Troubleshooting
Avaya Secure Router 2330/4134

Release 10.3.5
NN47263-700
Issue 04.03
August 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
- Related resources 13
  - Documentation 13
  - Training 13
  - Avaya Mentor videos 13
  - Support 14

Chapter 2: New in this release 15
- Features 15
- Other changes 15

Chapter 3: Determining the scope of a problem 17

Chapter 4: Global troubleshooting tasks 19
- Using debug commands 19
- Logging into the router 19
- Viewing debug commands through telnet 19
- Changing the password 20
- Password recovery 20
  - Loss of non-admin user password 20
  - Loss of Administrator password 21
- Rebooting the Secure Router 2330/4134 21
- Obtaining Configuration Mode access when occupied by an inactive or unresponsive session 21
  - Clearing an inactive session 21
  - Removing an unresponsive session 22
- Defining default boot parameters 22
- Upgrading the normal and golden bootroms 22
- Determining what modules are installed 24
- Hot swapping a card 27
- Dumping log files to another location 28
- Viewing debug output 28
- Viewing alarms 29
- Packet capture 29
  - Example of Packet Capture configuration 30
  - Packet capture commands 31
- Interpreting LEDs 38
  - Fan tray 39
  - Power supply 40
  - System 40
  - Small modules 40
  - Medium and large modules 40
  - Environment management (Secure Router 2330 only) 41
- Verifying the hardware serial number 41
- Verifying what software version is running 41
- Booting from a network FTP server 41
- Booting from USB 43
- Using the show tech-support command 44

Sending information to another source ... 45
Saving the config file ... 46
BERT ... 46
Configuring BERT testing ... 46
Showing BERT test results and status ... 47
Ending a BERT test ... 48
Resetting to factory defaults ... 48
Resetting to factory defaults from the boot menu ... 49
Importing a saved configuration ... 49
Importing from flash memory ... 49
Importing from a network location ... 50
Viewing the current configuration ... 50
Chapter 5: Troubleshooting an operational problem ... 51
Damaged router ... 51
Normal operation of the Avaya Secure Router 2330/4134 ... 51
Power problem ... 52
Fans ... 53
LEDs are off ... 54
Console problem ... 54
Boot problems ... 54
Making sure the software image is correct ... 55
Ping does not work ... 56
Chapter 6: Troubleshooting a physical media problem ... 57
Troubleshooting cable connections ... 57
Loopback testing ... 57
Loopback testing for T1 interfaces ... 57
Loopback testing for T3 interfaces ... 58
Loopback testing for E1 interfaces ... 58
Loopback testing for interfaces on the CT3 module ... 59
Loopback testing for serial interfaces ... 60
Troubleshooting FXS/FXO ... 60
Troubleshooting T1/E1 ... 61
Troubleshooting DS3 ... 62
Troubleshooting CT3 ... 63
Troubleshooting Serial ... 64
Troubleshooting HSSI ... 64
Troubleshooting ISDN ... 65
ISDN debugging commands ... 66
Chapter 7: Troubleshooting a Data Link Layer problem ... 73
Commonly used troubleshooting commands ... 73
Interface commands ... 73
VLAN commands ... 73
Clear commands ... 74
Debug commands ... 74
Troubleshooting MSTP ... 74
Troubleshooting a configuration failure ... 74
Troubleshooting an operational failure ... 76

Troubleshooting a Frame Relay connection ... 82
Frame Relay debugging commands ... 82
Troubleshooting a PPP connection ... 86
PPP debugging commands ... 86
Troubleshooting MAC configuration and switching ... 89
Troubleshooting a configuration failure ... 89
Troubleshooting an operational failure ... 89
Troubleshooting VLAN Configuration and Switching ... 90
Troubleshooting a configuration failure ... 90
Troubleshooting an operational failure ... 91
Troubleshooting VLAN Classification ... 91
Troubleshooting a configuration failure ... 92
Troubleshooting an operational failure ... 93
Troubleshooting VLAN stacking ... 93
Troubleshooting a configuration failure ... 93
Troubleshooting port mirroring ... 94
Troubleshooting a configuration failure ... 94
Troubleshooting an operational failure ... 95
Troubleshooting Link Aggregation ... 96
Troubleshooting a configuration failure ... 96
Troubleshooting a operational failure ... 97
Troubleshooting GVRP ... 99
Troubleshooting a configuration failure ... 99
Troubleshooting an operational failure ... 100
Troubleshooting IGMP Snooping ... 102
Troubleshooting a configuration failure ... 102
Troubleshooting an operational failure ... 103
Chapter 8: Troubleshooting Ethernet CFM ... 107
Ethernet CFM debug commands ... 107
debug oam cfm dump-data ... 107
debug oam cfm debug-feature debug-level ... 107
debug oam no cfm ... 109
Chapter 9: Troubleshooting an MPLS problem ... 111
General MPLS - Prerequisites for RSVP, LDP, L2VPN, Static LSP ... 111
Troubleshooting Static LSP ... 112
Troubleshooting LDP LSP ... 113
LDP session fail to establish/Label Binding Failure ... 113
More detailed analysis ... 116
Packets not forwarding ... 117
Isolating the cause and corrective action ... 117
Troubleshooting RSVP-TE LSP ... 118
RSVP session fails to establish ... 118
Troubleshooting L2 circuit ... 122
Static L2 circuit ... 123
Dynamic L2 circuit ... 123
Chapter 10: Troubleshooting unicast routing ... 125
The route table ... 126

Troubleshooting OSPF ... 127
OSPF debug options ... 127
OSPF show command options ... 130
OSPF clear command options ... 131
Troubleshooting BGP ... 131
BGP debug options ... 131
BGP show options ... 132
BGP clear options ... 133
Troubleshooting RIP ... 134
RIP debug options ... 134
RIP show options ... 134
RIP clear options ... 135
Debug command options for OSPF ... 136
debug ospf ... 136
debug ospf events ... 136
debug ospf ifsm ... 137
debug ospf lsa ... 137
debug ospf nfsm ... 137
debug ospf nsm ... 138
debug ospf packet ... 138
debug ospf route ... 139
debug ospf all ... 139
Debug command options for OSPFv3 for IPv6 ... 140
debug ipv6 ospf events ... 140
debug ipv6 ospf ifsm ... 140
debug ipv6 ospf lsa ... 141
debug ipv6 ospf nfsm ... 141
debug ipv6 ospf nsm ... 141
debug ipv6 ospf packet ... 142
debug ipv6 ospf route ... 142
debug ipv6 ospf all ... 143
Debug command options for BGP and BGP+ for IPv6 ... 143
debug bgp ... 143
debug bgp all ... 143
debug bgp dampening ... 144
debug bgp events ... 144
debug bgp filters ... 144
debug bgp fsm ... 144
debug bgp keepalives ... 145
debug bgp nsm ... 145
debug bgp updates ... 145
show debug bgp ... 145
Debug command options for RIP ... 146
debug rip ... 146
debug rip all ... 146
debug rip events ... 146
debug rip nsm ... 147

debug rip packet ... 147
Debug command options for RIPng for IPv6 ... 147
debug ipv6 rip ... 147
debug ipv6 rip all ... 148
debug ipv6 rip events ... 148
debug ipv6 rip nsm ... 148
debug ipv6 rip packet ... 148
debug ipv6 rip packet detail ... 149
debug ipv6 rip packet recv ... 149
debug ipv6 rip packet send ... 149
Debug command options for VRRP ... 149
debug ip vrrp ... 149
debug ip vrrp all ... 150
debug ip vrrp error ... 150
debug ip vrrp state ... 150
debug ip vrrp events ... 150
debug ip vrrp packet ... 151
Chapter 11: Troubleshooting IPv4 and IPv6 multicast routing ... 153
Troubleshooting multicast routing ... 153
IPv4 Multicast debugging commands ... 155
Troubleshooting DVMRP ... 157
DVMRP debugging commands ... 157
Troubleshooting PIM-SM ... 163
PIM-SM debugging commands ... 163
Troubleshooting IGMP ... 167
IGMP debugging commands ... 167
Troubleshooting IPv6 Multicast ... 169
IPv6 Multicast debugging commands ... 169
Troubleshooting PIM-SM for IPv6 ... 171
PIM-SM for IPv6 debugging commands ... 171
Troubleshooting MLD ... 175
MLD debugging commands ... 175
Chapter 12: Troubleshooting ADSL ... 179
ADSL show commands ... 179
ADSL SM Card initialization ... 179
ADSL Layer 1 ... 182
ADSL SM Card Software Image ... 183
ASDL bundle configuration ... 184
ADSL Traffic issues ... 186
Chapter 13: Troubleshooting SIP survivability ... 189
SIP survivability show commands ... 189
Debug/trace commands ... 190
Common issues ... 190
SIP survivability commands inaccessible ... 190
SIP survivability feature does not start: enable fails ... 191
SSM stuck in backup mode ... 191
SIP client registrations fail ... 193

Unable to call from SIP client ... 194
Unable to make SIP to gateway calls ... 195
Chapter 14: Troubleshooting security ... 197
Troubleshooting firewall ... 197
Prerequisites to firewall troubleshooting ... 197
Getting started ... 198
Getting details ... 198
Isolating faults ... 199
Common errors ... 199
Firewall troubleshooting commands ... 200
Troubleshooting NAT ... 202
Before getting started ... 202
Getting started ... 203
Getting details ... 203
Isolating faults ... 203
Common errors ... 204
Troubleshooting VPN ... 204
Before getting started ... 204
Getting started ... 205
Getting details ... 206
Isolating faults ... 207
Common errors ... 207
Troubleshooting tunnels ... 208
Tunnel debugging commands ... 208
Troubleshooting Static VPN Peer to Peer ... 213
Troubleshooting Static VPN ABOT ... 215
Troubleshooting Dynamic VPN Peer to Peer over IP-IP tunnels ... 217
Troubleshooting Dynamic VPN ABOT over IP-IP tunnels ... 219
Secure Router to Avaya VPN router interoperability tips ... 221
Troubleshooting OSPF over GRE/IPIP tunnels ... 222
Troubleshooting RIP over GRE/IPIP tunnels ... 223
OSPF debug commands ... 224
Common OSPF problems ... 224
Chapter 15: Troubleshooting Quality of Service ... 227
Chassis QoS troubleshooting ... 227
QoS troubleshooting ... 227
Troubleshooting QoS - Error conditions ... 238
Module QoS troubleshooting ... 262
CoS marking: ... 262
Classification ... 265
Policing ... 267
Congestion avoidance ... 269
Output queuing and scheduling ... 271
Shaping ... 272
Buffer management ... 273
Flow rate monitoring ... 274
Auto QoS ... 276

QoS status management ... 278
Limitations, errors and warnings ... 280
TCAM limitation ... 280
Policer limitation ... 280
Service Policy limitation ... 280
CoS marking of output queue 1 (highest priority queue) ... 280
Troubleshooting Module QoS - Error conditions ... 281
Chapter 16: Troubleshooting a SIP Media Gateway problem ... 303
Debug command overview ... 303
debug cas ... 304
debug ccsip all ... 304
debug ccsip api ... 305
debug ccsip errors ... 305
debug ccsip media ... 305
debug ccsip messages ... 306
debug isdn q921 ... 306
debug isdn q931 ... 307
debug pots ... 307
debug voice cc ... 307
debug voip dial-peer ... 308
Common problems and solutions ... 309
No voice commands available ... 309
New calls fail if more than 8 (or 16, 32, 64) simultaneous G.711 calls are attempted ... 313
Port 0/0 cannot be configured ... 316
Port 2/2 on the SR4134 cannot be configured ... 316
T1 Link: Amber or RED LED and alarms ... 316
Remote T1 link reports clock slip or frame drop errors ... 319
Network clock misconfigured, does not lock, or displays as bad clock ... 320
Configuration of BRI, T1, or PRI port as clock source produces error ... 322
Module LEDs for T1 or BRI are off ... 323
Creation of T1 CAS of addition of PRI link to bundle produces an error on the state of the slot ... 325
Unable to make calls on T1 PRI ... 325
Unable to make calls on T1 CAS ... 330
FXS/FXO port status LEDs ... 332
No dial tone on the analog FXS phones or ports ... 333
Unable to make FXS calls ... 333
FXS phones are not registered (Sylantro and BroadSoft only) ... 338
Unable to make FXO calls ... 341
Secure Router 2330/4134 not reachable from SIP Server ... 346
Unable to make outbound calls to SIP endpoints ... 354
Codec mismatch ... 356
Troubleshooting the Mediation Server Module ... 359
Problem scenario 1 ... 359
Problem scenario 2 ... 360
Problem scenario 3 ... 360
Collecting the OCS Mediation Server logs on the Secure Router 4134 Mediation Server module ... 361
Network packet capture ... 363

Re-imaging the Mediation Server Module ... 365
Cloning the Mediation Server Module image to a USB drive ... 366
Restoring the Mediation Server Module image from the backup on a USB drive ... 367
Chapter 17: Troubleshooting high CPU utilization ... 369
configure process cpu threshold total notify ... 369
CPU utilization debug commands ... 370
debug process start-history ... 371
debug process stop-history ... 371
CPU utilization show commands ... 371
show processes cpu color ... 372
show processes cpu history format ... 372
show processes cpu history process ... 373
show processes cpu show-config ... 373
show processes cpu utilization format ... 373
Chapter 18: Secure Router 2330/4134 system error messages ... 375
Message severity levels ... 375
Configuring the system for syslog reporting ... 376
Enabling and disabling syslog messages ... 376
Specifying the device to which the Secure Router 2330/4134 sends syslog messages ... 376
Configuring multiple Syslog servers ... 377
Specifying the syslog messages to report ... 378
Configuring the Syslog source address ... 381
Configuring the system for console logging ... 381
Syslog error messages that indicate a possible fault in the system ... 382
Chapter 19: Emergency Recovery Procedure ... 393

Chapter 1: Introduction

Purpose

This document contains troubleshooting techniques for the Secure Router 2330/4134 (SR2330/4134).

Related resources

Related topics:

Documentation on page 13
Training on page 13
Avaya Mentor videos on page 13
Support on page 14

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

The following section details what is new in *Avaya Secure Router 2330/4134 Troubleshooting (NN47263-700)* for Release 10.3.5.

Features

Troubleshooting security

See the following sections for information about troubleshooting Release 10.3.5 security features:

- Troubleshooting High CPU Utilization on page 369

Other changes

The following sections identify changes that are not feature related.

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 Troubleshooting ISDN on page 65. This section has been updated based on information that was previously documented in the Secure Router 2330/4134 Release Notes.

Showing installed modules

Added a procedure so you can quickly see what modules are installed in your chassis. For more information, see Determining what modules are installed on page 24.

Comments? infodev@avaya.com

Chapter 3: Determining the scope of a problem

This chapter provides information necessary to narrow the cause of a problem to such areas as router operation, router software, the physical layer, the data link layer, or the network layer. Subsequent chapters provide instructions on how to further isolate and solve problems in each category. The instructions in this chapter will help identify which chapters to go to after determining the scope of a problem.

To ensure you always have current troubleshooting techniques and information, check the Avaya Technical Support web site regularly for updates to *Avaya Secure Router 2330/4134 Troubleshooting* (NN47263-700), including updates for SIP Media Gateway and VoIP troubleshooting:

http://www.avaya.com/support

You can determine the scope of a problem by answering the following questions:

1. What are the symptoms of the problem?

   The more information you have about the symptoms of the problem, the more easily you can identify the cause.

   Note that the symptoms of a problem and the underlying cause of the problem are not necessarily the same. For example, if you cannot ping the router, the symptom is that you cannot ping the router, while the cause may be a loose cable.

2. When did each symptom begin?

   Write down the time you learned about each symptom. Examine the event log for event messages that indicate when the problem occurred. Read the event message descriptions for clues.

3. What recent changes could have contributed to the problem?

   - Reconfiguration?
   - Moved nodes?
   - Added segments?
   - Increased traffic?

4. Are you using a workaround to prevent the symptoms from occurring? If so, what?

   Consideration of the workaround you are using may help you to isolate the problem.

5. Which end stations are involved?

   Identifying the end stations involved can help you to determine the scope of the problem.

6. Research and consider the following additional causes:

   • Traffic congestion

     Examine the MIB statistics and the event log to check for traffic congestion. If you determine that traffic congestion is the problem, consider redistributing traffic to relieve congestion.

   • A software anomaly

     Check Release Notes for any potential issues.

7. Look at the LEDs on the router's front and rear panels, and refer to the event log and MIB statistics to answer the following questions:

   Are the symptoms limited to:

   • A single protocol on a single port?

     If so, the problem is most likely in the network layer or above.

   • Multiple protocols on a single port?

     If so, the problem is most likely in the physical or data link layer.

   • A single protocol on multiple ports in one slot?

     If so, the problem is most likely in the configuration of the network layer protocol.

   • Multiple protocols on multiple ports in one slot?

     If so, and if the same protocols are running successfully in other slots, the problem is most likely physical.

   • A single protocol on multiple ports in all slots running that protocol?

     If so, the problem is most likely in the configuration of the network layer protocol. Make sure you enabled the protocol.

   • Multiple protocols on multiple ports in all slots in the router?

     If so, the problem is most likely operational.

   • Multiple routers?

     If so, the problem is most likely due to an external device. Try to determine the cause of the problem.

Comments? infodev@avaya.com

Chapter 4: Global troubleshooting tasks

Using debug commands

Debug commands are used to troubleshoot various features of the Avaya Secure Router 2330/4134. While this book contains some common debug commands, you should refer to the *Avaya Secure Router 2330/4134 — Command Line Reference* (NN47263-507) for a complete listing and usage instructions.

Logging into the router

This procedure describes the steps necessary to log on to the Secure Router 2330/4134.

Procedure steps

To log on to the Secure Router 2330/4134, enter the username and password:

```
login: admin
password: setup
```

Viewing debug commands through telnet

This procedure describes the steps necessary to enable terminal monitor. Terminal monitor must be enabled to view debug commands when using telnet.

Procedure steps

1. Log on to the Secure Router 2330/4134 using telnet.
2. From the prompt, enter

   ```
   SR# configure terminal
   ```
3. Enter

   ```
   SR/ configure# terminal monitor
   ```

   Debug commands will now be displayed through the telnet connection.

Changing the password

This procedure describes the steps necessary to change a password.

Procedure steps

To change a password, enter the following command and follow the prompts:

```
password
```

Password recovery

This section describes the available options when a password is lost.

There are two different scenarios for lost passwords. The first scenario deals with the loss of the Administrator password, while the second scenario deals with the loss of an regular, non-admin user password.

Loss of non-admin user password

When a password for a non-admin user is lost, the only method of recovery is to remove the affected account and recreate it using the following procedure:

Procedure steps

1. Enter Configuration mode:

   ```
   configure terminal
   ```

2. Remove the user:

   ```
   no user <username>
   ```

3. Recreate the user:

   ```
   user <username> level <2-4>
   ```

4. When prompted, enter the user password, up to 10 characters.
5. Repeat the password.

For more information on adding users and user levels, see *Avaya Secure Router 2330/4134 — Commissioning* (NN47263-302).

To delete/reset all non-admin user accounts on the system, use the command **`system reset-to-factory users`**.

Comments? infodev@avaya.com

Loss of Administrator password

When the password for the Administrator account is lost, the only method of recovery is to reset the system to factory defaults, and use the default username (**admin**) and password (**setup**).

For information on resetting the system to factory defaults, see Resetting to factory defaults from the boot menu on page 49.

Rebooting the Secure Router 2330/4134

This procedure describes the steps necessary to reboot the router.

Procedure steps

Enter the command to reboot the router.

```
reboot
```

Important:
This command is issued from the CLI root.

Obtaining Configuration Mode access when occupied by an inactive or unresponsive session

This section describes steps used if an administrator level user needs to gain access to Configuration Mode in the Secure Router 2330/4134, but is unable to due to an inactive or unresponsive session.

An inactive session would be classified as a session where a user has failed to issue the **exit** command to properly end their console session. Failing to do so leaves Configuration Mode occupied for a short period of time.

An unresponsive session would be classified as a session where the router has entered a "hung" state and the user is unable to issue any further commands.

Clearing an inactive session

This procedure describes the steps to clear an inactive session.

Procedure steps

To clear an inactive session, issue the following command:

```
clear telnet_session <1-16>
```

To view active telnet sessions, use the command **show users**. Using this command will display which session (or user) owns Configuration Mode (conf term).

Removing an unresponsive session

This procedure describes the steps to remove an unresponsive session.

Procedure steps

To remove an unresponsive session, due to a "hung" router, issue the following command:

```
debug clear_clisession <1-16>
```

To view active telnet sessions, use the command **show users**. Using this command will display which session (or user) owns Configuration Mode (conf term).

Defining default boot parameters

This procedure describes the steps necessary to define default boot parameters.

Procedure steps

1. Enter Configuration Mode.

   ```
   configure terminal
   ```

2. Define boot parameters.

   ```
   boot_params
   ```

To see an example of defining boot parameters, see Booting from a network FTP server on page 41 or Booting from USB on page 43

Upgrading the normal and golden bootroms

Use the procedures in this section to upgrade the normal and golden bootroms on the Secure Router 2330/4134.

If you have a Secure Router 2330/4134 with an older version of the software image (filename: tor.Z), you must upgrade your bootrom to accommodate the new software image (filename: SR4134.Z or SR2330.Z).

It is important to upgrade both the normal and golden bootroms to prevent a bootrom mismatch.

Procedure steps

1. Copy the new software image file (SR4134.Z or SR2330.Z) to cf0 using an FTP server, USB drive, or Compact Flash card (refer to procedures in this section).
2. To access the bootrom command menu, press any key at the beginning of the boot sequence. The Secure Router 2330/4134 stops the auto-boot sequence and re-directs you to the bootrom prompt. The following figure shows you the prompt at which you can enter the bootrom command menu by pressing any key.

```
                  VxWorks System Boot

Copyright (c) 2009 Avaya

PROCESSOR     : Freescale MPC8541
SYSTEM MEMORY : 1G
VxWorks       : VxWorks5.5.1
BSP version   : 1.2/0
Boot version  : 0.0.0.51 (NORMAL Boot)
Creation date : Jun 24 2010, 13:27:12
NORMAL Bt ver : 0.0.0.51
GOLDEN Bt ver : 0.0.0.51
Baseline ver  : 0.0.0.51 (Internal version for checking)
System name   : SR 4134



Press any key to stop auto-boot...
Compact Flash Device: CF0, Filename: /cf0/SR4134.Z


[SYSTEM] User stops run-time image

[BOOT]:
```

3. At the prompt, enter **c** to change the boot parameters: `[BOOT]: c`
4. When prompted, enter the name of the device from which you prefer the router boots: `Boot dev [ftp,cf0,cf1,usb0]: cf0`
5. Enter the boot file name: `Boot file name: SR4134.Z` OR `SR2330.Z`
6. Enter the name of the server you use (the router provides this information if you have previously configured it): `Server name: sunserver`
7. Enter the server IP address (the router provides this information if you have previously configured it): `Server IP address: 10.10.11.12`
8. Enter the router IP address (the router provides this information if you have previously configured it): `My IP address: 10.10.13.14`
9. Enter the subnet mask (the router provides this information if you have previously configured it): `My subnet mask: 255.255.255.0`
10. Enter the gateway IP address (the router provides this information if you have previously configured it): `Gateway IP address: 10.10.15.16`
11. Enter your user name and password: `User name: kevx Password: kevx`

12. Enter 0 to disable or 1 to enable the checksum feature: `Checksum enable [0:Disable,1:Enable]: 1`
13. Enter 0 to disable or 1 to enable the display of the image header contents: `Show header enable [0:Disable,1:Enable]: 1`
14. Enter the number that corresponds to the type of bootrom image that you are updating (you must update the normal bootrom at this time): `Save bootrom image [0:AutoUpdate,1:NormalBTupd, 2:GoldenBTupd,3:NoUpd]: 1`
15. To update the normal bootrom, enter **D** at the prompt: `[BOOT]: D` Allow the boot sequence to complete.
16. When the boot sequence is complete, the Secure Router 2330/4134 returns a message indicating that the system will be rebooted again after updating the bootrom: `[SYSTEM] Bootrom image loading done [SYSTEM] Package validation pass System will be rebooted again after updating.`
17. When the Secure Router 2330/4134 begins the boot sequence again, interrupt the sequence by pressing any key (see Step 2).
18. Follow Steps 3 to 13.
19. Enter the number that corresponds to the type of bootrom image that you are updating (you must update the golden bootrom at this time): `Save bootrom image [0:AutoUpdate,1:NormalBTupd, 2:GoldenBTupd,3:NoUpd]: 2`
20. To update the golden bootrom, enter **D** at the prompt: `[BOOT]: D` Allow the boot sequence to complete.
21. When the boot sequence is complete, the Secure Router 2330/4134 returns a message verifying the boot image is updated: `[SYSTEM] Boot image is updated. System will be rebooted for running a new boot image.` The Secure Router 2330/4134 reboots. Allow the boot sequence to complete.

Note:

This procedure can also be performed in the CLI using the **boot_params** command while in Configuration Mode.

Determining what modules are installed

To find out what modules are installed in your chassis, use the following steps:

Procedure steps

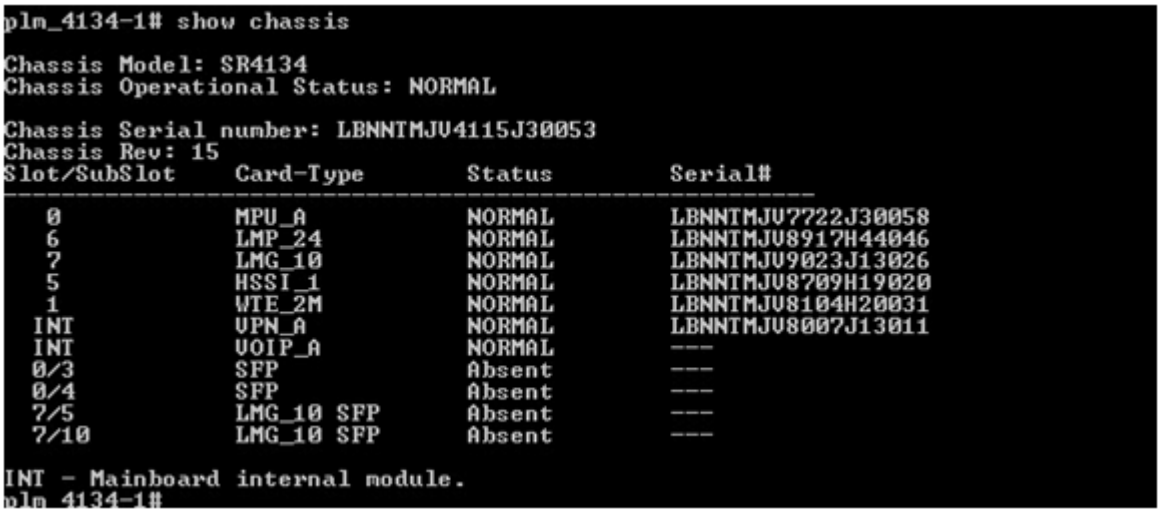
1. Enter either one of the following commands to display all the slots and card types in the chassis:

   ```
   show chassis
   ```


Comments? infodev@avaya.com

```
show tech-support
```

2. The following figure shows output from **`show chassis`**, which lists the slot that the module is in, its name, status, and serial number. Make a note of the names in the `Card-Type` column. They refer to the installed modules.



3. Match the Card Types that you noted above with the following table to see a description and order number for each module.

Card Type	Module Size	Description	Order Number
ADSL_ANX_A	Small	1-port ADSL2+ Annex A	SR0004060E6
ADSL_ANX_B	Small	1-port ADSL2+ Annex B	SR0004061E6
BRI_2ST	Small	2-port ST-interface ISDN BRI for both TDM and Packet .	SR0000009E5
FXO_2M	Small	Secure Router Voice Interface card - 2 port FXO	SR0000042E5
FXO_4M	Small	Secure Router Voice Interface card - 4 port FXO	SR0000044E5
FXS_2M	Small	Secure Router Voice Interface card - 2 port FXS	SR0000046E5
FXS_4M	Small	Secure Router Voice Interface card - 4 port FXS	SR0000048E5
HSSI_1	Medium	1-port High Speed Serial	SR0000014E5
LMF_24	Medium	24-port 10/100 Fast Ethernet Layer2/3 switch	SR0000015E5

Card Type	Module Size	Description	Order Number
LMG_10	Medium	10-port non-blocking 10/100/1000 Gigabit Ethernet Layer2/3 switch (10 RJ-45 and 2 SFP ports)	SR0000017E5
LMG_44	Large	44-port 10/100/1000 Gigabit Ethernet Layer 2/3 switch with over-subscription of 1:4 (44-port UTP, 2-port SFP sharing the 2 UTPS)	SR0000018E5
LMP_24	Medium	24-port 10/100 fast Ethernet Layer2/3 PoE switch	SR0000016E5
PVIM_A	Internal	Packetized Voice Module (PVIM) for SR2330	SR0004056E6
SCIM_A	Internal	Secure Router 2330 IPsec VPN Encryption Module (100 tunnels)	SR0004055E6
SERV_MOD	Medium	Unified Communication Mediation Services for OCS	SR0000051E6
SERV_MOD	Medium	Unified Communications Mediation Services module for MSFT OCS-R2, 64 bit.	SR0004062E6
SERV_MOD	Medium	Secure Router 4134 Server Module with SCS no user license included (250 user maximum)	SR4304004E6
SERV_MOD	Medium	Secure Router 4134 Server Module with SCS 50 user license included (250 user maximum)	SR4309001E6
SERV_MOD	Medium	Secure Router 4134 Module for server-hosted applications	SR0009001E6
VCM_A	Medium	Secure Router 4134 Medium Carrier module supports up to 4 FXO or FXS Small Modules *	SR0004002E5
VOIP_A	Internal	Packetized Voice Module (PVM) for Secure Router 4134. Includes 8 Digital Signal Processor (DSP) channels and 25 SIP Survivability Module (SSM) users activated.	SR3704001E6
VPN_A	Internal	SR4134 High Performance IPsec VPN Encryption Module (1000 IPsec tunnels)	SR0000024E5
WDS3_1C	Medium	1-port Clear Channel DS3 **	SR2104018E5
WT3/DS3_1C	Medium	1-port Channelized T3 **	SR0000013E5

Comments? infodev@avaya.com

Card Type	Module Size	Description	Order Number
WTE_1	Small	1-port T1/E1 (DS0 and DS1 support) for both TDM and Packet (Supports ISDN-PRI.)	SR000000 5E5
WTE_1S	Small	1-port Sync and Async Serial. (Routing license required to use on AG2330.)	SR000000 7E5
WTE_2M	Small	2-port T1/E1 (DS0 and DS1 support) for both TDM and Packet (Supports ISDN-PRI.)	SR000000 6E5
WTE_2S	Small	2-port Sync and Async Serial. (Routing license required to use on AG2330.)	SR000000 8E5
WTE_8	Medium	8-port T1/E1	SR000001 1E5

***** The modules installed in this module are identified by slot/subslot numbers. For example, if the **VCM_A** is in slot 7, then the modules plugged into it are slot/subslot: 7/1, 7/2, 7/3, and 7/4.

****** The functionality of the **Clear Channel DS3** and the **Channelized T3** modules are now combined into a single **Clear Channel DS3** module. The **Channelized T3** module is discontinued.

Hot swapping a card

To hot swap a card, use the following steps:

Procedure steps

1. Use the “show chassis” command to display all the slots and card types in the chassis.

   ```
   show chassis
   ```

2. Execute the following steps to Hot Swap a card in slot #5:

   ```
   /configure# chassis module 5
   ```

   ```
   /configure/chassis/module (5)# shutdown
   ```

   ```
   /configure/chassis/module (5)# no shutdown
   ```

Dumping log files to another location

This procedure describes the steps necessary to copy log files to another local device or send to a network FTP or TFTP server. The options available are:

- Copying locally to another device
- Sending to a network FTP or TFTP server

Procedure steps

1. Enter the command to copy to a local device:

   ```
   file copy </source/filename> </destination/filename>
   ```

2. Enter the command to upload to a network location:

   ```
   file upload </source/filename> <destaddr> <filename>
   [interface <ifname>] [id <username>] [passwd <password>]
   ```

Table 1: Variable definition

Variable	Value
<destaddr>	The network destination address.
<destination>	The destination device.
<filename>	The filename used.
<ifname>	The interface name.
<passwd>	The password used to authenticate on the FTP/TFTP server.
<source>	The source device.
<username>	The username used to authenticate on the FTP/TFTP server.

Viewing debug output

The Secure Router 2330/4134 CLI contains a variety of debug commands to assist in troubleshooting the router on a feature by feature basis. Please refer to the appropriate troubleshooting sections in this document for further details.

The **debug** series of commands are available at the top level of the CLI. If you cannot find the debug commands, first verify that you are not in Configuration Mode. Refer to *Avaya Secure Router 2330/4134 — Using the Command Line Interface* (NN47263-506) for more details.

Comments? infodev@avaya.com

Viewing alarms

The Secure Router 2330/4134 reports alarms when it detects irregular conditions in incoming signals to the interface modules. Use the **show module alarms** command to quickly check for any irregularities.

Procedure steps

1. To view the current alarms for any T1 WAN link on the Secure Router 2330/4134, enter:

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

2. To view the current alarms for any E1 port on the Secure Router 2330/4134, enter:

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

3. To view the current alarms for any CT3 port on the Secure Router 4134, enter:

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

4. To view the current alarms for any serial port on the Secure Router 2330/4134, enter:

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

5. To view the current alarms for any HSSI port on the Secure Router 4134, enter:

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

6. To view the current alarms for any T3 port on the Secure Router 4134, enter:

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

Packet capture

This section describes the usage of Packet Capture (PCap) as a troubleshooting tool.

Packet capture is a troubleshooting tool used to capture packets sent and/or received on supported interfaces in the Secure Router 2330/4134. Packet capture aids in debugging and troubleshooting network traffic issues.

Caution:

Packet capture is primarily a debug tool and should be used with care. Users should be aware that this debugging feature can generate a substantial amount of output and can use a substantial amount of system resources. This feature should be used with caution in any production network in order to avoid adversely affecting other activities on the network.

Packets captured contain all protocol headers including the L2 header. This feature can be enabled on any network layer interface while traffic is flowing through the system. Packet

capture can be performed on inbound traffic, outbound traffic, or both directions simultaneously. The default behavior is to capture both directions.

Prior to release 10.2, filters on packet capture worked only on IP packets. With the implementation of the PCAP over VLAN feature, ACL rules can be applied on both IP and non-IP interfaces. Also, MAC rules can be specified; packets are captured based on destination/source MAC addresses. Prior to release 10.2 PCAP was supported only on CPU ports. The PCAP over VLAN feature now supports Packet capture on Marvell/Broadcom LAN ports.

The number of packets to be captured can be specified, up to 10000, with the default behavior being to capture all packets (value of 0). The maximum capture length for a packet can also be specified, with a default value of 0 which captures the entire packet. The maximum (and default) memory that can be used by a packet capture session is 5 MB, but can be configured to a lower value. Captured packets can be saved both locally and as a remote file using FTP/TFTP.

Note:

Packet capture is not supported on loopback interfaces.

Example of Packet Capture configuration

Configure the interface

```
configure terminal
vlan database
vlan 100
vlan 200
exit
```

Configure Ethernet 1

```
interface ethernet 6/1
switchport mode trunk
switchport trunk allowed vlan all
exit
```

Configure PPP 1

```
interface bundle wan1
link t1 1/1
encap ppp
switchport mode trunk
switchport trunk allowed vlan all
exit
```

Configure packet capture

```
access-list acc1
add permit mac any any vlan 100
add permit mac any any vlan 200
add permit ip any 30.30.30.2
add permit ip any 50.50.50.2
exit

capture cap1
attach ethernet 6/1
```


Comments? infodev@avaya.com

```
filter acc1 in
commit
exit

capture cap2
filter acc1 out
attach bundle wan1
commit
exit
enable
```

Packet capture commands

debug pcap

Use this command to configure next level packet capture commands.

