port> <max-bwidth>
   ```

Table 103: Variable definitions

Variable	Value
<start-port>	Low-end port value in decimal - default 1024. Valid range: 1024 - 65535
<end-port>	High-end port value in decimal - default 65535. Valid range: 1024 - 65535
<max-bwidth>	Maximum bandwidth in Kb/s. Default is 32. Valid range: 4 - 2000

Configuring MLPPP properties

Configure the MLPPP properties.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure MLPPP properties, enter:

   ```
   mlppp [mrru <mrru_range> ] [sequence {long | short} ]
   [seg_threshold <64-9216> ] [differential_delay <0-128> ]
   [discriminator <A.B.C.D> ] [minimum_links <min-links>]
   ```

Table 104: Variable definitions

Variable	Value
[mrru <mrru_range>]	maximum receive reconstructed unit range, specified as <minimum-default-maxiumum>. Specifies the minimum, default, and maximum number of octets in the information fields of reassembled packets. Default value is 1500-1524-9216.
[sequence {long | short}]	MLPPP sequence number length. Short is 12 bits, long is 24 bits. The default is long.
[seg_threshold <64-9216>]	All packet fragments are equal to or less than seg_threshold. The range is 64 - 9216; the default is 512.
[differential_delay <0-128>]	Tolerance, in milliseconds, to differential delay between links (default: 128)
[discriminator <A.B.C.D>]	IP address of the MLPPP bundle (default: bundle IP address)
[minimum_links <min-links>]	Minimum number of links that have to be active for this interface to remain active (default: 1).

Configuring BCP on PPP bundles

Configuring the Layer 2 interface mode

Configure the Layer 2 interface mode for the PPP bundle.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To configure the Layer 2 interface mode, enter:

```
switchport mode {hybrid|trunk|access [vlan-stacking]}
```

Table 105: Variable definitions

Variable	Value
access [vlan-stacking]	Sets the Layer 2 interface as access. To enable VLAN stacking, include the vlan-stacking option.
hybrid	Sets the Layer 2 interface as hybrid.
trunk	Sets the Layer 2 interface as trunk (classify tagged frames only).

Configuring the hybrid interface properties

Configure the hybrid interface properties.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To configure the hybrid interface properties, enter:

```
switchport hybrid {allowed | remove} vlan {<vid> | all}
egress {tagged|untagged}
```

Table 106: Variable definitions

Variable	Value
{allowed | remove}	Sets (or removes) the VLANs that can transmit and receive through this Layer 2 interface.
{<vid> | all}	Specifies the VLANs to allow or remove. Enter all to specify all VLANs.
{tagged|untagged}	Specifies the tagging behavior on outgoing frames: tagged: enables egress tagging on outgoing frames untagged: disables egress tagging on outgoing frames.

Comments? infodev@avaya.com

Configuring trunk interface properties

Configure the trunk interface properties.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To configure the trunk interface properties, enter:

   ```
   switchport trunk {allowed | remove} vlan {vid|all}
   ```

Table 107: Variable definitions

Variable	Value
{allowed | remove}	Sets (or removes) the VLANs that can transmit and receive through this Layer 2 interface.
{vid | all}	Specifies the VLANs to allow or remove. Enter all to specify all VLANs.

Setting the default VLAN ID for the interface

Set the default VLAN on the interface.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To set the default VLAN ID, enter:

   ```
   switchport pvid <1-4000>
   ```

Assigning an IP address to the WAN bundle

Once the bundle is configured with an encapsulation, assign an IP address and subnet mask to the bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To set the IP address for the bundle, enter:

   ```
   ip address <A.B.C.D> <netmask>
   ```

Table 108: Variable definitions

Variable	Value
<A.B.C.D> <netmask>	Specifies the IP address and subnet mask of the bundle.

Comments? infodev@avaya.com

Chapter 14: Frame Relay configuration

Configuring encapsulation for WAN modules

In order to configure the encapsulation and IP address for a WAN interface, you must first associate the interface with a bundle. A bundle is a single, high speed virtual path consisting of one or more physical links. For instructions on configuring a bundle for an interface, see the preceding module-specific section.

All of the following procedures assume that you have already created a WAN interface bundle that is linked to a physical WAN port.

Configuring Frame relay

1. Enable Frame Relay Encapsulation on an Interface (Required)
2. Configure Dynamic or Static Address Mapping (Required)
3. Configure the LMI (Optional)
4. Configure Frame Relay Traffic Shaping (Optional)
5. Monitor and Maintain the Frame Relay Connections (Optional)

Setting bundle encapsulation to Frame Relay or MFR

Set the bundle encapsulation to Frame Relay or MFR.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To set the encapsulation, enter:

   ```
   encapsulation [frelay | mfr]
   ```

Enabling Frame Relay

Enable or disable Frame Relay on the bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To enable or disable Frame Relay on the bundle, enter:

   ```
   [no] enable interface
   ```

Enabling RFC 1490 fragmentation

Enable or disable RFC 1490 fragmentation on the bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To configure RFC 1490 fragmentation, enter:

   ```
   [no] enable fragment_rfc 1490
   ```

Configuring maximum frame size

Configure the maximum frame size for the Frame Relay bundle. This setting is applicable to all PVCs within a specific bundle.

Larger incoming frames are dropped. Outgoing frames are fragmented using RFC 1490/FRF 12 to stay within the max frame size.

Comments? infodev@avaya.com

On some occasions, providing a small frame size can cause problems when a large number of PVCs are configured within the same bundle. This is because the LMI frame size is restricted to the configured frame size. Since LMI frames carry the status of all PVCs within the bundle, if the frame size is too small, the LMI packet cannot carry all of the PVCs and their status information to the remote site. The CLI configuration does not allow a very low frame size.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To configure Frame Relay frame size, enter:

   ```
   fr frame_size <56-9216>
   ```

Table 109: Variable definitions

Variable	Value
56-9216	Maximum frame size in bytes (default 1600).

Configuring interleaving

Configure the traffic properties for high-priority packets and enable interleaving.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To specify interleaving, enter:

   ```
   interleave
   ```

5. To configure committed rate and burst rate for high priority packets, enter:

   ```
   hiprio <committed-rate> <burst-rate>
   ```

6. To enable interleaving, enter:

```
[no] enable
```

Table 110: Variable definitions

Variable	Value
<committed-rate>	Committed rate as a percentage of the total CIR of FRF.12 fragmentation enabled PVCs.
<burst-rate>	Burst (excess) rate as a percentage of the total CIR of FRF.12 fragmentation enabled PVCs.
[no]	Disables interleaving.

Configuring interface type

Configure the interface as DCE, DTE, or NNI.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To specify the interface type, enter:

   ```
   intf_type {dce | dte | nni}
   ```

Table 111: Variable definitions

Variable	Value
dce	Data circuit-terminating equipment.
dte	Data terminal equipment.
nni	Network to network interface.

Configuring local management interface

Configure the local management interface type.

Procedure steps

1. To enter the configuration mode, enter:

Comments? infodev@avaya.com

```
configure terminal
```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify Frame Relay, enter:

```
fr
```

4. To specify the local management interface type, enter:

```
lmi lmi_type {ansi | cisco | q933a}
```

Table 112: Variable definitions

Variable	Value
ansi	ANSI T1.617 Annex D (default)
cisco	Cisco LMI
q933a	ITU-T Q.933 Annex A

Configuring the LMI error threshold (DCE)

Configure the LMI status polling interval and error threshold parameters. In the DCE mode, the system responds to LMI polls from the remote DTE device.

This procedure applies for both DCE and NNI interface types.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify Frame Relay, enter:

```
fr
```

4. To specify the local management interface configuration, enter:

```
lmi
```

5. To configure the polling interval and error threshold, enter:

```
dce [n392 <1-10>] [n393 <1-10>] [t392 <5-255>]
```

Table 113: Variable definitions

Variable	Value
[n392 <1-10>]	Error threshold (the maximum number of unreceived LMI status inquiries accepted by the system before the interface is declared down). The range is 1 - 10; the default is 9. This value must always be less than the n393 value.
[n393 <1-10>]	Maximum number of LMI polling intervals during which the n392 error threshold is counted. The range is 1 - 10; the default is 10.
[t392 <5-255>]	Polling verification timer. The range is 5-255; the default is 15.

Configuring the LMI error threshold (DTE)

Configure the LMI status polling interval and error threshold parameters. In the DTE mode, the system sends LMI polls to the remote DTE device.

This procedure applies for both DTE and NNI interface types.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To specify the local management interface configuration, enter:

   ```
   lmi
   ```

5. To configure the polling interval and error threshold, enter:

   ```
   dte [n392 <1-10>] [n393 <1-10>] [n391 <1-255>]
   ```

Table 114: Variable definitions

Variable	Value
[n392 <1-10>]	Error threshold (maximum number of unanswered LMI status inquiries accepted by the system before the interface is declared down). The range is 1 - 10; the default is 9. This value must always be less than the n393 value below.

Comments? infodev@avaya.com

Variable	Value
[n393 <1-10>]	Maximum number of LMI polling intervals during which the n392 error threshold above is counted. The range is 1 - 10; the default is 10.
[n391 <1-255>]	Number of LMI status inquiries that pass before the system sends a full status inquiry message. The range is 1 - 255; the default is 6.

Configuring the LMI keepalive

Set the bundle LMI polling keepalive interval for all PVCs.

The DTE generates an LMI status inquiry message once every keepalive interval and sends it to the DCE, which expects to receive status inquiries once every keepalive interval. If the DCE does not receive an inquiry during a keepalive interval, the error count advances by one.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To specify the local management interface configuration, enter:

   ```
   lmi
   ```

5. To configure the polling interval and error threshold, enter:

   ```
   keepalive <5-255>
   ```

Table 115: Variable definitions

Variable	Value
<5-255>	The range is 5 - 255 seconds. The default is 10 seconds for DTE/NNI. The default is 15 seconds for DCE.

Configuring LMI fast recovery

Enable recovery measures if the LMI times out. By default, fast recovery is off.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To specify the local management interface configuration, enter:

   ```
   lmi
   ```

5. To configure fast recovery, enter:

   ```
   [no] fast_recovery
   ```

Table 116: Variable definitions

Variable	Value
<5-255>	The range is 5 - 255 seconds. The default is 10 seconds for DTE/NNI. The default is 15 seconds for DCE.

Configuring the inverse ARP polling timer

Configure the Inverse ARP polling timer interval. This is how often the system polls other frame relay devices for IP data. This function eliminates the need for PVC map entries.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the local management interface configuration, enter:

   ```
   fr invarp <interval>
   ```

Table 117: Variable definitions

Variable	Value
<interval>	Time interval for polling The range is 30 - 300 seconds; the default is 30 seconds.

Configuring Frame Relay PVCs

Adding a PVC to a Frame Relay bundle

Add a PVC to the Frame Relay bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To configure a PVC, enter:

   ```
   [no] pvc <16-1022>
   ```

Table 118: Variable definitions

Variable	Value
<16-1022>	Data link connection identifier (DLCI) of the PVC
[no]	Deletes the PVC.

Configure the network type for the PVC

Configure the specified PVC as a trusted or untrusted interface for security features.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To select the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To configure tagged frames, enter:

   ```
   crypto { trusted | untrusted }
   ```

Table 119: Variable definitions

Variable	Value
trusted	Interface is part of a trusted network.
untrusted	Interface is part of an untrusted network.

Configuring a description for the PVC

Configure a description for the PVC.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To specify the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To specify a name for the PVC, enter:

   ```
   desc <"name">
   ```

Table 120: Variable definitions

Variable	Value
<"name">	Name of the PVC Use a string of up to 64 characters, enclosed in quotes.

Enabling PVCs

Enable or disable PVCs on the bundle.

Comments? infodev@avaya.com

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To enable or disable one or all configured PVCs, enter:

   ```
   [no] enable pvc {<dlci> | all }
   ```

Table 121: Variable definitions

Variable	Value
{<dlci> | all }	Specifies the DLCI number. Enter all to specify all PVCs.
[no]	Disables the PVC.

Enabling and disabling a selected PVC

Enable or disable the selected PVC.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To select the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To enable or disable the selected PVC, enter:

   ```
   [no] enable
   ```

Table 122: Variable definitions

Variable	Value
no	Disables the PVC

Provisioning FRF12 on the PVC

Provision FRF12 on the PVC.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To specify the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To configure FRF12, enter:

   ```
   frf12 [framesize <56-4096>]
   ```

Table 123: Variable definitions

Variable	Value
[framesize <56-4096>]	Maximum frame size in bytes (default:1600)

Configuring FRF.20 IP header compression properties

Configure FRF.20 IP header compression properties.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To specify the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To configure FRF.20 properties, enter:

Comments? infodev@avaya.com

```
frf20 config [retries_timeout <retries_timeout>] [retries
<retries>] [f_max_period <f_max_period>] [f_max_time
<f_max_time>] [timeout <timeout>]
```

Table 124: Variable definitions

Variable	Value
[retries_timeout <retries_timeout>]	Specifies the timeout of the FRF.20 state machine. 1-10 (default 3).
[retries <retries>]	Specifies the number of retries for negotiation. 1-10 (default 3).
[f_max_period <f_max_period>]	Negotiable number of TCP headers before context state. 0-0xFFF. (default 256).
[f_max_time <f_max_time>]	Negotiable time interval between full headers. 0-0xff (default 5).
[timeout <timeout>]	Timeout for RTP entries in seconds. 3-1000. (default 5).

Enabling FRF.20 IP header compression

Enable FRF.20 IP header compression.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To specify the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To enable FRF.20, enter:

   ```
   [no] frf20 enable
   ```

Table 125: Variable definitions

Variable	Value
no	Disables FRF.20 compression.

Configuring IP address for the PVC

Configure an IP address for the PVC.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To select the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To set the IP address for the PVC, enter:

   ```
   {ip address <A.B.C.D> <netmask> [type <broadcast>]} | {ipv6
   address {<X:X::X:X/M>|<prefix-name> <Y:Y::Y:Y/M>}}
   ```

Assigning a static route to a PVC

Assign a static route to a PVC. Once a static route has been assigned, inverse ARP ceases to function. If a destination IP address is changed, the static route is not updated.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the PVC, enter:

   ```
   pvc <16-1022>
   ```

3. To assign a static route to the PVC, enter:

   ```
   [no] map ipv4 <A.B.C.D>
   ```

Table 126: Variable definitions

Variable	Value
A.B.C.D	Specifies the remote IP address.
no	Removes the static route.

Comments? infodev@avaya.com

Configuring PVC policing

Enable or disable PVC traffic policing on incoming traffic for a PVC.

Policing sets the committed information rate (CIR) and data burst parameters that control the data flow on the PVC in the incoming direction. Policing is automatically enabled on all PVCs of all Frame Relay bundles.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To select the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To configure policing for the PVC, enter:

   ```
   policing [cir <n>] [bc <n>] [be <n>] [<de>]
   ```

Table 127: Variable definitions

Variable	Value
cir <n>	The committed information rate for the PVC, in bits per second. Non-committed PVCs are created by setting the PVC CIR to 0.
bc <n>	Maximum committed (guaranteed) transmission burst size for the PVC, in bits. The default is bundle bandwidth rate. Generally, this value exceeds CIR and may be a multiple of that value.
be <n>	Excess burst size (number of bits in excess of bc value); non-guaranteed. Default is 0
<de>	Enable discard-eligible (DE) bit on a PVC. The default is OFF. This setting allows lower priority PVCs to designate their traffic as eligible for discard during the periods of heavy congestion.

Configuring PVC shaping

Enable or disable PVC traffic shaping on outgoing traffic for a PVC.

Shaping sets the committed information rate and data burst parameters that control the data flow on the PVC in the outgoing direction. Shaping is automatically enabled on all PVCs of all Frame Relay bundles.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To select the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To configure shaping for the PVC, enter:

   ```
   shaping [cir <n>] [bcmax <n>] [bcmin <n>] [be <n>]
   ```

Table 128: Variable definitions

Variable	Value
cir <n>	The committed information rate for the PVC, in bits per second. The default is bundle bandwidth rate. Setting the PVC CIR to 0 creates non-committed PVCs.
bcmax <n>	Maximum committed (guaranteed) transmission burst size for the PVC, in bits. The default is bundle bandwidth rate. Generally, this value exceeds CIR and may be a multiple of that value
bcmin <n>	Minimum committed (guaranteed) transmission burst size for the PVC, in bits. Generally, this is a value greater than cir and less than bcmax.
be <n>	Excess burst size (number of bits in excess of bcmax); non-guaranteed. Default is 0.

Comments? infodev@avaya.com

Enable Layer 2 switching on the PVC

Enable Layer 2 switching between the current PVC and another PVC on the same bundle, or between the current PVC and a PVC on another bundle.

To ensure correct switching, specify both the PVC number and the bundle name. Before enabling switching, configure the other bundle and associated PVC. Both of the bundles and PVCs must exist to enable switching.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To select the PVC, enter:

   ```
   pvc <16-1022>
   ```

5. To enable switching for the PVC, enter:

   ```
   [no] switch <dlci> <bundle>
   ```

Table 129: Variable definitions

Variable	Value
<dlci>	The DLCI number of the other PVC. Allowable range: 16-1022
<bundle>	The name of the WAN bundle to which the other PVC belongs. This entry is not required if both PVCs are on the same bundle.

Configuring MFR

Configuring ack message timer and retries

Configure the ack message timer and retries.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To configure MFR ack message timer and retries, enter:

   ```
   mfr ack_msg [ack_timer <1-10>] [max_retry (1-5>]
   ```

Table 130: Variable definitions

Variable	Value
[ack_timer <1-10>]	Time interval for which the system waits for an acknowledgement from the network device. The range is 1 - 10 seconds; the default is 4 seconds.
[max_retry (1-5>]	Maximum number of additional times the system sends an acknowledgement request to a device before dropping a link from the bundle. The range is 1 - 5 seconds; the default is 2 seconds.

Configuring number of links required to activate bundle

Configure the number of links required to activate the bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To configure the number of activated links required to activate the bundle, enter:

   ```
   mfr class [A | B | C] [threshold <1-28>]
   ```


Comments? infodev@avaya.com

Table 131: Variable definitions

Variable	Value
A	bundle is up when at least one link is up (default)
B	bundle is up when all links are up
C	bundle is up when user-specified number of links are up
[threshold <1-28>]	Minimum number of activated links required to activate the bundle (default: all).

Configuring differential delay

Configure the differential delay for the MFR bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To configure differential delay, enter:

   ```
   mfr diff_delay <diff-delay>
   ```

Table 132: Variable definitions

Variable	Value
<diff-delay>	Tolerance, in milliseconds, to differential delay between frame relay links The range is 10 - 128; the default is 100.

Configuring fragment size

Configure fragment size for the bundle above which a packet is fragmented.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