Syntax

```
[no] debug pcap
```

Example

```
SR# debug pcap
```

debug pcap capture

Use this command to access packet capture related commands.

Syntax

```
[no] debug pcap capture <capname>
```

Table 2: Variable definition

Variable	Value
<capname>	The name for the capture session.

Example

```
SR# debug pcap capture cap1
```

debug pcap capture direction

Use this command to configure packet capture direction.

Syntax

```
direction <in|out|both>
```

Table 3: Variable definition

Variable	Value
<both>	Both directions.
<in>	Incoming packets.
<out>	Outgoing packets.

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# direction in
```

debug pcap capture snaplen

Use this command to configure the number of bytes to be captured.

Syntax

```
snaplen <0-65535>
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# snaplen 1000
```

debug pcap capture count

Use this command to configure the number of packets to be captured.

Syntax

```
count <0 - 10000>
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# count 5000
```

debug pcap capture filter

Use this command to configure the ACL applied.

Syntax

```
filter <aclname>
```


Comments? infodev@avaya.com

Table 4: Variable definition

Variable	Value
<aclname>	The ACL name.

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# filter testacl
```

debug pcap capture wrap

Use this command to enable buffer wrap.

Syntax

```
wrap
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# wrap
```

debug pcap capture size

Use this command to configure the buffer size.

Syntax

```
size <64-5120>
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# size 2000
```

debug pcap capture drop-nonip

Use this command to disable the capturing of non-ip packets.

Syntax

```
drop-nonip
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# drop-nonip
```

debug pcap capture attach

Use this command to configure a packet capture session for the interface.

Syntax

```
attach [bundle <bundle>] [ethernet <ethernet>]
```

Table 5: Variable definition

Variable	Value
<bundle>	The bundle name.
<ethernet>	The ethernet interface name.

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# attach bundle bun1
```

debug pcap capture commit

Use this command to commit packet capture configurations.

Syntax

```
commit
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# commit
```

debug pcap capture show-config

Use this command to show packet capture configuration.

Syntax

```
show-config
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# show-config
```

debug pcap capture stats

Use this command to display packet capture statistics.

Syntax

```
stats
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# stats
```

debug pcap capture dump

Use this command to display a packet capture dump.

Syntax

```
dump
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# dump
```

debug pcap capture clear-stats

Use this command to clear packet capture statistics.

Syntax

```
clear-stats
```

Example

```
SR# debug pcap capture cap1
SR/debug/pcap/capture cap1# clear-stats
```

debug pcap access-list

Use this command to create or modify an IP access list.

Syntax

```
[no] debug pcap access-list <listname>
```

Table 6: Variable definition

Variable	Value
<listname>	The access list name.

Example

```
SR# debug pcap access-list acl1
```

debug pcap max-sessions

Use this command to configure the number of simultaneous packet capture sessions allowed.

Syntax

```
[no] debug pcap max-sessions <1-10>
```

Example

```
SR# debug pcap max-sessions 6
```

debug pcap enable

Use this command to enable or disable all configured packet capture sessions.

Syntax

```
[no] debug pcap enable
```

Example

```
SR# debug pcap enable
```

debug pcap cleanup

Use this command to delete all packet capture sessions, related statistics and data structures.

Syntax

```
debug pcap cleanup
```

Example

```
SR# debug pcap cleanup
```

debug pcap upload

Use this command to upload captured packets to a remote host.

Syntax

```
[no] debug pcap upload <X.X.X.X> <name> <username> <password>
```

Table 7: Variable definition

Variable	Value
<name>	The filename to store as.
<password>	The password to access the server.
<username>	The username to access the server.

Example

```
SR# debug pcap upload 10.10.10.1 testcap testuser testpass
```

debug pcap save

Use this command to save the packets captured.

Syntax

```
[no] debug pcap save [local <filename>] [network <address> <path>]
```

Table 8: Variable definition

Variable	Value
<address>	The network address.
<filename>	The filename to save as.
<path>	The path and filename for network storage.

Example

```
SR# debug pcap save local pcapinfo.log
```

debug pcap show-config

Use this command to display packet capture configurations.

Syntax

```
[no] debug pcap show-config
```

Example

```
SR# debug pcap show-config
```

debug pcap stats

Use this command to display packet capture stats.

Syntax

```
[no] debug pcap stats
```

Example

```
SR# debug pcap stats
```

debug pcap dump

Use this command to display a packet capture dump.

Syntax

```
[no] debug pcap dump
```

Example

```
SR# debug pcap dump
```

debug pcap clear-stats

Use this command to clear packet capture statistics.

Syntax

```
[no] debug pcap clear-stats
```

Example

```
SR# debug pcap clear-stats
```

Interpreting LEDs

This section describes how to interpret the various LED indicators on the rear panel of the Secure Router 2330/4134. The following figure shows the location of the system LEDs.

Comments? infodev@avaya.com

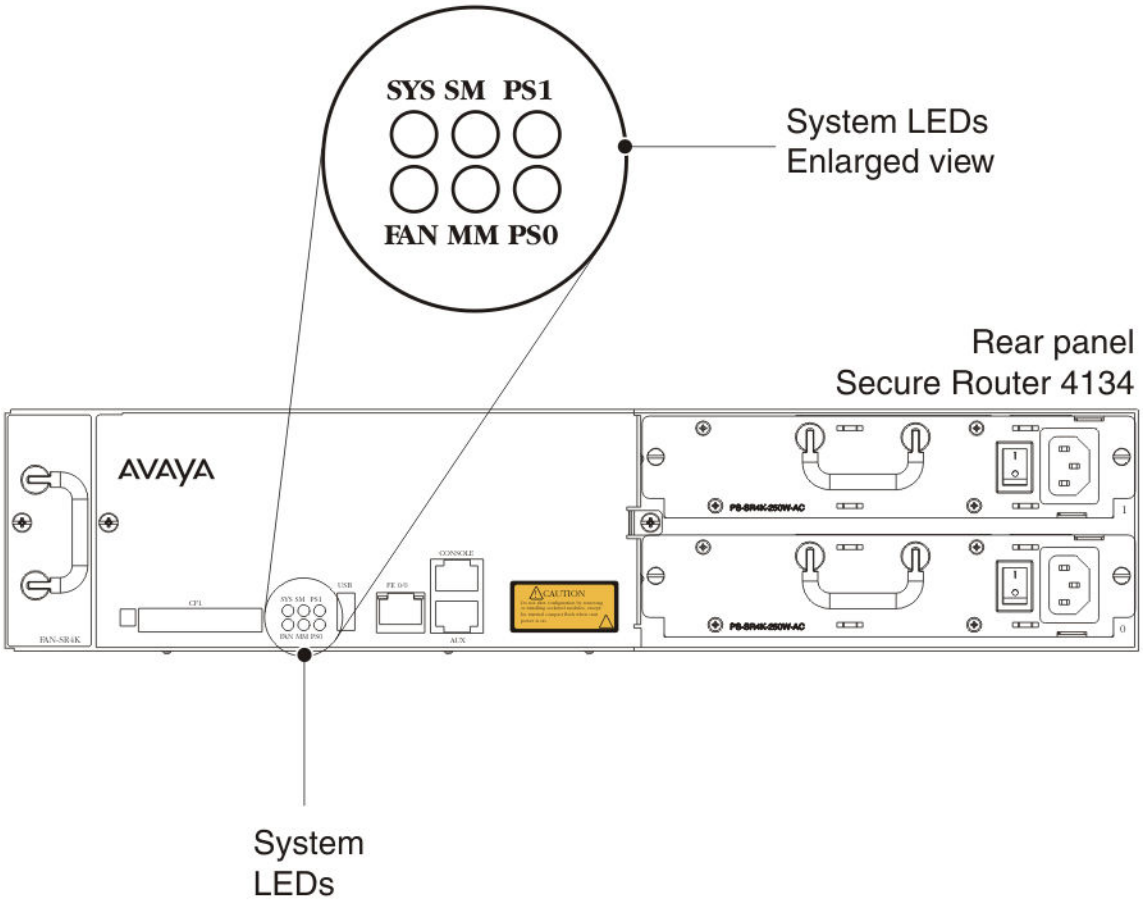


Figure 1: Secure Router 4134 rear panel LEDs

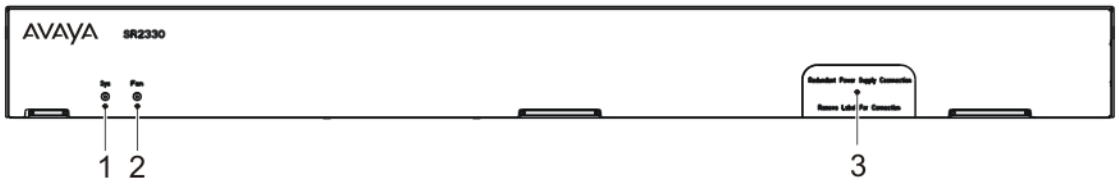


Figure 2: Secure Router 2330 rear panel LEDs

Fan tray

This section describes the LED behavior for the fan tray (FAN LED).

- Green - The fan tray is installed and all fans are functioning normally.
- Red - The fan tray is not present, or one or more fans have failed.
- Off - The router is not powered (Secure Router 4134 only).

Power supply

This section describes the LED behavior for the power supply (PS0 and PS1 LEDs).

- Green - A power supply is present and functioning normally.
- Red - A power supply is present, but has failed.
- Off - No power supply is present in the slot or the router is not powered (Secure Router 4134 only).

System

This section describes how to interpret system LED behavior (SYS LED).

- Green - The system is functioning normally.
- Red - The system is not functioning normally.
- Off - The router is not powered (Secure Router 4134 only).

Small modules

This section describes how to interpret small modules LED behavior (SM LED).

- Green - Small modules are installed and functioning normally.
- Red - Small modules are installed, but one or more are malfunctioning. For more information, see the status LEDs on the small modules.
- Off - If the Secure Router 4134/2330 is powered, and the LED is off, no small modules are installed.

Look at the LEDs on the router's front and rear panels and then use the event log, MIB statistics, and the following table to isolate a problem.

Medium and large modules

This section describes how to interpret medium and large modules LED behavior (MM LED).

- Green - Medium or large modules are installed and functioning normally.
- Red - Medium or large modules are installed, but one or more are malfunctioning. For more information, see the status LEDs on the modules.
- Off - If the router is powered, and the LED is off, no medium or large modules are installed (Secure Router 4134 only).

Comments? infodev@avaya.com

Environment management (Secure Router 2330 only)

This section describes how to interpret the sensors. Sensor states are shown by the SYS and FAN LEDs located on the rear panel of the chassis.

- Temperature Sensors - There is one temperature sensor on the board and the temperature is sampled every two minutes.
- Fan - The status of the fan is checked every two minutes.

Verifying the hardware serial number

This procedure describes the steps necessary to verify the hardware serial number.

Procedure steps

To show the hardware serial, run the following command:

```
show system configuration
```

Verifying what software version is running

This procedure describes the steps necessary to show what software version the system is running.

Procedure steps

To show the software version, run the following command:

```
show version
```

Booting from a network FTP server

You can configure the Secure Router 2330/4134 to boot from a network FTP server.

Procedure steps

1. Enter Configuration Mode:

   ```
   configure terminal
   ```

2. Enter the command to configure boot parameters:

```
boot_params
```

The router will return the following message:

```
WARNING: Configuration changes not yet saved!
```

3. When prompted, enter the name of the device from which you prefer the router boots:

   ```
   Boot dev [ftp,cf0,cf1,usb0]: ftp
   ```

4. Enter the boot file name (the router provides this information if you have previously configured it):

   ```
   Boot file name: SR4134.Z
   ```

   OR

   ```
   Boot file name: SR2330.Z
   ```

5. Enter the name of the server you use (the router provides this information if you have previously configured it):

   ```
   Server name: sunserver
   ```

6. Enter the server IP address (the router provides this information if you have previously configured it):

   ```
   Server IP address: 10.10.11.12
   ```

7. Enter the router IP address (the router provides this information if you have previously configured it):

   ```
   My IP address: 10.10.13.14
   ```

8. Enter the subnet mask (the router provides this information if you have previously configured it):

   ```
   My subnet mask: 255.255.255.0
   ```

9. Enter the gateway IP address (the router provides this information if you have previously configured it):

   ```
   Gateway IP address: 10.10.15.16
   ```

10. Enter your user name and password:

    ```
    User name: kevx Password: kevx
    ```

11. Enter 0 to disable or 1 to enable the checksum feature:

    ```
    Checksum enable [0:Disable,1:Enable]: 1
    ```

12. Enter 0 to disable or 1 to enable the display of the image header contents:

    ```
    Show header enable [0:Disable,1:Enable]: 1
    ```

13. Enter the number (0, 1, or 2) that corresponds to the type of bootrom image update that you prefer, or enter 3 if you prefer to not update the bootrom image:

Comments? infodev@avaya.com

```
Save bootrom image [0:AutoUpdate,1:NormalBTupd,
2:GoldenBTupd,3:NoUpd]: 0
```

If you select 0, 1, or 2, the router returns the following:

```
BOOT PARAMETERS HAVE BEEN SAVED.
```

14. Reboot the Secure Router 2330/4134 to activate changes, or continue with your configuration:

```
DO YOU WANT TO REBOOT: (Y/N) ? y
```

Booting from USB

You can configure the Secure Router 4134 to boot from a USB device.

Procedure steps

1. Enter Configuration Mode:

```
configure terminal
```

2. Enter the command to configure boot parameters:

```
boot_params
```

The router will return the following message:

```
WARNING: Configuration changes not yet saved!
```

3. When prompted, enter the name of the device from which you prefer the router boots:

```
Boot dev [ftp,cf0,cf1,usb0]: usb0
```

4. Enter the boot file name (the router provides this information if you have previously configured it):

```
Boot file name: SR4134.Z
```

5. Enter the name of the server you use (the router provides this information if you have previously configured it):

```
Server name: sunserver
```

6. Enter the server IP address (the router provides this information if you have previously configured it):

```
Server IP address: 10.10.11.12
```

7. Enter the router IP address (the router provides this information if you have previously configured it):

```
My IP address: 10.10.13.14
```

8. Enter the subnet mask (the router provides this information if you have previously configured it):

   ```
   My subnet mask: 255.255.255.0
   ```

9. Enter the gateway IP address (the router provides this information if you have previously configured it):

   ```
   Gateway IP address: 10.10.15.16
   ```

10. Enter your user name and password:

    ```
    User name: kevx Password: kevx
    ```

11. Enter 0 to disable or 1 to enable the checksum feature:

    ```
    Checksum enable [0:Disable,1:Enable]: 1
    ```

12. Enter 0 to disable or 1 to enable the display of the image header contents:

    ```
    Show header enable [0:Disable,1:Enable]: 1
    ```

13. Enter the number (0, 1, or 2) that corresponds to the type of bootrom image update that you prefer, or enter 3 if you prefer to not update the bootrom image:

    ```
    Save bootrom image [0:AutoUpdate,1:NormalBTupd,
    2:GoldenBTupd,3:NoUpd]: 0
    ```

    If you select 0, 1, or 2, the router returns the following:

    ```
    BOOT PARAMETERS HAVE BEEN SAVED.
    ```

14. Reboot the Secure Router 4134 to activate changes, or continue with your configuration:

    ```
    DO YOU WANT TO REBOOT: (Y/N) ? y
    ```

Using the show tech-support command

Use the show tech-support command to gather information about different layers on the Secure Router 2330/4134. This information may be used by a technical support professional to diagnose the source of a problem. You can show and save information per layer or as all layers.

The following procedure describes the steps required to use this command.

Enter the command to gather diagnostic information:

```
show tech-support <layer>
```

Table 9: Variable definition

Variable	Value
<layer>	Specify which layer you want to gather information for. Possible values are:

Comments? infodev@avaya.com

Variable	Value
	• layer1 - Gather Layer 1 information • layer2 - Gather Layer 2 information • layer3 - Gather Layer 3 information • all - Gather information for all layers

Sending information to another source

After gathering layer diagnostic information using the **`show tech-support`** command, you can copy or send the output file (showtech.txt) to another location for use in diagnosis. The options available are:

- Copying locally to another device
- Sending to a network FTP or TFTP server

This procedure shows how to copy the file to another local device or send to a network FTP or TFTP server.

Procedure steps

1. Enter the command to copy to a local device:

   ```
   file copy </source/filename> </destination/filename>
   ```

2. Enter the command to upload to a network location:

   ```
   file upload </source/filename> <destaddr> <filename>
   [interface <ifname>] [id <username>] [passwd <password>]
   ```

Table 10: Variable definition

Variable	Value
<destaddr>	The network destination address.
<destination>	The destination device.
<filename>	The filename used.
<ifname>	The interface name.
<passwd>	The password used to authenticate on the FTP/TFTP server.
<source>	The source device.
<username>	The username used to authenticate on the FTP/TFTP server.

Saving the config file

The system configuration file can be saved locally or to the network.

Procedure steps

1. To save the system configuration file locally, run the following command:

   ```
   save local [file <filename>]
   ```

2. To save the system configuration file to the network, run the following command:

   ```
   save network <address> <path>
   ```

Table 11: Variable definition

Variable	Value
<address>	The IP address of the network location.
<filename>	The filename used.
<path>	The fully qualified path of the remote file.

BERT

As an aid to isolating problems on an interface, Bit-Error-Rate-Tests (BERT) configurations can be setup on CT3, T3, E1, and T1 interfaces. A BERT test configures the hardware to transmit a predefined pattern of bits in the payload for a selected channel. Test equipment at the far end of the connection can then detect that pattern, and test the data for bit errors, or the bit pattern can be transmitted back to the interface by the remote device and used by the interface hardware to detect the incoming pattern and any bit errors in the pattern.

To start a test on a specific module, use the **`test`** command with the module identifier. The **`show`** command may now be used to display the results of the test. After the test is completed, the test is terminated using the **`no`** command.

Configuring BERT testing

To configure a BERT test, perform the following steps:

Procedure steps

1. Issue the test command, accompanied by the module type and identifier.

Comments? infodev@avaya.com

```
test <module> <identifier>
```

Example:**`test t1 6/3`**

2. Issue the command to begin BERT testing, accompanied by the pattern type and duration.

```
bert <patterntype> <interval>
```

Table 12: Variable definition

Variable	Value
<identifier>	The module identifier.
<interval>	The duration of the test, in minutes. If not otherwise specified, the default setting will be continuous.
<module>	The module type. Applicable modules are T1, E1, T3, and CT3. Only modules that are present will be available for testing.
<patterntype>	The BERT test pattern type. Possible choices are: • **`2^11`** - 2^11 pattern • **`2^15`** - 2^15 pattern • **`2^20`** - 2^20 pattern • **`QRSS`** - QRSS pattern (default)

Showing BERT test results and status

To display BERT testing results and status, perform the following steps:

Procedure steps

1. Issue the test command, accompanied by the module type and identifier.

```
test <module> <identifier>
```

Example:**`test t1 6/3`**

2. Issue the command to display test results and status. Note that this command can also be issued from the CLI root.

```
show module test <module> <identifier>
```

Table 13: Variable definition

Variable	Value
<identifier>	The module identifier.

Variable	Value
<module>	The module type. Applicable modules are T1, E1, T3, and CT3. Only modules that are present will be available for testing.

Ending a BERT test

To end a BERT test, perform the following steps.

Procedure steps

1. Issue the test command, accompanied by the module type and identifier.

   ```
   test <module> <identifier>
   ```

   Example:**`test t1 6/3`**
2. Issue the command to end the BERT test.

   ```
   no bert
   ```

Table 14: Variable definition

Variable	Value
<identifier>	The module identifier.
<module>	The module type. Applicable modules are T1, E1, T3, and CT3. Only modules that are present will be available for testing.

Resetting to factory defaults

This procedure describes the steps necessary to reset the Secure Router 2330/4134 to factory defaults. This command clears all the information stored in NvRam, including user information. Other major information that will be cleared includes event logs, crash logs, command logs, and boot parameters.

Procedure steps

1. Enter Configuration Mode.

   ```
   configure terminal
   ```
2. To reset to factory defaults, run the following command:

   ```
   system reset-to-factory system
   ```


Comments? infodev@avaya.com

Resetting to factory defaults from the boot menu

This procedure describes the steps necessary to reset the Secure Router 2330/4134 to factory defaults from the boot menu in the event that the administration password has been lost. This command clears all the information stored in NvRam, including user information. Other major information that will be cleared includes event logs, crash logs, command logs, and boot parameters.

Procedure steps

1. Enter the command to reboot the switch.

   ```
   reboot
   ```

   Important:

   This command is issued from the CLI root.
2. When prompted, press any key to stop the auto-boot.

   The boot menu appears.
3. Press

   ```
   X
   ```

   to reset the switch to factory defaults.

Importing a saved configuration

The following procedures describe the steps necessary to import a saved configuration from flash memory or from a network location.

Importing from flash memory

Import a saved configuration from flash memory.

Procedure steps

1. To import a saved configuration from flash memory, enter the following command:

   `configuration flash`
2. When prompted, enter the filename. For example:

   `fileName:` **`system.cfg`**

Importing from a network location

Import a saved configuration from a network location.

Procedure steps

1. To import a saved configuration from a network location, enter the following command:

   configuration network

2. When prompted, enter the host and filename. For example:

   host: **X.X.X.X**

   fileName: **/path/folder/system.cfg**

Viewing the current configuration

This procedure describes the steps necessary to view the current system configuration.

Procedure steps

To view the current system configuration, run either of the following commands:

```
show running-config
show configuration running
```


Comments? infodev@avaya.com

Chapter 5: Troubleshooting an operational problem

Damaged router

If you detect physical damage to the router, contact Avaya Technical Support.

Normal operation of the Avaya Secure Router 2330/4134

To troubleshoot an issue, you must be familiar with the normal boot sequence of the Secure Router 2330/4134. In normal operating conditions, the following events occur when you power up the router:

- The fans start and the Secure Router 2330/4134 performs a self-test.
- At the successful conclusion of the self-test sequence, LED activity begins. The following table describes LED behavior at power-up.

Table 15: Secure Router 4134 LED behavior at power-up

Front panel LEDs	Rear panel LEDs	Description
	SYS	Illuminate red, and then green
	FAN	Illuminate red, and then green
	PS0 and PS1	Illuminate green for each power supply module that is installed.
	SM and MM	Illuminate green if Small and Medium Modules are installed. The MM LED also monitors a Large Module, if installed.
Module status and link status LEDs		Illuminate in various states until you configure the

Front panel LEDs	Rear panel LEDs	Description
		Secure Router 4134 for specific network line conditions. Generally, the status LEDs on interface modules illuminate yellow initially, and then green. The link status LEDs illuminate green, but turn off if there is no link
Ports GE 0/1, GE 0/2, GE 0/3, and GE 0/4		LEDs illuminate if a link is present and established.
As a general rule, an LED illuminates green for items that you installed. If the SM and MM LEDs on the rear panel of the Secure Router 4134 do not illuminate green, refer to the LEDs on the modules to identify issues.		

- The logon prompt appears on the console screen.

Power problem

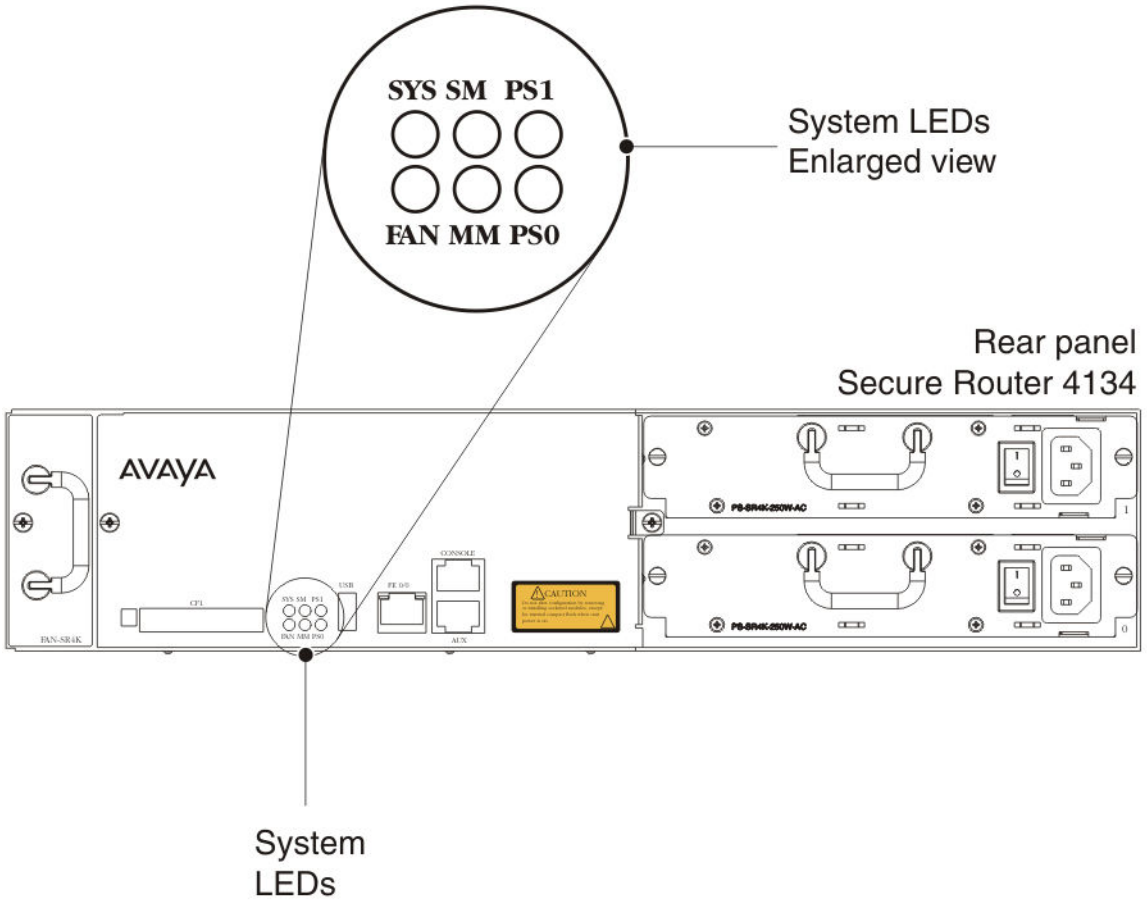
You can identify a power problem by the inactivity of the LEDs and the fans on the Avaya Secure Router 2000/4134. Use the procedure in this section to troubleshoot a power problem.

Procedure steps

1. Make sure the power cable is firmly connected to the router and to the electrical outlet or DC power source.
2. Ensure that breakers associated with the electrical outlet or DC power source are in the "on" position.
3. If neither of the power supply LEDs is on, verify that at least one power supply is turned on, and has AC or DC power input (depending on the type of power supply you have installed in the chassis).

   The following figure shows the location of the chassis system (SYS) and power supply (PS0 and PS1) LEDs on the SR4134.

Comments? infodev@avaya.com



4. Verify that at least one power supply LED is green.

   If any power supply LED is red, replace that power supply.

Fans

Use the procedure in this section if fans are not functioning.

Procedure steps

1. Check the status of the FAN LED on the rear panel of the chassis.
2. Verify that there is power reaching the router (LEDs are active). Ensure that the power cable is firmly connected to the router and to the electrical outlet or DC power source, and that associated breakers are in the "on" position.
3. Ensure the fan tray module is fully inserted and secured in place.
4. If there is power to the router (LEDs are active), enter the following command to collect information about the fans and the internal temperature of the router: **`show environment`**

Warning:

Do not run the Secure Router 2330/4134 for extended periods of time if the fans are non-operational. On the Secure Router 4134, if the router is receiving power, but the FAN LED is red and the fans remain inactive, replace the fan tray. If you do not have another fan tray to install on the SR4134, or if the fans are not operational on the SR2330, contact Avaya Technical Support.

LEDs are off

If all LEDs are off, make sure the power cable is firmly connected to the router and to an electrical outlet. If there is power to the unit, and all LEDs remain off, contact Avaya Technical Support. Be sure to note whether the fans are running or not.

Console problem

Use the procedure in this section if you have verified that power is reaching the Secure Router 2330/4134 and the chassis LEDs are working, but you cannot get a prompt at the console port.

Procedure steps

1. Verify that your terminal emulator uses the following settings:
   - 9600 bps
   - 8 data bits
   - 1 stop bit
   - no parity
   - flow control: None
2. Make sure the console cable is firmly connected to the router and to your terminal.
3. Verify that the transmit and receive signals are not crossed.

Boot problems

If the router does not boot properly or you see improper text at the console, contact Avaya Technical Support.

Comments? infodev@avaya.com

For additional information, see the following sections:

- Making sure the software image is correct on page 55
- Damaged router on page 51
- LEDs are off on page 54
- Power supply on page 40
- Power problem on page 52

Making sure the software image is correct

Make sure that the router software image on the router is compatible with the type of router you are using. To verify that the software version is correct and current, use the **show version** command to determine what version of software the router is running. You can then verify this version against the most recent copy of the Secure Router 2330/4134 Release Notes.

Example

```
SR# show version
```

Ensure that the router software image is compatible with the interface modules that are installed in the chassis, and that the image supports the features and functionality you are attempting to use. For example, Secure Router Release 10.0 software does not support voice features and functionality.

Ensure the normal and golden bootrom partitions are running the same image version. Use the **show version** command to find information for the image version running on the normal and golden bootrom partitions of your Secure Router 2330/4134. It is important that the normal and golden bootrom partitions use the same image version.

Example

```
SR# show version
Kernel: WIND version 2.6.
Boot: 0.0.0.29 (NORMAL Boot)
Runtime: 10.1.0.97
Created: Feb 13 2008, 08:49:19
Bld Path: "/tools/dailybuilds/srmain"
By: bldmstr
NorBoot: 0.0.0.29
GolBoot: 0.0.0.29
```

Ping does not work

This section describes steps you can use to troubleshoot a scenario where ping does not work.

In a scenario where you cannot ping the Secure Router 2330/4134, first try to ping the router from an adjacent device. If you are able to ping from an adjacent device you can troubleshoot the issue by invoking a traceroute to the Secure Router management IP address from both machines in an attempt to determine the source of the error. You can also check and compare routing tables on a problem machine and a functioning machine.

If you are not able to ping the Secure Router 2330/4134 from an adjacent machine you can troubleshoot the issue by first checking to make sure cables are present, securely and properly attached, and not damaged. You can also check the link status in the CLI and check IP address information to make sure systems are operating on the same subnet.

Comments? infodev@avaya.com

Chapter 6: Troubleshooting a physical media problem

Troubleshooting cable connections

This section details the steps used to troubleshoot cable connections.

To troubleshoot cable connections, you can:

- Check the cable - Use another cable
- Check the source - Try another source
- Verify the port on the Avaya Secure Router 2330/4134 is functioning

Loopback testing

Perform loopback tests to troubleshoot a circuit. For example, use a loopback test on a port to verify that the port is functioning.

When you use loopback testing to verify the circuit function, you may need to enable BERT simultaneously.

Procedure steps

To access loopback test commands, enter:

```
test {t1|e1|t3|ct3|serial|hssi} <slot/port>
```

Loopback testing for T1 interfaces

Use the commands in this section to run loopback tests on a T1 interface.

Procedure steps

1. To access loopback testing commands, enter:

```
test t1 <slot/port>
```

2. To begin a loopback test of the local line, enter:

```
loopback line
```

3. To begin a loopback test of the local payload, enter:

```
loopback payload
```

4. To begin a line loopback test with a remote device, enter:

```
loopback remote line loopback_type {ansi_fdl|
inband_standard|inband_alternate}
```

5. To begin a payload loopback test with a remote device, enter:

```
loopback remote payload loopback_type ansi_fdl
```

6. To configure a smartjack interface for remote payload loopback testing, enter:

```
loopback remote smartjack loopback_type smart_jack
```

Table 16: Variable definitions

Variable	Value
{ansi_fdl | inband_standard | inband_alternate}	The loop code for the remote line loopback test. The default value is ansi_fdl (FDL loop code as defined in ANSI T1.403).

Loopback testing for T3 interfaces

Use the commands in this section to run loopback tests on a T3 interface.

Procedure steps

1. To access loopback testing commands, enter:

```
test t3 <slot/port>
```

2. To begin a loopback test of the local line, enter:

```
loopback line_t3
```

3. To begin a line loopback test with a remote device, enter:

```
loopback remote line_t3
```

Loopback testing for E1 interfaces

Use the commands in this section to run loopback tests on an E1 interface.

Comments? infodev@avaya.com

Procedure steps

1. To access loopback testing commands, enter:

   ```
   test e1 <slot/port>
   ```
2. To begin a loopback test of the local line, enter:

   ```
   loopback line
   ```
3. To begin a loopback test of the local payload, enter:

   ```
   loopback payload
   ```
4. To begin a local inward 1 loopback test, enter:

   ```
   loopback inward1
   ```
5. To begin a local inward 1 analog loopback test, enter:

   ```
   loopback inward1_analog
   ```
6. To begin a local inward 2 loopback test, enter:

   ```
   loopback inward2
   ```

Loopback testing for interfaces on the CT3 module

Use the commands in this section to run loopback tests on the CT3 module interfaces.

Procedure steps

1. To access loopback testing commands, enter:

   ```
   test ct3 <slot/port>
   ```
2. To begin a loopback test of a local line at the CT3 level, enter:

   ```
   loopback line_ct3
   ```
3. To begin a loopback test of a local line at the T1 level, enter:

   ```
   loopback line_t1 <number>
   ```
4. To begin a loopback test of a local payload at the T1 level, enter:

   ```
   loopback payload_t1 <number>
   ```
5. To begin a line CT3 loopback test with a remote device, enter:

   ```
   loopback remote line_ct3
   ```
6. To begin a line T1 loopback test on the CT3 with a remote device, enter:

   ```
   loopback remote line_t1 <number>
   ```
7. To begin a payload T1 loopback test on the CT3 with a remote device, enter:

   ```
   loopback remote payload_t1 <number>
   ```

Table 17: Variable definitions

Variable	Value
<number>	The T1 number or range of T1s (1–28). For example: • **loopback line_t1 1** – applies to T1 1 • **loopback remote line_t1 1-3** – applies to T1 1 to T1 3

Loopback testing for serial interfaces

Use the commands in this section to run loopback tests on a serial interface.

Procedure steps

1. To access loopback testing commands, enter:

   ```
   test {serial|hssi} <slot/port>
   ```

2. To begin a loopback test of the serial interface in DTE mode, enter:

   ```
   dte_loop
   ```

3. To begin a line test for a serial interface in DCE mode, enter:

   ```
   dce_loop line
   ```

4. To begin a cable test for a serial interface in DCE mode, enter:

   ```
   dce_loop cable
   ```

5. To begin a remote test for a serial interface in DCE mode, enter:

   ```
   dce_loop remote
   ```

Troubleshooting FXS/FXO

Ensure you use straight cables with FXS and FXO modules. TIP must connect to TIP and RING must connect to RING. FXS ground start does not work if polarity is reversed.

The following table describes the LED states for the 2- and 4-port FXO and FXS Small Modules.

Comments? infodev@avaya.com

Table 18: FXS and FXO Module LEDs

LED	Description
LINK/STAT 1	Status of interface 1: • Red: The port is not configured • Green: A call is in progress • Yellow: The port is configured and ready to accept calls
LINK/STAT 2	Status of interface 2: • Red: The port is not configured • Green: A call is in progress • Yellow: The port is configured and ready to accept calls
LINK/STAT 3 (applicable to 4-port module only)	Status of interface 3: • Red: The port is not configured • Green: A call is in progress • Yellow: The port is configured and ready to accept calls
LINK/STAT 4 (applicable to 4-port module only)	Status of interface 4: • Red: The port is not configured • Green: A call is in progress • Yellow: The port is configured and ready to accept calls
Embedded LEDs at the RJ11 ports	Activity at the interface: • Red: The module is up, but the interface is not configured • Amber: The interface is configured and ready to use • Green: The interface has an active call

Troubleshooting T1/E1

This section describes steps you use to troubleshoot T1/E1.

Important:

Slot 2 of the Secure Router 4134 supports only one port of any WAN data Small Module. If you install a 2-port Small Module in Slot 2, and use the Small Module for data connections, one port only 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. This limitation does not apply to FXS or FXO voice modules.

The following table describes the LED states for the T1/E1 Small and Medium Modules.

Table 19: T1/E1 Module LEDs

LED	Description
STAT	General module status: • Off: No power available to the module • Yellow: Out of service, or failed to initiate • Green: Power on and the module is operational.
LINK/STAT	Status of each interface: • Off: Not connected or the interface is out of service. • Yellow: The interface is in a loopback mode or is running diagnostics • Green: The link or channel is active and receiving a valid signal

To view T1/E1 alarms, run the following command:

```
show module alarms {t1|e1}
```

To test a T1/E1 configuration, enter the following command:

```
test {t1|e1} <slot/port>
```

Troubleshooting DS3

This section describes steps you use to troubleshoot DS3.

Important:

The Clear Channel DS3 interface module does not support the use of the M13 framing format. Use only the default framing format of C-BIT on Clear Channel DS3 interface modules.

The following table describes the LED states for the DS3 Medium Module.

Table 20: DS3 Module LEDs

LED	Description
STAT	General module status:

Comments? infodev@avaya.com

LED	Description
	• Off: No power available to the module • Yellow: Out of service, or failed to initiate • Green: Power on and the module is operational.
LINK/STAT	Status of each interface: • Off: Not connected or the interface is out of service. • Yellow: The interface is in a loopback mode or is running diagnostics • Green: The link or channel is active and receiving a valid signal

To view DS3 alarms, run the following command:

```
show module alarms ds3
```

Troubleshooting CT3

This section describes steps you use to troubleshoot CT3.

The following table describes the LED states for the CT3 Medium Module.

Table 21: CT3 Module LEDs

LED	Description
STAT	General module status: • Off: No power available to the module • Yellow: Out of service, or failed to initiate • Green: Power on and the module is operational.
LINK/STAT	Status of each interface: • Off: Not connected or the interface is out of service. • Yellow: The interface is in a loopback mode or is running diagnostics • Green: The link or channel is active and receiving a valid signal

To view CT3 alarms, run the following command:

```
show module alarms ct3
```

Troubleshooting Serial

This section describes steps you use to troubleshoot serial.

Important:

Slot 2 of the Secure Router 4134 supports only one port of any WAN data Small Module. If you install a 2-port Small Module in Slot 2, and use the Small Module for data connections, one port only is functional (port 1).

The following table describes the LED states for the Serial Small Module.

Table 22: Serial Module LEDs

LED	Description
LINK/STAT	Status of each interface: • Off: Not connected or the interface is out of service. • Yellow: The interface is in a loopback mode or is running diagnostics • Green: The link is active and receiving a valid signal
When you power on the Secure Router 2330/4134 with a serial configuration, the serial interface software polls the port hardware status to ensure the connected cable matches the port configuration. If a connected cable does not match the cable type and operational mode settings, the interface LED turns red and the port hardware is disabled. This prevents damage to internal and external hardware components.	

To view serial alarms, run the following command:

```
show module alarms serial
```

Troubleshooting HSSI

This section describes steps you use to troubleshoot HSSI.

The following table describes the LED states for the HSSI Medium Module.

Table 23: HSSI Module LEDs

LED	Description
STAT	General module status:

Comments? infodev@avaya.com

LED	Description
	• Off: No power available to the module • Yellow: Out of service, or failed to initiate • Green: Power on and the module is operational.
LINK/STAT	Status of each interface: • Off: Not connected or the interface is out of service. • Yellow: The interface is in a loopback mode or is running diagnostics • Green: The link or channel is active and receiving a valid signal

To view HSSI alarms, run the following command:

```
show module alarms hssi
```

Troubleshooting ISDN

This section describes steps you use to troubleshoot issues with your ISDN modules.

Important:

Slot 2 of the Secure Router 4134 supports only one port of any WAN data Small Module. If you install a 2-port Small Module in Slot 2, and use the Small Module for data connections, one port only 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. This limitation does not apply to FXS or FXO voice modules.

The following table describes the LED states for the ISDN BRI modules.

Table 24: ISDN BRI S/T and ISDN BRI U Module LEDs

LED	Description
STAT	General module status: • Off: No power available to the module • Yellow: Out of service, or failed to initiate • Green: Power on and the module is operational.
LINK/STAT	Status of each interface:

LED	Description
	• Off: Not connected or the interface is out of service. • Yellow: The interface is in a loopback mode or is running diagnostics • Green: The link or channel is active and receiving a valid signal

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.

ISDN debugging commands

debug isdn

Use this command to configure ISDN debugging.

Syntax

```
[no] debug isdn
```

Example

```
SR# debug isdn
```

debug isdn all

Use this command to enable or disable all ISDN debug commands.

Syntax

```
[no] debug isdn all <bundle>
```

Table 25: Variable definition

Variable	Value
<bundle>	The ISDN bundle name.

Example

```
SR# debug isdn all test
```

debug isdn cc

Use this command to enable or disable call control debug messages.

Comments? infodev@avaya.com

Syntax

```
[no] debug isdn cc <bundle>
```

Table 26: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn cc test
```

debug isdn q921

Use this command to enable or disable q.921 debug messages.

Syntax

```
[no] debug isdn q921 <bundle>
```

Table 27: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn q921 test
```

debug isdn q921-timers

Use this command to display q.921 timers.

Syntax

```
[no] debug isdn q921-timers <bundle>
```

Table 28: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn q921-timers test
```

debug isdn q931

Use this command to enable or disable q.931 debug messages.

Syntax

```
[no] debug isdn q931 <bundle>
```

Table 29: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn q931 test
```

debug isdn q931-timers

Use this command to display q.931 timers.

Syntax

```
[no] debug isdn q931-timers <bundle>
```

Table 30: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn q931-timers test
```

debug isdn physical-layer

Use this command to enable or disable physical layer debug messages.

Syntax

```
[no] debug isdn physical-layer <bundle>
```

Table 31: Variable definition

Variable	Value
<bundle>	The bundle name.

Comments? infodev@avaya.com

Example

```
SR# debug isdn physical-layer test
```

debug isdn data-path

Use this command to enable or disable ISDN data path debug messages.

Syntax

```
[no] debug isdn data-path <bundle>
```

Table 32: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn data-path test
```

debug isdn test-isdn-call

Use this command to make an ISDN call.

Syntax

```
[no] debug isdn test-isdn-call <bundle>
```

Table 33: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn test-isdn-call test
```

debug isdn test-isdn-drop

Use this command to release an ISDN call.

Syntax

```
[no] debug isdn test-isdn-drop <bundle>
```

Table 34: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn test-isdn-drop test
```

debug isdn isdn-status

Use this command to display ISDN status for a SAP.

Syntax

```
[no] debug isdn isdn-status <bundle>
```

Table 35: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn isdn-status test
```

debug isdn q931Statistics

Use this command to display or reset q.931 statistics.

Syntax

```
[no] debug isdn q931Statistics <bundle>
```

Table 36: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn q931Statistics test
```

debug isdn q921Statistics

Use this command to display or reset q.921 statistics.

Comments? infodev@avaya.com

Syntax

```
[no] debug isdn q921Statistics <bundle>
```

Table 37: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug isdn q921Statistics test
```

Comments? infodev@avaya.com

Chapter 7: Troubleshooting a Data Link Layer problem

Commonly used troubleshooting commands

Interface commands

- Use the **`show bridge port`** command to display interfaces, their states, modes, and VLAN membership information.
- Use the **`show bridge port <interface_name>`** command to display a detailed information about a bridge port.
- Use the **`show interface ethernets`** to display all the created Ethernet interfaces and a summary information about them.
- Use the **`show interface <interface>`** command to display a detailed information including state and counters for an Ethernet interface.
- Use the **`show interface bundles`** to display all the configured bundle interfaces and a summary information about them.
- Use the **`show interface bundle <interface_name>`** to display a detailed information including state and counters for a bundle interface.

VLAN commands

- Use the **`show bridge vlan`** command to display all the static and dynamic (learned by GVRP) VLANs, their types, and port membership.
- Use the **`show bridge vlan <vid>`** to display a detailed information about a VLAN including its type (static/dynamic) and membership.

Clear commands

- Use the **clear bridge mac** command to clear all the non-static MAC entries learned by bridge.
- Use the **clear spanning-tree** command to clear MSTP states.
- Use the **clear gvrp state-machine [port-name]** to clear the current state of GVRP.

Debug commands

Most subsystems in the Avaya Secure Router 2330/4134 support debug tracing. This feature can be turned on using the following commands:

- debug all
- debug dot1x <all | event | packet | timer>
- debug gvrp <all | cli | event | packet | timer>
- debug igmp <all | decode | encode | event | fsm | tib>
- debug igmp-snooping <all | event | packet | timer>
- debug lacp <all | event | packet | timer>
- debug spanning-tree <all | cli | event | packet | timer>

Use the **no** form of these commands to disable debugging.

Troubleshooting MSTP

The main function of MSTP is to prevent loops that redundant links create in network. So the failure in MSTP causes loops in the network.

Troubleshooting a configuration failure

Regional Root ID is not showing as expected

- Issue the **show spanning-tree** command

Comments? infodev@avaya.com

```
SR4134# show spanning-tree
 Bridge Status : up
 Spanning Tree Enabled

 CIST Information :
   RootId         2000000cf8613c00
   Reg RootId     2000000cf86ddc00
   BridgeId       8000005052f26901
   Root Port      ethernet6/1
   Root PathCost 0
   Priority       32768
   Fwd Delay      15
   Hello Time     2
   Max-Age        20
   Max-Hops       20
   Region         MyName
   Revision       0
```

- Check the region name on all switches in the topology.
- Check the revision number on all switches in the topology.

```
SR4134# show spanning-tree
 Bridge Status : up
 Spanning Tree Enabled

 CIST Information :
   RootId         2000000cf8613c00
   Reg RootId     2000000cf86ddc00
   BridgeId       8000005052f26901
   Root Port      ethernet6/1
   Root PathCost 0
   Priority       32768
   Fwd Delay      15
   Hello Time     2
   Max-Age        20
   Max-Hops       20
   Region         MyName
   Revision       0

 Port Information :
```

If all switches has to be in same region then check whether there equal number of instances on all the switches and check whether the same VLANs are mapped to same instance ID on all switches using the **`show spanning-tree mstp instance vlan`**.

```
SR4134# show spanning-tree mstp instance vlan
Instance 1
  Vlan List:
        (10 -19)
Instance 2
  Vlan List:
        (20 -29)
Instance 3
  Vlan List:
        (30 -39)
Instance 4
  Vlan List:
        (40 -49)
```

VLAN traffic not flowing

Check whether all the ports in the spanning tree (common/internal) path are tagged ports that support forwarding of specified tagged packet using the **`show bridge port`** command. Note that, if all the switches are not in same region then the traffic will flow through common spanning tree outside region.

```
SR4134# show bridge port
Interface     State  Mode         Pvid  Vlan Membership
ethernet6/1   UP     TRUNK        ----  1,10-79
ethernet6/2   UP     TRUNK        ----  1,10-79
ethernet6/6   DOWN   ACCESS
```

Configuration fails with Can't set VID 90 to instance error message

Add a VLAN first, before associating with instance.

Troubleshooting an operational failure

Traffic looping

Check the states of spanning tree state machine using the **`show spanning-tree detail`** command. In the case the bridge is a root bridge all the links should be in Designated Forwarding states. In the case the bridge is a non-root, only one link to the root bridge should be in ROOT Forwarding state (others should be in Alternate Discarding) and other links (not to the root bridge) should be in Designated Forwarding states. There should be only one Root Port/Master Port per spanning tree.

```
SR4134/configure# show spanning-tree detail
 Bridge Status : up
 Spanning Tree Enabled
 CIST Information :
   RootId         2000000cf8613c00
   Reg RootId     2000000cf8613c00
   BridgeId       f000005052f26902
   Root Port      ethernet6/2
   Root PathCost 0
   Priority       61440
   Fwd Delay      15
   Hello Time     2
   Max-Age        20
   Max-Hops       20
   Region         MyName
   Revision       0
 Port Information :
  Port Name      Instance  Priority Role         State       PortFast/Filter/Guard
  ethernet6/4        CIST       128 Alternate    Discarding  Disable
  ethernet6/3        CIST       128 Alternate    Discarding  Disable
  ethernet6/2        CIST       128 Rootport     Forwarding  Disable
 Instance Information :
  Instance Id  1
    Priority   61440
    Ports List :
       Interface      Priority  Path Cost  role         state
       ethernet6/4         128   20000000  Alternate    Discarding
       ethernet6/3         128   20000000  Alternate    Discarding
       ethernet6/2         128   20000000  Rootport     Forwarding
    Vlan List :
          (10 -19)
```

Issue the **`clear spanning-tree mstp all`** command. Even if traffic looping did not stop then shutdown the redundant path links.

Bridge is selected as a Root bridge even though there is another bridge with the Lower Priority

- Issue the **`show spanning-tree detail`** command.

```
SR4134/configure# show spanning-tree detail

CIST Information :
   RootId         0000005052f26902
   Reg RootId     0000005052f26902
   BridgeId       0000005052f26902
   Root Port      -
   Root PathCost 0
   Priority       0
   Fwd Delay      15
   Hello Time     2
   Max-Age        20
   Max-Hops       20
   Region         MyName
   Revision       0

 Port Information :

  Port Name      Instance  Priority Role        State       PortFast/Filter/Guard
  ethernet6/4        CIST       128 Designated  Forwarding  Disable
  ethernet6/3        CIST       128 Designated  Forwarding  Disable
  ethernet6/2        CIST       128 Designated  Forwarding  Disable
```

- Check whether there is flow of BPDUs between devices.
- Check whether the port is receiving any packets from the peer. First clear the statistics and issue the above command using the **`clear spanning-tree statistics`** command.

```
SR4134# clear spanning-tree statistics
SR4134# show spanning-tree statistics
  Port                                : ethernet6/6
  ..................................  :
  TOTAL BPDUS recieved                : 2189
  BPDU ERROR pkts recieved            : 0
  BPDU proposal recieved              : 0
  BPDU tcn Packet                     : 33
  BPDU agrement recieved              : 0
  BPDU inside region Packet           : 0
  BPDUS outside region rx             : 0
  BPDU superior Packet  rx            : 1
  BPDU inferior recieved  rx          : 0
  BPDU repeated Packet rx             : 2188
  Total BPDUS Trasmited               : 3
  Total BPDUS Agree pkts tx           : 0
  Total BPDUS Porposal pkts tx        : 1
  BPDU Skew recieved                  : 0
  BPDU Skew rx due to delay/loss      : 0
  BPDUS Skew rx due 2 change in tpgy  : 0
```

- Check to see whether the port is receiving any BPDU using the **`show spanning-tree statistics`** command.

The number of packets received should be incrementing on a regular basis if this bridge is not root-bridge. If the bridge is non-root and if it is not receiving the packets then it could be a hardware problem. Try to hot swap the card.

Comments? infodev@avaya.com

BPDU Skew detected

- Skew message will appear when the network is bad. Check whether the number of packets transmitted by sender is almost same as that of receiver using the **`show spanning-tree statistics`** command. Number of packets received on receiver switch should be almost same as the number of BPDU packets transmitted by sender switch.

```
SR4134# clear spanning-tree statistics
SR4134# show spanning-tree statistics
  Port                                 : ethernet6/6
  ..................................   :
  TOTAL BPDUS recieved                 : 2189
  BPDU ERROR pkts recieved             : 0
  BPDU proposal recieved               : 0
  BPDU tcn Packet                      : 33
  BPDU agrement recieved               : 0
  BPDU inside region Packet            : 0
  BPDUS outside region rx              : 0
  BPDU superior Packet  rx             : 1
  BPDU inferior recieved  rx           : 0
  BPDU repeated Packet rx              : 2188
  Total BPDUS Trasmited                : 3
  Total BPDUS Agree pkts tx            : 0
  Total BPDUS Porposal pkts tx         : 1
  BPDU Skew recieved                   : 0
  BPDU Skew rx due to delay/loss       : 0
  BPDUS Skew rx due 2 change in tpgy   : 0
```

Problem with interoperating with CISCO device

- Check whether the cisco-interoperability command is enabled on port connected to Cisco using **`show spanning-tree interface <interface>`** command. If TRUE then the user can check the packets sent to CISCO and received from CISCO and analyze whether the packet structure is according to the standard.

```
SR4134# show spanning-tree interface ethernet6/2
Interface Name       : ethernet6/2
Port Id              : 32775
Mac Id               : 0050.52f2.6902
Interface State      : UP
Spanning-tree Role   : Designated
Spanning-tree State  : Forwarding
RootId               : 0000005052f26902
Reg RootId           : 0000005052f26902
Designated BridgeId  : 0000005052f26902
Designated PathCost  : 0
Configured PathCost  : 20000000
Configured Priority  : 128
Message Age          : 0
Max Age              : 20
Hello Time           : 2
Forward Delay        : 15
Forward Timer        : 0
Msg Age Timer        : 0
Hello Timer          : 0
topo change timer    : 0
State Change timer   : 0
forward-transitions  : 10
Force Version        : MSTP
link-type            : Point-to-Point
Received Version     : MSTP
Send Version         : MSTP
cisco-interop Admin  : TRUE
cisco-interop Oper   : FALSE
PortFast Admin       : No portfast configured
Portfast Oper        : portfast off
portfast bpduguard   : Admin - disabled, Oper - disable
portfast bpdufilter  : Admin - disabled, Oper - disable
```

- Enable the debug tracing to monitor MSTP BPDUs exchanged between Cisco and the SR2330/4134 using the **`debug spanning-tree packet <transmit|receive>`** command.

Ports configured as Port Fast BPDU Guard are in Disable Discarding states

Make sure the port in not receiving any BPDUs. Use debug tracing to monitor the packets received by port with the **`debug spanning-tree packet <transmit|receive>`** command.

Comments? infodev@avaya.com

Port state is Disable Discarding

```
SR4134# show spanning-tree detail
  Bridge Status : up
  Spanning Tree Enabled

  CIST Information :
    RootId         2000000cf8613c00
    Reg RootId     2000000cf8613c00
    BridgeId       f000005052f26902
    Root Port      ethernet6/3
    Root PathCost  0
    Priority       61440
    Fwd Delay      15
    Hello Time     2
    Max-Age        20
    Max-Hops       20
    Region         MyName
    Revision       0

  Port Information :

   Port Name      Instance  Priority Role        State    PortFast/Filter/Guard
   ethernet6/2        CIST       128 Disabled    Discarding  Disable
   ethernet6/4        CIST       128 Alternate   Discarding  Disable
   ethernet6/3        CIST       128 Rootport    Forwarding  Disable
```

Check whether the port is administratively down using the **`show bridge port`** command.

```
SR4134# show bridge port
Interface      State  Mode         Pvid  Vlan Membership
ethernet6/2    DOWN   ACCESS          1
ethernet6/3    UP     TRUNK        ----  1,10-79,90
ethernet6/4    UP     TRUNK        ----  1,10-79,90
```

The lowest priority bridge is not selected as Regional Root

This may not be an issue. The path cost to the CIST root has higher precedence for regional root selection.

- Check the path-cost of the ports to the CIST root bridge. The lower the path cost the more changes the bridge becoming regional root. If the root bridge is outside region then the root past cost is same on all the bridges inside the region. So the configured path cost on the interfaces connected to root plays major role in selection of regional root.

```
SR4134# show spanning-tree interface ethernet6/2
Interface Name       : ethernet6/2
Port Id              : 32775
Mac Id               : 0050.52f2.6902
Interface State      : DOWN
Spanning-tree Role   : Disabled
Spanning-tree State  : Discarding
RootId               : 2000000cf8613c00
Reg RootId           : 2000000cf8613c00
Designated BridgeId  : 80000018b06fd001
Designated PathCost  : 0
Configured PathCost  : 20000000
Configured Priority  : 128
Message Age          : 0
Max Age              : 20
Hello Time           : 2
Forward Delay        : 15
Forward Timer        : 0
Msg Age Timer        : 0
Hello Timer          : 0
topo change timer    : 0
State Change timer   : 0
forward-transitions  : 1
Force Version        : MSTP
link-type            : Point-to-Point
Received Version     : MSTP
Send Version         : MSTP
cisco-interop Admin  : FALSE
cisco-interop Oper   : FALSE
PortFast Admin       : No portfast configured
Portfast Oper        : portfast off
portfast bpduguard   : Admin - default, Oper - disable
```

Egress traffic rate is more than expected

Check if any other ports in the bridge are receiving Unknown Mac address packets.

Troubleshooting a Frame Relay connection

This section details the commands used to troubleshoot a Frame Relay connection.

Frame Relay debugging commands

debug fr

Use this command to access Frame Relay debug commands.

Comments? infodev@avaya.com

Syntax

```
debug fr
```

Example

```
SR# debug fr
```

debug fr pvc-info

Use this command to show detailed frame relay virtual circuit information.

Syntax

```
[no] debug fr pvc-info <bundle> <dlci>
```

Table 38: Variable definition

Variable	Value
<bundle>	The bundle name.
<dlci>	The DLCI number, in the range 16 to 1022.

Example

```
SR# debug fr pvc-info test 200
```

debug fr bundle-info

Use this command to show detailed frame relay bundle interface information.

Syntax

```
[debug] fr bundle-info <bundle>
```

Table 39: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug fr bundle-info test
```

debug fr packet

Use this command to enable all fr/mfr packet level debugging. Be advised that using this command can significantly impact system performance.

Syntax

```
[no] debug fr packet
```

Example

```
SR# debug fr packet
```

debug fr packet lmi

Use this command to show frame relay virtual circuit information.

Syntax

```
[no] debug fr packet lmi [debug_direction <tx|rx|both>]
```

Table 40: Variable definition

Variable	Value
<both>	Both directions.
<debug_direction>	The debug direction.
<tx>	Transmit direction.
<rx>	Receive direction.

Example

```
SR# debug fr packet lmi debug_direction tx
```

debug fr packet inverse-arp

Use this command to dump FR inverse arp packets.

Syntax

```
[no] debug fr packet inverse-arp
```

Example

```
SR# debug fr packet inverse-arp
```

debug fr packet mfr

Use this command to dump FRF.16.1 UNI/NNI MFR control packets.

Syntax

```
[no] debug fr packet mfr [content <brief|detailed>]
```


Comments? infodev@avaya.com

Table 41: Variable definition

Variable	Value
<brief>	Print single line information.
[content]	The content level to print.
<detailed>	Print detailed information.

Example

```
SR# debug fr packet mfr content detailed
```

debug fr mfr

Use this command to access MFR debug commands.

Syntax

```
[no] debug fr mfr
```

Example

```
SR# debug fr mfr
```

debug fr mfr states

Use this command to print the current state of links in an MFR bundle.

Syntax

```
[no] debug fr mfr states <bundle>
```

Table 42: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug fr mfr states test
```

debug fr mfr state-machine

Use this command to print dynamic MFR state machine changes.

Syntax

```
[no] debug fr mfr state-machine
```

Example

```
SR# debug fr mfr state-machine
```

debug fr bundle-buffers

Use this command to shows current and max buffers and other stats for all bundles.

Syntax

```
[no] debug fr bundle-buffers
```

Example

```
SR# debug fr bundle-buffers
```

debug fr frf20

Use this command to show frf20 configuration and status.

Syntax

```
[no] debug fr frf20 <bundle> <16-1022>
```

Table 43: Variable definition

Variable	Value
<bundle>	The bundle name.

Example

```
SR# debug fr frf20 test 200
```

Troubleshooting a PPP connection

This section details the commands used to troubleshoot a PPP connection.

PPP debugging commands

debug ppp

Use this command to enable or disable PPP debug commands.

Comments? infodev@avaya.com

Syntax

```
[no] debug ppp
```

Example

```
SR# debug ppp
```

debug ppp mlpinfo

Use this command to display MLPPP information.

Syntax

```
[no] debug ppp mlpinfo
```

Example

```
SR# debug ppp mlpinfo
```

debug ppp pppstates

Use this command to display PPP states information.

Syntax

```
[no] debug ppp pppstates
```

Example

```
SR# debug ppp pppstates
```

debug ppp debug_link

Use this command to set link-specific debug.

Syntax

```
[no] debug ppp debug_link
```

Example

```
SR# debug ppp debug_link
```

debug ppp negotiation

Use this command to show ppp negotiation.

Syntax

```
[no] debug ppp negotiation
```

Example

```
SR# debug ppp negotiation
```

debug ppp lcp

Use this command to show lcp debug information.

Syntax

```
[no] debug ppp lcp
```

Example

```
SR# debug ppp lcp
```

debug ppp ipcp

Use this command to display ipcp debug information.

Syntax

```
[no] debug ppp ipcp
```

Example

```
SR# debug ppp ipcp
```

debug ppp bcp

Use this command to display bcp debug information.

Syntax

```
[no] debug ppp bcp
```

Example

```
SR# debug ppp bcp
```

debug ppp ipv6cp

Use this command to display ipv6cp debug information.

Syntax

```
[no] debug ppp ipv6cp
```

Example

```
SR# debug ppp ipv6cp
```

Troubleshooting MAC configuration and switching

To add a list of interfaces and associated MAC addresses to the Layer 2 forwarding table, use the **mac address <mac address> {forward|discard} <interface> vlan <vid>** command. For more information please refer to *Avaya Secure Router 2330/4134 Configuration — Layer 2 Ethernet* (NN47263-501).

Troubleshooting a configuration failure

MAC command will fail if either the interface is not created or the interface is not a member of the VLAN

- Make sure the interfaces is created and it's VLAN membership using the **show bridge port** command.

```
SR4134# show bridge port
Interface      State  Mode         Pvid  Vlan Membership
Ethernet5/1    UP     TRUNK          1   10
```

Troubleshooting an operational failure

Traffic is not flowing

- For untagged packets, verify the receiving interface is configured as either Access or Hybrid using the **show bridge port** command.

```
SR4134# show bridge port
Interface      State  Mode         Pvid  Vlan Membership
Ethernet5/1    UP     ACCESS          1
```

- For untagged unicast packets, verify there is a MAC entry in the bridge (either learned dynamically or configure as static) using the **show bridge mac** command.

```
SR4134# show bridge mac
mac Address       Vlan    Interface     M/U-Cast   Type     Timeout
0000.2222.4545     1      ethernet5/1   Unicast    Static       ---
```

- For untagged multicast and unicast packets use the **show interface <interface>** command to check the Rx/Tx packets on both ingress and egress ports.

```
SR4134# show interface ethernet5/1
port counters since last boot/clear
Bytes Rx          1200     Bytes   Tx  1200
Packets Rx        10      Packets  Tx  10
```

Troubleshooting VLAN Configuration and Switching

Use the following commands to create VLANs in the bridge global database. The created VLANs have to functionally or characteristic unless used in an interface.

`/configure#` **vlan database**

`/configure/vlan#` **vlan <vid> [name <WORD>]**

To bind a VLAN to an interface use the following command:

`/configure/interface/ethernet (5/1)#`**switch trunk allow vlan 10**

Troubleshooting a configuration failure

Assigning a VLAN to an interface fails

- VLAN may not be created in the VLAN database yet. Use the **show bridge vlan** to verify.

Comments? infodev@avaya.com

```
SR4134# show bridge vlan
VLAN Name              Type    Member Ports ([u]-Untagged, [t]-Tagged)
   1 Default           Static  [t]ethernet5/1
  10                   Static  [t]ethernet5/1
  11                   Static  [t]ethernet5/1
  12                   Static  [t]ethernet5/1
```

Troubleshooting an operational failure

Traffic is not flowing

- For tagged unicast or multicast packets, verify the receiving and transmitting interfaces are configured as either Trunk or Hybrid interfaces and both are members of the VLAN. Use the **`show bridge port`** command.

```
SR4134# show bridge port
Interface      State  Mode         Pvid  Vlan Membership
Ethernet5/1    DOWN   TRUNK        ----  1,10-13
Ethernet6/1    DOWN   TRUNK        ----  1,10-13
```

Troubleshooting VLAN Classification

There are two types of VLAN classification rules that you can create:

- IPv4 subnet-based VLAN classification rule. If the source IP address matches the IP subnet specified in the VLAN classification rule, the received packets are mapped to the specified VLAN: **`/configure# vlan classification /configure/vlan classification# rule <id> ip4 {ipaddr/netmask|ipaddr} vlan <vid>`** The valid range for the Rule Id is 1-12. The IP address field can be either an IP address, or a subnet.
- protocol-based VLAN classification rule. If the protocol type matches the protocol specified in the VLAN classification rule, the received packets are mapped to the specified VLAN. **`/configure# vlan classification /configure/vlan classification# rule <id> protocol <protocol> encap <encapsulation>`** The protocol parameter is either a number (between 0-65535) or ipv4, ipv6, mpls, arp, rarp, vlan-tagged, appletalk, ipx, pppoe-disc, pppoe-session. The supported encapsulations are Ethernet Type II, LLC SNAP, or LLC Only.

For more information please refer to *Avaya Secure Router 2330/4134 Configuration — Layer 2 Ethernet* (NN47263-501).

Note:
VLAN Classification is supported on Hybrid ports only.

Troubleshooting a configuration failure

VLAN Classification fails with VLAN doesn't exist error

- Make sure the VLAN is already created using the **show bridge vlan** command.

```
SR4134# show bridge vlan
VLAN Name              Type    Member Ports ([u]-Untagged, [t]-Tagged)
   1 Default           Static  [t]ethernet5/1
  10                   Static  [t]ethernet5/1
```

Assigning a VLAN Classification Rule to an interface fails

- Make sure the interface is in Hybrid mode using the **show bridge port** command.

```
SR4134# show bridge port
Interface     State    Mode        Pvid     Vlan Membership
Ethernet5/1   UP    HYBRID       ----  1,10-13
```

Configuration fails with Rule Subnet overlaps with ruleId error

- Verify the previously configured rule X is not in the same subnet. Use **show running-config** command.

Comments? infodev@avaya.com

```
SR4134# show running-config

vlan classification
rule 1 ipv4 10.10.10.10/24 vlan 1000
exit classification
```

Troubleshooting an operational failure

The configure rule is not being applied

- Verify the rule is assigned to the interface. Use the **show running-config** command.

```
SR4134# show running-config
interface ethernet 5/1
aaa
exit aaa
switchport
switchport mode hybrid
vlan classification ipv4
exit ethernet
```

- Use a network sniffer to verify that the incoming packets fulfill the configured rules.
- Disable the rule on the interface, delete the rule, recreate the rule, and configure it on the interface again.
- Shutdown and restart the interface.
- Hot Swap the card if possible.

Troubleshooting VLAN stacking

Troubleshooting a configuration failure

The configuration command may fail because of the following reasons:

Command fails with Error: Specified interface does not exist error

This problem occurs when one side of a link is configured as trunk, hybrid, or access mode but on the other end VLAN Stacking is configured without setting the port first to trunk, hybrid

or access mode. Hence it is mandatory to configure port either as trunk, hybrid or access port.

WAN link with PPP encapsulation goes into Down state when VLAN Stacking enabled

On PPP L2 interfaces, the PPP protocol negotiates the frame format (802.3 or 802.1Q) based on the type configured. For example, if you have a port configured as ACCESS then it will try to negotiate based on 802.3. Similarly the trunk ports try to negotiate based on 802.1Q. For a link to come up both sides should either be negotiating based on either 802.1Q or 802.3. If the non-compatible types are configured, the negotiation fails and link never comes up. VLAN Stacking does not play any part in frame format negotiations and work on top of it. To resolve this issue, configure both end of the link as access, trunk or hybrid mode prior to configuring VLAN Stacking.

Troubleshooting port mirroring

Use the following procedures to troubleshoot port mirroring problems.

Troubleshooting a configuration failure

- The port mirroring feature is supported only on the non-CPU Ethernet ports.
- You can configure a maximum of one analyzer (destination) port for each slot.
- Each analyzer port can only monitor 8 ports for TX and RX (both mode). There is no limit for number of ports that can be monitored for RX (receive mode).

```
/configure# mirror source ethernet5/1 destination ethernet6/1
direction both
```

As shown above the analyzer and monitor ports can reside either on the same or different slot. The direction of packets can be specified as both or receive. Use a value of both to mirror both transmit and receive packets. Use a value of receive to mirror receive packets only.

```
/configure# mirror source ethernet5/1 destination ethernet7/1
direction receive
```

The configuration command may fail for one of the following reasons:

Comments? infodev@avaya.com

Command fails with invalid interface error

- Make sure the interfaces are all non-CPU Ethernet ports using the **show bridge port** command.

```
SR4134# show bridge port
Interface      State  Mode         Pvid  Vlan Membership
ethernet0/1    UP     ACCESS          1                      << CPU port
ethernet7/1    DOWN   ACCESS          1                    <<non-cpu port
ethernet5/1    DOWN   ACCESS       ----  1,10                <<non-cpu port
```

- Verify the interface name is not misspelled.
- Verify both source and destination interfaces are created by executing the **show bridge port** command.

Command fails with There is already one analyzer port configured for this card error

- There can not be more than one Analyzer port on each card. Use the **show mirror** command to get a list of the configured Monitored and Analyzer ports.

```
SR4134# show mirror
Analyzer Port      Monitored Port      Direction
ethernet7/1         ethernet5/1           Both
```

Troubleshooting an operational failure

Traffic is not mirrored

- Verify the configuration using the **show mirror** command.
- Verify the port states. Use **show bridge port** command. All the involved ports must be in UP state.

```
SR4134# show bridge port
Interface      State  Mode         Pvid  Vlan Membership
Ethernet5/1    UP     ACCESS          1
ethernet7/1    DOWN   ACCESS          1
```

- Verify the traffic flow (both Tx/Rx) on the source port. Use the **show interface <interface>** command.

```
SR4134# show interface ethernet5/1
port counters since last boot/clear
Bytes Rx                                0     Bytes      Tx  1200
Packets Rx                              0     Packets    Tx  10
```

- Verify the traffic flow (both Tx/Rx) on the destination port. Use the **show interface <interface>** command.
- If possible, switch the Analyzer ports to a different card. Hot Swap the card if Mirroring is working on the new card.

Troubleshooting Link Aggregation

This section details techniques used to troubleshoot Link Aggregation.

Troubleshooting a configuration failure

Link Aggregation is supported on all Ethernet ports. There can be only 8 Link Aggregation groups (LAG) per bridge. The number of interfaces in each link can not exceed 4. The below command will add the physical port 6/1 to the link (channel group) #1.

`/configure/interface/ethernet (6/1)/lacp#` **channel-group 1 static**

In static mode, the link aggregation is forced to be formed without any LACP negotiation. In other words, the switch will neither send the LACP packet nor process any incoming LACP packet.

`/configure/interface/ethernet (6/1)/lacp#` **channel-group 1 mode passive**

In passive mode, the switch does not initiate the channel, but does understand incoming LACP packets. The peer (in active state) initiates negotiation to form the aggregation channel with the peer.

`/configure/interface/ethernet (6/1)/lacp#` **channel-group 1 mode active**

In the active state, the switch initiates the negotiation. The link aggregate will be formed if the other end is running in LACP active or passive mode.

Command fails with invalid interface error

Make sure the interfaces are all non-CPU Ethernet ports using the command **show bridge port**.

Comments? infodev@avaya.com

```
SR4134# show bridge port
Interface     State  Mode        Pvid  Vlan Membership
ethernet0/1   UP     ACCESS         1                      << CPU port
ethernet7/1   DOWN   ACCESS         1                    <<non-cpu port
ethernet5/1   DOWN   ACCESS         1                      <<non-cpu port
```

Command fails with Maximum # of member ports reached for Channel-Group error

Verify the number of lines in the LAG does not exceed the maximum. Use the **`show lacp member-port`** and **`show lacp channel-group`** commands.

```
SR4134# show lacp channel-group
IfIndex    Name     Member-Ports (S-Static, A-Active, P-Passive)
  88        lag1     ethernet5/1-A  ethernet5/2-A
  89       lag2     ethernet5/5-A

SR4134# show show lacp member-port
fIndex    Name              Channel    Priority    Timeout    Mode
  16      ethernet5/1          1       32768       Long       Active
  17      ethernet5/2          1       32768       Long       Active
```

Troubleshooting a operational failure

First verify created channel groups (lag) using the **`show bridge port`** command.

LAG interface is down

- You should have verified the port states prior to adding them in the channel group. Use **`show interface <interface>`** command to verify the port state.

```
SR4134# show show interface ethernet5/1
ethernet5/3
description  -
status       down
```

- In the case the interface is in down state, check other end of the connection.
- In the case all the ports are configured correctly and are in UP states, verify that LACP configuration on both sides. Use **`show lacp member-port`** and **`show lacp channel-group`** commands. Verify at least one end of each interface is configured as Active.

```
SR4134# show show lacp member-port
fIndex    Name              Channel    Priority    Timeout     Mode
  16      ethernet5/1         1        32768       Long        Active
```

- If the problem still persists, use the **show lacp dynamic detail** command to verify that at least one port in the link is able to communicate with the other end.

```
SR4134#show lacp dynamic detail
Aggregator(lag1) Index(1000000) Admin-Key(0001) Oper-Key(0001)
   Partner LAG:
     MAC Address          : 0000.5052.f2c8
     Priority             : 32768
     Oper-Key             : 0001

     Member Ports:
     Name          Channel  Sync-State
     ethernet5/1        18           1

   ethernet5/1: IfIndex(18) Channel(1) Priority(32768) Timeout(61) Status(UP)
     Receive State        : 6 (Current)
     Periodic TX State    : 3 (Slow-Periodic)
     Mux Machine State    : 5 (Collecting-n-Distributing)
     Actor Churn State    : 0 (Invalid)
     Partner Chrun State  : 0 (Invalid)
     Port Selected        : 1 (Selected)
   ethernet5/2: IfIndex(23) Channel(1) Priority(32768) Timeout(69) Status(UP)
     Receive State        : 5 (Defaulted)
     Periodic TX State    : 3 (Slow-Periodic)
     Mux Machine State    : 1 (Waiting)
     Actor Churn State    : 0 (Invalid)
     Partner Chrun State  : 0 (Invalid)
     Port Selected        : 2 (Stand-by)
```

- Enable LACP debug trace to dump LACP protocol packets, events, and timers. Look for any error message, timeouts, failures and etc. using the **debug lacp <all | packet | event | timer>** command. Use the **no** form of the command to stop debugging.

Traffic rate is low

- Verify the sum of the port rates on both sides using the **show interface <interface>** command.
- Verify that all the ports in the LAG are in Current and Selected states using the **show lacp dynamic detail** command.
- Verify the Tx and Rx rates at the edge of the bridge. Use the **show interface <interface>** command.

Comments? infodev@avaya.com

Troubleshooting GVRP

This section details techniques used to troubleshoot GVRP problems.

Troubleshooting a configuration failure

GVRP will run only on trunk ports. Use the following steps to configure GVRP.

Enable GVRP globally.

```
/configure#gvrp
/configure/gvrp#gvrp-enable
```

By default GVRP is not enabled for the switch. You must first enable GVRP on the switch before you can configure the trunk ports for GVRP operation.

Procedure steps

1. Configure the port as trunk. Please refer to *Avaya Secure Router 2330/4134 Configuration — Layer 2 Ethernet* (NN47263-501) for information.
2. Configure the port GVRP:

   ```
   /configure/interface/ethernet (6/1)#gvrp
   /configure/interface/ethernet (6/1)/gvrp#gvrp-enable
   ```

   GVRP must be configured on both sides of the trunk to work correctly.
3. Configure the port registration state (optional):

   ```
   /configure/interface/ethernet (6/1)/gvrp#registration-state
   [normal|fixed|forbidden]
   ```

   By default GVRP ports are in normal registration mode. Please refer to *Avaya Secure Router 2330/4134 Configuration — Layer 2 Ethernet* (NN47263-501) for information.
4. Enable dynamic VLAN creation (optional):

   ```
   /configure#gvrp
   /configure/gvrp#dynamic-vlan-creation
   ```

Enabling GVRP on an interface fails with Access Port can not be set to gvrp error

Make sure the interface is in either trunk or hybrid mode. Use the **show bridge port** command.

```
SR4134# show bridge port
Interface      State  Mode         Pvid  Vlan Membership
ethernet5/1    UP     HYBRID          1   2-4000
```

Any other configuration errors

Enable GVRP CLI debug trace using the **debug gvrp cli** command. Use the **no** form of the command to stop debugging.

Troubleshooting an operational failure

VLANs are not learned

- Verify the port state using the **show bridge port** command.

```
SR4134# show bridge port
Interface      State  Mode         Pvid  Vlan Membership
ethernet5/1    UP     TRUNK        ----  1,100,200,300,500,1000,2000, 3000
ethernet5/2    UP     HYBRID          1  100,200,300,500,1000,2000,3000
```

- Verify the dynamic and static VLANs using the **show bridge vlan** command.

```
SR4134# show bridge vlan
VLAN Name              Type    Member Ports ([u]-Untagged, [t]-Tagged)
   1 Default           Static  [t]ethernet5/1 [t]ethernet5/2
 100                   Dynamic [t]ethernet5/1 [t]ethernet5/2
 200                   Dynamic [t]ethernet5/1 [t]ethernet5/2
 300                   Dynamic [t]ethernet5/1 [t]ethernet5/2
 500                   Dynamic [t]ethernet5/1 [t]ethernet5/2
1000                   Static  [t]ethernet5/1 [t]ethernet5/2
2000                   Static  [t]ethernet5/1 [t]ethernet5/2
3000                   Static  [t]ethernet5/1 [t]ethernet5/2
```

- Verify GVRP configuration and dynamic information using **show gvrp detail** command.

Comments? infodev@avaya.com

```
SR4134# show gvrp detail
GVRP                          :enable
 Dynamic VlanCreation:enable
 Gvrp Vlan Count:8
 GVRP Ports:
  Interface      Registration  JOIN Timer  LEAVE Timer  LEAVEALL Timer
  ethernet5/1    Normal           20          60           1000
  ethernet5/2    Normal           20          60           1000

GVRP Vlans
 GVRP VLAN  Interface List
      100  ethernet5/1
      200  ethernet5/1
      300  ethernet5/1
      500  ethernet5/1
```

- Verify GVRP Statistics using the **`show gvrp statistics`** command.

```
SR4134# show gvrp statistics
Interface            JoinEmpty   JoinIn      LeaveEmpty  LeaveIn     Empty
-------------------------------------------------------------------------------
ethernet5/1    RX          0         30          0           0           3
               TX          0         24          0           0           8
ethernet5/2    RX         24         40          0           0           0
               TX          0          0          0           0           0
```

As shown above interface ethernet5/1 is both receiving and transmitting JoinIn packet. However, interface ethernet5/2 is only receiving JoinIn packets but not transmitting (interface is set to Alternate Discarding by MSTP). If an interface is in Forwarding state and still is not transmitting and receiving JoinnIn messages, disable GVRP and re-enable GVRP both globally and on the interface. Execute this on both side of the link.

```
/configure# gvrp /configure/gvrp# no gvrp-enable /configure/
interface/ethernet (5/1)# gvrp /configure/interface/ethernet
(5/1)/gvrp# no gvrp-enable /configure/interface/ethernet (5/1)/
gvrp# gvrp-enable /configure/interface/ethernet (5/1)/gvrp#
exit /configure/interface/ethernet (5/1)# exit /configure# gvrp /
configure/gvrp# gvrp-enable
```

If the problem persists, restart the interface by executing “shutdown” and “no shutdown” on both end of the link:

```
/configure# interface ethernet5/1 /configure/interface/
ethernet5/1# shutdown /configure/interface/ethernet5/1# no
shutdown
```

- Verify GVRP State Machine using the **`show gvrp state-machine`** command.

```
SR4134# show gvrp state-machine
  Interface ethernet5/1
            VlanId    1  applicant state[0] = QA  registrar state[0] = INR
            VlanId 1000  applicant state[1] = QA  registrar state[1] = INR
            VlanId 2000  applicant state[2] = QA  registrar state[2] = INR
            VlanId 3000  applicant state[3] = QA  registrar state[3] = INR
            VlanId  100  applicant state[4] = QO  registrar state[4] = INN
            VlanId  200  applicant state[5] = QO  registrar state[5] = INN
            VlanId  300  applicant state[6] = QO  registrar state[6] = INN
            VlanId  500  applicant state[7] = QO  registrar state[7] = INN
  Interface ethernet5/2
            VlanId    1  applicant state[0] = QA  registrar state[0] = INR
            VlanId 1000  applicant state[1] = QA  registrar state[1] = INR
            VlanId 2000  applicant state[2] = QA  registrar state[2] = INR
            VlanId 3000  applicant state[3] = QA  registrar state[3] = INR
```

- Clear GVRP state machine using **`clear gvrp state-machine [port-name]`** command.
- • Enable GVRP debug traces using the **`debug gvrp <all | packet | event | timer>`** command. This will allow you to trace packets, events, and verify timers. Use the **`no`** for of this command to disable debugging.

Troubleshooting IGMP Snooping

This section details techniques used to troubleshoot IGMP Snooping.

Troubleshooting a configuration failure

VLAN not present

```
Error: Invalid vlan-id (3)
```

For IGMP Snooping to be enabled on a VLAN, the VLAN has to be present during configuration. Refer user guide on how to create a VLAN.

Mrouter port configuration failure

```
Error: Interface (ethernet1/1) not found
```

For configuring a mrouter port, the port needs to be present as a bridge port before configuration. Refer user guide on how to create a bridge port.

Comments? infodev@avaya.com

IGMP Version configuration failure on an interface

```
Error: Port [ethernet2/1] is not switchport
```

For configuring IGMP version on an interface the interface needs to be a bridge port. Refer user guide on how to create a bridge port.

Troubleshooting an operational failure

Host not added to a multicast group

This problem may result in the following symptoms:

- Multicast traffic is not received by host
- Multicast traffic is flooded to all the ports in the VLAN
- IGMP Snooping is not working properly

1. Ensure the host ports, ports connected to traffic source and mrouter port are all configured as bridge ports using the **`show bridge port`** command. Also ensure they are members of VLAN on which traffic is sent.

```
SR4134# show bridge port
Interface      State  Mode         Pvid  Vlan Membership
ethernet2/1    UP     ACCESS          3
ethernet1/1    UP     TRUNK          --  1-10
```

2. Ensure the spanning-tree states of the ports are forwarding using the **`show spanning-tree detail`** command.

```
SR4134# show spanning-tree detail
 Bridge Status : up
 Spanning Tree Enabled

 CIST Information :
   RootId         8000005052f42104
   Reg RootId     8000005052f42104
   BridgeId       8000005052f42104
   Root Port      -
   Root PathCost  0
   Priority       32768
   Fwd Delay      15
   Hello Time     2
   Max-Age        20
   Max-Hops       20
   Region         MyName
   Revision       0

 Port Information :

  Port Name     Instance  Priority Role        State     PortFast/Filter/Guard
  Ethernet2/1       CIST       128   Designated  Forwarding  Disable
  Ethernet1/1      CIST       128   Designated  Forwarding  Disable
```

3. Ensure IGMP Snooping is enabled globally and on the VLAN using the **`show ip igmp snooping config`** command.

```
SR4134# show ip igmp snooping config
 IGMP Snooping  : ENABLED
 Proxy Status   : DISABLED

 Vid   Snooping  Fast      Querier   IGMP  Query     Last      Max   Mrouter
                 Leave               Ver   Interval  Query     Resp  Interface
                                                     Interval  Time
    1  DISABLED  DISABLED  DISABLED  2     125000    1000      100
    3  ENABLED   DISABLED  DISABLED  2     125000    1000      100
```

4. Ensure the multicast group IP/MAC address has been learned on the host interface using the **`show ip igmp snooping groups`** command.

```
SR4134# show ip igmp snooping groups
Vid   GroupIPAddress     Interface
  3   225.0.0.1          ethernet2/1
SR4134# show bridge
Mac Address      Vlan Interface    M/U-Cast  Type    Timeout
0100.5e00.0001    3  ethernet2/1  Multicast Static      ---
```

5. If the multicast group association with host interface is not seen, it means that the IGMP messages from Host interface is not received by IGMP Snooping module. Verify the IGMP Snooping counters using the **`show ip igmp snooping statistics`** command. If the RX Invalid pkts counter is getting incremented then the incoming IGMP messages are not valid. This might be the reason for multicast group not being associated with host port.

Comments? infodev@avaya.com

```
SR4134# show ip igmp snooping statistics
Interface    RXCNT: Join  Leave Query Invalid TXCNT: Join  Leave Query Invalid
 Name                Pkts  Pkts        Pkts            Pkts  Pkts        Pkts
 Ethernet1/1          0     0     1      0              0     0     0     0
 Ethernet2/1          0     0     0      2              1     0     0     0
```

6. To analyze the reason for Invalid Pkts counter, enable appropriate debugs to verify the packets, timers and event notifications on IGMP Snooping module using the **debug igmp-snooping <all | packet | event | timer>** command. Use **no debug igmp-snooping <all | packet | event | timer>** to disable the debug trace.

   One possible reason for packet being considered INVALID is the IGMP message can be of IGMPv3 type, which is not supported. For successful operation ensure only IGMP v1/v2 messages are sent by the host or mrouter.

   Enabling packet dump should dump the details of IGMP messages received on host/mrouter interfaces on console. If none of the IGMP messages are seen, then it means that IGMP Snooping module is not getting any messages from the ports.

7. Recover from the issue. If the multicast group association with host interface is not seen, try the following options:

   a. Ensure the host interface receives IGMP v1/v2 messages of valid range of multicast groups.

   b. Execute command **clear ip igmp snooping groups**.

   c. Disable IGMP Snooping globally and on VLAN.

   d. Administratively DOWN the host port, mrouter port, and port connected to traffic source using the **shutdown** command.

   e. Administratively UP the host port, mrouter port, and port connected to traffic source using the **no shutdown** command.

   f. Enable IGMP Snooping globally and on VLAN.

   g. Repeat steps 1 to 4.

Mrouter ports are not getting cleared properly

- Check whether the mrouter ports are Dynamic (Learned) or Static (Configured) using the **show ip igmp snooping mrouter** command.

```
SR4134# show ip igmp snooping mrouter
Vid    Interface
  3    ethernet1/1   -Configured
  4    ethernet5/2   -Learned
```

- Static mrouter ports have to be cleared explicitly using “no mrouter <interface name>” command. Dynamic mrouter ports can be cleared using the **`clear ip igmp snooping mrouter`** command.

```
SR4134# clear ip igmp snooping mrouter
SR4134# show ip igmp snooping mrouter
Vid    Interface
  3    ethernet1/1   -Configured
```


Comments? infodev@avaya.com

Chapter 8: Troubleshooting Ethernet CFM

Use the commands in this section to troubleshoot Ethernet Connectivity Fault Management (CFM). To configure Ethernet CFM, see *Avaya Secure Router 2330/4134 Configuration — Layer 2 Ethernet* (NN47263-501).

Ethernet CFM debug commands

This section provides the Ethernet CFM debug commands.

debug oam cfm dump-data

Use this command to enable or disable the dump of data for Ethernet CFM.

Syntax

```
cfm dump-data {0|1}
```

Table 44: Variable definitions

Variable	Value
{0 | 1}	Enables or disables the "dump" of data. Enter 0 to disable and 1 to enable. The default value is 0.

Example

```
SR/debug/oam# cfm dump-data 0
```

debug oam cfm debug-feature debug-level

Use this command to specify the feature to debug and the level at which to debug.

The Avaya Secure Router 2330/4134 does not write the debug information to a log file. The Secure Router 2330/4134 displays the debug information only on your screen.

Important:

You can use a debug level of 1 to 4. As the level increases, the amount of debug information also increases.

Important:

Use the debug commands with caution. The debug command output is code-specific. Use the **show** commands to understand the behavior of your system.

Syntax

```
cfm debug-feature <"value"> debug-level <level>
```

Table 45: Variable definitions

Variable	Value
<level>	Sets the debug level. Enter a value in the range of 0 to 4. The default value is 0. The level values correspond to the following descriptions: • 0 = none • 1 = major • 2 = minor • 3 = detail • 4 = flood
<"value">	Specifies the feature. Use quotation marks around the feature description. The feature description can be up to 127 characters and uses any of the following words: • ALL • CCI • CCR • CLI • DISPATCH • ERR • FRAME • LB • LPORT • LT • MA • MD • MEP • MIP • PORT

Comments? infodev@avaya.com

Variable	Value
	• QUE • RMEP • RSP • RX • STARTUP • TIMERS • TX

Example

```
SR/debug/oam# cfm debug-feature "LT LPORT MIP" debug-level 3
```

debug oam no cfm

Use the command in this section to end the output of CFM-related debug and dump messages.

Syntax

```
no cfm
```

Example

```
SR/debug/oam# no cfm
```

Comments? infodev@avaya.com

Chapter 9: Troubleshooting an MPLS problem

For troubleshooting an MPLS network, you should use a step by step approach for isolating the problems. The first step is to ensure the dependency interfaces are functioning properly, and in an “up” state. Other items to check include making sure the route exists, that you can ping the peer, and that the MPLS protocol is globally enabled. These are basic prerequisites for MPLS troubleshooting.

General MPLS - Prerequisites for RSVP, LDP, L2VPN, Static LSP

Before debugging ensure all MPLS prerequisites are satisfied:

1. Verify the Interfaces

   Check that routers are connected, the interfaces are UP and configured correctly by issuing the following commands:

   ```
   show interface show ip interface brief
   ```

2. Verify the Routing Protocol

   - Issue the command **`show ip route`** to verify the routing table
   - Ensure the routes to the network are present
   - If the routes are not present check routing protocol configuration

3. Ping the neighbors

   - Ensure that a ping to the MPLS peer / Router ID is successful

4. Verify MPLS

   - Ensure MPLS is enable in the required interfaces
   - Issue the command **`show mpls interface`** to verify the MPLS interfaces
   - Ensure the required MPLS protocol is enabled in the required interfaces
   - Issue the commands **`show rsvp interface`** and **`show ldp interface`**

Troubleshooting Static LSP

This section details the steps and commands used to troubleshoot Static LSPs.

For static LSP, since there is no signaling most problems might be due to the configuration and forwarding plane. Follow the below steps to troubleshoot the problem.

Procedure steps

1. Ensure all MPLS prerequisites are satisfied.
2. Ensure the static FTN and static ILM are configured properly with valid interface and labels: **show mpls static-ftn show mpls static-ilm**
3. Check the forwarding table entry for CLI-FTN: **show mpls table-forwarding**

```
SR4134# show mpls table-forwarding
Codes: > - selected FTN, K - CLI FTN, L - LDP FTN M - RSVP Mapped FTN, R - RSVP-TE FTN

Code      FEC              FTN-ID  Pri  Out-Label  Nexthop          Out-Intf       LSP Name
M>     4.4.4.0/24            4     Yes   2064     24.61.1.61       ethernet0/3      a1
K>     61.61.61.0/24         1     Yes   1048     24.61.1.24       ethernet0/3      -
R>     61.61.61.61/32        3     Yes   2064     24.61.1.61       ethernet0/3      a1
```

4. Check the routing table for MPLS static routes: **show ip route**

```
SR4134# show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, M - MPLS
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default


IP Load balancing policy is per_flow

C       3.3.3.0/24 is directly connected, ethernet7/1
M       4.4.4.0/24 [10/0] via 24.61.1.61, ethernet0/3, label 2064, RSVP-RSVP_MAP, a1
C       24.24.24.24/32 is directly connected, l0
C       24.61.1.0/24 is directly connected, ethernet0/3
C       24.77.1.0/24 is directly connected, ethernet0/1
C       24.102.1.0/24 is directly connected, ethernet0/2
S       47.100.0.0/16 [1/0] via 47.100.106.1, ethernet0/0
C       47.100.106.0/24 is directly connected, ethernet0/0
M       61.61.61.0/24 [10/0] via 24.61.1.24, ethernet0/3, label 1048, CLI-REG
C       106.50.50.20/30 is directly connected, R4-0-1
O       106.50.50.60/30 [110/130] via 106.50.50.61, R4-0-1, 01:01:16
C       106.50.50.61/32 is directly connected, R4-0-1
C       127.0.0.0/8 is directly connected, lo0
```

5. Make sure the particular MPLS route is selected: **show ip route database**

Comments? infodev@avaya.com

```
SR4134# show ip route d
Codes: C - connected, S - static, R - RIP, B - BGP, M - MPLS
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info


IP Load balancing policy is per_flow

C     *> 3.3.3.0/24 is directly connected, ethernet7/1
M     *> 4.4.4.0/24 [10/0] via 24.61.1.61, ethernet0/3, label 2064, RSVP-RSVP_MAP, a1
C     *> 24.24.24.24/32 is directly connected, l0
C     *> 24.61.1.0/24 is directly connected, ethernet0/3
C     *> 24.77.1.0/24 is directly connected, ethernet0/1
C     *> 24.102.1.0/24 is directly connected, ethernet0/2
S     *> 47.100.0.0/16 [1/0] via 47.100.106.1, ethernet0/0
C     *> 47.100.106.0/24 is directly connected, ethernet0/0
M     *> 61.61.61.0/24 [10/0] via 24.61.1.24, ethernet0/3, label 1048, CLI-REG
O        61.61.61.61/32 [110/1] via 24.61.1.61, ethernet0/3, 01:01:12
C     *> 106.50.50.20/30 is directly connected, R4-0-1
O     *> 106.50.50.60/30 [110/130] via 106.50.50.61, R4-0-1, 01:01:22
C     *> 106.50.50.61/32 is directly connected, R4-0-1
C     *> 127.0.0.0/8 is directly connected, lo0
```

6. Make sure the forwarding entry and route database are in sync
7. Check the static LSP statistics for transmitted packets: **`show mpls stats-lsp`**
8. Check the MPLS forwarding statistics for transmitted packets: **`show mpls stats-ftn show mpls stats-interface`**
9. If the statistics are not getting updated, check the incoming data packet: **`show interface <interface name>`**

Troubleshooting LDP LSP

This section details the steps and commands used to troubleshoot LDP LSPs.

LDP session fail to establish/Label Binding Failure

- Ensure all MPLS prerequisites are satisfied.
- Ensure the LDP protocol is enabled globally. Issue the command **`show ldp`**. Check whether the transport address shown is used. It is better to configure the transport address as the router-id. Whenever you want to use a new transport address, it is recommended that you first remove the old transport address and then configure the new transport address. Failing to do so will result in failure of LDP adjacency establishment.

```
SR4134# show ldp
Router ID                  : 24.24.24.24
LDP Version                : 1
Global Merge Capability    : Non Merge Capable
Label Advertisement Mode   : Downstream Unsolicited
Label Retention Mode       : Liberal
Label Control Mode         : Independent
Loop Detection             : Off
Loop Detection Count       : 0
Request Retry              : Off
Propagate Release          : Disabled
Hello Interval             : 5
Targeted Hello Interval    : 15
Hold time                  : 15
Targeted Hold time         : 45
Keepalive Interval         : 10
Keepalive Timeout          : 30
Request retry Timeout      : 5
Transport Address data     :
  Labelspace 0             : 24.77.1.24 (not in use)

SR4134# conf t
SR4134/configure# router ldp
SR4134/configure/router/ldp# transport-address 24.24.24.24
SR4134/configure/router/ldp# show ldp
Router ID                  : 24.24.24.24
LDP Version                : 1
Global Merge Capability    : Non Merge Capable
Label Advertisement Mode   : Downstream Unsolicited
Label Retention Mode       : Liberal
Label Control Mode         : Independent
Loop Detection             : Off
Loop Detection Count       : 0
Request Retry              : Off
Propagate Release          : Disabled
Hello Interval             : 5
Targeted Hello Interval    : 15
Hold time                  : 15
Targeted Hold time         : 45
Keepalive Interval         : 10
Keepalive Timeout          : 30
Request retry Timeout      : 5
Transport Address data     :
  Labelspace 0             : 24.24.24.24 (in use)
```

- Ensure the LDP protocol is enabled on the interface. Issue the command **`show ldp interface`**.

```
SR4134# show ldp interface
Interface          Merge-Capability        LDP-Identifier
ethernet0/1        Non merge capable       24.24.24.24:0
ethernet0/3        Non merge capable       24.24.24.24:0
R4-0-1             Non merge capable       24.24.24.24:0
```


Comments? infodev@avaya.com

- Check the session adjacency information by issuing command **show ldp adjacency**.

```
SR4134# show ldp adjacency
IP Address        Intf Name     Holdtime   Targeted-Peer    LDP-Identifier
24.61.1.61        ethernet0/3   15         No               61.61.61.61:0
24.77.1.77        ethernet0/1   15         No               77.77.77.77:0
```

- Check the session status by issuing command **show ldp session** and **show ldp session <session peer ip address>**.

```
SR4134# show ldp session
Peer IP Address    My Role    State          KeepAlive    Targeted-Peer
24.61.1.61         Active     OPERATIONAL    30           No
24.77.1.77         Passive    OPERATIONAL    30           No
```

- Ensure there is no access list to block the LDP messages.
- Ensure advertise-labels are enabled in the LDP mode and in the peer router: **show ldp advertise-labels**
- Check the FEC table to get the FEC-Label binding for a particular prefix. **show ldp fec**
- Check the LDP lsp: **show ldp lsp**
- Label binding correspond to the best route will be available in the Routing table and the forwarding entry. **show ip route** **show ip route database** **show mpls table-forwarding**

```
SR4134# show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, M - MPLS
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default


IP Load balancing policy is per_flow

C   24.77.1.0/24 is directly connected, ethernet0/1
C   24.102.1.0/24 is directly connected, ethernet0/2
S    47.100.0.0/16 [1/0] via 47.100.106.1, ethernet0/0
C    47.100.106.0/24 is directly connected, ethernet0/0
M    61.61.61.61/32 [10/0] via 24.61.1.61, ethernet0/3, label IPV4-EXP-NULL, LDP-REG
C       106.50.50.20/30 is directly connected, R4-0-1
M       106.50.50.60/30 [10/0] via 106.50.50.61, R4-0-1, label IPV4-EXP-NULL, LDP-REG
C       106.50.50.61/32 is directly connected, R4-0-1
C       127.0.0.0/8 is directly connected, lo0


SR4134# show ip route database
Codes: C - connected, S - static, R - RIP, B - BGP, M - MPLS
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info

IP Load balancing policy is per_flow

C    *> 24.77.1.0/24 is directly connected, ethernet0/1
C    *> 24.102.1.0/24 is directly connected, ethernet0/2
S    *> 47.100.0.0/16 [1/0] via 47.100.106.1, ethernet0/0
C    *> 47.100.106.0/24 is directly connected, ethernet0/0
M    *> 61.61.61.61/32 [10/0] via 24.61.1.61, ethernet0/3, label IPV4-EXP-NULL, LDP-REG
O       61.61.61.61/32 [110/1] via 24.61.1.61, ethernet0/3, 07:10:33
C    *> 106.50.50.20/30 is directly connected, R4-0-1
M    *> 106.50.50.60/30 [10/0] via 106.50.50.61, R4-0-1, label IPV4-EXP-NULL, LDP-REG
O       106.50.50.60/30 [110/130] via 106.50.50.61, R4-0-1, 04:56:13
C    *> 106.50.50.61/32 is directly connected, R4-0-1
C    *> 127.0.0.0/8 is directly connected, lo0


SR4134# show mpls table-forwarding
Codes: > - selected FTN, K - CLI FTN, L - LDP FTN
       M - RSVP Mapped FTN, R - RSVP-TE FTN

Code  FEC              FTN-ID  Pri  Out-Label  Nexthop          Out-Intf       LSP Name
L>    61.61.61.61/32      1    Yes  0          24.61.1.61       ethernet0/3      -
L>    106.50.50.60/30     2    Yes  0          106.50.50.61     R4-0-1           -
```

More detailed analysis

For a more detailed analysis a user can issue the **debug ldp** command. If there are more sessions, there will be more prints to the console and user needs to filter this information by the ldp-id of the particular session to debug. The ldp-id will be printed in the debugs and can be cross checked with the show command. For LDP start with **debug ldp events** - this will give all the events of LDP. Make sure the protocol messages are sending out and receiving. Make sure the state machine is working by issuing **debug ldp fsm**. For further filtering, depending on the router type like upstream, down stream, transient, a user can issue the commands **debug ldp usm**, **debug ldp dsm**, and **debug ldp tsm**. Make sure the finite

Comments? infodev@avaya.com

state machine is working fine. With **debug ldp nsm** a user can debug the events from NSM, route add delete and entries to forwarding. With **debug ldp advertise-labels** a user can debug access list issues. For detail information about the LDP packet send and receive use **debug ldp packet**. For detailed analysis of the packet send and receive and to dump the packet use **debug ldp hexdump**.

Packets not forwarding

Follow the below steps to troubleshoot the problem.

Procedure steps

1. Ensure LDP adjacency is established session is UP **show ldp adjacency**
2. Ensure LDP session is UP
3. Check the session status **show ldp session** **show ldp session <session peer ip address>**
4. Check the label binding and LDP lsp **show ldp fec** **show ldp lsp**
5. Check the forwarding table entry for LDP FTN **show mpls table-forwarding**
6. Check the routing table for the MPLS-LDP routes **show ip route**
7. Check the particular MPLS-LDP route is selected **show ip route database**
8. Make sure the forwarding entry and route database are in sync
9. Check the LDP LSP statistics for transmitted packets **show mpls stats-lsp**
10. Check the MPLS-LDP forwarding statistics for transmitted packets **show mpls stats-ftn**
11. If the statistics are not getting updated, check the incoming data packet **show interface <interface name>**

Isolating the cause and corrective action

- Are label bindings advertise correctly? Isolate the problem by removing the policies.
- Is Forwarding at fault?
- Is Configuration correct in the peer routers, and in the entire LSP path? Execute the command **clear ldp adjacency <LDP adjacency address>** in global mode to clear a particular ldp adjacency. Make sure the session comes up after the traffic is flowing correctly. Execute the command **clear ldp adjacency all** to clear all ldp adjacency. Apart from the protocol the problem may be related to another system. Shut down and restart the incoming and outgoing interfaces

If there is a problem, take appropriate action to fix it, then make sure the LSP is operating as expected. If problem still exists contact Avaya support for help.

Troubleshooting RSVP-TE LSP

This section details the steps and commands used to troubleshoot RSVP-TE LSPs.

RSVP session fails to establish

Follow the below steps to troubleshoot the problem:

Procedure steps

1. Ensure all the MPLS prerequisites are satisfied
2. Ensure the RSVP protocol is enabled globally by issuing the command **show rsvp**

```
SR4134# show rsvp
RSVP Version                    : 1
Process uptime                  : 4 hours 2 minutes
RSVP Refresh Reduction          : Enabled
RSVP Message Acknowledgement    : Disabled
Bundle Send                     : Disabled
NSM Connection                  : Up
CSPF Connection                 : Up
CSPF usage                      : Enabled
RSVP Refresh Timer              : 30
Keep Multiplier                 : 3
Acknowledgement Await Timeout   : 10
Explicit-Null For Direct Conn   : Disabled
Local Protection                : Disabled
Hello Receipt                   : Disabled
Hello Interval                  : 2
Hello Timeout                   : 7
Loop detection                  : Enabled (all interface)
Ingress                         : 47.100.106.115
Penultimate Hop Popping         : Enabled
Refresh PATH msg parsing        : Enabled
Refresh RESV msg parsing        : Enabled
Detour identification           : Sender-Template
```

3. Ensure the RSVP protocol is enabled on interface level by issuing the command **show rsvp interface**

Comments? infodev@avaya.com

```
SR4134# show rsvp interface
Interface      Interface-Type
ethernet0/3    Ethernet
```

4. Check session information by issuing the commands **show mpls traffic-eng-lsp session** and **show mpls traffic-eng-lsp session <session name>**

```
SR4134# show mpls traffic-eng-lsp session a1
Ingress (Primary)
61.61.61.61
From: 24.24.24.24, LSPstate: Dn, LSPname: a1
Setup priority: 7, Hold priority: 0
CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
LSP Protection: None
Label in: -,  Label out: -,
Tspec rate: 0, Fspec rate: 0
Tunnel Id: 1, LSP Id: 1, Ext-Tunnel Id: 47.100.106.115
Downstream: 24.61.1.61, N/A
Retry count: 0, intrvl: 30 seconds, # remaining: inf., next retry in: 23 seconds
RRO re-use as ERO: Disabled
Label Recording: Disabled
Admin Groups: none
Configured Path: none
Session Explicit Route Detail :
24.61.1.61/32 strict
Record route: <self>  ...incomplete
Style: Shared Explicit Filter
Traffic type: N/A
Minimum Path MTU: N/A
Last Recorded Error Code: Routing Problem (24)
Last Recorded Error Value: MPLS label allocation failure (9)
Node where Last Recorded Error originated: None
```

The resulting display will record session failure reasons like ingress problems, CSPF configuration errors, routing problems, MPLS label allocation failures, etc. The below table explains the major error codes/sub error codes, as well as root cause and corrective action for these error codes.

Table 46: Error scenarios

Error scenario	Cause/Corrective Action
Routing Problem	Routing issues. RSVP trying to send packets but not able to send to peer. Problem can be solved by adding the route to the destination configuration
No route available toward destination	No route to destination. Add route to destination and ping to the peer
Non RSVP-TE router encountered	Interface is not rsvp enabled. Enable rsvp on the required interfaces
MPLS label allocation failure	Interface is not rsvp enabled. Enable rsvp on the required interfaces

Error scenario	Cause/Corrective Action
Ingress Problem	Error in the ingress side, mainly because of wrong configuration.
CSPF configuration error	Mismatch in the CSPF configuration, like CSPF disable globally, but enabled in lsp level etc. Cross check the configuration and correct it
Egress configuration error	Wrong Configuration in Egress side. Cross check the configuration and correct it
PATH configuration error	Wrong Path Configured, ensure mpls and rsvp is enabled in the desired path. Cross check the configuration and correct it.
First hop unreachable	First hop not reachable. Configure the required ip address/mask
Hop limit conflict	Configured invalid/mismatched Hop limit for the lsp. Cross check the configuration and correct it
Setup priority conflict	Configured invalid/mismatched setup priority for the lsp. Cross check the configuration and correct it

If this does not isolate the problem, you can go to debug mode for further analysis.

More detailed analysis

For more detailed analysis you can issue the **debug rsvp** commands. If there are more sessions, there will be more prints to the console and the user needs to filter this information by lsp-id of the particular session to debug. The lsp-id will be printed in the debug output and can be cross checked with the show command **show mpls traffic-eng-lsp session <session name>**.

For RSVP start with **debug rsvp events** - this will output all RSVP events. Make sure the protocol messages are sending and receiving.

Make sure the state machine is functioning by issuing **debug rsvp fsm**. For further filtering depending on the router, the user can give the options like ingress, egress, and transient. Make sure the Finite state machine is functioning properly.

For RSVP sessions with CSPF enabled, check the CSPF flow with the command **debug rsvp cspf**. This debug command combined with **debug cspf lsp <lsp-name>** will give more detailed information and make sure there are no errors in the CSPF flow.