```
interface bundle <bundle-name>
```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To configure fragment size, enter:

   ```
   mfr fragment_size <56-9216>
   ```

Table 133: Variable definitions

Variable	Value
<56-9216>	Maximum number of bytes in each frame. The range is 56 – 4096; default is 1500.

Configuring hello timer

Configure the hello timer for the MFR bundle. This is the time interval between acknowledgement requests sent to destination devices.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To configure hello timer, enter:

   ```
   mfr hello_timer <1-180>
   ```

Table 134: Variable definitions

Variable	Value
1-180	Interval in seconds (default: 10).

Configuring segmentation threshold

Configure the segmentation threshold.

The segmentation threshold can never be greater than the frame size. This is the time interval between acknowledgement requests sent to destination devices.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify Frame Relay, enter:

   ```
   fr
   ```

4. To configure hello timer, enter:

   ```
   mfr seg_threshold <56-4096>
   ```

Table 135: Variable definitions

Variable	Value
<56-4096>	All packet fragments will be equal to or greater than seg_threshold. Packets less than 2 x seg_threshold will be forwarded rather than fragmented. The range is 56 - 4096; the default is 512. If the segmentation threshold you enter is greater than the frame size, the system disregards it.

Configuring AVCs

Configuring number of links required to activate the AVC

Configure the number of links required to activate the AVC.

In class D and E, only the administrator can bring the AVC status up or down by modifying the configured shaping parameters of one or more CVCs. In such cases, the remote AVC does not learn of the updated status.

If the network administrator sets an AVC in the class “D” parameter and then administratively reduces the CIR of any CVC that causes the local AVC to go down (because of the class D setting), the remote AVC will not go down because the local and remote CIR values do not match. To avoid this problem, either change the CIR for the remote CVC to match the local CIR value or reduce the class D CIR value.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the AVC bundle, enter:

```
interface avc <avc-name> <dlci>
```

3. To configure the number of activated links required to activate the bundle, enter:

```
mfr class [A | B | C ][D | E]
```

Table 136: Variable definitions

Variable	Value
A	If any CVC is up, AVC is up. This is the default.
B	If all CVCs are up, AVC is up.
C	If the user-supplied threshold is satisfied, AVC is up
D	If every CVC has a CIR greater than or equal to user supplied threshold value, AVC is up
E	If the total CIR is above the user supplied threshold, then AVC is up

Enabling the AVC

Enable the AVC.

Procedure steps

1. To enter the configuration mode, enter:

```
configure terminal
```

2. To select the AVC bundle, enter:

```
interface avc <avc-name> <dlci>
```

3. To enable the AVC, enter:

```
[no] enable avc
```

Table 137: Variable definitions

Variable	Value
no	Disables the AVC.

Comments? infodev@avaya.com

Adding a PVC to the AVC

Add a PVC from a specific bundle to the AVC. The system can bundle as many as 28 PVCs into one AVC. A CVC cannot be shared between separate AVCs..

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. Add the CVC, enter:

   ```
   cvc <dlci> <bundle-name>
   ```

Table 138: Variable definitions

Variable	Value
dlci	DLCI of the virtual PVC. The range is 16 – 1022
bundle-name	Name of the bundle the CVC belongs to.

Enabling CVCs

Enable individual CVCs on an AVC.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. To enable the CVC, enter:

   ```
   [no] enable cvc <dlci> <bundle-name>
   ```

Table 139: Variable definitions

Variable	Value
no	Disables the CVC.

Configuring MFR enhanced mode for a specified AVC

Switch the MFR mode from MFR End-to-End standard FRF.15 mode (default) to MFR End-to-End Router enhanced FRF.15 mode.

Enhanced FRF.15 is a proprietary protocol and can only work between Avaya Secure Router 2330/4134 systems.

In addition to the features of Standard FRF.15, Enhanced mode calculates differential delay between CVCs; those with unacceptable delay are taken out of active data transfer, thus improving overall throughput of the AVC. Also, end-to-end keepalive messages are sent per CVC, thus helping to maintain the VC integrity across both ends. Keepalive messages also detect software/hardware loopbacks.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. To configure enhanced MFR, enter:

   ```
   [no] mfr_e2e_enhanced
   ```

Table 140: Variable definitions

Variable	Value
[no]	Reverts to standard MFR mode.

Configuring enhanced FRF.15 mode for all AVCs

Switch the MFR mode from MFR End-to-End standard FRF.15 mode (default) to MFR End-to-End Router enhanced FRF.15 mode.

This command automatically applies the settings to all existing AVCs without rebooting the system. However, if the settings are saved, they are used the next time that the system is rebooted.

Enhanced FRF.15 is a proprietary protocol and can only work between Secure Router 2330/4134 systems.

In addition to the features of Standard FRF.15, Enhanced mode calculates differential delay between CVCs; those with unacceptable delay are taken out of active data transfer, thus improving overall throughput of the AVC. Also, end-to-end keepalive messages are sent per

Comments? infodev@avaya.com

CVC, thus helping to maintain the VC integrity across both ends. Keepalive messages also detect software/hardware loopbacks.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To configure enhanced MFR, enter:

   ```
   [no] fr mfr_e2e_enhanced
   ```

Table 141: Variable definitions

Variable	Value
[no]	Reverts to standard FRF.15 mode.

Configuring differential delay

Configure the maximum differential delay allows for a CVC.

When the AVC is in Router Enhanced FRF.15 mode, using the “no diff_delay” command will disable differential delay calculations and will not take any action toward dropping any CVC that is above the configured differential delay limit. The display of CVCs will, however, display the individual differential delay values for the system Administrator’s awareness when the show interface avc x 16 command is used.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. To configure differential delay, enter:

   ```
   [no] diff_delay <diff-delay>
   ```

Table 142: Variable definitions

Variable	Value
diff-delay	Tolerance, in milliseconds, to differential delay between frame relay links The range is 10 - 128; the default is 100.

Configuring fragment size

Configure fragment size for the bundle above which a packet is fragmented. Packets are intelligently fragmented when the fragment size is exceeded.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. To configure fragment size, enter:

   ```
   fragment_size <56-4096>
   ```

Table 143: Variable definitions

Variable	Value
56-4096	Maximum number of bytes in each frame. The range is 56 – 4096; default is 1500.

Configuring segmentation threshold

Configure the segmentation threshold for the AVC.

The segmentation threshold can never be greater than the frame size. This is the time interval between acknowledgement requests sent to destination devices.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. To configure hello timer, enter:

   ```
   mfr seg_threshold
   ```


Comments? infodev@avaya.com

Table 144: Variable definitions

Variable	Value
56-4096	All packet fragments will be equal to or greater than this value. Packets less than 2xseg_threshold will be forwarded rather than fragmented. The range is 56 – 4096; default is 512 If the segmentation threshold you enter is greater than the frame size, the system disregards it.

Configuring AVC sequence

Set the sequence length of an AVC. You can choose either 12- or 24-bit spacing.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. To configure hello timer, enter:

   ```
   sequence [long | short]
   ```

Table 145: Variable definitions

Variable	Value
long	24-bit sequence space
short	12-bit sequence space

Configuring an IP address for the AVC

Assign a routing destination IP address and subnet to the AVC.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. To configure the IP address, enter:

```
ip address <A.B.C.D> <mask>
```

Table 146: Variable definitions

Variable	Value
A.B.C.D	IP address of the AVC is dotted notation.
mask	Subnet mask of the AVC.

Enabling directed broadcasts on the AVC

Enable or disable forwarding of direct broadcasts from this interface. By default, directed broadcasts are enabled.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. To enable directed broadcasts, enter:

   ```
   [no] ip directed_broadcast
   ```

Table 147: Variable definitions

Variable	Value
no	Disables directed broadcasts.

Assigning a static route to an AVC

Assign a static route to an AVC. Once a static route has been assigned, inverse ARP ceases to function. If a destination IP address is changed, the static route is not updated.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the AVC bundle, enter:

   ```
   interface avc <avc-name> <dlci>
   ```

3. To assign a static route to the AVC, enter:

```
[no] map <A.B.C.D>
```

Table 148: Variable definitions

Variable	Value
A.B.C.D	Specifies the remote IP address.
no	Removes the static route.

Assigning an IP address to the WAN bundle

Once the bundle is configured with an encapsulation, assign an IP address and subnet mask to the bundle.

Procedure steps

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select the WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To set the IP address for the bundle, enter:

   ```
   ip address <A.B.C.D> <netmask>
   ```

Table 149: Variable definitions

Variable	Value
<A.B.C.D> <netmask>	Specifies the IP address and subnet mask of the bundle.

Displaying Frame Relay information

Displaying the configured AVCs

Display the configured AVCs on the router.

Procedure steps

To display the configured AVCs, enter:

```
show fr avcs
```

Displaying the configured CVCs

Display the configured CVCs on the router.

Procedure steps

To display the configured CVCs, enter:

```
show fr cvcs
```

Displaying the configured PVCs

Display all PVCs including their bundle name, PVC number and status, and policing (enabled or disabled) information. If the PVC is switched to another PVC, that PVC number is shown. If the PVC terminates at a LAN, the PVC IP address is shown.

Procedure steps

To display the configured PVCs, enter:

```
show fr pvcs
```

Displaying virtual circuit statistics

Display virtual circuit statistics for a frame relay bundle.

Procedure steps

To display virtual circuit statistics, enter:

```
show fr vcstats <bundle-name> <16-1022> [stat-type <1-3>]
```

Table 150: Variable definitions

Variable	Value
<bundle-name>	Specifies the bundle name.
<16-1022>	Specifies the DLCI number.
[stat-type <1-3>]	Specifies the type of statistics: 1=RXMON, 2=INJECT, 3=1490. Default is 1.

Comments? infodev@avaya.com

Clearing virtual circuit statistics

Clear the virtual circuit statistics for a frame relay bundle.

Procedure steps

To clear virtual circuit statistics, enter:

```
clear fr vcstats <bundle-name> <16-1022> [stat-type <1-3>]
```

Table 151: Variable definitions

Variable	Value
<bundle-name>	Specifies the bundle name.
<16-1022>	Specifies the DLCI number.
[stat-type <1-3>]	Specifies the type of statistics: 1=RXMON, 2=INJECT, 3=1490. Default is 1.

Displaying inverse ARP statistics

Display inverse ARP statistics for a frame relay bundle.

Procedure steps

To display virtual circuit statistics, enter:

```
show fr invarp {<bundle-name> | all}
```

Clearing inverse ARP statistics

Clear the inverse ARP statistics for a frame relay bundle.

Procedure steps

To clear virtual circuit statistics, enter:

```
clear fr invarp {<bundle-name> | all}
```

Displaying inverse ARP time interval

Display the time interval configured for the frame relay inverse ARP timer.

Procedure steps

To display virtual circuit statistics, enter:

```
show fr invarp_int
```

Displaying LMI statistics

Display the LMI statistics for a bundle.

Procedure steps

To display virtual circuit statistics, enter:

```
show fr lmistats <bundle-name>
```

Clearing LMI statistics

Clear the LMI statistics for a bundle.

Procedure steps

To clear virtual circuit statistics, enter:

```
clear fr lmistats <bundle-name>
```

Chapter 15: ADSL small module configuration

This chapter describes how to configure the Asymmetric Digital Subscriber Line (ADSL) small module.

Navigation

- Upgrading the ADSL small module software on page 171
- Configuring the ADSL small module on page 172
- Displaying the ADSL small module configuration on page 173
- Displaying ADSL small module user statistics on page 174
- Configuring ATM on an ADSL module on page 175
- Configuring the maximum VC circuits on page 177

Upgrading the ADSL small module software

Upgrade the ADSL small module software to ensure you have the latest available software version.

Prerequisites

- The new ADSL small module software must be in Compact Flash 0 [/cf0].
- The new ADSL small module software must be named *bcm96338R_fs_kernel*.

Procedure steps

1. To access configuration mode, enter:

   ```
   configuration terminal
   ```

2. To configure the ADSL small module, enter:

   ```
   [no] module xdsl <slot/subslot>
   ```

3. To upgrade to the latest ADSL software version, enter:

   ```
   software_upgrade
   ```

Configuring the ADSL small module

Configure the ADSL small module to operate as a primary interface for an Integrated Services Digital Network (ISDN) interface.

Procedure steps

1. To access configuration mode, enter:

   ```
   configuration terminal
   ```

2. To configure the ADSL small module, enter:

   ```
   [no] module xdsl <slot/subslot>
   ```

3. To configure Seamless Rate Adaption (SRA), enter:

   ```
   [no] sra
   ```

4. To configure bitswap coding, enter:

   ```
   [no] bitswap-coding
   ```

5. To configure the L3 power state, enter:

   ```
   [no] L3-power-state
   ```

6. To configure trellis coding, enter:

   ```
   [no] trellis_coding
   ```

7. To configure the modulation mode, enter:

   ```
   modulation-mode {ansi-dmt|adsl| adsllite|adsl2|adsl2plus|
   reach-adsl2| adsl2plusm|all}
   ```

Table 152: Variable definitions

Variable	Value
`[no] bitswap-coding`	Enables or disables bitswap coding on the ADSL small module.
`[no] L3-power-state`	Enables or disables L3 power state on the ADSL small module.
`modulation-mode`	Specifies the modulation mode for the ADSL small module. Values include: • ansi-dmt—ANSI T1.413 • adsl—ITU G.992.1 (G.DMT) • adsllite—ITU G.992.2 (G.Lite) • adsl2—ITU G.992.3 (ADSL2)

Comments? infodev@avaya.com

Variable	Value
	• adsl2plus—ITU G.992.5 (ADSL2+) • reach-adsl2—ITU G.992.3 (Annex L) • adsl2plusm—ITU G.992.5 (Annex M) • all—All (default)
[no] sra	Enables or disables Seamless Rate Adaptation (SRA) on the ADSL small module.
[no] trellis_coding	Enables or disables trellis coding on the ADSL small module.

Displaying the ADSL small module configuration

Display the ADSL small module configuration to view the module parameter configuration.

Procedure steps

To display the ADSL small module configuration, enter:

```
show module configuration xdsl <slot/subslot>
```

The following job aid shows sample output for the **show module configuration xdsl <slot/subslot>** command.

Table 153: Job aid: show module configuration xdsl command output

```
show module configuration xdsl 1/1

Software Version : 3.10L.05.A2pB022g.d20h

adsl: ADSL driver and PHY status

Status: ShowtimeRetrain Reason: 0

Channel: FAST, Upstream rate = 1023 Kbps, Downstream rate =
23724 Kbps

Link Power State: L0

Mode: ADSL2+

Line Status: No Defect

SNR (dB): 6.2 10.0

Attn(dB): 1.5 0.0
```

```
Pwr(dBm): -25.6 0.8
Trellis Coding : Enable
BitSwap Coding : Disable
SRA : Disable
L3 Power State : Disable
```

Displaying ADSL small module user statistics

Display ADSL small module user statistics to view information about any occurrences of errors, losses, or module unavailability for the ADSL small module.

Procedure steps

To display ADSL small module user statistics, enter:

```
show module userstats xdsl <slot/subslot>
```

The following job aid shows sample output for the **show module userstats xdsl <slot/subslot>** command.

Table 154: Job aid: show module userstats xdsl command output

```
show module userstats xdsl 3/1
USER Current Statistics (145 seconds elapsed)
-----------------------------------------
LOSS : 0, LOFS : 0, ES : 0, SES : 0
UAS : 0, CRC : 0
USER Lifetime Statistics:
------------------------
LOSS : 0, LOFS : 0, ES : 378, SES : 21
UAS : 43, CRC : 1714
```

List of acronyms for **show module userstats xdsl** command output:

- ES (errored Seconds)—Seconds during which an error occured
- SES (severly errored seconds)—Seconds during which a severe error occured
- LOFS (loss of frame seconds)—Loss of frame detected count

Comments? infodev@avaya.com

- LOSS (loss of signal seconds)—Loss of signal count
- UAS (Unavailable seconds)—Unavailable seconds count

Configuring ATM on an ADSL module

Use the following procedure to configure ATM on an ADSL module.

Any ADSL bundle interface that is configured with ATM encapsulation can be configured as an Ethernet Layer 2 switched interface, or as an IP routed interface (supporting static, OSPF, or RIP routing). The commands used to configure the bundles are the same as those used to configure Ethernet ports. For detailed information about these commands, see *Avaya Secure Router 2330/4134 Configuration—Layer 2 Ethernet, NN47263-501* and *Avaya Secure Router 2330/4134 Configuration—IPv4 and Routing, NN47263-502* .

Procedure steps

1. To access the configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To link the bundle to the ADSL module, enter:

   ```
   link {xdsl <slot/port> | xdsl-pvc <bundle:pvc>}
   ```

4. To enable ATM encapsulation, enter:

   ```
   encapsulation atm
   ```

5. To specify ATM configuration, enter:

   ```
   atm
   ```

6. To specify a PVC to configure, enter:

   ```
   pvc <vpi/vci>
   ```

   If you do not enter a **<vpi/vci>** value with the **pvc** command, the Avaya Secure Router 2330/4134 automatically uses the default value (0/35).

7. To specify the ATM encapsulation, enter:

   ```
   atm-encapsulation {aal5Snap | aal5Mux}
   ```

8. To specify the VC class type, enter:

   ```
   class-vc <class-vc>
   ```

9. To specify the PVC protocol, enter:

   ```
   protocol {pppoe | pppoa | ipoe | ipoa | bridge}
   ```

10. To specify a description for the PVC, enter:

    ```
    description "<description>"
    ```

11. To enable the PVC, enter:

    ```
    enable
    ```

12. To display the bundle configuration, enter:

    ```
    show interface bundle <bundle-name>
    ```

Table 155: Variable definitions

Variable	Value
`link {xdsl <slot/port> | xdsl-pvc <bundle:pvc>}`	Links the bundle to the specified module slot/port or bundle/PVC.
`pvc <vpi/vci>`	Specifies the virtual channel identifier (VCI) and virtual path identifier (VPI) in the ATM cell header. The VCI is a 16 bit field that identifies a virtual channel and the VPI is an eight bit field that identifies the virtual path. The default is 0/35.
`atm-encapsulation {aal5Snap | aal5Mux}`	Specifies the ATM encapsulation: • aal5Snap: Multiplexes multiple protocols over the same PVC (LLC multiplexing). • aal5mux: Assigns a single protocol to the PVC (VC multiplexing).
`class-vc <class-vc>`	Specifies the VC class type.
`protocol {pppoe | pppoa | ipoe | ipoa | bridge}`	Specifies the protocol on the PVC: • pppoe: Point to Point Protocol over Ethernet • pppoa: Point to Point Protocol over ATM • ipoe: IP over Ethernet • ipoa: IP over ATM • bridge: Multi-Protocol Over ATM **Important:** Secure Router 2330/4134 release 10.2 does not support RIPv1 with IPoA or IPoE. Only RIPv2 with IPoA or IPoE is supported.
`description "<description>"`	Specifies a description for the PVC, delimited by double quotes (“”).

Comments? infodev@avaya.com

Variable	Value
`enable`	Enables the PVC. Use the no version of this command to disable the PVC.

Configuring the maximum VC circuits

Use the following procedure to configure the required maximum number of ATM VCs.

1. To enter the configuration mode, enter:

   ```
   configure terminal
   ```

2. To create a WAN bundle, enter:

   ```
   interface bundle <bundle-name>
   ```

3. To specify ATM configuration, enter:

   ```
   atm
   ```

4. To specify ATM configuration, enter:

   ```
   max-vcc <1-8>
   ```

Comments? infodev@avaya.com

Chapter 16: WAN interface bundle optional parameter configuration

WAN interface bundle optional parameters are not critical to the function of the interface bundle.

Configuring WAN interface bundle optional parameters

Configure WAN interface bundle optional parameters to specify an interface bundle contact name and description for the interface bundle.

Procedure steps

1. To access the configuration mode, enter:

   ```
   configure terminal
   ```

2. To select a WAN interface bundle, enter:

   ```
   interface bundle <WORD>
   ```

3. To configure WAN interface contact, enter:

   ```
   contact <WORD>
   ```

4. To configure WAN interface description, enter:

   ```
   description <WORD>
   ```

Table 156: Variable definitions

Variable	Value
`interface bundle <WORD>`	<*WORD*>—specifies a character string to identify an interface bundle. The maximum string length is 8 characters.
`contact <WORD>`	<*WORD*>—specifies character string to identify an interface bundle contact name. The maximum string length is 15 characters. You must enter the character string between quotation marks ("").
`description <WORD>`	<*WORD*>—specifies a description for the interface bundle. The maximum length of the description is 76 characters. You must enter the character string between quotation marks ("").

Comments? infodev@avaya.com

Chapter 17: Configuration examples

The following sections provide WAN configuration examples.

FR/MFR configuration

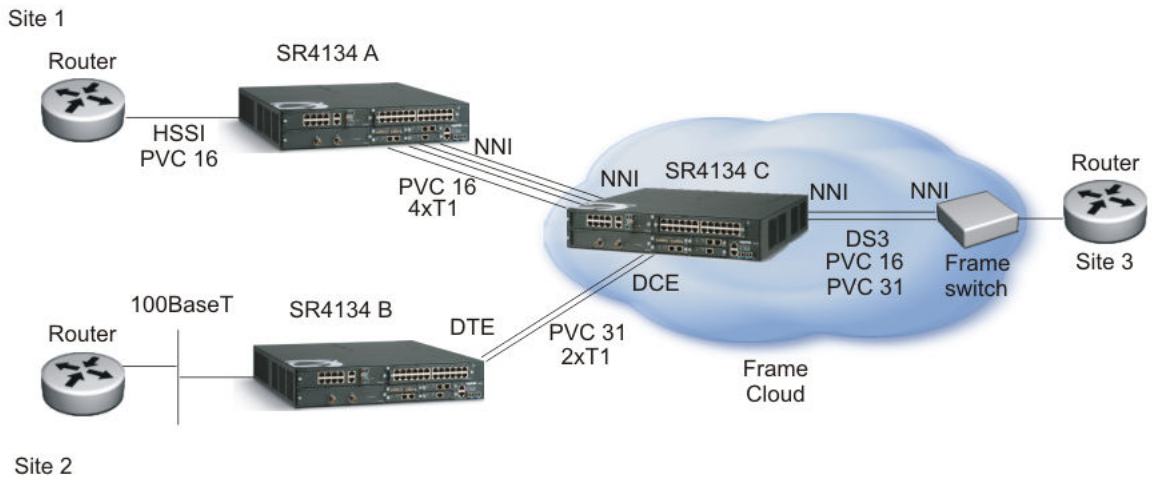


Figure 3: FR/MFR configuration example

The preceding figure outlines an FR/MFR configuration with 3 sites. PVC 16 connects Site 1 to Site 3 while PVC 31 connects Site 2 to Site 3 over multiple T1 links. The frame relay switching equipment is represented in the frame cloud.

Frame relay configuration for SR 4134A and SR 4134C

Configuring the HSSI FR bundle on SR 4134 A

SR 4134A at Site 1 provides frame relay switching between a HSSI interface, connecting to the local router, and a 4 x T1 MFR bundle, connecting to the SR 4134C. Continuity of PVC 16 is maintained through SR 4134A, though this is not required.

The HSSI connection between the local router and the SR 4134 is defined as type UNI. The SR 4134A serves as Frame Relay DCE and the local router as the Frame Relay DTE. Note that the Frame Relay (Layer 2) interface type is independent of, and not necessarily the same as, the HSSI (Layer 1) interface type.

Procedure steps

To configure the HSSI bundle, enter:

```
SR4134/configure#interface bundle toRouter

SR4134/configure/interface/bundle toRouter# link hssi 5/1

SR4134/configure/interface/bundle toRouter#encap fr

SR4134/configure/interface/bundle toRouter#fr

SR4134/configure/interface/bundle toRouter/fr#intf_type dce

SR4134/configure/interface/bundle toRouter/fr#lmi ansi

SR4134/configure/interface/bundle toRouter/fr/lmi#exit

SR4134/configure/interface/bundle toRouter/fr#pvc 16

SR4134/configure/interface/bundle toRouter/fr/pvc 16# shaping
cir 6144000 bcmax 6144000 bcmin 3072000

SR4134/configure/interface/bundle/fr/pvc>pop
```

Configure the DS3 FR bundle on SR 4134C

SR 4134C serves as a Frame Relay switch, connecting PVCs 16 and 31 through to another Frame Switch using a Clear Channel DS3 interface. Note that the Bcmin setting of 3.072 Mbps is maintained across all PVC 16 configurations, to correspond to the Class C setting of the MFR portion of the PVC.

Procedure steps

To configure the DS3 FR bundle on SR 4134C, enter:

```
SR4134/configure# int bundle toFRSwit

SR4134/configure/interface/bundle toFRSwit# link t3 1/1

SR4134/configure/interface/bundle toFRSwit# description "DS3
bundle to FR Switch"

SR4134/configure/interface/bundle toFRSwit# encap fr

SR4134/configure/interface/bundle toFRSwit# fr

SR4134/configure/interface/bundle toFRSwit/fr# intf_type nni
SR4134/configure/interface/bundle toFRSwit/fr# lmi ansi
```


Comments? infodev@avaya.com

```
SR4134/configure/interface/bundle toFRSwit/fr/lmi# exit

SR4134/configure/interface/bundle toFRSwit/fr# pvc 16

SR4134/configure/interface/bundle toFRSwit/fr/pvc# shaping cir
6144000 bcmax 6144000 bcmin 3072000

SR4134/configure/interface/bundle toFRSwit/fr/pvc# switch 16
to4134A

SR4134/configure/interface/bundle toFRSwit/fr/pvc# exit

SR4134/configure/interface/bundle toFRSwit/fr# pvc 31

SR4134/configure/interface/bundle toFRSwit/fr/pvc# shaping cir
3072000 bcmax 3072000 bcmin 1536000

SR4134/configure/interface/bundle/ toFRSwitfr/pvc# switch 31
to4134B
```

MFR configuration between SR 4134A and SR 4134C

The 4 x T1 MFR bundle between the SR 4134A and SR 4134C connects two Frame Relay switches, therefore it represents an NNI interface. The sample configuration defines the 4 x T1 bundle to be of Class C; that is, a minimum of 2 T1 links are required to be up in order to keep the bundle up. Settings for Bcmin on the MFR bundle are set to correspond with the Class C configuration; that is, the minimum anticipated bandwidth will be 2 x T1.

Configuring the 4xT1 MFR links from SR 4134C to SR 4134A

Procedure steps

To configure the 4xT1 MFR links from SR 4134C to SR 4134A, enter:

```
SR4134/configure# int bundle to4134A

SR4134/configure/interface/bundle# link t1 6/1-4

SR4134/configure/interface/bundle# description "6Mbps MFR to
4134A"

SR4134/configure/interface/bundle# encap fr

SR4134/configure/interface/bundle# fr

SR4134/configure/interface/bundle/fr# intf_type nni

SR4134/configure/interface/bundle/fr# mfr class C 2 /* specifies that
the bundle remain up as long as two T1s are up */

SR4134/configure/interface/bundle/fr# lmi ansi

SR4134/configure/interface/bundle/fr/lmi# keepalive 10
```

```
SR4134/configure/interface/bundle/fr/lmi# exit

SR4134/configure/interface/bundle/fr# pvc 16

SR4134/configure/interface/bundle/fr/pvc# shaping cir 6144000
bcmax 6144000 bcmin 3072000

SR4134/configure/interface/bundle/fr/pvc# pop
```

Configuring the 4xT1 MFR links from SR 4134A to SR 4134C

Procedure steps

To configure the 4xT1 MFR links from SR 4134A to SR 4134C, enter:

```
SR4134/configure# int bundle wan1

SR4134/configure/interface/bundle wan1# link t1 7/1-4

SR4134/configure/interface/bundle wan1# encap fr

SR4134/configure/interface/bundle wan1# fr

SR4134/configure/interface/bundle wan1/fr# intf_type nni

SR4134/configure/interface/bundle wan1/fr# mfr class C 2

SR4134/configure/interface/bundle wan1/fr# lmi ansi

SRSR4134/configure/interface/bundle wan1/fr/lmi# keepalive 8

SR4134/configure/interface/bundle/fr/lmi wan1# exit

SR4134/configure/interface/bundle wan1/fr# pvc 16

SR4134/configure/interface/bundle wan1/fr/pvc 16# shaping cir
6144000 bcmax 6144000 bcmin 3072000

SR4134/configure/interface/bundle wan1/fr/pvc 16# switch 16
to4134A
```

MFR configuration between SR 4134B and SR 4134C

SR 4134B at Site 2 serves as the Frame Relay termination point, connecting the Site 2 IP network to SR 4134A. This MFR bundle utilizes 2 T1 links for an approximate 3 Mbps bandwidth. Since it is the Frame Relay terminating point and is defined as a DTE frame relay interface, an IP address is assigned to the WAN bundle.

Comments? infodev@avaya.com

Configure the 2xT1 MFR links from SR 4134B to SR 4134C

Procedure steps

To configure the 2xT1 MFR links from SR 4134B to SR 4134C, enter:

```
SR4134/configure# int bundle frame1

SR4134/configure/interface/bundle# link t1 1/1-2

SR4134/configure/interface/bundle# description "3 Mbps to the
Internet"

SR4134/configure/interface/bundle# encap fr

SR4134/configure/interface/bundle# fr

SR4134/configure/interface/bundle/fr# intf_type dte /* this is default
*/

SR4134/configure/interface/bundle/fr# mfr class A /* this is default */

SR4134/configure/interface/bundle/fr# lmi ansi

SR4134/configure/interface/bundle/fr/lmi# keepalive 10

SR4134/configure/interface/bundle/fr/lmi# exit

SR4134/configure/interface/bundle/fr# pvc 31 /* pvc's default cir set to
3072000 bps*/

SR4134/configure/interface/bundle/fr/pvc# ip addr 10.0.2.1
255.255.255.252

SR4134/configure/interface/bundle/fr/pvc# enable

SR4134/configure/interface/bundle/fr/pvc# exit
```

Configuring the 2xT1 MFR links from SR 4134C to SR 4134B

Procedure steps

To configure the 2xT1 MFR links from SR 4134C to SR 4134B, enter:

```
SR4134/configure# int bundle to4134B

SR4134/configure/interface/bundle# link t1 6/5-6

SR4134/configure/interface/bundle# description "3Mbps MFR to
4134B"

SR4134/configure/interface/bundle# encap fr
```

```
SR4134/configure/interface/bundle# fr
SR4134/configure/interface/bundle/fr# intf_type dce
SR4134/configure/interface/bundle/fr# lmi ansi
SR4134/configure/interface/bundle/fr/lmi# keepalive 10
SR4134/configure/interface/bundle/fr/lmi# exit
SR4134/configure/interface/bundle/fr# pvc 31
SR4134/configure/interface/bundle/fr/pvc# exit 3
```

Configuration of AVCs

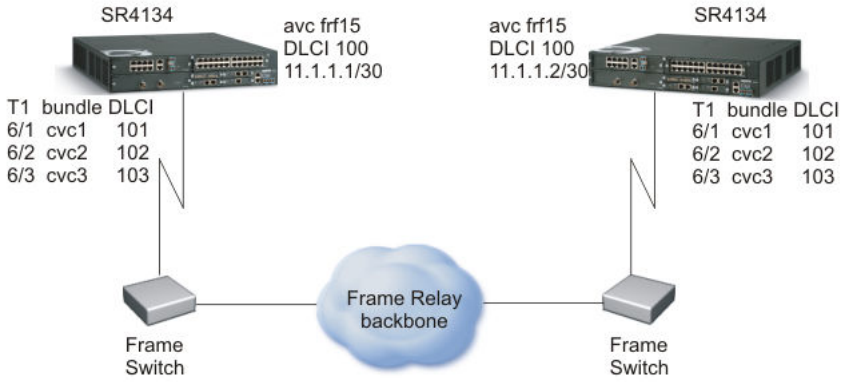


Figure 4: AVC configuration example

The preceding figure depicts an FRF15 deployment scenario. The above AVC, frf15, is assigned a DLCI of 100 on both sides and an IP address in the 11.1.1.0/30 subnet.

Configure CVC1

Procedure steps

To configure CVC1, enter:

```
SR4134/configure# interface bundle cvc1
SR4134/configure/interface/bundle cvc3# link t1 6/1
SR4134/configure/interface/bundle cvc3# encapsulation frelay
```


Comments? infodev@avaya.com

```
SR4134/configure/interface/bundle cvc3# fr
SR4134/configure/interface/bundle cvc3/fr# intf_type dte
SR4134/configure/interface/bundle cvc3/fr# pvc 101
SR4134/configure/interface/bundle cvc3/fr/pvc 101# exit
```

Configure CVC2

Procedure steps

To configure CVC2, enter:

```
SR4134/configure# interface bundle cvc2
SR4134/configure/interface/bundle cvc3# link t1 6/2
SR4134/configure/interface/bundle cvc3# encapsulation frelay
SR4134/configure/interface/bundle cvc3# fr
SR4134/configure/interface/bundle cvc3/fr# intf_type dte
SR4134/configure/interface/bundle cvc3/fr# pvc 102
SR4134/configure/interface/bundle cvc3/fr/pvc 102# exit 3
```

Configure CVC3

Procedure steps

To configure CVC3, enter:

```
SR4134/configure# interface bundle cvc3
SR4134/configure/interface/bundle cvc3# link t1 6/3
SR4134/configure/interface/bundle cvc3# encapsulation frelay
SR4134/configure/interface/bundle cvc3# fr
SR4134/configure/interface/bundle cvc3/fr# intf_type dte
SR4134/configure/interface/bundle cvc3/fr# pvc 103
```

```
SR4134/configure/interface/bundle cvc3/fr/pvc 103#exit 3
```

Configuring AVC

Procedure steps

To configure the AVC, enter:

```
SR4134/configure# interface avc frf15 100

SR4134/configure/interface/avc frf15 100#cvc 101 cvc1

SR4134/configure/interface/avc frf15 100# cvc 102 cvc2

SR4134/configure/interface/avc frf15 100# cvc 103 cvc 3

SR4134/configure/interface/avc frf15 100# ip address 11.1.1.1
255.255.255.252

SR4134/configure/interface/avc frf15 100# exit
```

PPP/MLPPP and HDLC configuration

Avaya Secure Router 2330/4134s can be used at POPs to aggregate data for WAN transmission. The following figure details PPP and multilink PPP connections from two CPE sites to a main site using SR 4134s.

Comments? infodev@avaya.com

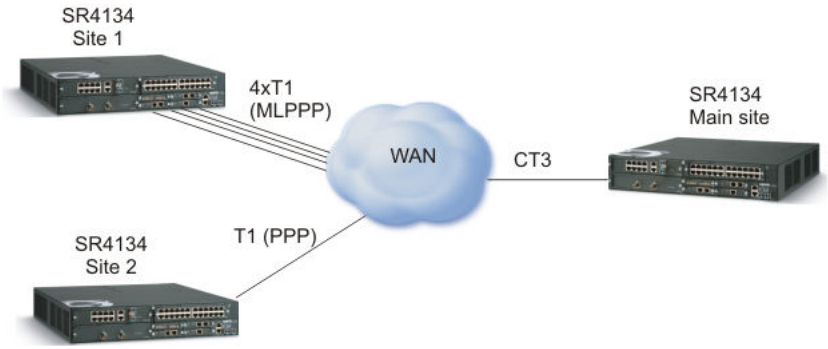


Figure 5: PPP/MLPPP configuration

Site 1 uses an SR 4134 to establish a 6 Mbps MLPPP connection (four T1 lines) to the main site. In this example, MLPPP segmentation is configured lower than the default setting of 512 bytes, and the differential delay tolerance is tighter than the default 128 milliseconds.

The SR 4134 at site 2 connects to the main site over a single T1 link with PPP encapsulation. The Channelized T3 Router PPP parameters (that is, the maximum transmit and receive byte sizes) are adjusted to comply with the Site 1 router configuration.

MLPPP Configuration

Configure the SR 4134 at Site 1

Procedure steps

To configure the SR 4134 at site 1, enter:

```
SR4134# configure term
SR4134/configure# interface bundle ToMain
SR4134/configure/interface/bundle# link t1 6/1-4
SR4134/configure/interface/bundle# encap ppp
```

Note:

MLPPP is not explicitly configured via the encapsulation command. Instead, multilink PPP is automatically invoked when a bundle with PPP encapsulation has two or more T1 links.

```
SR4134/configure/interface/bundle# mlppp seg_threshold 1400
differential_delay 50

SR4134/configure/interface/bundle#ip addr 192.168.1.2 24

SR4134/configure/interface/bundle# exit
```

PPP and MLPPP Configuration

Configure the SR 4134 at the Main Site

Procedure steps

To configure the SR 4134 at the main site with PPP, enter:

```
SR4134/configure# interface bundle ToSite1

SR4134/configure/interface/bundle#link ct3 7/1/5-8

SR4134/configure/interface/bundle# encap ppp

SR4134/configure/interface/bundle# ip addr 192.168.1.1
255.255.255.0

SR4134/configure/interface/bundle# exit

SR4134/configure#interface bundle ToSite2

SR4134/configure/interface/bundle# link t3 7/1/9

SR4134/configure/interface/bundle# encap ppp

SR4134/configure/interface/bundle# ip addr 192.168.2.1
255.255.255.0

SR4134/configure/interface/bundle# exit
```

HDLC Configuration

If desired, HDLC encapsulation can be substituted for PPP between the main site and site 2

Configure the SR 4134 at the Main Site with HDLC

Procedure steps

To configure the SR 4134 at the main site with HDLC, enter:

```
SR4134/configure# interface bundle ToSite2
```

```
SR4134/configure/interface/bundle# link t3 7/1/ 9

SR4134/configure/interface/bundle# encap hdlc

SR4134/configure/interface/bundle# hdlc keepalive 20

SR4134/configure/interface/bundle# ip addr 192.168.2.1
255.255.255.0

SR4134/configure/interface/bundle# exit
```

Note:

In the above command sequence, the HDLC keepalive time interval was changed from its default setting of 10 seconds to 20 seconds

BRI as backup interface using DDR with idle timeout

ISDN can be configured as a regular WAN interface having DDR. The following figure illustrates how a BRI interface can be configured to serve as a backup WAN interface to a leased T1 line

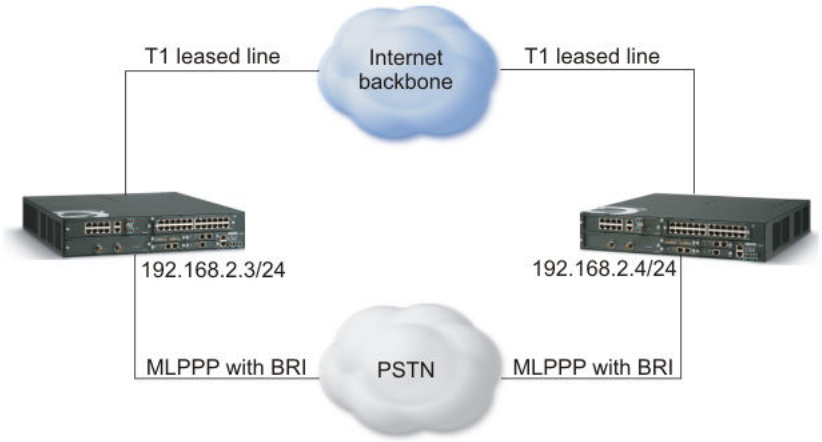


Figure 6: BRI as backup interface using DDR

Assume that there is a PPP bundle already existing between the two devices via a leased T1 line. A customer can configure BRI as a backup interface using DDR with idle timeout using the following steps:

1. Configure a BRI bundle with correct TEI type, switch type, connect-delay, called num, and so on.
2. Configure idle-timeout to Zero to make sure that calls are not dropped when there is no activity on ISDN.
3. Add a static route to the destination with the route as less preferred compared to that of the leased line.

Now when the T1 line goes down for any of the reasons like physical links goes down or negotiation failure, the following occurs:

- Calls are placed on BRI after a connect delay time duration.
- Once the calls are established, MLPPP negotiation starts and when successful, MLPPP links come up.
- Traffic passes through the BRI bundle.

Note: Calls in this case do not come down when the T1 bundle comes up. To disconnect a call, either use the debug command or shut down the BRI bundle.

To configure the sample configuration shown, perform the following steps.

Procedure steps

1. To configure the BRI bundle, enter:

```
interface bundle wan
link bri 2/1:2
encapsulation mlppp
ip address 192.168.2.3 255.255.255.0
ppp authentication-database local
```

2. To configure the ISDN parameters, enter:

```
isdn
switch-type basic-ccitt
idle-timeout 0  --> (Ensures that calls are not dropped
when ISDN is not being used.)
connect-delay 10
callednum 4081234567
tei-mode point-to-point
activate
exit
exit
```

PRI as primary interface with no DDR

ISDN can also exist as an independent interface to provide remote connectivity to Head Quarters and/or for Internet connectivity very similar to the other interfaces like T1/E1. In certain countries, ISDN connections are not very expensive and can therefore be used as the primary connections as well. The following figure shows a PRI T1 configured as the primary interface between two devices.

Comments? infodev@avaya.com

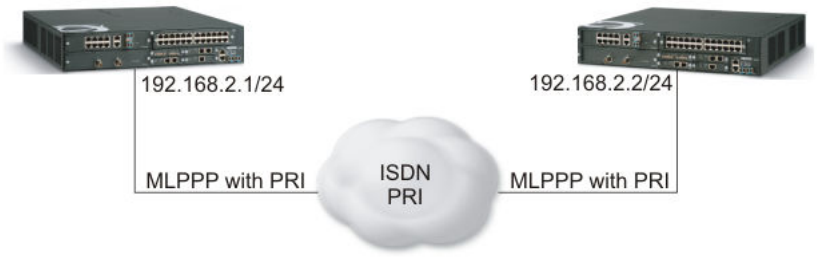


Figure 7: PRI as primary interface with no DDR

Customers can go about configuring ISDN as a primary WAN interface using the following steps

1. Configure the ISDN Bundle with proper connect delay, called num, and so on.
2. Add a static route for the ISDN interface.

With this configuration, the following actions take place on the router:

- When there is a requirement, the router initiates the call to the peer.
- After the call is successful, PPP negotiates with the peer.
- After the PPP negotiation is successful, traffic starts to flow.

Note: By properly provisioning the idle-timeout value, you can allow ISDN to disconnect the calls when there is no activity on ISDN bundle for that duration.

To configure the sample configuration shown, perform the following steps.

Procedure steps

1. To configure the PRI WAN bundle, enter:

```
interface bundle wan
link pri 2/1
encapsulation mlppp
ip address 192.168.2.1 255.255.255.0
ppp authentication-database local
```

2. To configure ISDN properties, enter:

```
isdn
switch-type primary-ccitt
idle-timeout 10
connect-delay 5
callednum 4081234567
activate
exit
exit
```

ADSL module configuration example

The following sections show example configurations for asynchronous transfer mode (ATM) on the Asymmetric Digital Subscriber Line (ADSL) module for each of the following ATM Adaptation Layer 5 (AAL5) encapsulation types:

- Multi-Protocol Over ATM (MPoA)
- IP over ATM (IPoA)
- IP over Ethernet (IPoE)
- Negotiated IPoE on an IPoE bundle
- Point to Point Protocol over ATM (PPPoA)
- Point to Point Protocol over Ethernet (PPPoE)

MPoA

1. To access the configuration mode, enter:

   `configuration terminal`

2. To create or select a VLAN, enter:

   `vlan database vlan <vid> exit`

3. To configure a WAN bundle named **xdsl**, enter:

   `interface bundle xdsl`

4. To add a link to the bundle, enter:

   `link xdsl 3/1`

5. To select the ATM encapsulation mode for the bundle, enter:

   `encapsulation atm`

6. To configure ATM MPoA parameters, enter:

```
atm
pvc 0/35
protocol bridge
switchport
switchport mode access | trunk | hybrid
switchport pvid <1 - 4000>
enable
exit
exit
```


Comments? infodev@avaya.com

7. To view and confirm the **xdsl** bundle configuration, enter:

   show interface bundle xdsl

IPoA

1. To access the configuration mode, enter:

   configuration terminal

2. To configure a WAN bundle named **xdsl**, enter:

   interface bundle xdsl

3. To add a link to the bundle, enter:

   link xdsl 3/1

4. To select the ATM encapsulation mode for the bundle, enter:

   encapsulation atm

5. To configure ATM IPoA parameters, enter:

```
atm
pvc 0/35
protocol ipoa
ip address <ip address> <netmask>
enable
exit
exit
```

6. To view and confirm the **xdsl** bundle configuration, enter:

   show interface bundle xdsl

IPoE

1. To access the configuration mode, enter:

   configuration terminal

2. To configure a WAN bundle named **xdsl**, enter:

   interface bundle xdsl

3. To add a link to the bundle, enter:

   link xdsl 3/1

4. To select the ATM encapsulation mode for the bundle, enter:

```
encapsulation atm
```

5. To configure ATM IPoE parameters, enter:

```
atm
pvc 0/35
protocol ipoe
ip address <ip address> <netmask>
enable
exit
exit
```

6. To view and confirm the **xdsl** bundle configuration, enter:

```
show interface bundle xdsl
```

Negotiated IPoE on an IPoE bundle

1. To access the configuration mode, enter:

```
configuration terminal
```

2. To configure a WAN bundle named **xdsl**, enter:

```
interface bundle xdsl
```

3. To add a link to the bundle, enter:

```
link xdsl 3/1
```

4. To select the ATM encapsulation mode for the bundle, enter:

```
encapsulation atm
```

5. To configure ATM IPoE parameters, enter:

```
atm
pvc 0/35
protocol ipoe
dhcp-client enable
enable
exit
exit
```

6. To view and confirm the **xdsl** bundle configuration, enter:

```
show interface bundle xdsl
```

PPPoA

1. To access the configuration mode, enter:

```
configuration terminal
```

2. To configure a WAN bundle named **xdsl**, enter:

```
interface bundle xdsl
```

3. To add a link to the bundle, enter:

```
link xdsl 3/1
```

4. To select the ATM encapsulation mode for the bundle, enter:

```
encapsulation atm
```

5. To configure ATM PPPoA parameters, enter:

```
atm
pvc 0/35
protocol pppoa
enable
exit
exit
```

6. To configure a WAN bundle named **ppp**, enter:

```
interface bundle ppp
```

7. To add a link to the bundle, enter:

```
link xdsl-pvc xdsl:0/35
```

8. To select the PPP encapsulation mode for the bundle, enter:

```
encapsulation ppp
```

9. To configure PPP parameters, enter:

```
ppp authentication <chap | pap>
ppp <pap | chap> sent-username <username> <password>
ppp pap/chap peer-name
ip address 0.0.0.0 24 (dynamic IP)
exit
exit
```

10. To view and confirm the **xdsl** bundle configuration, enter:

```
show interface bundle xdsl
```

11. To view and confirm the **ppp** bundle configuration, enter:

```
show interface bundle ppp
```

PPPoE

1. To access the configuration mode, enter:

```
configuration terminal
```

2. To configure a WAN bundle named **xdsl**, enter:

```
interface bundle xdsl
```

3. To add a link to the bundle, enter:

   ```
   link xdsl 3/1
   ```

4. To select the ATM encapsulation mode for the bundle, enter:

   ```
   encapsulation atm
   ```

5. To configure ATM PPPoE parameters, enter:

   ```
   atm
   pvc 0/35
   protocol pppoe
   ip address <ip address> <netmask>
   enable
   exit
   ```

6. To configure a firewall named **internet**, enter:

   ```
   firewall internet
   interface xdsl:35
   exit
   ```

7. To configure a virtual access interface named **pppoe**, enter:

   ```
   interface virtual-access pppoe
   ip negotiated
   ppp authentication <pap | chap> sent-username <username> password
   <password>
   pppoe xdsl-atm xdsl:0/35
   protocol pppoe pppoe-mode client
   pppoe ac-name <ac-name>
   exit
   ```

8. To view and confirm the **xdsl** bundle configuration, enter:

   ```
   show interface bundle xdsl
   ```

9. To view and confirm the **internet** firewall configuration, enter:

   ```
   show firewall interface internet
   ```

10. To view and confirm the **pppoe** virtual access interface configuration, enter:

    ```
    show interface virtual-access pppoe
    ```