For RSVP sessions with QOS parameters, **debug rsvp nsm** will give more detailed information about the flow and the interfaces with QOS.

Comments? infodev@avaya.com

For detail information about RSVP packet send and receive use **debug rsvp packet**.

For detailed analysis of packet send and receive and to dump the packet use **debug rsvp hexdump**.

Troubleshooting packets not forwarding

Follow the below steps to troubleshoot the problem.

Procedure steps

1. Ensure RSVP session is UP
   - Check the session status **show mpls traffic-eng-lsp session show mpls traffic-eng-lsp session <session name>**

```
SR4134# show mpls traffic-eng-lsp session
Ingress RSVP:
To                   From            State Pri    Rt    Style Labelin Labelout LSPname
61.61.61.61          24.24.24.24       Up   Yes     1     SE       -     2064      a1
Total 1 displayed, Up 1, Down 0
```

2. Ensure the map routes are configured properly for the particular LSP
3. Check the Table forwarding entry for RSVP-TE FTN and RSVP Mapped FTN **show mpls table-forwarding**

```
SR4134# show mpls table-forwarding
Codes: > - selected FTN, K - CLI FTN, L - LDP FTN M - RSVP Mapped FTN, R - RSVP-TE FTN

Code  FEC                FTN-ID  Pri  Out-Label  Nexthop          Out-Intf       LSP Name
M>    4.4.4.0/24         4       Yes      2064   24.61.1.61        ethernet0/3        a1
R>    61.61.61.61/32     3       Yes      2064   24.61.1.61        ethernet0/3        a1
```

4. Check the routing table for MPLS routes **show ip route**

```
SR4134# show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, M - MPLS
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default


IP Load balancing policy is per_flow

C       3.3.3.0/24 is directly connected, ethernet7/1
M       4.4.4.0/24 [10/0] via 24.61.1.61, ethernet0/3, label 2064, RSVP-RSVP_MAP, a1
C       24.24.24.24/32 is directly connected, l0
C       24.61.1.0/24 is directly connected, ethernet0/3
C       24.77.1.0/24 is directly connected, ethernet0/1
C       24.102.1.0/24 is directly connected, ethernet0/2
S       47.100.0.0/16 [1/0] via 47.100.106.1, ethernet0/0
C       47.100.106.0/24 is directly connected, ethernet0/0
M       61.61.61.61/32 [10/0] via 24.61.1.61, ethernet0/3, label 2064, RSVP-REG, a1
C       106.50.50.20/30 is directly connected, R4-0-1
O       106.50.50.60/30 [110/130] via 106.50.50.61, R4-0-1, 00:06:40
C       106.50.50.61/32 is directly connected, R4-0-1
C       127.0.0.0/8 is directly connected, lo0
```

5. Check that the particular MPLS route is selected **show ip route database**

```
SR4134# show ip route d
Codes: C - connected, S - static, R - RIP, B - BGP, M - MPLS
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info


IP Load balancing policy is per_flow

C     *> 3.3.3.0/24 is directly connected, ethernet7/1
M     *> 4.4.4.0/24 [10/0] via 24.61.1.61, ethernet0/3, label 2064, RSVP-RSVP_MAP, a1
C     *> 24.24.24.24/32 is directly connected, l0
C     *> 24.61.1.0/24 is directly connected, ethernet0/3
C     *> 24.77.1.0/24 is directly connected, ethernet0/1
C     *> 24.102.1.0/24 is directly connected, ethernet0/2
S     *> 47.100.0.0/16 [1/0] via 47.100.106.1, ethernet0/0
C     *> 47.100.106.0/24 is directly connected, ethernet0/0
M     *> 61.61.61.61/32 [10/0] via 24.61.1.61, ethernet0/3, label 2064, RSVP-REG, a1
O        61.61.61.61/32 [110/1] via 24.61.1.61, ethernet0/3, 00:06:37
C     *> 106.50.50.20/30 is directly connected, R4-0-1
O     *> 106.50.50.60/30 [110/130] via 106.50.50.61, R4-0-1, 00:06:47
C     *> 106.50.50.61/32 is directly connected, R4-0-1
C     *> 127.0.0.0/8 is directly connected, lo0
```

6. Check to make sure the forwarding entry and route data base are in sync
7. Check RSVP LSP statistics for transmitted packets **`show mpls stats-lsp`**
8. Check MPLS forwarding statistics for transmitted packets **`show mpls stats-ftn`**

Isolating the cause and corrective action

- Is CSPF at fault? For RSVP session with CSPF enabled, ensure that the underlying protocol used is OSPF. Issue the command ip ospf-te database for the TE-database information. You can isolate the problem by disabling CSPF from the LSP and check for the session establishment.
- Is QOS at fault? Check to see if there any policies configured and if that is giving the problem. Isolate the problem by removing the policies. Also isolate the problem by removing the QoS parameters from the LSP.
- Is Forwarding at fault? Is Configuration correct in the peer routers, and in the entire Lsp path? Execute the command **`traffic-eng-lsp-restart`** in lsp mode to restart the particular lsp. Check to see if the session comes up after the traffic is flowing correctly. Execute the command **`clear rsvp session all`** to restart all the rsvp sessions. Check to see if the session comes up and the traffic is flowing correctly. Delete the particular session and then create with the same configuration. Check for the session establishment. Apart from the protocol the problem may be related to another system. Shut down and restart the incoming and outgoing interfaces. If there is a problem, take appropriate actions to fix it, then check to see if LSP is operating as expected. If problem still exist, contact Avaya support for help.

Troubleshooting L2 circuit

This section details the steps and commands used to troubleshoot L2 circuits.

Comments? infodev@avaya.com

Static L2 circuit

For static L2VPN VC, since there is no signaling, most problems might be due to the configuration and forwarding plane. Follow the below steps to troubleshoot the problem.

Procedure steps

1. Ensure all MPLS prerequisites are satisfied.
2. Ensure the static L2VPN FTN and static L2VPN ILM are configured properly with valid interface and labels **show mpls static-l2-circuit-ftn show mpls static-l2-circuit-ilm**
3. Ensure the VPN is configured with the correct VC ID and peer IP address **show mpls l2-circuit**
4. Ensure there is an underlying MPLS tunnel to the destination. The MPLS tunnel can be RSVP,LDP or static tunnel.
5. Check the Tunnel is UP and running and verify the session, forwarding entry, and route data base are in sync: **show mpls table-forwarding show ip route show ip route database**
6. Check the static L2VPN VC statistics for transmitted packets **show mpls stats-vc**

```
SR4134# show mpls stats-vc
VC-ID  VC-Name  Up       Rx       Rx       Tx       Tx       Discarded   Discarded
                Time     Bytes    Pkts     Bytes    Pkts     Rx Pkts     Tx Pkts

200    vpn2    0h:11m   19704    241      19704    241      0           0
```

7. Check the MPLS forwarding statistics for L2VPN traffic **show mpls stats-ftn show mpls stats-interface**
8. If the statistics are not getting updated, check the incoming data packet: **show interface <interface name>**

Dynamic L2 circuit

Follow the below steps to troubleshoot the problem:

Procedure steps

1. Ensure all MPLS prerequisites are satisfied.
2. Ensure the MPLS L2VPN is configured with required VC ID and the peer IP address: **show mpls l2-circuit**
3. Ensure there is an LDP session to the destination: **show ldp session**

4. Check the L2 Circuit status information: **show ldp mpls-l2-circuit**
5. Debug LDP signaling for l2 circuit: **debug ldp vc**
6. Check the MPLS forwarding statistics for L2VPN traffic: **show mpls stats-ftn show mpls stats-interface**
7. If the statistics are not getting updated, check the incoming data packet: **show interface <interface name>**

Comments? infodev@avaya.com

Chapter 10: Troubleshooting unicast routing

Use the information in this section to assist you in troubleshooting issues with unicast routing.

Begin troubleshooting routing issues by verifying that the IP interfaces in the system are "up". Use the following commands to check the status of IP interfaces: **`show ip interfaces format brief`** (IPv4) **`show ipv6 interfaces format brief`** (IPv6)

Use the ping feature to perform reachability tests for a specific destination. A useful ping option is the sweep that tests for varied packet sizes. For example: **`ping 10.0.0.1 sweepmin 36 sweepmax 1500`**

The ping "sweep" option helps to identify issues with particular packet sizes in the network. Routing protocols send varied sizes of packets. Drops of specific sizes can affect the routing operations.

When routing protocol adjacencies are "stuck", and certain packets are not flowing properly over specific interfaces, enter the **`shutdown`** command followed by the **`no shutdown`** command on that interface to try and clear the issue.

The route tracing feature is also useful in identifying points of failure in the network. You use route tracing for network testing and management. A route tracing command records the route (the specific gateway address at each hop) through the Internet between your source device and a specified destination device. Route tracing also calculates and displays the duration of time from each hop to the next.

The Avaya Secure Router 2330/4134 provides tools for tracing an IPv4 route and an IPv6 route. For information about multicast route tracing, see Troubleshooting multicast routing on page 153.

Procedure steps

1. To trace an IPv4 route, enter:

   ```
   trace <WORD> [sipaddress <ipaddr>] [proto {icmp|udp}] [timeout
   <value>] [probecnt <value>] [minttl <value>] [maxttl <value>] [portno
   <port>] [symdisp {on|off}]
   ```

2. To trace an IPv6 route, enter:

   ```
   trace6 <WORD> [sipaddress <ipaddr>] [proto {icmp|udp}] [timeout
   <value>] [probecnt <value>] [minttl <value>] [maxttl <value>] [portno
   <port>] [symdisp {on|off}]
   ```

3. To end a route trace, enter the following keyboard escape sequence:

   ```
   CTRL + C
   ```

Table 47: Variable definitions

Variable	Value
maxttl <value>	The maximum time-to-live value (that is, number of hops before the probe packet is dropped). The trace ends when the destination is reached, or when the TTL value is reached, whichever occurs first. Values are in the range 1 to 255. The default value is 1.
minttl <value>	The minimum time-to-live value (that is, the minimum number of hops you want the packet to make). Values are in the range 1 to 255.
portno <port>	The destination port used by the UDP probe. The default port number is 33434. You can enter a port number in the range 1 to 65535.
probecnt <value>	The number of probe packets to send. The default value is 3. Valid values are in the range 1 to 65535.
proto {icmp | udp}	The probe packet protocol. Enter either icmp or udp. The default value is udp.
sipaddress <ipaddr>	The source IP address for the probing packet. Enter the IP address in IPv4 format if you are using the **`trace`** command. Enter the IP address in IPv6 format (the address prefix and IPv6 interface ID) if you are using the **`trace6`** command.
symdisp {on | off}	The symbolic display toggle. Symbolic display is either on or off (turn off symbolic display if you prefer to have numeric display only). Symbolic display is turned on by default.
timeout <value>	Timeout value for the probe packet. Valid values are in the range 1 to 3600 seconds. The default value is 5 seconds.
<WORD>	The target host name or IP address. There is no default value.

The route table

The system route table contains the best routes learnt through different protocols and includes the connected and static routes. The route table is, therefore, the best place to find which networks are reachable by the system.

Comments? infodev@avaya.com

For the routing table display that consists of all the active routes (not recommended when you have a large number of routes), enter: `show ip route` `show ipv6 route`

For a quick quantitative status of the number of routes for each protocol, enter: `show ip route summary` `show ipv6 route summary`

To display the routes learned from a specific protocol (for example, OSPF), enter: `show ip route ospf` `show ipv6 route ospf`

To display routing table information that consists of all the active, inactive, and non-preferred routes (not recommended when you have a large number of routes), enter: `show ip route database` `show ipv6 route database`

Ensure you always verify the presence of the route for a specific network or destination. Enter the following commands to display information about routes for a specific network or destination:

- `show ip route <ipaddr>` (for example, `show ip route 10.0.0.1`)
- `show ip route <ipaddr/mask>` (for example, `show ip route 10.0.0.0/8`)

A route must be “selected" (>) and “FIB" (*) for it to be active and in operation in the forwarding plane. The preceding command options for displaying the entire database or a specific destination provide this detail.

If the route is available but not active, take corrective action to ensure the gateway is reachable and that the gateway interface is "up".

If the expected route is not present, then perform troubleshooting tasks within the respective protocol. The following sections provide information for troubleshooting within a protocol:

- Troubleshooting OSPF on page 127
- Troubleshooting BGP on page 131
- Troubleshooting RIP on page 134

For information about VRRP debug command options, see Debug command options for VRRP on page 149.

Troubleshooting OSPF

Use the **`show`** and **`debug`** commands in this section for debugging issues related to the OSPF routing protocol behavior, including issues related to the OSPF routes.

OSPF debug options

You can enable the debug options selectively at the global level for different aspects of the OSPF protocol behavior. The following figure shows the **`debug ospf`** options for an IPv4 network.

```
SR4134# debug ospf ?

      all                       Enable/disable all Debugging
      events                    OSPF events information
      ifsm                      OSPF Interface State Machine
      lsa                       OSPF Link State Advertisement
      nfsm                      OSPF Neighbor State Machine
      nsm                       OSPF RIB information
      packet                    OSPF packets
      route                     OSPF route information
```

Figure 3: debug ospf command options for IPv4 network

The following figure shows the **debug ipv6 ospf** options for an IPv6 network.

```
SR4134# debug ipv6 ospf ?

     all                        Enable/disable all Debugging
     events                     OSPFv3 event
     ifsm                       OSPFv3 Interface State Machine
     lsa                        OSPFv3 Link State Advertisement
     nfsm                       OSPFv3 Neighbor State Machine
     nsm                        OSPFv3 RIB information
     packet                     OSPFv3 packets
     route                      OSPFv3 route information
```

Figure 4: debug ipv6 ospf command options for IPv6 network

You can also debug issues with adjacencies and packet flows on specific interfaces. To debug issues at the interface, enable OSPF packet tracing on a specific interface. The following figure shows IPv4 command options for OSPF packet tracing on an interface.

```
SR4134/configure/interface/ethernet (0/1)# ip ospf debug packet ?
  dd                            OSPF Database Description
  detail                        Detail information
  hello                         OSPF Hello
  ls-ack                        OSPF Link State Acknowledgment
  ls-request                    OSPF Link State Request
  ls-update                     OSPF Link State Update
  recv                          Packet received
  send                          Packet sent
     <cr>
```

Figure 5: ip ospf debug packet command options for IPv4 network

The following figure shows IPv6 command options for OSPF packet tracing on an interface.

Comments? infodev@avaya.com

```
SR4134/configure/interface/ethernet (0/1)# ipv6 ospf debug packet ?
  dd                            OSPF Database Description
  detail                        Detail information
  hello                         OSPF Hello
  ls-ack                        OSPF Link State Acknowledgment
  ls-request                    OSPF Link State Request
  ls-update                     OSPF Link State Update
  recv                          Packet received
  send                          Packet sent
     <cr>
```

Figure 6: ipv6 ospf debug packet command options for IPv6 network

For debugging issues related to adjacency formation, the following options can be particularly useful:

- **`ip ospf debug packet`** (on a specific interface) **`ipv6 ospf debug packet`** (on a specific interface)
- **`debug ospf nfsm`** **`debug ipv6 ospf nfsm`**
- **`debug ospf ifsm`** **`debug ipv6 ospf ifsm`**

For debugging issues related to OSPF database calculations, SPF, LSA generation and processing, and related aspects, use the following specific command options:

- **`debug ospf lsa`** **`debug ipv6 ospf lsa`**
- **`debug ospf events`** **`debug ipv6 ospf events`**
- **`debug ospf route`** **`debug ipv6 ospf route`**

The following figure shows the **`debug ospf lsa`** command options for an IPv4 network.

```
SR4134# debug ospf lsa ?
  flooding                      LSA Flooding
  generate                      LSA Generation
  install                       LSA Installation
  maxage                        LSA MaxAge processing
  refresh                       LSA Refreshment
     <cr>
```

Figure 7: debug ospf lsa command options

The following figure shows the **`debug ospf events`** command options for an IPv4 network.

```
SR4134# debug ospf events ?
  abr                           OSPF ABR events
  asbr                          OSPF ASBR events
  lsa                           OSPF LSA events
  nssa                          OSPF NSSA events
  os                            OSPF OS interaction events
  router                        OSPF router events
  vlink                         OSPF Virtual-Link events
     <cr>
```

Figure 8: debug ospf events command options

The following figure shows the **`debug ospf route`** command options for an IPv4 network.

```
SR4134# debug ospf route ?
  ase                           External route calculation information
  ia                            Inter-Area route calculation information
  install                       Route installation information
  spf                           SPF calculation information
     <cr>
```

Figure 9: debug ospf route command options

For more information about the **debug ospf** commands for IPv4, see Debug command options for OSPF on page 136. For information about the **debug ospf** commands for IPv6, see Debug command options for OSPFv3 for IPv6 on page 140.

OSPF show command options

You can use CLI **show** commands to help you troubleshoot OSPF issues.

Use the following **show** commands for issues related to adjacency, interface, and associated attributes, and status:

- **show ip ospf interface** **show ipv6 ospf interface**
- **show ip ospf neighbor detail** **show ipv6 ospf neighbor detail**

Use the following commands for a quick summary of the OSPF operations and configuration on the system:

- **show ip ospf** **show ipv6 ospf**
- **show ip protocols ospf** **show ipv6 protocols ospf**

Use the following commands and related options to collect very specific information when troubleshooting the OSPF route database: **show ip ospf database** **show ipv6 ospf database**

The OSPF route database includes LSA information (both detailed and summary) in the network. The following figure shows commands options for the OSPF route database for an IPv4 network.

```
SR4134# show ip ospf database ?

      adv-router                Advertising Router Link states
      asbr-summary              ASBR summary link states
      database-summary          Summary of database
      external                  External link states
      max-age                   LSAs in MaxAge list
      network                   Network link states
      nssa-external             NSSA external link state
      opaque-area               Link area Opaque-LSA
      opaque-as                 Link AS Opaque-LSA
      opaque-link               Link local Opaque-LSA
      router                    Router link states
      self-originate            Self-originated link states
      summary                   Network summary link states

      <cr>
```

Figure 10: show ip ospf database command options

The **summary** option gives you a quick overview of the LSA types present in the system and the network, which is a good starting point for discovering missing routes or LSAs: **show ip**

Comments? infodev@avaya.com

ospf database database-summary **show ipv6 ospf database database-summary**

Other CLI commands that you can use to collect and debug specific problems are the following:

- **show ip ospf border-routers** **show ipv6 ospf border-routers**
- **show ip ospf virtual-links** **show ipv6 ospf virtual-links**
- **show ip ospf te-database**

OSPF clear command options

In certain extreme situations, you must completely delete the OSPF database and adjacencies to force the OSPF processes to rebuild the database. Use the following CLI commands to remove existing OSPF processes: **clear ip ospf** **clear ipv6 ospf**

Be aware that clearing the OSPF processes deletes all OSPF routes, affecting all adjacencies in the router, which also has a corresponding effect on the OSPF network.

Troubleshooting BGP

Use the **show** and **debug** commands in this section for debugging issues related to BGP routing behavior, including issues related to the BGP routes.

BGP debug options

You can enable the debug options selectively at the global level for different aspects of BGP behavior. The following figure shows the **debug bgp** options.

```
SR4134# debug bgp ?

     all                        all debugging
     dampening                  BGP Dampening
     events                     BGP events
     filters                    BGP filters
     fsm                        BGP Finite State Machine
     keepalives                 BGP keepalives
     nsm                        FIB message
     updates                    BGP updates

     <cr>
```

Figure 11: debug bgp command options

Begin with the following commands for debugging issues with BGP sessions:

- **debug bgp fsm**
- **debug bgp events**

Use the following commands for debugging issues with BGP route update processing, including policy filters:

- **debug bgp updates {in|out}**
- **debug bgp filters**

For more information about the **debug bgp** commands for IPv4 and IPv6, see Debug command options for BGP and BGP+ for IPv6 on page 143.

BGP show options

There are many **show** commands available for troubleshooting BGP operations. The BGP **show** commands provide information that ranges from a quick summary or status of peers to very detailed filters for displaying BGP routes, and even how and which routes are affected by the BGP policies on the system.

Begin with the following commands for troubleshooting issues related to BGP peering sessions, or to get a quick summary of information on the prefixes and routes received from specific neighbors:

- **show bgp all neighbors** **show bgp ipv6 neighbors**
- **show bgp all summary** **show bgp ipv6 summary**
- **show ip protocols bgp**

Use the following commands to get information about the BGP routes learned and the route status: **show bgp ipv4** **show bgp ipv6**

The following figure shows the command syntax to use to get more detailed and complete information about routes to a specific destination or network (IPv4 network):

```
SR4134# show bgp ipv4 ?
  A.B.C.D                     IP prefix <network>, e.g.,35.0.0.0
  A.B.C.D/M                   IP prefix <network>/<length>,
                              e.g.,35.0.0.0/8
```

Figure 12: show bgp ipv4 command options for specifying destination

The following figure shows the command syntax to use to get more detailed and complete information about routes to a specific destination or network (IPv6 network):

```
SR4134# show bgp ipv6 ?
  X:X::X:X                    IPv6 prefix <network>, e.g.,2003::
  X:X::X:X/M                  IPv6 prefix <network>/<length>,
                              e.g.,2003::/16
```

Figure 13: show bgp ipv6 command options for specifying destination

BGP routes can be subjected to various policy configurations that can change the route attributes. Also, certain features (for example, dampening) can cause the routes to be suppressed in the event of excessive route flaps. It is often useful to selectively see the routes that are affected or modified as a result of a specific policy, attribute, or dampening when

Comments? infodev@avaya.com

debugging issues with BGP routes and the route attributes. The following figure shows the CLI commands, as well as the options, that you can use to find specific information.

```
SR4134# show bgp all ?

     attribute-info          List all bgp attribute information
     community               Display routes matching the communities
     community-info          List all bgp community information
     community-list          Display routes matching the community-list
     dampening               Display detailed information about dampening
     filter-list             Display routes conforming to the filter-list
     inconsistent-as         Display routes with inconsistent AS Paths
     neighbors               Detailed information on TCP and BGP neighbor
                             connections
     paths                   Path information
     peer-group              Display information on peer-groups
     prefix-list             Display routes matching the prefix-list
     quote-regexp            Display routes matching the AS path regular
                             expression (Quoted string)
     regexp                  Display routes matching the AS path regular
                             expression
     route-map               Display routes matching the route-map
     scan                    BGP scan status
     summary                 Summary of BGP neighbor status

     <cr>
```

Figure 14: show bgp all command options

BGP clear options

In certain extreme situations, you must completely delete all BGP routes or selectively delete routes based on specific filters such as peer, AS, and so on. The following figure shows the CLI command options you use to clear BGP routes.

```
SR4134# clear bgp all ?
  *                           Clear all peers
     or
  v4                          Clear all ipv4 peers
     or
  v6                          Clear all ipv6 peers
     or
   1  -  65535                Clear peers with the AS number

     or
  A.B.C.D                     BGP neighbor address to clear
     or
  X:X::X:X                    BGP neighbor address to clear
     or
  dampening                   Clear route flap dampening information
     or
  external                    Clear all external peers
     or
  flap-statistics             Clear route flap statistics
     or
  peer-group                  Clear all members of peer-group
```

Figure 15: clear bgp all command options

You can also selectively delete BGP routes based on the Secure Router 2330/4134 either generating or receiving the updates. Configure features such as soft-reconfiguration and route-refresh to help avoid disruptions in the network and to provide a quick recovery and reconvergence from the **clear** operation. In the absence of these features, clearing routes can cause routes to flap throughout the BGP network.

Troubleshooting RIP

Use the **show** and **debug** commands in this section for debugging issues related to RIP routing behavior, including issues related to the RIP routes.

RIP debug options

You can enable the debug options selectively at the global level for different aspects of RIP behavior. The following figure shows the **debug rip** options.

```
SR4134# debug rip ?

     all                         Enable all Debugging
     events                      RIP events
     nsm                         RIP RIB information
     packet                      RIP packets

     <cr>
```

Figure 16: debug rip command options

The following figure shows the **debug ipv6 rip** options.

```
SR4134# debug ipv6 rip ?

     all                          Enable all Debugging
     events                       RIPng events
     nsm                          RIPng and  NSM communication
     packet                       RIPng packets

     <cr>
```

Figure 17: debug ipv6 rip command options

Use the following commands for debugging issues related to route learning and packet flows:

- **debug rip packet** **debug ipv6 rip packet**
- **debug rip events** **debug ipv6 rip events**

For more information about the **debug rip** commands for IPv4, see Debug command options for RIP on page 146. For more information about the **debug ipv6 rip** commands for IPv6, see Debug command options for RIPng for IPv6 on page 147.

RIP show options

Use the RIP **show** commands to help you troubleshoot.

Use the following commands for a quick summary of information about the status of the RIP operations and the high-level configuration options: **show ip protocols rip** **show ipv6 protocols rip**

Use the following command for issues related to interfaces, the status, and associated attributes: **show ip rip interface** **show ipv6 rip interface**

Use the following commands to access the current RIP route database and to troubleshoot issues that relate to RIP routes:

- **show ip rip** **show ipv6 rip**
- **show ip rip database** **show ipv6 rip database**

RIP clear options

In certain situations, you must delete specific RIP routes to delete stale information, or you must force RIP to delete its entire database and relearn all routes. The following figure shows the CLI command options you use to clear RIP routes on an IPv4 network.

```
SR4134# clear ip rip route ?
  all                          all of the RIP routing table
  bgp                          Border Gateway Protocol(BGP)
  connected                    connected
  isis                         ISO ISIS
  ospf                         Open Shortest Path First
  rip                          Routing Information Protocol
  static                       static Routes
     or
  A.B.C.D/M                    IP prefix <network>/<length>, e.g.,
                              10.0.0.0/8
```

Figure 18: clear ip rip route command options

The following figure shows the CLI command options you use to clear RIP routes on an IPv6 network.

```
SR4134# clear ipv6 rip route ?
  all                          all of the RIPng routing table
  bgp                          Border Gateway Protocol (BGP)
  connected                    Connected
  ospf                         Open Shortest Path First (OSPF)
  rip                          Routing Information Protocol (RIP)
  static                       Static routes
    or
  X:X::X:X/M                   IPv6 route <prefix>/<prefixlen>, e.g.,
                               3ffe::/16
```

Figure 19: clear ipv6 rip route command options

Be aware that clearing RIP routes deletes the specified routes. RIP routes are relearned after the next advertisement, which can affect routing in the RIP network.

Debug command options for OSPF

This section describes debug command options that you use to troubleshoot issues with OSPF.

debug ospf

Use this command to configure OSPF debugging.

Syntax

```
[no] debug ospf
```

Example

```
SR# debug ospf
```

debug ospf events

Use this command to debug OSPF event information.

Syntax

```
[no] debug ospf events <event>
```

Table 48: Variable definition

Variable	Value
<event>	The event type. Available options are: • abr - ABR events • asbr - ASBR events • lsa - LSA events • nssa - NSSA events • os - OS interaction events • router - Router events • vlink - Virtual-Link events

Example

```
SR# debug ospf events nssa
```


Comments? infodev@avaya.com

debug ospf ifsm

Use this command to debug OSPF Interface State Machine.

Syntax

```
[no] debug ospf ifsm [events|status|timers]
```

Table 49: Variable definition

Variable	Value
[events]	IFSM event information.
[status]	IFSM status information.
[timers]	IFSM timer information.

Example

```
SR# debug ospf ifsm timers
```

debug ospf lsa

Use this command to debug OSPF Link State Advertisement.

Syntax

```
[no] debug ospf lsa [flooding|generate|install|maxage|refresh]
```

Table 50: Variable definition

Variable	Value
[flooding]	LSA flooding.
[generate]	LSA generation.
[install]	LSA installation.
[maxage]	LSA maximum age processing.
[refresh]	LSA refreshment.

Example

```
SR# debug ospf lsa install
```

debug ospf nfsm

Use this command to debug OSPF Neighbor State Machine.

Syntax

```
[no] debug ospf nfsm [events|status|timers]
```

Table 51: Variable definition

Variable	Value
[events]	NFSM event information.
[status]	NFSM status information.
[timers]	NFSM timer information.

Example

```
SR# debug ospf nfsm status
```

debug ospf nsm

Use this command to debug OSPF RIB information.

Syntax

```
[no] debug ospf nsm [interface|redistribute]
```

Table 52: Variable definition

Variable	Value
[interface]	The RIB interface.
[redistribute]	RIB redistribution.

Example

```
SR# debug ospf nsm interface
```

debug ospf packet

Use this command to debug OSPF packets.

Syntax

```
[no] debug ospf packet <pkttype>
```

Table 53: Variable definition

Variable	Value
<pkttype>	The packet type. Available choices are:

Comments? infodev@avaya.com

Variable	Value
	• dd - database description • detail - detail information • hello - hello • ls-ack - link state acknowledgement • ls-request - link state request • ls-update - link state update • recv - received packets • send - sent packets

Example

```
SR# debug ospf packet dd
```

debug ospf route

Use this command to debug OSPF route information.

Syntax

```
[no] debug ospf route [ase|ia|install|spf]
```

Table 54: Variable definition

Variable	Value
[ase]	External route calculation information.
[ia]	Inter-area route calculation information.
[install]	Route installation information.
[spf]	SPF calculation information.

Example

```
SR# debug ospf route ase
```

debug ospf all

Use this command to enable or disable all OSPF debugging.

Syntax

```
[no] debug ospf all
```

Example

```
SR# debug ospf all
```

Debug command options for OSPFv3 for IPv6

This section describes debug command options that you use to troubleshoot issues with OSPFv3 for IPv6.

debug ipv6 ospf events

Use this command to debug OSPFv3 events.

```
debug ipv6 ospf events <event>
```

Table 55: Variable definition

Variable	Value
<event>	The type of event. Possible choices are: • **abr** - OSPF ABR events • **asbr** - OSPF ASBR events • **lsa** - OSPF LSA events • **nssa** - OSPF NSSA events • **os** - OSPF OS interaction events • **router** - OSPF router events • **vlink** - OSPF virtual-link events

debug ipv6 ospf ifsm

Use this command to debug OSPFv3 Interface State Machine.

```
debug ipv6 ospf ifsm [<events>|<status>|<timers>]
```

Table 56: Variable definition

Variable	Value
<events>	IFSM event information.

Comments? infodev@avaya.com

Variable	Value
<status>	IFSM status information.
<timers>	IFSM timer information.

debug ipv6 ospf lsa

Use this command to debug OSPFv3 Link State Advertisement.

```
debug ipv6 ospf lsa [<flooding>|<generate>|<install>|<maxage>|
<refresh>]
```

Table 57: Variable definition

Variable	Value
<flooding>	LSA flooding.
<generate>	LSA generation.
<install>	LSA Installation.
<maxage>	LSA MaxAge processing.
<refresh>	LSA Refreshment.

debug ipv6 ospf nfsm

Use this command to debug OSPFv3 Neighbor State Machine.

```
debug ipv6 ospf nfsm [<events>|<status>|<timers>]
```

Table 58: Variable definition

Variable	Value
<events>	NFSM event information.
<status>	NFSM status information.
<timers>	NFSM timer information.

debug ipv6 ospf nsm

Use this command to debug OSPFv3 RIB information.

```
debug ipv6 ospf nsm [<interface>|<redistribute>]
```

Table 59: Variable definition

Variable	Value
<interface>	RIB interface.
<redistribute>	RIB redistribute.

debug ipv6 ospf packet

Use this command to debug OSPFv3 packets.

```
debug ipv6 ospf packet [<dd>|<detail>|<hello>|<ls-ack>|<ls-
request>|<ls-update>|<recv>|<send>]
```

Table 60: Variable definition

Variable	Value
<dd>	OSPF database description.
<detail>	Detailed information.
<hello>	OSPF Hello.
<ls-ack>	OSPF Link-state acknowledgement.
<ls-request>	OSPF Link-state request.
<ls-update>	OSPF Link-state update.
<recv>	Packets received.
<send>	Packets sent.

debug ipv6 ospf route

Use this command to debug OSPFv3 route information.

```
debug ipv6 ospf route [<ase>|<ia>|<install>|<spf>]
```

Table 61: Variable definition

Variable	Value
<ase>	External route calculation information.
<ia>	Inter-area route calculation information.

Comments? infodev@avaya.com

Variable	Value
<install>	Route installation information.
<spf>	SPF calculation information.

debug ipv6 ospf all

Use this command to enable or disable all OSPFv3 debugging.

```
debug ipv6 ospf all
```

Debug command options for BGP and BGP+ for IPv6

This section describes debug command options that you use to troubleshoot issues with BGP and BGP+ for IPv6.

debug bgp

Use this command to debug the Border Gateway Protocol.

Syntax

```
[no] debug bgp
```

Example

```
SR# debug bgp
```

debug bgp all

Use this command to enable all BGP debugging features.

Syntax

```
[no] debug bgp all
```

Example

```
SR# debug bgp all
```

debug bgp dampening

Use this command to debug BGP dampening.

Syntax

```
[no] debug bgp dampening
```

Example

```
SR# debug bgp dampening
```

debug bgp events

Use this command to debug BGP events.

Syntax

```
[no] debug bgp events
```

Example

```
SR# debug bgp events
```

debug bgp filters

Use this command to debug BGP filters.

Syntax

```
[no] debug bgp filters
```

Example

```
SR# debug bgp filters
```

debug bgp fsm

Use this command to debug BGP Finite State Machine.

Syntax

```
[no] debug bgp fsm
```

Example

```
SR# debug bgp fsm
```


Comments? infodev@avaya.com

debug bgp keepalives

Use this command to debug BGP keepalives.

Syntax

```
[no] debug bgp keepalives
```

Example

```
SR# debug bgp keepalives
```

debug bgp nsm

Use this command to debug BGP FIB messages.

Syntax

```
[no] debug bgp nsm
```

Example

```
SR# debug bgp nsm
```

debug bgp updates

Use this command to debug BGP updates.

Syntax

```
[no] debug bgp updates <in|out>
```

Table 62: Variable definition

Variable	Value
<in>	Debug inbound updates.
<out>	Debug outgoing updates.

Example

```
SR# debug bgp updates in
```

show debug bgp

Use this command to display information about the BGP debugging option set.

Syntax

```
show debug bgp
```

Example

```
SR# show debug bgp
```

Debug command options for RIP

This section describes debug command options that you use to troubleshoot issues with RIP.

debug rip

Use this command to configure RIP debugging.

Syntax

```
[no] debug rip
```

Example

```
SR# debug rip
```

debug rip all

Use this command to enable all RIP debugging.

Syntax

```
[no] debug rip all
```

Example

```
SR# debug rip all
```

debug rip events

Use this command to debug RIP events.

Syntax

```
[no] debug rip events
```

Example

```
SR# debug rip events
```


Comments? infodev@avaya.com

debug rip nsm

Use this command to debug RIP RIB information.

Syntax

```
[no] debug rip nsm
```

Example

```
SR# debug rip nsm
```

debug rip packet

Use this command to debug RIP packets.

Syntax

```
[no] debug rip packet <detail|recv|send>
```

Table 63: Variable definition

Variable	Value
<detail>	Detailed information displayed.
<recv>	Debug RIP receive packets.
<send>	Debug RIP send packets.

Example

```
SR# debug rip packet detail
```

Debug command options for RIPng for IPv6

This section describes debug command options that you use to troubleshoot issues with RIPng for IPv6.

debug ipv6 rip

Use this command to enable RIP debugging for IPv6.

Syntax

```
[no] debug ipv6 rip
```

Example

```
SR# debug ipv6 rip
```

debug ipv6 rip all

Use this command to enable all RIP debugging.

Syntax

```
[no] debug ipv6 rip all
```

Example

```
SR# debug ipv6 rip all
```

debug ipv6 rip events

Use this command to debug RIPng events.

Syntax

```
[no] debug ipv6 rip events
```

Example

```
SR# debug ipv6 rip events
```

debug ipv6 rip nsm

Use this command to debug RIPng and NSM communications.

Syntax

```
[no] debug ipv6 rip nsm
```

Example

```
SR# debug ipv6 rip nsm
```

debug ipv6 rip packet

Use this command to debug RIPng packets.

Syntax

```
[no] debug ipv6 rip packet
```

Example

```
SR# debug ipv6 rip packet
```

debug ipv6 rip packet detail

Use this command to display detailed information.

Syntax

```
[no] debug ipv6 rip packet detail
```

Example

```
SR# debug ipv6 rip packet detail
```

debug ipv6 rip packet recv

Use this command to debug RIPng receive packets.

Syntax

```
[no] debug ipv6 rip packet recv
```

Example

```
SR# debug ipv6 rip packet recv
```

debug ipv6 rip packet send

Use this command to debug RIPng send packets.

Syntax

```
[no] debug ipv6 rip packet send
```

Example

```
SR# debug ipv6 rip packet send
```

Debug command options for VRRP

This section describes debug command options that you use to troubleshoot issues with VRRP.

debug ip vrrp

Use this command to enable or disable VRRP debugging.

Syntax

```
[no] debug ip vrrp
```

Example

```
SR# debug ip vrrp
```

debug ip vrrp all

Use this command to debug all VRRP messages.

Syntax

```
[no] debug ip vrrp all
```

Example

```
SR# debug ip vrrp all
```

debug ip vrrp error

Use this command to debug VRRP error messages.

Syntax

```
[no] debug ip vrrp error
```

Example

```
SR# debug ip vrrp error
```

debug ip vrrp state

Use this command to debug VRRP state transitions.

Syntax

```
[no] debug ip vrrp state
```

Example

```
SR# debug ip vrrp state
```

debug ip vrrp events

Use this command to debug all VRRP events.

Syntax

```
[no] debug ip vrrp events
```


Comments? infodev@avaya.com

Example

```
SR# debug ip vrrp events
```

debug ip vrrp packet

Use this command to debug VRRP packet errors.

Syntax

```
[no] debug ip vrrp packet
```

Table 64: Variable definition

Variable	Value
<all>	All packets.
<arp>	ARP packets.
<recv>	Packets received.
<send>	Packets sent.

Example

```
SR# debug ip vrrp packet [<all>|<arp>|<send>|<recv>]
```

Comments? infodev@avaya.com

Chapter 11: Troubleshooting IPv4 and IPv6 multicast routing

This section describes commands that you use to troubleshoot multicast routing.

Troubleshooting multicast routing

Begin troubleshooting multicast routing issues by verifying that the IP interfaces in the system are "up". Use the following commands to check the status of IP interfaces: **`show ip interfaces format brief`** (IPv4) **`show ipv6 interfaces format brief`** (IPv6)

If you use PIM as the multicast routing protocol, it relies on the routes learned through the unicast routing protocols for building the multicast delivery trees. Troubleshooting for multicast routing with PIM, therefore, should start with the verification of unicast reachability. For more information, see Troubleshooting unicast routing on page 125.

The multicast route tracing feature is also useful in tracing the multicast distribution tree for specific groups and sources in the network. The multicast traceroute tool (mtrace) is similar to the traceroute tool for unicast traffic. Use **`mtrace`** to trace IPv4 multicast traffic flow routes. Unlike unicast route tracing, multicast route tracing basically prints a path from the receiver to the source. Issue the following multicast traceroute command from the root of the CLI: **`mtrace <source> [<destination>] [<group>] [<ttl>]`**

Table 65: Variable definitions

Variable	Value
<source>	IP address of a multicast-capable source. You must enter information for this parameter.
[<destination>]	Address of the unicast destination. This parameter is optional. If omitted, the multicast traceroute starts from the system at which you enter the command.
[<group>]	Multicast address of the group to be traced. This parameter is optional.
[<ttl>]	Time-to-live (TTL) threshold for a multicast trace request. The range of values is 1 to 255 router hops. This parameter is optional. The default value is 255.

The following is an example of a multicast route trace:

```
SR# mtrace 80.0.0.10 30.0.0.1 227.0.0.1 Type escape sequence to abort
Querying full reverse path... 0 30.0.0.1 - 1 50.0.0.1 PIM - 2 50.0.0.4
- 3 70.0.0.4 PIM - 4 70.0.0.5 - 5 80.0.0.5 PIM [PRUNE SENT]
```

Use the following CLI **show** commands to determine which interfaces on the router have multicast routing enabled: **show ip mvif show ipv6 mvif**

You must enable multicast routing at the global level. If you do not enable multicast routing globally, the multicast routing protocols do not become operational even if you enable individual protocols. Use the following command to enable multicast routing at the global level: `SR/configure#` **ip multicast-routing** (IPv4) `SR/configure#` **ipv6 multicast-routing** (IPv6)

Use the following commands to determine the multicast forwarding entries currently in use (that is, for traffic that is being forwarded): **show ip mroute <source or group ipaddr> [summary] show ipv6 mroute <group ipaddr> [summary]**

The command has options to filter based on the source and the group. The following are examples of the **show ip mroute** command for an IPv4 network:

- **show ip mroute 10.0.0.1**
- **show ip mroute 10.0.0.1 229.0.0.1**
- **show ip mroute 229.0.0.1**
- **show ip mroute 229.0.0.1 10.0.0.1**

The preceding **show** command provides details of the multicast forwarding entry including the incoming interface, the list of outgoing interfaces, as well as when the entry was created. The "up" time and expiry time is useful for determining how long the entry has been active, and for detecting disruptions.

Note that even though the multicast path may be set up in the multicast routing protocol control path, the multicast forwarding entry is created only when data actually starts to flow.

Use the "summary" option with the preceding **show** command for an overview of the multicast forwarding entries.

When troubleshooting multicast forwarding, it can be necessary to clear all entries or certain specific entries. This is very useful as a workaround for issues where entries are caught in an inconsistent state. Clearing entries triggers a clean state setup. Enter the following commands to clear all entries: **clear ip mroute all clear ipv6 mroute all**

Enter the following commands to clear specific entries: **clear ip mroute <group ipaddr> [source ipaddr] clear ipv6 mroute <group ipaddr> [source ipaddr]**

The following are examples of the **clear ip mroute** command for an IPv4 network:

- **clear ip mroute 229.0.0.1**
- **clear ip mroute 229.0.0.1 10.0.0.1**

The **clear ip mroute** command not only deletes the entries in the forwarding plane, but also ensures that the corresponding states in the multicast routing protocol (viz. DVMRP and

Comments? infodev@avaya.com

PIM-SM), as well as IGMP, are deleted. Everything associated with the multicast state is cleared and relearned by the protocols, which helps to resolve issues related to multicast tree setup and forwarding.

Be aware that this command affects the associated multicast flows and causes disruptions in the traffic flow.

IPv4 Multicast debugging commands

debug ip multicast

Use this command to debug IP multicast information.

Syntax

```
[no] debug ip multicast
```

Example

```
SR# debug ip multicast
```

debug ip multicast all

Use this command to enable all IPv4 multicast debugging.

Syntax

```
[no] debug ip multicast all
```

Example

```
SR# debug ip multicast all
```

debug ip multicast fib-msg

Use this command to debug multicast FIB messages.

Syntax

```
[no] debug ip multicast fib-msg
```

Example

```
SR# debug ip multicast fib-msg
```

debug ip multicast mrt

Use this command to debug a multicast route.

Syntax

```
[no] debug ip multicast mrt
```

Example

```
SR# debug ip multicast mrt
```

debug ip multicast register

Use this command to debug multicast PIM Register messages.

Syntax

```
[no] debug ip multicast register
```

Example

```
SR# debug ip multicast register
```

debug ip multicast stats

Use this command to debug multicast statistics.

Syntax

```
[no] debug ip multicast stats
```

Example

```
SR# debug ip multicast stats
```

debug ip multicast vif

Use this command to debug multicast interface information.

Syntax

```
[no] debug ip multicast vif
```

Example

```
SR# debug ip multicast vif
```


Comments? infodev@avaya.com

Troubleshooting DVMRP

DVMRP debugging commands

debug dvmrp

Use this command to access DVMRP debugging commands.

Syntax

```
[no] debug dvmrp
```

Example

```
SR# debug dvmrp
```

debug dvmrp all

Use this command to enable all DVMRP debugging.

Syntax

```
[no] debug dvmrp all
```

Example

```
SR# debug dvmrp all
```

debug dvmrp events

Use this command to debug DVMRP events.

Syntax

```
[no] debug dvmrp events
```

Example

```
SR# debug dvmrp events
```

debug dvmrp events igmp

Use this command to debug DVMRP IGMP events.

Syntax

```
[no] debug dvmrp events igmp
```

Example

```
SR# debug dvmrp events igmp
```

debug dvmrp events kernel

Use this command to DVMRP kernel events.

Syntax

```
[no] debug dvmrp events kernel
```

Example

```
SR# debug dvmrp events kernel
```

debug dvmrp events neighbor

Use this command to debug DVMRP neighbor events.

Syntax

```
[no] debug dvmrp events neighbor
```

Example

```
SR# debug dvmrp events neighbor
```

debug dvmrp events packet

Use this command to debug DVMRP packet events.

Syntax

```
[no] debug dvmrp events packet
```

Example

```
SR# debug dvmrp events packet
```

debug dvmrp events prune

Use this command to debug DVMRP prune events.

Syntax

```
[no] debug dvmrp events prune
```


Comments? infodev@avaya.com

Example

```
SR# debug dvmrp events prune
```

debug dvmrp events route

Use this command to debug DVMRP route events.

Syntax

```
[no] debug dvmrp events route
```

Example

```
SR# debug dvmrp events route
```

debug dvmrp mfc

Use this command to debug multicast forwarding cache events.

Syntax

```
[no] debug dvmrp mfc
```

Example

```
SR# debug dvmrp mfc
```

debug dvmrp mib

Use this command to debug the DVMRP MIB.

Syntax

```
[no] debug dvmrp mib
```

Example

```
SR# debug dvmrp mib
```

debug dvmrp nsm

Use this command to debug FIB messages.

Syntax

```
[no] debug dvmrp nsm
```

Example

```
SR# debug dvmrp nsm
```

debug dvmrp packet

Use this command to debug all DVMRP packets.

Syntax

```
[no] debug dvmrp packet
```

Example

```
SR# debug dvmrp packet
```

debug dvmrp packet graft

Use this command to debug graft packets.

Syntax

```
[no] debug dvmrp packet graft
```

Example

```
SR# debug dvmrp packet graft
```

debug dvmrp packet graft-ack

Use this command to debug graft-ack packets.

Syntax

```
[no] debug dvmrp packet graft-ack
```

Example

```
SR# debug dvmrp packet graft-ack
```

debug dvmrp packet in

Use this command to debug incoming DVMRP packets.

Syntax

```
[no] debug dvmrp packet in
```

Example

```
SR# debug dvmrp packet in
```


Comments? infodev@avaya.com

debug dvmrp packet out

Use this command to debug outgoing DVMRP packets.

Syntax

```
[no] debug dvmrp packet out
```

Example

```
SR# debug dvmrp packet out
```

debug dvmrp packet probe

Use this command to debug probe packets.

Syntax

```
[no] debug dvmrp packet probe
```

Example

```
SR# debug dvmrp packet probe
```

debug dvmrp packet prune

Use this command to debug prune packets.

Syntax

```
[no] debug dvmrp packet prune
```

Example

```
SR# debug dvmrp packet prune
```

debug dvmrp packet report

Use this command to debug report packets.

Syntax

```
[no] debug dvmrp packet report
```

Example

```
SR# debug dvmrp packet report
```

debug dvmrp timer

Use this command to debug DVMRP timers.

Syntax

```
[no] debug dvmrp timer
```

Example

```
SR# debug dvmrp timer
```

debug dvmrp timer probe

Use this command to debug all probe timers.

Syntax

```
[no] debug dvmrp timer probe
```

Example

```
SR# debug dvmrp timer probe
```

debug dvmrp timer prune

Use this command to debug all prune timers.

Syntax

```
[no] debug dvmrp timer prune
```

Example

```
SR# debug dvmrp timer prune
```

debug dvmrp timer route

Use this command to debug all route timers.

Syntax

```
[no] debug dvmrp timer route
```

Example

```
SR# debug dvmrp timer route
```

Troubleshooting PIM-SM

PIM-SM debugging commands

debug pim

Use this command to access next-level PIM Sparse-Mode debugging commands.

Syntax

```
[no] debug pim
```

Example

```
SR# debug pim
```

debug pim sparse-mode

Use this command to debug PIM Sparse-Mode.

Syntax

```
[no] debug pim sparse-mode
```

Example

```
SR# debug pim sparse-mode
```

debug pim sparse-mode all

Use this command to enable all PIM debugging.

Syntax

```
[no] debug pim sparse-mode all
```

Example

```
SR# debug pim sparse-mode all
```

debug pim sparse-mode events

Use this command to debug PIM events.

Syntax

```
[no] debug pim sparse-mode events
```

Example

```
SR# debug pim sparse-mode events
```

debug pim sparse-mode mfc

Use this command to debug PIM MFC updates.

Syntax

```
[no] debug pim sparse-mode mfc
```

Example

```
SR# debug pim sparse-mode mfc
```

debug pim sparse-mode mib

Use this command to debug the PIM MIB.

Syntax

```
[no] debug pim sparse-mode mib
```

Example

```
SR# debug pim sparse-mode mib
```

debug pim sparse-mode nexthop

Use this command to debug the PIM next hop.

Syntax

```
[no] debug pim sparse-mode nexthop
```

Example

```
SR# debug pim sparse-mode nexthop
```

debug pim sparse-mode database

Use this command to debug PIM database information.

Syntax

```
[no] debug pim sparse-mode database
```

Example

```
SR# debug pim sparse-mode database
```

debug pim sparse-mode packet

Use this command to debug PIM packets.

Syntax

```
[no] debug pim sparse-mode packet <packettype>
```

Table 66: Variable definition

Variable	Value
<packettype>	The packet type to debug. Possible choices are: • **all** - All packets. • **hello** - Hello packets. • **register** - PIM register messages. • **jp** - Join/Prune messages. • **bsr** - BSR messages. • **assert** - PIM assert messages. • **crp** - CRP messages. • **in** - Incoming PIM packets. • **out** - Outgoing PIM packets.

Example

```
SR# debug pim sparse-mode packet in
```

debug pim sparse-mode state

Use this command to debug the PIM state.

Syntax

```
[no] debug pim sparse-mode state
```

Example

```
SR# debug pim sparse-mode state
```

debug pim sparse-mode timer

Use this command to debug PIM timers.

Syntax

```
[no] debug pim sparse-mode timer
```

Example

```
SR# debug pim sparse-mode timer
```

debug pim sparse-mode timer assert

Use this command to debug PIM assert timers.

Syntax

```
[no] debug pim sparse-mode timer assert
```

Example

```
SR# debug pim sparse-mode timer assert
```

debug pim sparse-mode timer bsr

Use this command to debug PIM bootstrap timers.

Syntax

```
[no] debug pim sparse-mode timer bsr
```

Example

```
SR# debug pim sparse-mode timer bsr
```

debug pim sparse-mode timer hello

Use this command to debug PIM hello timers.

Syntax

```
[no] debug pim sparse-mode timer hello
```

Example

```
SR# debug pim sparse-mode timer hello
```


Comments? infodev@avaya.com

debug pim sparse-mode timer joinprune

Use this command to debug PIM joinprune timers.

Syntax

```
[no] debug pim sparse-mode timer joinprune
```

Example

```
SR# debug pim sparse-mode timer joinprune
```

debug pim sparse-mode timer register

Use this command to debug PIM register timers.

Syntax

```
[no] debug pim sparse-mode timer register
```

Example

```
SR# debug pim sparse-mode timer register
```

Troubleshooting IGMP

IGMP debugging commands

debug igmp

Use this command to debug IGMP.

Syntax

```
[no] debug igmp
```

Example

```
SR# debug igmp
```

debug igmp all

Use this command to enable all IGMP debugging.

Syntax

```
[no] debug igmp all
```

Example

```
SR# debug igmp all
```

debug igmp decode

Use this command to enable IGMP decode debugging.

Syntax

```
[no] debug igmp decode
```

Example

```
SR# debug igmp decode
```

debug igmp encode

Use this command to enable IGMP encode debugging.

Syntax

```
[no] debug igmp encode
```

Example

```
SR# debug igmp encode
```

debug igmp events

Use this command to enable IGMP event debugging.

Syntax

```
[no] debug igmp events
```

Example

```
SR# debug igmp events
```

debug igmp fsm

Use this command to enable IGMP FSM debugging.

Syntax

```
[no] debug igmp fsm
```

Example

```
SR# debug igmp fsm
```

debug igmp tib

Use this command to enable IGMP Tree Info Base debugging.

Syntax

```
[no] debug igmp tib
```

Example

```
SR# debug igmp tib
```

Troubleshooting IPv6 Multicast

IPv6 Multicast debugging commands

debug ipv6 multicast

Use this command to debug multicast information.

Syntax

```
[no] debug ipv6 multicast
```

Example

```
SR# debug ipv6 multicast
```

debug ipv6 multicast all

Use this command to debug all multicast information.

Syntax

```
[no] debug ipv6 multicast all
```

Example

```
SR# debug ipv6 multicast all
```

debug ipv6 multicast fib-msg

Use this command to debug multicast FIB messages.

Syntax

```
[no] debug ipv6 multicast fib-msg
```

Example

```
SR# debug ipv6 multicast fib-msg
```

debug ipv6 multicast mrt

Use this command to debug multicast routes.

Syntax

```
[no] debug ipv6 multicast mrt
```

Example

```
SR# debug ipv6 multicast mrt
```

debug ipv6 multicast register

Use this command to debug multicast PIM register messages.

Syntax

```
[no] debug ipv6 multicast register
```

Example

```
SR# debug ipv6 multicast register
```

debug ipv6 multicast stats

Use this command to debug multicast statistics.

Syntax

```
[no] debug ipv6 multicast stats
```

Example

```
SR# debug ipv6 multicast stats
```


Comments? infodev@avaya.com

debug ipv6 multicast mif

Use this command to debug a multicast interface.

Syntax

```
[no] debug ipv6 multicast mif
```

Example

```
SR# debug ipv6 multicast mif
```

Troubleshooting PIM-SM for IPv6

PIM-SM for IPv6 debugging commands

debug ipv6 pim

Use this command to access next level IPv6 PIM commands.

Syntax

```
[no] debug ipv6 pim
```

Example

```
SR# debug ipv6 pim
```

debug ipv6 pim sparse-mode

Use this command to access debug commands for PIM-SM for IPv6.

Syntax

```
[no] debug ipv6 pim sparse-mode
```

Example

```
SR# debug ipv6 pim sparse-mode
```

debug ipv6 pim sparse-mode all

Use this command to enable all PIM debugging.

Syntax

```
[no] debug ipv6 pim sparse-mode all
```

Example

```
SR# debug ipv6 pim sparse-mode all
```

debug ipv6 pim sparse-mode events

Use this command to debug PIM events.

Syntax

```
[no] debug ipv6 pim sparse-mode events
```

Example

```
SR# debug ipv6 pim sparse-mode events
```

debug ipv6 pim sparse-mode mfc

Use this command to debug PIM MFC updates.

Syntax

```
[no] debug ipv6 pim sparse-mode mfc
```

Example

```
SR# debug ipv6 pim sparse-mode mfc
```

debug ipv6 pim sparse-mode mib

Use this command to debug the PIM MIB.

Syntax

```
[no] debug ipv6 pim sparse-mode mib
```

Example

```
SR# debug ipv6 pim sparse-mode mib
```

debug ipv6 pim sparse-mode nexthop

Use this command to debug the PIM nexthop.

Syntax

```
[no] debug ipv6 pim sparse-mode nexthop
```


Comments? infodev@avaya.com

Example

```
SR# debug ipv6 pim sparse-mode nexthop
```

debug ipv6 pim sparse-mode database

Use this command to debug PIM database information.

Syntax

```
[no] debug ipv6 pim sparse-mode database
```

Example

```
SR# debug ipv6 pim sparse-mode database
```

debug ipv6 pim sparse-mode packet

Use this command to debug a PIM packet.

Syntax

```
[no] debug ipv6 pim sparse-mode packet <packettype>
```

Table 67: Variable definition

Variable	Value
<packettype>	The packet type to debug. Possible choices are: • **all** - All packets. • **hello** - Hello packets. • **register** - PIM register messages. • **jp** - Join/Prune messages. • **bsr** - BSR messages. • **assert** - PIM assert messages. • **crp** - CRP messages. • **in** - Incoming PIM packets. • **out** - Outgoing PIM packets.

Example

```
SR# debug ipv6 pim sparse-mode packet
```

debug ipv6 pim sparse-mode state

Use this command to debug the PIM state.

Syntax

```
[no] debug ipv6 pim sparse-mode state
```

Example

```
SR# debug ipv6 pim sparse-mode state
```

debug ipv6 pim sparse-mode timer

Use this command to debug PIM timers.

Syntax

```
[no] debug ipv6 pim sparse-mode timer
```

Example

```
SR# debug ipv6 pim sparse-mode timer
```

debug ipv6 pim sparse-mode timer assert

Use this command to debug assert timers.

Syntax

```
[no] debug ipv6 pim sparse-mode timer assert
```

Example

```
SR# debug ipv6 pim sparse-mode timer assert
```

debug ipv6 pim sparse-mode timer bsr

Use this command to debug bootstrap timers.

Syntax

```
[no] debug ipv6 pim sparse-mode timer bsr
```

Example

```
SR# debug ipv6 pim sparse-mode timer bsr
```


Comments? infodev@avaya.com

debug ipv6 pim sparse-mode timer hello

Use this command to debug hello timers.

Syntax

```
[no] debug ipv6 pim sparse-mode timer hello
```

Example

```
SR# debug ipv6 pim sparse-mode timer hello
```

debug ipv6 pim sparse-mode timer joinprune

Use this command to debug joinprune timers.

Syntax

```
[no] debug ipv6 pim sparse-mode timer joinprune
```

Example

```
SR# debug ipv6 pim sparse-mode timer joinprune
```

debug ipv6 pim sparse-mode timer register

Use this command to debug register timers.

Syntax

```
[no] debug ipv6 pim sparse-mode timer register
```

Example

```
SR# debug ipv6 pim sparse-mode timer register
```

Troubleshooting MLD

MLD debugging commands

debug mld

Use this command to configure MLD debugging.

Syntax

```
[no] debug mld
```

Example

```
SR# debug mld
```

debug mld all

Use this command to enable all MLD debugging.

Syntax

```
[no] debug mld all
```

Example

```
SR# debug mld all
```

debug mld decode

Use this command to enable MLD decode debugging.

Syntax

```
[no] debug mld decode
```

Example

```
SR# debug mld decode
```

debug mld encode

Use this command to enable MLD encode debugging.

Syntax

```
[no] debug mld encode
```

Example

```
SR# debug mld encode
```

debug mld events

Use this command to enable MLD event debugging.

Syntax

```
[no] debug mld events
```


Comments? infodev@avaya.com

Example

```
SR# debug mld events
```

debug mld fsm

Use this command to enable MLD FSM debugging.

Syntax

```
[no] debug mld fsm
```

Example

```
SR# debug mld fsm
```

debug mld tib

Use this command to enable MLD Tree Info Base debugging.

Syntax

```
[no] debug mld tib
```

Example

```
SR# debug mld tib
```

Comments? infodev@avaya.com

Chapter 12: Troubleshooting ADSL

This section describes commands that you use to troubleshoot ADSL.

ADSL show commands

- Use the **show system configuration** command to display the hardware version and card type in each slot.
- Use the **show chassis** command to display all slots and card types in chassis.
- Use the **show module configuration xdsl<slot>/<port>** to display ADSL Layer 1 configuration.
- Use the **show module userstats xdsl <slot>/<port>** command to display ADSL user statistics.
- Use the **show module alarms xdsl <slot>/<port>** to display Layer 1 alarms.
- Use the **show interface bundle <bundlename>** to display ADSL bundle status and configuration.

ADSL SM Card initialization

If the ADSL card is not working or no LEDs are illuminated:

Solution:

- Check the LED status - The LINK-STAT LED should be GREEN and the STAT LED should be AMBER when no ADSL bundle has been configured.
- Use the **show chassis** and **show system configuration** commands to make sure that the correct hardware version and card type are installed. Confirm that the card has been detected by the Avaya Secure Router 2330/4134.

If the above fails:

- Reset the ADSL SM Card in the slot.
- If the problem persists, perform a hot-swap of the module, reset the card, and verify operation.

show chassis sample output for ADSL card

PPPoA_TOR# show chassis

Chassis Model: SR4134

Chassis Operational Status: NORMAL

Slot/SubSlot	Card-Type	Status	Serial#
0	MPU_A	NORMAL	---
3	--	EMPTY	---
4	ADSL_ANX_A	NORMAL	ADSL_A#02
INT	VPN_A	NORMAL	VPN#51

INT - Mainboard internal module

Table 68: ADSL Module LEDs

LED	Description
STAT	Indicates the status of the card: • OFF: No power available to the module • Yellow: Card is down or is being initialized • GREEN: Power on and the module is operational
LINK/STAT	Indicates the status of the WAN bundle: • OFF: Interface isout of service • Yellow: Bundle not configured or when PVC/link is down • GREEN: Bundle is UP

Use the **show system configuration** command to verify the hardware version and card type.

Only the following ADSL SM Cards are supported currently:

- ANNEX A (ADSL_ANX_A)
- ANNEX B (ADSL_ANX_B)

The current CPLD Engineering Revision for the ADSL SM cards is 0x3

MT-6013 **#show system configuration**

NCM System Configuration:

Comments? infodev@avaya.com

Chassis Serial number:

Chassis Rev: 65535

Slot	Card-Type	Status	Serial#
0	MPU_A	NORMAL	MT#80
1	ADSL_ANX_A	NORMAL	ADSL_A#35
2	UNKNOWN	EMPTY	---
3	ADSL_ANX_B	NORMAL	ADSL_B#04

Hardware Status:

Processor: MPC8349

Memory Size: 1G

Model Number: SR4134

Serial Number: MT#80

Runtime: 10.2.0.0

Created: Jul 24 2009, 04.44.23

Boot:0.0.0.45 (NORMAL Boot)

NorBoot: 0.0.0.45

GolBoot:0.0.0.45

Slot/ SubSlot	Card-Type	Status	FPGA-Rev	FPGA-Eng-Rev	CPLD-Rev	CPLD-Eng-Rev
0/-	MPU_A	NORMAL	---	---	---	0x16
1/-	ASDL_ANX_A	NORMAL	---	---	---	0x3
3/-	ASDL_ANX_B	NORMAL	---	---	---	0x3

ADSL Layer 1

This section outlines solutions to the following issues:

- ADSL Line fails to train
- ADSL link down

Solution

- Verify Layer 1 configuration using **`xdsl <slot>/<port> command`**.
- Verify the Layer 1 configuration on DSLAM.
- Verify that the cable is plugged in.
- Use **`show module alarms xdsl <slot>/<port>`** to verify that the link is UP.

`show module configuration` sample output for layer 1 parameters

MT-6013# show module configuration xdsl 1/1

Software Version: 3.10L.06.A2pB022g.d20h

adsl: ADSL driver and PHY status

Status: ShowtimeRetrain Reason: 1

Channel: FAST, Upstream rate = 1094 Kbps, Downstream rate = 22624 Kbps

Link Power State: L0

Mode: ADSL2+

Line Status: No Defect

SNR (dB): 6.8 7.0

Attn(dB): 1.0 0.0

Pwr(dBm): 7.5 0.8

Trellis Coding: Enable

BitSwap Coding: Enable

SRA: Disable

L3 Power State: Disable

Comments? infodev@avaya.com

ADSL SM Card Software Image

Use this section to solve the issues if:

- the ADSL configuration commands fail
- the ADSL bundles fail to come-up

Solution

- Issue a **`show module configuration xdsl <slot/1>`** command at the CLI prompt and look for the software version.
- Compare the software version with the version recommended for the card type.

`show module configuration` sample output for software version

MT-6013# show module configuration xdsl 1/1

Software Version: 3.10L.06.A2pB022g.d20h

adsl: ADSL driver and PHY status

Status: ShowtimeRetrain Reason: 1

Channel: FAST, Upstream rate=1094 Kbps, Downstream rate = 22624 Kbps

Link Power State: LO

Mode: ADSL2+

Line Status: No Defect

SNR (dB): 6.8 7.0

Attn(dB): 1.0 0.0

Pwr(dBm): 7.5 0.8

Trellis Coding: Enable

BitSwap Coding: Disable

SRA: Disable

L3 Power State: Disable

ASDL bundle configuration

Use the following section to solve issues if:

- ADSL bundles fail to come-up
- There are traffic issues related to ADSL bundles

Solution

- Use **show interface bundle <xdslBundleName>** to verify the ADSL bundle configuration.
- Verify that the PVC vpi/vci are configured.
- Verify that PVC is enabled.
- Verify that ATM encapsulated protocols are supported.
  - PPPoA
  - PPPoE
  - IPoA
  - IPoE
  - MPoA
- Verify the authentication parameters for PPPoA and PPPoE bundles.

Verify the ADSL bundle configuration using the **show interface bundle <adslBundleName>** command.

```
SR# show interface bundle xdsl

bundle xdsl

status up

number of links 1

total bandwidth 1023 kbps

 link                  speed        bw          status

 xdsl 4/1              255          1023        up
 encapsulation atm
 PVC 0/35

status up

shaping(cir-bcmax-bcmin-be) 1023000-0-0-0

policing(de-cir-bc-be) D-1023000-1023000-0
```


Comments? infodev@avaya.com

```
protocol support PPPOA

counters since last boot/clear

Bytes Rx 59436 Bytes Tx 46800

Packets Rx 1036 Packets Tx 780

Dropped Rx 0 Dropped Tx 0

Overruns Rx 0 Overruns Tx 0

Err Packets Rx 0 Err Packets Tx 0

ATM QoS Configurations

Class_vc Name : defClassVc

Service Category : ubr

PCR Value : 0

SCR Value : 0

MBS value : 0
```

Another possible cause of the bundle not coming up is the authentication configuration for PPPoA and PPPoE bundles.

Solution

- Verify the authentication protocol on both the router and ISP.
- Verify that the sent-username/password is configured.
- Ensure that the user understands the need to configure peer-name and password for CHAP authentication for PPPoA.

Configuration steps for PAP authentication on PPPoA

```
configure terminal
interface bundle ppp
link xdsl-pvc xdsl:0/35
encapsulation ppp
ppp pap sent-username test123 pass123
ip negotiated
```

(dynamic IP)

Configuration steps for CHAP authentication on PPPoA

```
configure terminal
interface bundle ppp
link xdsl-pvc xdsl:0/35
encapsulation ppp
ppp chap sent-username test123 pass123
ppp chap peer-name peer123 peerPass123
ip negotiated
```

(dynamic IP)

```
ppp authentication chap
```

(To enable local-chap authentication i.e. our end of the link sends ‘chap-challenge’ to the peer).

ADSL Traffic issues

Use the following section when faced with traffic issues (upstream or downstream) related to an ADSL bundle.

Solution:

- Verify that the ADSL, link, PVC, and bundle are up.
- Perform a PVC 'no enable/enable'.
- Perform a 'shut/no-shut' on the bundle.
- Perform a hot-swap of the card.

Steps for PVC 'no enable/enable' on PVC 0/35: **SR# configure term SR/configure# int bundle xdsl2 configuring existing WAN bundle interface xdsl2 SR/configure/interface/bundle xdsl2# atm SR/configure/interface/bundle xdsl2/atm# pvc 0/35 Configuring existing PVC connection SR/configure/interface/bundle xdsl2/atm/pvc#**no enable **SR/configure/interface/bundle xdsl2/atm/pvc# show int bundle xdsl2**

status up

number of links 1

total bandwidth 1065 kbps

link	speed	bw	status
xdsl 2/1 encapsulation atm PVC 0/35	41	1065	up

```
status          down, administratively disabled
```

shaping(cir-bcmax-bcmin-be) 1065000-0-0-0

policing(de-cir-bc-be) D-1065000-1065000-0

protocol support BRIDGE

counters since last boot/clear

Bytes Rx 0

Packets Rx 0

Comments? infodev@avaya.com

Dropped Rx 0

Overruns Rx 0

Err Packets Rx 0

Err Packets Tx 0

Bytes Tx 0

Packets Tx 0

Dropped Tx 0

Overruns Tx 0

ATM QoS Configurations

Class_vc Name : bqos

Service Category : nrtvbr

PCR Value : 235

SCR Value : 2300

MBS value : 100

Comments? infodev@avaya.com

Chapter 13: Troubleshooting SIP survivability

This section describes commands that you use to troubleshoot SIP survivability. For more information about SIP survivability, see *Avaya Secure Router 2330/4134 Configuration—SIP Survivability* (NN7263-510).

- SIP survivability show commands on page 189
- Debug/trace commands on page 190
- Common issues on page 190

SIP survivability show commands

- show ssm sip-server status
- show ssm sip-server configuration
- show ssm sip-server statistics
- show ssm configuration
- show ssm registrar
- show ssm dial-plan
- show ssm cac status
- show ssm session-timer
- show ssm protocol-header
- show ssm registered-users {<username> |all}
- show ssm licensed users
- show ssm subscriber {<username> |all}

Debug/trace commands

- debug ssm traces error {all|critical|major|minor}
- debug ssm traces message
- debug ssm traces brief-traces {all|cac|call|handlers|media|stack|routing|registrar|keepalive}
- debug ssm traces detailed-traces {all|cac|call|handlers|media|stack|routing|registrar|keepalive}

Common issues

SIP survivability commands inaccessible

Possible cause 1: SIP survivabililty software image not installed.

Solution: The SIP survivability features are only supported in release 10.2.0.0 and later. Verify that the current release on the Avaya Secure Router 2330/4134 is supported by using the show version command.

```
SR/configure# show version
 Runtime: 10.2.0.0
 Created: Sep 16 2009, 18:12:58
    Boot: 0.0.0.44 (NORMAL Boot)
 NorBoot: 0.0.0.44
 GolBoot: 0.0.0.44


Slot/SubSlot  Card-Type  Status   FPGA-Rev FPGA-Eng-Rev CPLD-Rev CPLD-Eng-Rev
-------------------------------------------------------------------------------
   0/-        MPU_A      NORMAL   0x1      0x3          ---      0xb
   2/-        FXS_4M     NORMAL   ---      ---          0x1      0x9
   4/-        FXO_4M     NORMAL   ---      ---          0x1      0x6
```

Figure 20: show version sample output for software release

Possible cause 2: PVM/PVIM module is not installed.

Solution: The internal PVM/PVIM must be purchased/installed for the Secure Router 2330/4134 to support SIP survivability features. Ensure that the PVM/PVIM module is installed properly using show chassiscommand.

Comments? infodev@avaya.com

```
SR# show chassis

Chassis Model: SR4134
Chassis Operational Status: NORMAL

Chassis Serial number: LBNNTMJV4111H34034
Chassis Rev: 8
Slot/SubSlot    Card-Type       Status        Serial#
-------------------------------------------------------
   0            MPU_A           NORMAL        LBNNTMJV7718H29088
  INT           VOIP_A          NORMAL        ---
  0/3           SFP             Absent        ---
  0/4           SFP             Absent        ---

INT - Mainboard internal module.
```

Figure 21: show chassis sample output for PVM module

SIP survivability feature does not start: enable fails

Possible cause: Bind IP address for SIP survivability not configured.

Solution: Before enabling the SIP survivability, bind IP address for the SIP survivability should be configured. This is the IP addresses on which SIP survivability module (SSM) expects to receive SIP messages. Configure the bind IP address for SIP survivability using bind ip command under **`configure/voice/service/voip/ssm`**.

```
SR/configure/voice/service/voip/ssm# enable
VoIP:SSM bind not configured
SR/configure/voice/service/voip/ssm#
```

Figure 22: Sample output for SSM enable

```
SR/configure/voice/service/voip/ssm# bind ip ipv4:47.80.235.72
SR/configure/voice/service/voip/ssm#
```

Figure 23: Sample Bind IP configuration for SSM

SSM stuck in backup mode

Possible cause 1: SIP server for SSM not configured.

Verify the central SIP server or keepalive server configuration for SIP survivability using show ssm sip-server configuration. If none is configured, configure the SIP server or keepalive server for the deployment using the keepalive-server CLI command under configure/voice/service/voip/ssm/sip-server.

```
SR/configure/voice/service/voip/ssm# sip-server keepalive-server
ipv4:47.80.235.177:5060
SR/configure/voice/service/voip/ssm#
```

Figure 24: SIP server/keepalive server configuration for SSM sample

```
SR# show ssm sip-server configuration
Forking policy in backup mode : first-only
Polled SIP Server :
        47.80.235.177:5060
        Interval          : 60s
        Number of retries : 1
        Transport used for SIP OPTIONS : udp
SSM domain server:
DNS lookup timeout : 20000ms
Reject SUBSCRIBE/NOTIFY requests in backup mode : True

SIP timer configuration (in ms):
        RTT estimate (T1): 500
        Max retransmit Interval (T2): 4000
        Invite transaction timeout (B): 32000
        Proxy invite transaction timeout (C): 180000
        UDP response retransmit Wait time (D): 32000
        Non-invite transaction timeout (F): 32000
        Ack receipt Wait time (H): 32000
        UDP ack retransmit Wait time (I): 5000
        UDP non-invite request retransmit Wait time (J): 32000
        UDP response retransmit Wait time (K): 5000
```

Figure 25: show ssm sip-server configuration sample output

Possible cause 2: CAC interfaces are not configured for SIP survivability.

Verify CAC interface configuration using show ssm cac status. If none is configured, configure the CAC links (WAN or LAN links through which central SIP server is reachable) using the cac max-calls CLI command under configure/voice/service/voip/ssm.

```
SR# show ssm cac status
Interface           Max     Current
ethernet0/1         100     0
SR#
```

Figure 26: show ssm cac status

```
SR/configure/voice/service/voip/ssm# cac max-calls ethernet0/1 100
Please remove this link explicitly by executing 'no max-calls' when this
interface is de-configured.
SR/configure/voice/service/voip/ssm#
```

Figure 27: cac interface configuration output for ssm

```
SR# show ssm cac status
Interface           Max     Current
ethernet0/1         100     0
SR#
```

Figure 28: show ssm cac status output sample

Comments? infodev@avaya.com

SIP client registrations fail

Possible cause 1: Incorrect SIP client configuration.

Solution: Verify the SIP client configuration. The SIP clients must be configured with SSM as their outbound proxy. Also ensure that the username and password configured on the client matches with the ones configured on the central SIP server.

Possible cause 2: SIP domain name for SIP survivability is not configured.

Solution: Verify SSM mode using the show ssm sip-server status command. If SIP survivability module is running in either Backup Wan Up Mode or Backup Wan Down Mode, verify that the SIP domain name is configured using the show ssm sip-server configuration command. If none are configured, configure the SIP domain name for the deployment using the domain CLI command under configure/voice/service/voip/ssm/sip-server.

```
SR/configure/voice/service/voip/ssm# sip-server domain dns:scs500.us.nortel.com
SR/configure/voice/service/voip/ssm#
```

Figure 29: Sample SIP domain configuration

```
SR# show ssm sip-server configuration
Forking policy in backup mode : first-only
Polled SIP Server :
        47.80.235.177:5060
        Interval          : 60s
        Number of retries : 1
        Transport used for SIP OPTIONS : udp
SSM domain server: scs500.us.nortel.com
DNS lookup timeout : 20000ms
Reject SUBSCRIBE/NOTIFY requests in backup mode : True

SIP timer configuration (in ms):
        RTT estimate (T1): 500
        Max retransmit Interval (T2): 4000
        Invite transaction timeout (B): 32000
        Proxy invite transaction timeout (C): 180000
        UDP response retransmit Wait time (D): 32000
        Non-invite transaction timeout (F): 32000
        Ack receipt Wait time (H): 32000
        UDP ack retransmit Wait time (I): 5000
        UDP non-invite request retransmit Wait time (J): 32000
        UDP response retransmit Wait time (K): 5000
```

Figure 30: show ssm sip-server configuration output after SIP domain name configuration

Possible cause 3: CAC exclude pool not configured.

Solution: If the central SIP server and SIP clients are reachable through a single interface on the Secure Router, then a special configuration is required on SSM to distinguish the SIP clients. Use cac exclude pool to configure the subnet mask used by SIP clients in the branch. SSM only accepts the REGISTER requests from endpoints belonging to this pool. When SSM rejects a REGISTER request for this reason, it adds a warning header with the string Warning:

399 AvayaSR "Invalid Endpoint trying to Register" in the SIP response. Use show ssm cac status to verify the CAC exclude pool configuration.

```
SR# show ssm cac status
Interface           Max     Current
ethernet0/1         100     0
CAC Exclude IP pool
134.177.109.48 netmask 255.255.255.0
```

Figure 31: show ssm cac status sample output

Possible cause 4: Exceeded SSM licensing limit.

Solution:The maximum number of SIP registrations accepted by SSM is controlled by SSM user license. If the current registrations exceeds the licensed value, new registration request will be rejected with a 403 forbidden response. Verify the licensed number of SSM users using show ssm licensed-users. To upgrade the SSM user capacity, contact Avaya customer support using the procedure outlined in *Avaya Secure Router 2330/4134 Configuration—SIP Survivability User Guide* (NN47263-510).

```
SR# show ssm licensed-users
Licensed SSM user capacity = 25
```

Figure 32: show ssm licensed-users sample output

Unable to call from SIP client

Possible cause 1: SIP client not registered.

Solution: Verify whether SIP client is registered using the show ssm registered-users command. If the SIP client is not registered, register the SIP client before initiating the call.

```
SR# show ssm registered-users 5087541000 dns:scs500.us.nortel.com
Subscriber    Destination            Expires(sec) Mode        Contact
5087541000    scs500.us.nortel.com   139          backup(udp) 47.80.235.246:5060
```

Figure 33: show ssm registered-users sample output (registered user)

```
SR# show ssm registered-users 5087541010 dns:scs500.us.nortel.com
Subscriber    Destination            Expires(sec) Mode        Contact
VoIP: Entry does not exists.
```

Figure 34: show ssm registered-users sample output (unregistered user)

Possible cause 2: Bandwidth not available for the call.

Solution: Verify current simultaneous call count and maximum number of calls allowed on the CAC links using show ssm cac status command. If the current simultaneous call count is equal to maximum allowed calls, attempt the call again after few existing calls are terminated.

Comments? infodev@avaya.com

```
SR/configure/voice/service/voip/ssm# show ssm cac status
Interface           Max     Current
ethernet0/1         100     100
```

Figure 35: show ssm cac status sample output (insufficient bandwidth)

```
SR/configure/voice/service/voip/ssm# show ssm cac status
Interface           Max     Current
ethernet0/1         100     20
```

Figure 36: show ssm cac status sample output (insufficient bandwidth)

Unable to make SIP to gateway calls

Possible cause 1: SSM default gateway configuration missing.

Solution: Verify whether default gateway is configured using the show ssm configuration command. If the default gateway is not configured, configure the same using default-gateway command under the configure/voice/service/voip/ssm subtree.

Possible cause 2: Bandwidth not available for the call.

Solution: Verify current simultaneous call count and maximum number of calls allowed on the CAC links using show ssm cac status command. If the current simultaneous call count is equal to maximum allowed calls, attempt the call again after few existing calls are terminated.

```
SR/configure/voice/service/voip/ssm# show ssm cac status
Interface           Max     Current
ethernet0/1         100     100
```

Figure 37: show ssm cac status sample output (insufficient bandwidth)

```
SR/configure/voice/service/voip/ssm# show ssm cac status
Interface           Max     Current
ethernet0/1         100     20
```

Figure 38: show ssm cac status sample output (sufficient bandwidth)

Comments? infodev@avaya.com

Chapter 14: Troubleshooting security

Troubleshooting firewall

This section details commands and ideas used to troubleshoot firewall issues.

Prerequisites to firewall troubleshooting

Achieving network connectedness is a complex achievement. It can be said of firewalls that after the network is functioning, we are selectively breaking connectivity for users/devices which we discriminate against. When a device is unreachable to the network, the unreachability may be intentional. Several debugging options are available to general network administrators and end users to attempt to see where the 'break' is. But when a firewall is in play, several complicating factors are introduced:

- Policy Goals Description - There must be an authority somewhere who can describe the canonical policy goal of which devices are allowed and which are not. This set of policy goals must be understood by anyone attempting to troubleshoot a network reachability problem when a firewall is involved.
- Network map - Since firewall policies are expressed in terms of subnets (which are either permitted or denied) one must know where these subnets are located. In simple cases, there may be only one directly connected subnet to protect from the internet. But anything more complicated than a single directly connected subnet will generate the question of where the subnet exists.
- Access to the firewall login - A troubleshooting engineer must also have access to the firewall to review the policy configuration and compare it to the policy goals. Also, login access grants the ability to see firewall events on the console and to enter debugging commands.

It is typical that Policy Goals Description and access to the firewall login are kept secret and will be unavailable to all end users and also unavailable to a fair portion of network administration staff. A network map is sometimes a secret document and sometimes a public document depending upon site policy. The accuracy of the network map listing subnets and firewall interfaces must be assured.

Keep in mind that without a policy goal description, a network map, and access to the firewall login it is unlikely you will be able to troubleshoot firewall issues. Technicians with Avaya would almost certainly require this information to assist in troubleshooting such issues.

Getting started

The following three commands are crucial to successful examination of firewall issues. Using these commands, along with the policy goals and network map, you can compare the current configuration and check for obvious issues.

```
show ip interfaces brief

show firewall interfaces all

show firewall policy <zoneName> [detail]
```

The <zoneName> variable represents the zone you are interested in debugging. Adding the [detail] parameter provides a detailed version of the policy listing.

Getting details

After comparing the configured policy to the goals and map, view the events with debug show commands:

```
debug firewall all

debug firewall packet
```

The `debug firewall packet` command is stunningly verbose as it prints at least two lines (IN and OUT) for every packet. Keep in mind that it severely degrades system performance and may even degrade the stability of the system. The console printing simply cannot keep up with packet rates on network interfaces. Thus, Avaya has implemented a feature within the **`debug firewall all`** command will, somewhat counter intuitively disable **`debug firewall packet`**. This leaves a firewall system with **`debug firewall all`** enabled still in a stable and moderately performing state.

If you need to debug firewall packets on a busy network, you may limit what it prints with packet filters. See the **`debug firewall packet`** command description for details.

When firewall connections are made, you may see the list and their associated byte counts and remaining lifetime using the command **`show firewall connection all`**.

Firewall connections are cached after the first few packets. The connection entry in the cache table has a lifetime. You may clear firewall connections with **`clear firewall connections <all | ip-address>`**. This will force all client/server sessions through the firewall to break and need to restart.

Comments? infodev@avaya.com

Isolating faults

- Is the firewall at fault?
  - Try disabling the firewall so see if connectivity is restored. The simplest way to disable the firewall is not to remove the policy from the zone, but to remove the interface from the zone. Remember to remove the necessary interfaces from both the trusted and untrusted zones.
- Is an ALG at fault?
  - Application level gateways examine packets into the application area (beyond the protocol area) to make allow/deny decisions. But applications are not standardized. Using SIP as an example, a SIP application from different vendors, or even different versions of a SIP application from the same vendor may exhibit different behaviors which the firewall's SIP ALG did not anticipate. The Avaya Secure Router firewall ALGs are enabled by default. If you are having trouble with one particular application, try disabling the relevant ALG(s).

    ```
    firewall global algs no <algName | all> exit exit show firewall algs
    ```
- Does the packet leave the firewall?
  - You may find the answer to this with a packet sniffer, or with an interface based packet capture. But **`debug firewall packet`** will also show which packets are egressing the firewall. The absence of any printing of a "FW out: ..." means that a packet did not egress the firewall. Most often the firewall will log reasons when it drops packets. But in a few cases, the firewall may silently drop packets.
- Which type of packets seems to cause the problem?
  - If some packets get through and some don't, try to determine which property the firewall does not like about the offending packets. Is it a particular address or protocol? Is it fragmented or non-fragmented?
- Are other systems besides the firewall dropping packets?
  - In particular, is the QOS system dropping packets?

Common errors

- At least one interface must be in a trusted zone and at least one interface must be in the untrusted zone.
- Firewalling requires that the Secure Router know the route to both the destination as well as the source of every packet.

- The procedure for describing a subnet or a range which will be firewalled is very similar at leads to a common mistake:
  - This policy describes a subnet (it has a subnet prefix for the 10.1.1.0 network):

    ```
    policy 10 out address 10.1.1.0 24 any any
    ```

  - This policy describes a range (it has a start and end address):

    ```
    policy 11 out address 20.1.1.1 20.1.1.200 any any
    ```

  - This policy describes a range (it has a start and end address) but is almost certainly not what was intended:

    ```
    policy 12 out address 30.1.1.0 255.255.255.0 any any
    ```

    Policy 12 describes the range of addresses starting from 30.1.1.0 and continuing up through (almost) all the available IP address range to 255.255.255.0. Policy 12 does *not* describe the subnet 30.1.1.0/24.
- Firewall policies intended to protect end hosts behind the firewall must be expressed in a trusted zone. Policies in the untrusted zone, internet, only protect the firewall internet interface itself.

Firewall troubleshooting commands

debug firewall alg

```
debug firewall alg
```

debug firewall attack

```
debug firewall attack
```

debug firewall connections

```
debug firewall connections
```

debug firewall ip-reassembly

Comments? infodev@avaya.com

```
debug firewall ip-reassembly
```

debug firewall packet

```
debug firewall packet [<direction>|<srcip>|<destip>|
<protocol>|<numpkts>]
```

Table 69: Variable definition

Variable	Value
<destip>	Match the destination IP address. Default is **any**.
<direction>	The packet direction. Possible choices are **in**, **out**, or **both**. Default is **both**.
<numpkts>	The number of packets to display. The default is 100.
<protocol>	Match a protocol, by identifying number. Possible choices are: • **1** - ICMP protocol. • **6** - TCP protocol. • **17** - UDP protocol. • **47** - GRE protocol. • **50** - ESP protocol. • **51** - AH protocol. • **any** - Any protocol.
<srcip>	

debug firewall all

```
debug firewall all
```

debug tacacs

Use this command to debug RSA secure-ID related messages.

Syntax

```
[no] debug tacacs
```

This command is used for both RADIUS and TACACS+ protocols.

Example

```
SR# debug tacacs
```

Troubleshooting NAT

This section details techniques used to troubleshoot NAT.

Before getting started

In the Secure Router series, the Network Address Translation and Port Translation features are implemented as a feature of the firewall. This gives the firewall and Application Level Gateways visibility into the NAT mappings and provides a rich capability in terms of tracking the opening of new control/data connections and being sure to also allow them through the firewall. On the other hand, bringing in the firewall to the NAT capability leads to some complexity.

Troubleshooting NAT connections brings in all the necessary knowledge and privilege of Troubleshooting firewall connections. To summarize those points, you will need a Policy Goals Description and a network map.

Because NAT policies ride on firewall policies, and because transit firewall policies are expressed in a trusted zone, NAT policies must be expressed in the trusted zone. This may appear counter-intuitive as many NAT devices administrators are historically used to equipment which expresses NAT policy on the egress/untrusted interface, not the ingress interface/trusted.

In the Secure Router, several different forms of NAT may be configured. Most commonly the "nat-ip" or "pat" form will be used which uses a port restricted Cone NAT port allocation algorithm. This allows STUN and STUN like protocols to work through NATting Secure Routers.

- nat-ip or pat: Many to one address and port mangling with a cone nat allocation
- static: one to one address (only) mangling
- dynamic: Many to Many address (only) mangling

Generally, the policy configuration of NAT requires a two step process; first configure a NAT-object in the firewall global area, and second apply the NAT-object to a policy in the firewall <zoneName> area. The NAT-object selects the type of NAT and the size of the address pool, but in the case of a pat type of NAT-object, the address-pool size is always exactly 1. Therefore, in the case of pat, the Secure Router allows a configuration short cut where, without defining a pat type of NAT-object, a 'nat-ip' parameter may be configured directly onto the policy. A NAT-ip policy is the same as a policy with a pat type of NAT-object applied.

Comments? infodev@avaya.com

NAT policies are configured in a trusted zone. A firewall "out" policy will be a "forward" NAT policy. A firewall "in" policy will be a reverse NAT policy.

A NAT failover feature is also available in the Secure Router. If you have named an interface to NAT out on and that interface goes down, then a named backup interface may take over the NATting function. Both the NATting interface and the backup NATting interface must be in the untrusted, "internet" zone.

Getting started

First get your general firewall orientation:

```
show ip interfaces brief show firewall interfaces all show firewall
nat-failover show firewall policy <zoneName> [detail]
```

From these three commands, if you have the goals and map in hand, you may compare the current configured policy to the goals and map.

In the **`show firewall policy <zoneName>`** version (without detail), the "N" flag will be printed in the "Advanced" column for policies which have a NATing action.

Getting details

After comparing the configured policy to the goals and map, you will move into seeing the events with debug and show commands. NAT is part of the firewall, so the commands to reveal the NAT events are the same as the commands to reveal the firewall events.

```
debug firewall all debug firewall packet
```

Isolating faults

- Can the Secure Router itself reach the target?
  - Send a ping from the Secure Router CLI. Pings which leave the untrusted interface will use the public source address and will not be NATted. The Secure Router does not allow pings to be sent from a private, self address through the NAT translation. Those packets will be sent out of the firewall without NAT translation and will not be routed back.
- Is the firewall at fault?
  - This is more difficult to isolate than in the plain firewall case because the Internet will not know the routes back to your private NAT address range. There is no ability to simply remove the firewall configuration and see if plain routing works because we know that

plain routing will fail. If the NAT-translation shows up in the NAT-translation table, then very likely, the firewall is working fine.

- Is an ALG at fault?
  - See the "Troubleshooting Firewall" section.
- Does the packet leave the firewall?
  - See the "Troubleshooting Firewall" section.
- Is the return packet routing back to the Secure Router?
  - Watch the output of **`debug firewall packet`** or use a packet sniffer on the untrusted/public side. If a packet does not return to the router, confirm that the egress packet was actually NATted. Otherwise, a non-returning packet indicates a problem outside the NATting secure router.

Common errors

- See the "Troubleshooting Firewall" section. A proper nat-failover configuration is the conjunction of two necessary commands.
  a. On the firewall policy, name the primary egress interface, for example: **`policy 1000 out nat-ip wan1`**
  b. In the firewall global area, name the backup interface, for example: **`firewall global nat-failover wan1 wan2`**

Troubleshooting VPN

This section details techniques used to troubleshoot VPN.

Before getting started

Avaya Secure Routers offer an IPsec VPN capability for IPv4 networks. IPsec VPNs offer the security services of privacy (encryption), data integrity (hashed message authentication codes), peer authentication (through IKE), replay protection and access control (through policy filtering). These security services are provided to protected networks beyond the security gateways. IPsec VPN relationships always involve a set of exactly two IPsec peer security gateways and some number of protected networks on the trusted side of each gateway.

To troubleshoot a site to site VPN you need a network map. The network map must accurately reveal the security gateways, with their public addresses, protected networks, and interface names all labeled. A VPN map may or may not be a secret document depending upon site

policy, but there is little hope of troubleshooting (or soliciting support help with troubleshooting) VPN problems without a network map.

A site to site IPsec VPN may be either native IPsec tunnels or may be IPsec transport protected GRE/IPIP tunnels. In Secure Router implemented IPsec tunnels, the tunnel does not become an interface in the system and IPsec does not provide the outer/inner IP encapsulation. In IPsec transport protected GRE/IPIP tunnels, the GRE/IPIP tunnels become a named interface in the system and GRE/IPIP, not IPsec, provides the outer/inner IP encapsulation. The IPsec system no longer filters packets, but if routes change in your system IPsec administrative filtering does not become a black hole.

IPsec tunnels with access control are configured entirely through the `crypto` sub tree in the configuration CLI. Tunnel interfaces with IPsec protection are mostly configured through the `interface tunnel` sub tree but you can alter the details of the default cryptographic parameters by modifying them in the `crypto` sub tree.

In the Secure Router, the VPN capability comes bundled with the firewall capability. You may configure firewall without VPN, but enabling VPN brings along the firewall. This means that you will need site appropriate firewall policies to allow your VPN traffic "in". Each Secure Router must know the IP route to the far end protected network(s) behind the peer security gateway(s).

IPsec VPNs have a well deserved reputation for being difficult to configure. A fairly long list of parameters must be meticulously configured on each of two peer security gateways to exactly match. Any disagreement in any Security Association configured parameter will almost always result in non-communicating systems. This leads to the choice of whether the VPN forms SAs and carries traffic, or if no traffic gets through. Troubleshooting IPsec VPN systems tends to become a matter of seeking out the hidden, mismatched parameter. Therefore you need access to the configuration of both security gateway peers.

When you have a set of VPN peers which are not forming SAs or carrying traffic, you should compare their IKE, IPsec and firewall policies. A human, visual review of policies is often the quickest way to 'see' the problem. If the issue is not quickly revealed in a policy review, then enable debug logging and seek out the error messages. In general, you should attempt to isolate between routing, firewalling, phase-I, and phase-II problems.

Getting started

First get the general VPN orientation with the following commands:

```
show ip interfaces brief

show crypto interfaces

show crypto ike policy all [detail]

show crypto ipsec policy all [detail]

show ip route
```

```
show firewall policy internet

show firewall policy corp
```

From these commands, if you have the map in hand, you may compare the current configured policy to the map with the following commands:

```
show ip in br

show ike po

show crypto ike policy all

show crypto ipsec policy all

show ip route

show firewall policy internet

show firewall policy corp
```

Getting details

After comparing the configured policy on each of the two peers, turn on debug with the following commands:

```
debug firewall all

debug firewall packet

debug crypto all
```

Keep in mind that an IKE initiator and an IKE responder will log different chains of events.

From an initiator's perspective, scan through the logged events for "good" messages.

From a responder’s perspective, scan through the logged events for these "good" messages.

You may see current IKE and IPsec SAs with the following show commands:

```
show crypto ike sa all [detail]

show crypto ipsec sa all [detail]
```

You may see current IKE and IPsec policies with the following show commands:

```
show crypto ike policy all [detail]

show crypto ipsec policy all [detail]
```

You may clear current IKE and IPsec SAs with the following clear commands:

```
clear crypto ipsec sa [all | name]
```

```
clear crypto ike sa [all | name]
```

When clearing SAs, it makes sense to clear the IPsec SAs before the IKE SAs. This is because when you clear the IPsec SAs, that action will send a message through the IKE SA to the peer that an IPsec SA is being deleted. But if you had cleared the IKE SA first, that message about deleting an IPsec SA will have no channel to travel through.

Isolating faults

- Are the phase-I parameters mismatched? Phase-I negotiations must have matched parameters for: 1. authentication-method 2. Diffie-Hellman Group 3. encryption-algorithm 4. hash-algorithm 5. lifetime 6. pfs (on or off)
- Are the phase-II parameters mismatched? Phase-II negotiations must have matched parameters for: 1. encryption-algorithm 2. hash-algorithm 3. mode (tunnel or transport) 4. pfs group
- Is the firewall at fault? The firewalling requirements for VPN are: 1. that the "internet" zone accept IKE packets in 2. that the "internet" zone accept udp port 4500 in 3. that the "corp" zone accept general traffic in from the far-end protected network.

Use the `debug firewall all` command to seek out error messages about dropping packets. Use the `debug firewall packet` command to seek out which packets are entering / leaving the firewall and VPN systems.

Common errors

- Lack of a firewall policy on the "internet" side to allow IKE in.
- Mismatching some parameters of phase-I or phase-II. Read through those log events.
- If you are using a traffic generator to test your setup, be sure to send well formed UDP packets.
- Misconfiguring the `match address` line. The format of the `match address` line gives the source subnet and the destination subnet. If you "reverse the polarity" you will never start IKE if you are the initiator, or fail in phase-II if you are the responder.
- Attempting to load certificate with a difference in time. If you wish to use a PKI signature based authentication in IKE, you must first configure a `ca trustpoint` with private key(s) and certificates. That is quite a tricky process unto itself, and the most common problem is when you get a new certificate issued from a CA but can not successfully import it into your box. The most likely cause is a mismatch in the date/time on your Secure Router clock and the CA clock which causes the Secure Router to believe that the certificate is not yet valid.
- Getting lost debugging a stale SA. As you work to bring up your first VPN session, you may go through several configuration attempts and trials. Some of these may partially succeed, leaving phase-I SAs in place or partially formed phase-II SAs in place. Each

time you make a failed test, you should clear the IPsec and IKE SAs before starting a new test.

Troubleshooting tunnels

This section details the commands used to troubleshoot IPv4 and IPv6 tunnels.

Tunnel debugging commands

debug ip tunnel

Use this command to enable or disable tunnel debug commands.

Syntax

```
[no] debug ip tunnel
```

Example

```
SR# debug ip tunnel
```

debug ip tunnel all

Use this command to debug all tunnel messages.

Syntax

```
[no] debug ip tunnel all
```

Example

```
SR# debug ip tunnel all
```

debug ip tunnel error

Use this command to debug tunnel error messages.

Syntax

```
[no] debug ip tunnel error
```

Example

```
SR# debug ip tunnel error
```


Comments? infodev@avaya.com

debug ip tunnel encap

Use this command to debug encapsulation related messages.

Syntax

```
[no] debug ip tunnel encap
```

Example

```
SR# debug ip tunnel encap
```

debug ip tunnel decap

Use this command to debug decapsulation related messages.

Syntax

```
[no] debug ip tunnel decap
```

Example

```
SR# debug ip tunnel decap
```

debug ip tunnel packet

Use this command to debug packet trace messages.

Syntax

```
[no] debug ip tunnel packet
```

Example

```
SR# debug ip tunnel packet
```

debug ip tunnel keepalive

Use this command to debug keepalive messages.

Syntax

```
[no] debug ip tunnel keepalive
```

Example

```
SR# debug ip tunnel keepalive
```

debug ip tunnel state

Use this command to debug interface state change messages.

Syntax

```
[no] debug ip tunnel state
```

Example

```
SR# debug ip tunnel state
```

debug ipv6 tunnel

Use this command to enable or disable tunnel debug commands.

Syntax

```
[no] debug ipv6 tunnel
```

Example

```
SR# debug ipv6 tunnel
```

debug ipv6 tunnel all

Use this command to debug all messages.

Syntax

```
[no] debug ipv6 tunnel all
```

Example

```
SR# debug ipv6 tunnel all
```

debug ipv6 tunnel error

Use this command to debug error messages.

Syntax

```
[no] debug ipv6 tunnel error
```

Example

```
SR# debug ipv6 tunnel error
```


Comments? infodev@avaya.com

debug ipv6 tunnel encap

Use this command to debug encapsulation related messages.

Syntax

```
[no] debug ipv6 tunnel encap
```

Example

```
SR# debug ipv6 tunnel encap
```

debug ipv6 tunnel decap

Use this command to debug decapsulation related messages.

Syntax

```
[no] debug ipv6 tunnel decap
```

Example

```
SR# debug ipv6 tunnel decap
```

debug ipv6 tunnel packet

Use this command to debug packet trace messages.

Syntax

```
[no] debug ipv6 tunnel packet
```

Example

```
SR# debug ipv6 tunnel packet
```

debug ipv6 tunnel keepalive

Use this command to debug keepalive messages.

Syntax

```
[no] debug ipv6 tunnel keepalive
```

Example

```
SR# debug ipv6 tunnel keepalive
```

debug ipv6 tunnel state

Use this command to debug interface state change messages.

Syntax

```
[no] debug ipv6 tunnel state
```

Example

```
SR# debug ipv6 tunnel state
```

debug crypto ike

Use this command to debug tunnel failover using round robin DNS and key usage extension checking related messages.

Syntax

```
[no] debug crypto ike
```

Example

```
SR# debug crypto ike
```

debug crypto ipsec mode spd

Use this command to debug nailed-up tunnel related messages.

Syntax

```
[no] debug crypto ipsec mode spd
```

Example

```
SR# debug crypto ipsec mode spd
```

debug crypto failover

Use this command to debug static weighted tunnel and dynamic tunnel failover messages.

Syntax

```
[no] debug crypto failover
```

Example

```
SR# debug crypto failover
```

Troubleshooting Static VPN Peer to Peer

Use the following steps to troubleshoot Static routing over VPN (where nailed-up configuration and periodic DPD are optional).

Procedure steps

1. To verify that the internal VPN accelerator card is installed on the SR2330/4134, enter:

   ```
   show chassis
   ```

   For the SR4134, verify that internal card type VPN_A is installed.

   For the SR2330, verify that internal card type SCIM_A is installed.

2. To display the interface configuration, enter:

   ```
   show ip interfaces brief
   ```

   ```
   show interface ethernet <slot/port>
   ```

   Verify that the public VPN interface is up and has the correct IP address configured.

3. To display the crypto interface configuration, enter:

   ```
   show crypto interfaces
   ```

   Verify that the public VPN interface is configured as an untrusted interface, and that the internal network interfaces are configured as trusted interfaces.

   Similarly, you can use the **`show firewall interface all`** command to verify that the public VPN interface is a member of the internet zone, and that the internal network interfaces are members of the corp zone (or another user-configured trusted zone).

   ```
   show firewall interface all
   ```

4. The SR2330/4134 automatically creates firewall maps, internet and corp, at boot-up. (You can also create custom firewall maps.)

   To display the firewall configuration, enter:

   ```
   show firewall policy corp
   ```

   ```
   show firewall policy internet
   ```

   You must verify that the following policies exist:

- You require an internet firewall policy allowing ISAKMP packets from the VPN peer to the local VPN endpoint (for example, 3.3.3.1). The following is a sample configuration:

```
#firewall internet
#policy 100 in permit address any any 3.3.3.1 32 service ike self
```

- In cases where there is a NAT in the middle between the VPN peers, you require an internet firewall policy that allows IKE self connections to UDP port 4500, to support NAT traversal.

  The following is a sample configuration:

```
#firewall internet
#policy 101 in permit address any any 3.3.3.1 32 protocol udp port any
4500 self
```

  (In cases where the NAT is enabled on one of the peers, you do not have to open port 4500.)

- You also require a corp firewall policy that allows data packets from the remote VPN protected network (for example 30.1.1.0/24) to the local VPN protected network (for example, 10.1.1.0/24).

  The following is a sample configuration:

```
#firewall corp
#policy 200 in permit address 30.1.1.0 24 10.1.1.0 24
#exit
```

5. To display the statistics for connections that are occurring through the firewall, enter:

   ```
   show firewall connections all
   ```

   Verify that traffic is passing through the policies you have configured.

6. To display the number of connections that have been traversing each map, enter:

   ```
   show firewall connections all summary
   ```

   If no traffic is passing through the firewall, ensure that there is a route for the transit traffic from the corp zone to the internet zone.

   In addition, for high traffic networks, make sure that the maximum firewall connection limit configured for a given map is sufficient to allow new connections. (The default for “corp” is 2500).

   You can increase the **max-connection-limit** parameter using the **`firewall global`** command.

7. To display debug commands on the console, enter:

   ```
   system logging console priority debug

   system logging console enable
   ```

8. To enable debugging on the firewall, enter:

   ```
   debug firewall connections
   ```

   Verify that the policy exists and connections are being made.

Comments? infodev@avaya.com

9. To verify whether the packets are traversing the firewall or whether they are being dropped, enter:

   ```
   debug firewall packet
   ```

10. To verify the VPN configuration by displaying the IKE policy, enter:

    ```
    show crypto ike policy all detail
    ```

    Confirm that the IKE proposal properties (such as **local-address**, and **pre-shared key**) match on the peers. When the public interface has a static IP address, the local-id must be of type **ip-address**. In this case, the local-address attribute is the static IP address.

11. To display the IPSec policy, enter:

    ```
    show crypto ipsec policy all detail
    ```

    Be sure that the peer IP address is properly configured, the network to be protected is properly configured, and IPSec proposal properties match on the peers.

12. To display the IKE SA state and counters, enter:

    ```
    show crypto ike sa all
    ```

13. To display the IPSEC SA statistics, enter:

    ```
    show crypto ipsec sa all
    ```

Troubleshooting Static VPN ABOT

Use the following steps to troubleshoot static routing over VPN ABOT (where nailed-up configuration and periodic DPD are optional).

In typical ABOT scenarios, the branch offices often use DHCP-acquired IP addresses from the ISP. This requires enabling a DHCP client on the interface connecting to the public network.

The following is a sample configuration on the public Ethernet interface facing the internet:

```
interface ethernet 0/2
dhcp-client request-default-router
dhcp-client enable
crypto untrusted
exit
```

Procedure steps

1. To display the configured IP interfaces, enter:

   ```
   show ip interfaces brief
   ```

   Verify that the status on the public IP interface is up, and that the IP address was acquired through DHCP.

2. To enable debugging on the router, enter:

```
system logging console enable

system logging console priority debug
```

3. To debug the DHCP client, enter:

   ```
   debug dhcp-client
   ```

4. To display the firewall configuration, enter:

   ```
   show firewall policy corp

   show firewall policy internet
   ```

   You must verify that the following policies exist:

   - You require an internet firewall policy allowing ISAKMP packets from the VPN peer to the local VPN endpoint.

     The following is a sample configuration:

     ```
     firewall internet
     Policy 100 in permit service ike self
     ```

     A static VPN policy generally requires the configuration of a static IP address. However, since the IP address with VPN ABOT is not static, no IP address is specified.

   - In cases where there is a NAT in the middle between the VPN peers, you also require an internet firewall policy that allows IKE self connections to UDP port 4500, to support NAT traversal.

     The following is a sample configuration:

     ```
     firewall internet
     policy 101 in permit protocol udp port any 4500 self
     ```

     (In cases where the NAT is enabled on one of the peers, you do not need to open port 4500.)

   - You also require a corp firewall policy that allows data packets from the remote VPN protected network (for example 30.1.1.0/24) to the local VPN protected network (for example, 10.1.1.0/24).

     The following is a sample configuration:

     ```
     firewall corp
     policy 200 in permit address 30.1.1.0 24 10.1.1.0 24
     ```

     This last configuration is the same as that required for non-ABOT static VPN.

5. To verify the VPN configuration by displaying the IKE policy, enter:

   ```
   show crypto ike policy all detail
   ```

   Confirm that the IKE proposal properties match on the peers. Also, as the local public address is obtained through DHCP, be sure to specify a local ID in order to have a local identifier for IKE negotiation and authentication in phase 1. The local-address must be configured as 0.0.0.0.

Comments? infodev@avaya.com

The following is a sample configuration:

```
crypto
ike policy toNVR 4.4.4.1
local-id key-id 12345
local-address 0.0.0.0
key avaya123
```

6. To display the IPSec policy, enter:

   ```
   show crypto ipsec policy all detail
   ```

   Be sure that the peer IP is properly configured, the network to be protected is properly configured, and IPSec proposal properties match on the peers.

7. To display the IKE SA state and counters, enter:

   ```
   show crypto ike sa all
   ```

8. To display the IPSEC SA statistics, enter:

   ```
   show crypto ipsec sa all
   ```

9. To display the statistics for connections that are occurring through the firewall, enter:

   ```
   show firewall connections all
   ```

   Verify that traffic is passing across the policies you have configured.

The following are some additional commands that can be useful for debugging static VPN:

- **debug crypto ike**—enables IKE negotiation debug
- **debug crypto ipsec**—enables IPSec policy-related debug
- **debug crypto ca**—enables PKI debug
- **debug dhcp-client**—enables DHCP client debug messages (for VPN ABOT)

Troubleshooting Dynamic VPN Peer to Peer over IP-IP tunnels

This section describes how to troubleshoot dynamic routing over IP-IP encapsulated tunnels.

The following list provides prerequisites and notes for configuring Dynamic IP-IP VPNs:

- The Secure Router requires that the IP-IP tunnel be created manually to enable routing over VPN.
- Periodic DPD must be enabled on both peers.
- An IP address must be assigned to the IP-IP tunnel to make it a layer 3 interface.
- The tunnel interface must always be configured as crypto untrusted.

- RIP and OSPF protocols use the tunnel interface name as the next hop for the routes learnt over this tunnel interface.
- Locally generated packets that go through tunnel interface carry the tunnel IP address as the source address before IP-IP encapsulation.

With Dynamic VPN, the firewall configuration is similar to static VPN firewall configuration. For details, see Troubleshooting Static VPN Peer to Peer on page 213.

Procedure steps

1. To display the tunnel configuration, enter:

   ```
   show interface tunnel <tunnel-name>
   ```

   Verify the source address, destination address, and crypto type as untrusted.

2. To display the IKE policy details, enter:

   ```
   show crypto ike policy all detail
   ```

   Verify the local address, the peer address, the local identity and the remote identity.

3. When the tunnel protection command is applied to a tunnel interface, the command creates an IKE policy with the following default attributes:

   - Encryption algorithm: 3des
   - Hash Algorithm: sha1
   - Authentication Mode: pre-shared-key
   - DH Group: group2

   The Tunnel protection command also creates an IPSec policy with the following default attributes:

   - Protocol: esp
   - Mode: transport
   - Encryption Algorithm: 3des
   - Hash Algorithm: sha1-hmac

   The following is a sample configuration:

   ```
   interface tunnel toNVR
   tunnel protection policy1 avaya123
   ```

   The auto-created IKE and IPsec policies can be modified and saved to suit the deployment requirements.

   Note:

   In order to interoperate with NVR at HO, IKE and IPsec proposals have to be modified. For details, see Secure Router to Avaya VPN router interoperability tips on page 221.

4. To display the IPSec policy details, enter:

Comments? infodev@avaya.com

```
show crypto ipsec policy all detail
```

Confirm the source address and destination address, and that the IPSec parameters match on the peers.

5. To display the IKE SA state and counters, enter:

   ```
   show crypto ike sa all
   ```

6. To display the IPSEC SA statistics, enter:

   ```
   show crypto ipsec sa all
   ```

7. To display the statistics for connections that are occurring through the firewall, enter:

   ```
   show firewall connections all
   ```

   Verify that traffic is passing across the configured policies.

Troubleshooting Dynamic VPN ABOT over IP-IP tunnels

This section describes how to troubleshoot dynamic routing over IP-IP encapsulated tunnels.

The following is a list of requirements for configuring Dynamic VPN ABOT over IP-IP:

- The Secure Router requires the IP-IP tunnel to be created manually to enable routing over VPN.
- Periodic DPD must be enabled on the peers.
- An IP address has to be assigned to the IPIP tunnel to make it a layer 3 interface.
- When configuring the tunnel, the tunnel source must be an interface name rather than an IP address, as the IP address can change. (For example, `tunnel source ethernet0/1`).
- Locally generated packets that go through the tunnel interface will carry the tunnel IP address as source before IPIP encapsulation.
- RIP and OSPF protocols use the tunnel interface name as the next hop for the routes learned over this VPN interface.
- The tunnel interface must always be configured as *crypto untrusted*.

In typical ABOT scenarios, the branch offices often use DHCP-acquired IP addresses from the ISP. This requires enabling a DHCP client on the interface connecting to the public network.

The following is a sample configuration for the public Ethernet interface facing the internet. (This configuration is similar to static VPN ABOT.)

```
interface ethernet 0/2
dhcp-client request-default-router
dhcp-client enable
```

```
crypto untrusted
exit
```

Procedure steps

1. To display the tunnel configuration, enter:

   ```
   show interface tunnel
   ```

   Verify that the source interface is an interface name, not an IP address, and that the crypto type is untrusted.

2. To display the IP interfaces, enter:

   ```
   show ip interface brief
   ```

   Under the **Method** column, verify that the IP address for the public interface was obtained using DHCP.

3. When the **`tunnel protection`** command is applied to a tunnel interface, the command creates an IKE policy with the following default attributes:

   - Encryption algorithm: 3des
   - Hash Algorithm: sha1
   - Authentication Mode: pre-shared-key
   - DH Group: group2

   The **`tunnel protection`** command also creates an IPSec policy with the following default attributes:

   - Protocol: esp
   - Mode: transport
   - Encryption Algorithm: 3des
   - Hash Algorithm: sha1-hmac

   A sample configuration is as follows:

   ```
   interface tunnel toNVR
   tunnel protection policy1 avaya123
   ```

   The auto-created IKE and IPsec policies can be modified and saved to suit the deployment needs.

   Note:

   In order to interoperate with the Avaya VPN Router at the head office, IKE and IPsec proposals have to be modified. For details, see Secure Router to Avaya VPN router interoperability tips on page 221.

4. To display the IKE policy details, enter:

   ```
   show crypto ike policy all detail
   ```

   Verify the local address is 0.0.0.0.

5. To display the IPSec policy details, enter:

```
show crypto ipsec policy all detail
```

Verify the source and destination IP addresses.

6. To display the IKE SA state and counters, enter:

```
show crypto ike sa all
```

7. To display the IPSEC SA statistics, enter:

```
show crypto ipsec sa all
```

8. To display the statistics for connections that are occurring through the firewall, enter:

```
show firewall connections all
```

Verify that traffic is passing across the configured policies.

The following are some additional commands that can be useful for debugging Dynamic VPN:

- **debug crypto ike**—enables IKE negotiation debug
- **debug crypto ipsec**—enables IPSec policy related debug
- **debug crypto ca**—enables PKI debug
- **debug ip tunnel encap**—enables debug for encapsulation related messages
- **debug ip tunnel decap**—enables debug for decapsulation related messages
- **debug ip tunnel state**—enables debug for interface state change messages
- **debug dhcp-client**—enables DHCP client debug messages (for VPN ABOT)

Secure Router to Avaya VPN router interoperability tips

In both static and dynamic tunnels, if the peer is an Avaya VPN router and a NAT exists between the two peers, use the **`enable-natt-rfc3947`** command under the IKE policy for NAT traversal to work with Avaya VPN router. To confirm the configuration, use the **`show crypto ike policy all detail`** command.

The following table describes default VPN attributes on the Secure Router and the Avaya VPN router, and the action required for interoperability between these two routers.

Attributes	SR2330/4134 (Default values)	Avaya VPN router (Default values)	Action
IKE Phase1	Pre-3des-g2-sha1	Pre-des-g1-sha1	Modify the proposal attributes in either of the devices.
IKE Phase2	ESP-3des-sha-TU	ESP-3des-MD5-TU	Modify the proposal attributes in either of the devices.

Attributes	SR2330/4134 (Default values)	Avaya VPN router (Default values)	Action
PFS	Disabled	Enabled	Disable PFS on Avaya VPN router or enable the appropriate key exchange group in SR.
IPSec compression	Not supported	Enabled	Disable on Avaya VPN router.
Keepalives	On-demand	Disabled	If keepalives are required, they can be enabled on the Avaya VPN router to detect peer failure. For dynamic VPN scenarios, periodic keepalive must be enabled on both SR and the Avaya VPN router.

Troubleshooting OSPF over GRE/IPIP tunnels

This section describes how to troubleshoot OSPF over GRE/IP-IP encapsulated tunnels. Note that with tunnel routing, you must configure an IP address on the tunnel interface, and you must enable routing for both the tunnel interface and the interface on which the tunnel is configured. OSPF uses the tunnel interface name as the next hop for the routes learned over the tunnel interface.

Procedure steps

1. To display the IP interfaces, enter:

   ```
   show ip interfaces brief
   ```

2. To verify the OSPF enabled interfaces, enter:

   ```
   show ip ospf interface brief
   ```

3. To verify the OSPF adjacencies, enter:

   ```
   show ip ospf neighbor
   ```

4. To verify OSPF LSA database to find originated and received LSAs, enter:

   ```
   show ip ospf database
   ```

   Note that the asterisk (*) indicates self-originated LSAs.

Comments? infodev@avaya.com

5. To verify the routes calculated by the OSPF protocol, enter:

   ```
   show ip ospf route
   ```

6. To verify that OSPF learned routes are in the forwarding table, enter:

   ```
   show ip route
   ```

7. To verify redistributed routes in the local OSPF database, enter:

   ```
   show ip ospf database
   ```

Troubleshooting RIP over GRE/IPIP tunnels

This section describes how to troubleshoot RIP over GRE/IP-IP encapsulated tunnels. Note that with tunnel routing, you must configure an IP address on the tunnel interface, and you must enable routing for both the tunnel interface and the interface on which the tunnel is configured. RIP uses the tunnel interface name as the next hop for the routes learned over the tunnel interface.

Procedure steps

1. To display the IP interfaces, enter:

   ```
   show ip interfaces brief
   ```

2. To display the RIP enabled interfaces, enter:

   ```
   show ip rip interface
   ```

   Verify that RIP is enabled on the interface and on the tunnel.

3. To display RIP neighbors, enter:

   ```
   show ip protocols rip
   ```

   This command displays all protocol-related information for RIP, including networks enabled with RIP, and the neighbors that are providing routes to this router.

4. To display the RIP database, enter:

   ```
   show ip rip database
   ```

   This command displays all RIP-learned routes.

5. To display the RIP learned routes in the forwarding route table, enter:

   ```
   show ip route
   ```

6. To display redistributed routes in the local RIP database, enter:

   ```
   show ip rip database
   ```

OSPF debug commands

OSPF global debug commands

`debug ospf packet`	This debug command can be used to verify if the two routers are successfully exchanging OSPF control packets or not. It helps debugging the OSPF adjacency if it is failing due to a mismatch or misconfiguration of protocol settings at the OSPF endpoint routers. Sub options of this command can be used to selectively enable debugging for some of the OSPF protocol packets.

`debug ospf ifsm`
and
`debug ospf nfsm`
	Use these debug commands to debug adjacency related issues. These commands will display the information about the interface state machine (ifsm) or neighbor state machine (nfsm). If adjacencies are stuck in some state for longer than expected duration, then these options help to debug and find the cause.

`debug ospf route`	This debug command can be used to debug issues in routing calculations. For example: if the adjacency has reached the Full state, but an expected route in the router is missing in the routing table. In this case, the route calculation can be traced using this option

OSPF interface-level debug command

```
configure/interface/tunnel <tunnel-name># ip ospf debug packet
```

This debug command can be used to enable debugging of OSPF protocol packets on selected interface. Sub options of this command can be used to selectively enable debugging for some of the OSPF protocol packets.

Common OSPF problems

The following sections describe some common OSPF routing problems and potential solutions.

OSPF Neighbor in INIT State

If two-way communication is not established by the neighbors, the following debug option can be used to display the hello packet and its contents:

Comments? infodev@avaya.com

```
debug ospf packet hello detail
```

This command displays the full content of the hello packets exchanged between the peers. Verify that there are no parameter mismatches. For example, the hello interval and dead interval must match on both neighbors.

OSPF Neighbor in 2-way state

If the neighbor is in a 2-way state, it is not a cause for concern. On a broadcast network, full adjacency is maintained only with the DR and the BDR. Other OSPF adjacencies remain in the 2-way state.

OSPF Neighbor in Exstart or Exchange state

Neighbors exchange DBD packets in this state. MTU mismatch can cause neighbors to get stuck in this state.

The following debug option can be used to display the DBD packet exchanges:

```
debug ospf packet dd detail
```

By default, the Avaya VPN router sends 1500 as the MTU in database description packets. However, the Secure Router default tunnel MTU is 1420 bytes. As a result, one of the following changes is required on the Secure Router OSPF settings:

- Set OSPF MTU to 1500

  ```
  interface/tunnel toNVR# ip ospf mtu 1500
  ```

- Set OSPF to ignore MTU mismatch

  ```
  interface/tunnel toNVR# ip ospf mtu-ignore
  ```

The following table describes the source of some additional OSPF adjacency problems, and the appropriate command to diagnose the problem.

Reason for OSPF Adjacency Problem	Commands to Diagnose
OSPF is not configured on one of the routers.	`show ip ospf`
OSPF is not enabled on an interface where it is needed.	`show ip ospf interface`
OSPF HELLO or Dead timer interval values are mismatched.	`show ip ospf interface`
IP OSPF network-type mismatch on the adjoining OSPF interfaces.	`show ip ospf interface`
MTU mismatch between neighboring interfaces.	`show interface <intType> <intNum>` `show system jumbo-mtu-limit`
OSPF area-type is stub on one neighbor, but the adjoining neighbor in the same area is not configured for stub.	`show running-config` `show ip ospf interface`

Reason for OSPF Adjacency Problem	Commands to Diagnose

OSPF neighbors have duplicate Router IDs.	`show ip ospf`
	`show ip ospf interface`
	`show router-id`

Comments? infodev@avaya.com

Chapter 15: Troubleshooting Quality of Service

This section details the commands and procedures used to troubleshoot QoS.

Chassis QoS troubleshooting

This section contains the basic step-by-step troubleshooting procedure for QoS in order to isolate the issue for further troubleshooting.

QoS troubleshooting

Enable QoS

The **show qos chassis system** command shows the global auto-qos status and the status of global QoS, whether enabled or disabled.

```
SR4134#show qos chassis system
qos enabled, auto-qos disabled

Historical Statistics Configuration
-----------------------------------

Sample Interval       : 5 minutes
Uploading             : DISABLED

FTP parameters not yet configured
```

Auto QoS status

Auto QoS functions as a tool to apply the default QoS configurations for an interface. Auto QoS is applicable only for ethernet and bundles. For bundles auto-qos will be applied on egress direction and for ethernet interfaces it will be applied on the ingress direction. To know whether auto-qos is enabled for an interface **show qos chassis <ethernet/bundle> <ethernet slot/bundle name>**

```
SR4134#show qos chassis bundle wan

Interface: Bundle wan (Bandwidth = 1536Kbps)
Auto QoS State: Enabled (Interface)     QoS Status: Enabled
Service Policy Outbound: AutoQoSPolicyOut
```

While Auto QoS is enabled, CBQ is enabled internally for bundle interfaces and policing is enabled for ethernet interfaces.

SLA

For measuring SLA parameters such as delay, jitter and packet-loss SLA feature can be used. To view the statistics of the configured SLA profile **show sla profile <sla-id>** command can be used. To view all the active and inactive SLAs **show sla profile** command can be used.

Comments? infodev@avaya.com

```
SR4134# show sla profile 4
CONFIGURATION:
---------------
SLA Profile                : 4
Description                :
Type                       : UDP Jitter
Destination IP address     : 1.1.1.2
Destination Port           : 50001
Status                     : Enabled
Ready Status               : READY
Transmit Status            : IN IDLE
Operation                  : jitter
Packet Spacing             : 20 ms
Packet Size                : 80 bytes
Packet Count               : 20
Periodicity                : 10 min
TTL                        : 64
Time to start              : 0 min
Time Out                   : 5 sec
STATISTICS :
--------------
Remaining Lifetime                          : Forever
Minimum Two Way Delay Recorded(RTT)         : 0.000 ms
Maximum Two Way Delay Recorded(RTT)         : 0.000 ms
Average Two Way Delay Recorded(RTT)         : 0.000 ms
Number of Packets Transmitted               : 20
Number of Packets Received                  : 20
Number of Packets Lost                      : 0
Number of Transmit Drops                    : 0
Number of Late Arrivals                     : 0
Number of Out of Order Pkts                 : 0

SR4134# show sla profile
Active SLA Profiles :
+-------------------------------------------------------------------------------++
SLA Profile Ready status Transmit status  SLA Type      Description
+-------------------------------------------------------------------------------++
4           READY        IN IDLE          UDP Jitter
Number of active SLA Profiles : 1

Inactive SLA Profiles :
+-------------------------------------------------------------------------------++
SLA Profile Ready status Transmit status  SLA Type      Description
+-------------------------------------------------------------------------------++
1           NOT ACTIVE   IN IDLE          UDP Jitter
2           NOT ACTIVE   IN IDLE          UDP Echo
3           NOT ACTIVE   IN IDLE          UDP v6 Echo
Number of Inactive SLA Profiles : 3
```

Policy-map

When a policy map is created it will be listed with other policy-maps when “show qos chassis policy-map” command is executed. Policy-maps are used to configure class-maps with required parameters for classification, CBQ and policing. These policy-maps can be mapped to any valid interface and direction.

```
SR4134# show qos chassis policy-map
List of Policy Maps Created:
----------------------------
AutoQoSPolicyOut
AutoQoSPolicyOut4Q
AutoQoSPolicyIn
p1
map1
```

The classes configured on a policy-map and their configurations can be displayed using **show qos chassis policy-map <policy-name>**. This will also list the interfaces to which this policy-map is mapped. For detailed information about a class **show qos chassis policy-map <map-name> class <class-name>**. The configurations displayed include classification keys assigned to the class, CBQ, policing parameters and RED configurations.

Comments? infodev@avaya.com

```
SR4134# show qos chassis policy-map AutoQoSPolicyOut

Policy-map: AutoQoSPolicyOut
   Serviced Interfaces:
      Policy map is not attached to interface(s)

Class-map Details
+--------------------+--------+----------------------+-----------------------------------+
         CBQ                                 Police          Class-map
   CR(%)       PR(%)    Priority       CIR          PIR   ID.<name>(<pID>)
+--------------------+--------+----------------------+-----------------------------------+
      10.0       100.0        1           -           -1.critical(*)(+)
      10.0       100.0        2           -           - 2.control(*)(+)
      35.0       100.0        3           -           - 3.voice(*)(+)
      10.0       100.0        4           -           - 4.video(*)(+)
      10.0       100.0        4           -           - 5.streaming(*)(+)
       5.0       100.0        5           -           - 6.transaction(*)(+)
      10.0       100.0        5           -           - 7.oam(*)(+)
       9.0       100.0        8           -           - 8.best-effort(*)(+)
 (*) - Parent class-map is root. (+) - Leaf Class
```

```
SR4134#show qos chassis policy-map AutoQoSPolicyOut class oam
Policy-map: AutoQoSPolicyOut
class-map: oam         parent class: root
-------------------------------------------------------------------------
   Classification type:
      DiffServ Codepoints assigned to this Class:  cs1 af11 af12 af13
   Police:
      None
   RED:
      WRED - Status: OFF
               minth%   maxth%   mpd
      red        40       70      5
      yellow     50       80      5
      green      75      100      5
      EWF: 5
      DS RED - Status: ON
      dscp: cs1, minth%:  75, maxth%:  99, mpd:  5
      dscp: af11, minth%:  75, maxth%:  99, mpd:  5
      dscp: af12, minth%:  60, maxth%:  80, mpd:  5
      dscp: af13, minth%:  40, maxth%:  70, mpd:  5
   CBQ:
      cr-percent: 10.000000, pr-percent: 100.000000, priority: 5
   PBR:
      None
```

Policing

You can also configure the Avaya Secure Router 2330/4134 to police the traffic. There are two types of policing available: srTCM and trTCM. The steps included configuring policing are: create policy-map, class-map, and policer(srTCM/trTCM), and issue the service-policy-input command in order to apply the policy-map to the interface. You can also verify the policy-map statistics and interface level applied configuration.

```
SR4134# show qos chassis policy-map map

Policy-map: map
  Serviced Interfaces:
     ethernet0/1   - input


Class-map Details
+--------------------+--------+----------------------+-----------------------------------+
         CBQ                                 Police          Class-map
   CR(%)       PR(%)    Priority       CIR          PIR   ID.<name>(<pID>)
+--------------------+--------+----------------------+-----------------------------------+
      99.0       100.0        1           -           - 1.WAN(*)
       1.0         1.0        1        2000           - 2.voip(1)(+)
       1.0       100.0        7        2000           - 3.nonvoip(1)(+)
       0.0         0.0        8           -           - 4.c11(*)(+)
 (*) - Parent class-map is root. (+) - Leaf Class

SR4134/configure/qos/chassis/policy-map map/class-map nonvoip/police# show qos chassis policy-map
map class nonvoip

Policy-map: map
class-map: nonvoip        parent class: WAN
------------------------------------------------------------------------

   Classification type:
      Source IP Addresses assigned to this Class:  4.4.4.3

   Police:
      active, srTCM, color-aware, cir: 2000 kbps, committed-burst-time: 1000 ms, excess-burst-
time: 2000 ms, Green Action: Permit, Yellow Action: Permit, Red Action: Drop

   RED:

      WRED - Status: ON
             minth%   maxth%   mpd
      red      40       70      5
      yellow   50       80      5
      green    75      100      5
      EWF: 5

   CBQ:
      cr-percent: 1.000000, pr-percent: 100.000000, priority: 7

   PBR:
      None
```

Service policy

Mapping a policy-map to an interface is called as servicing the police-map. When a policy-map is serviced to an interface the classes that are created in the policy-map and their configurations will be instantiated on the interface. The commands **`show qos chassis service-policy`** and **`show qos chassis [interface-type] [interface-name]`** will help in identifying the successful mapping of the policy-map. The **`show qos chassis service-policy`** command lists all the policy-maps that are mapped to all the available interfaces. When the same command is entered with interface name as “show qos chassis service-policy [interface-type] [interface-name]”, it will display the policy-maps that are mapped to that interface on both directions. Show qos chassis interface command displays the policy-map attached and the classes that are created through the service-policy.

Comments? infodev@avaya.com

```
SR4134# show qos chassis service-policy
+------------------------------+---------------------+----------------------+
Interface                      Service-policy-input Service-policy-output
+------------------------------+---------------------+----------------------+
 ethernet0/1                   map1                      map1
 bundle  wan                   map1                 AutoQoSPolicyOut

SR4134# show qos chassis service-policy  bundle wan
  Interface : Bundle wan
      Service Policy Input  : map1
      Service Policy Output : AutoQoSPolicyOut

SR4134# show qos chassis bundle wan
Interface: Bundle wan (Bandwidth = 1536Kbps)
Auto QoS State: Enabled (Interface)                          QoS Status: Enabled
Service Policy Inbound: map1
Service Policy Outbound: AutoQoSPolicyOut
Interface Outbound Configuration & Statistics
-----------------------------------------------
CBQ: ON  Policing: OFF  MON: OFF
+--------------+---------------+---------------+---------------------+--------------------+
 CBQ-CR  CBQ-PR      Police     Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                         ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+---------------+---------------+---------------------+--------------------+
      0    1536       -       -       0       0          0          0 3.app-module-mpls(*)
      0    1536       -       -       0       0          0          0 2.app-module-default(*)
  138.2    1536       -       -       0       0          0          0 36.best-effort(2)
  153.6    1536       -       -       0       0          0          0 35.oam(2)
   76.8    1536       -       -       0       0          0          0 30.control(2)
  153.6    1536       -       -       0       0          0          0 29.critical(2)
   15.3    1536       -       -       0       0        440         16 1.outbound-default(*)

Interface Inbound Configuration & Statistics
-----------------------------------------------
Policing: OFF  MON: OFF   PBR: OFF
+--------------+---------------+---------------+---------------------+--------------------+
 CBQ-CR  CBQ-PR      Police     Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                         ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+---------------+---------------+---------------------+--------------------+
      -       -       -       -       0       0          0          0 28.c1(*)
```

Class configurations

The configurations that are done for a class-map can be verified by the **`show qos chassis policy-map [policy-name] class-map [class-name]`** command. After mapping the policy-map to an interface, the configurations for the instantiated classes on the interface can be verified by **`show qos chassis [interface-type] [interface-name] class [class-name] [inbound/outbound]`**. These commands will list all the configurations that are done on the class such as CBQ, Policing, RED parameters. The show command for interface class will also display the statistics of that class, such as packets forwarded, packets lost and policing statistics.

```
SR4134# show qos chassis policy-map map1 class c1

Policy-map: map1
class-map: c1         parent class: root
------------------------------------------------------------------------

   Classification type:
      DiffServ Codepoints assigned to this Class:  Default

   Police:
      None

   RED:

      WRED - Status: ON
              minth%    maxth%    mpd
      red       40        70      5
      yellow    50        80      5
      green     75       100      5
      EWF: 5

      DS RED - Status: OFF

   CBQ:
      cr-percent: 20.000000, pr-percent: 20.000000, priority: 8

   PBR:
      None

SR4134# show qos chassis bundle wan class c1 inbound

Class: c1 (Inbound )
Parent Class: root-in (CR = 1536 kbps ; PR = 1536 kbps)
Interface: Bundle wan (Bandwidth = 1536Kbps)
Auto QoS State: Enabled (Interface)                          QoS Status: Enabled
MON IN: OFF, Policing IN: OFF,  PBR Redirect IN: OFF

Configuration
-------------

Policing - Not Configured

DiffServ Codepoints assigned to this Class:
Default

Traffic Statistics
------------------
Avg Rate Out: 0 Kbps
Avg Rate In : 0 Kbps

Counters (since last boot/clear):       Packet drop details
---------------------------------       -------------------
Packets Forwarded:                   0 Queue overflow:                      0
Bytes Forwarded:                     0 No buffers:                          0
Packets Dropped:                     0 Policing pkts drop:                  0
Bytes Dropped:                       0 RED pkts dropped:                    0
```


Comments? infodev@avaya.com

Policy Based Routing

The PBR redirect action is specified for each policy class. The PBR redirection action includes configuring either next-hop IP address or interface. The command **show qos chassis policy-map [policy-map name] detail** will display the PBR configuration for a class.

```
SR4134/configure/qos/chassis/policy-map p2/class-map c2# show qos chassis policy-map p2 detail

Policy-map: p2
   Serviced Interfaces:
      bundle wan  - output

class-map: c2        parent class: root
---------------------------------------------------------------------
   Classification type:
      DiffServ Codepoints assigned to this Class:  af33

   Police:
      None
   RED:
      WRED - Status: ON
              minth%   maxth%   mpd
      red       40       70      5
      yellow    50       80      5
      green     75      100      5
      EWF: 5

      DS RED - Status: OFF
   CBQ:
      cr-percent: 2.000000, pr-percent: 2.000000, priority: 8
   PBR:
      Next Hop Ip:  10.1.1.1
```

Marking

After classification, marking a field in the packet such that it can be easily recognized later (for instance, an http packet from a certain source needs to be classified only once, after which it is marked. The network core looks at the marking to figure out what packet it is and services it appropriately). The command **show qos chassis policy-map [policy-map name] detail** will display marking parameter for a class.

```
SR4134/configure/qos/chassis/policy-map p2/class-map c2# mark  dscp 44
SR4134/configure/qos/chassis/policy-map p2/class-map c2# show qos chassis policy-map p2 detail

Policy-map: p2
   Serviced Interfaces:
      bundle wan  - output


class-map: c2        parent class: root
---------------------------------------------------------------------

   Classification type:
      DiffServ Codepoints assigned to this Class:  af33

   Police:
      None
   Mark DSCP: 44
```

Policy-map cloning

The policy-maps can be cloned to another policy-map name. This feature will help to create a same set of configuration, but can be edited for minor changes from its original policy-map configuration. The command **clone-policy-map [cloned-policy-map] [policy-map-to-be-cloned]** used to clone a policy-map. We can use **show qos chassis policy-map [policy-map-name] detail** to view the details of cloned policy-map.

```
SR4134/configure/qos/chassis# clone-policy-map clone p2
Policy profile created succesfully
SR4134/configure/qos/chassis# show qos chassis policy-map clone detail

Policy-map: clone
   Serviced Interfaces:
      Policy map is not attached to interface(s)
class-map: c2        parent class: root
-------------------------------------------------------------------------
   Classification type:
      DiffServ Codepoints assigned to this Class:  af33
   Police:
      None
   Mark DSCP: 44
   RED:
      WRED - Status: ON
               minth%   maxth%   mpd
      red        40       70      5
      yellow     50       80      5
      green      75      100      5
      EWF: 5

      DS RED - Status: OFF
   CBQ:
      cr-percent: 2.000000, pr-percent: 2.000000, priority: 8
   PBR:
      Next Hop Lsp: mpls1
```

Historical statistics

When traffic classes are created and QoS features are enabled, per-class traffic statistics will get updated during traffic classification. These statistics cab be viewed on system console using CLI commands. But the user can view only the statistics at that time. If the user wants to have the statistics for every hour, then the user has to manually take a log from the CLI. To make this process as automated Historical statistics is used. It helps the user to upload these Historical statistics to an FTP server. Once upload is enabled, the historical statistics will be uploaded to the FTP server for every upload interval. The user can configure the upload interval. The user can also turn off the upload feature. For each upload a new file will be created in the FTP server. The file name will have the time at which it is uploaded. Statistics are taken for every sample interval for a period of upload interval time. Then this statistics will be

Comments? infodev@avaya.com

uploaded to the FTP server. The command **show qos chassis historical-stats configuration** used to verify the historical statistics configuration.

```
SR4134/configure# show qos chassis historical-stats configuration

Historical Statistics Configuration
-----------------------------------

Sample Interval       : 5 minutes
Uploading             : ENABLED
Upload interval       : 1 hrs
Upload File ID        : 222

FTP parameters
        Primary FTP server    : 100.1.1.1
        Secondary FTP server  : 200.1.1.1
        Ftp user name         : qosteam
        Ftp password          : *****
```

MPLS-QoS

The command **show qos chassis [interface-name] mpls lsp [lsp-name]** will display the MPLS configuration.

```
SR4134/configure/mpls/traffic-eng-lsp# show qos chassis ethernet 0/1 mpls ?
  class                         Policy class name
  direction                     Specify inbound/outbound
  lsp                           MPLS LSP interface name
      <cr>


SR4134/configure/mpls/traffic-eng-lsp# show qos chassis ethernet 0/1 mpls lsp ?
  WORD                          MPLS LSP interface name

SR4134/configure # show qos chassis ethernet 0/1 mpls lsp lsp1
```

Interface RED

The command **show qos chassis red [bundle name]** will display interface RED configuration for a bundle. Also **show interface bundle [bundle name]** will display the RED details.

```
SR4134/configure # show qos chassis red ?
  WORD                          Bundle name

SR4134/configure # show qos chassis red wan

Interface buffer/queue management info:
Maximum allowed driver queue size in buffers     : 21 (20, 1)
Maximum class queue buffers                      : 0
Total buffers                                    : 21
Current queue size in buffers                    : 0
Current queue size in buffers(wred)              : 0
Current queue size in bytes                      : 0

RED Information
-----------------
WRED Status: Enabled    DS-RED Status: Disabled

Current queue size     = 0          Maximum queue size     = 0
Current avg queue size = 0          Maximum avg queue size = 0
Current Q size for WRED= 0          Queue overflows                = 0

WRED Configuration:
Wq Bias Factor  : 5                 Maxth High Bound : 20
----------+---------+----------+---------+-----+
     color       min       max  min  max  mpd
           threshold threshold    %    %
----------+---------+----------+---------+-----+
     green        15         20   75  100    5
    yellow        10         16   50   80    5
       red         8         14   40   70    5
```

Troubleshooting QoS - Error conditions

Classification

Not able to add classification keys to a class

Symptom: The following error message will come. 'Error! Invalid classification type requested'.

Problem description: In MF classification tree Each level should have unique classification type i.e. all the classes in same level should have the same classification type.

Prerequisite: Policy-map should be created successfully

Comments? infodev@avaya.com

```
SR4134/configure/qos/chassis/policy-map p1/class-map c1# match dscp 40
SR4134/configure/qos/chassis/policy-map p1/class-map c1#
SR4134/configure/qos/chassis/policy-map p1/class-map c1#
SR4134/configure/qos/chassis/policy-map p1# class-map c2 root
SR4134/configure/qos/chassis/policy-map p1/class-map c2#
SR4134/configure/qos/chassis/policy-map p1/class-map c2# match tos ?
  WORD                          IP ToS field value/range or 'default' (E.g.
                                match tos 5-8). Valid: 0-255

SR4134/configure/qos/chassis/policy-map p1/class-map c2# match tos 255
Error! Invalid classification type requested
SR4134/configure/qos/chassis/policy-map p1/class-map c2#
```

Troubleshooting tips: We can't assign different classification type for the classes at the same level.

Same classification key should not be assigned to some other class in the same level

Symptom: The following error message will come. 'Error! [classification type] was already assigned.'

Problem description: In MF classification tree, different classes at the same level can not have same classification key value. But classes at different level can have same classification type and classification key value.

Prerequisite: Policy-map should be created successfully.

```
SR4134/configure/qos/chassis/policy-map p1/class-map c1# match dscp 40
SR4134/configure/qos/chassis/policy-map p1# class-map c2 root
SR4134/configure/qos/chassis/policy-map p1/class-map c2# match dscp 40
Error! DSCP Codepoint 40 was already assigned.
```

Troubleshooting tips: We can't assign same classification key values for the classes at the same level, because this may lead to confusion while classifying the packets.

Assigning multiple keys to a class

Symptom: The following error message will come. 'Error! Invalid classification type requested'

Problem description: A class can have only one classification type but can have multiple keys. If we try to assign a different key, which is of different classification type, it won't accept.

Prerequisite: Policy-map should be created successfully.

```
SR4134/configure/qos/chassis/policy-map p1/class-map c2#
SR4134/configure/qos/chassis/policy-map p1/class-map c2# match dscp 40
Error! DSCP Codepoint 40 was already assigned.
SR4134/configure/qos/chassis/policy-map p1/class-map c2# match dscp 30
SR4134/configure/qos/chassis/policy-map p1/class-map c2#
SR4134/configure/qos/chassis/policy-map p1/class-map c2# match tos 5
Error! Invalid classification type requested
SR4134/configure/qos/chassis/policy-map p1/class-map c2#
```

Troubleshooting tips: All keys should belong to the same classification type for a class.

Not able to modify the assigned key

Symptom:

Problem description: If we want to change or reassign a key to a class, we can't just assign the key with new value. If we do so it will add the new key as additional one instead of over write the existing one.

Prerequisite: Policy-map should be created successfully.

```
SR4134/configure/qos/chassis# policy-map p2
Policy profile created successfully
SR4134/configure/qos/chassis/policy-map p2# class-map c1 root
SR4134/configure/qos/chassis/policy-map p2/class-map c1# match protocol tcp
SR4134/configure/qos/chassis/policy-map p2/class-map c1# match protocol udp
SR4134/configure/qos/chassis/policy-map p2/class-map c1#
SR4134/configure/qos/chassis/policy-map p2/class-map c1# show qos chassis policy-map p2 detail

Policy-map: p2
   Serviced Interfaces:
      Policy map is not attached to interface(s)

class-map: c1        parent class: root
-----------------------------------------------------------------------
   Classification type:
      IP Protocol values assigned to this class:  6(TCP) 17(UDP)
   Police:
      None
   RED:
      WRED - Status: ON
               minth%   maxth%   mpd
      red        40       70      5
      yellow     50       80      5
      green      75      100      5
      EWF: 5
   CBQ:
      None
   PBR:
      None
```

Troubleshooting tips: First give '**no**' form of the command then assign the new key value to the class.

Comments? infodev@avaya.com

```
SR4134/configure/qos/chassis# policy-map p2
SR4134/configure/qos/chassis/policy-map p2# class-map c1
SR4134/configure/qos/chassis/policy-map p2/class-map c1# match protocol tcp
SR4134/configure/qos/chassis/policy-map p2/class-map c1# show qos chassis policy-map p2 detail

Policy-map: p2
   Serviced Interfaces:
      Policy map is not attached to interface(s)

class-map: c1        parent class: root
---------------------------------------------------------------------
   Classification type:
      IP Protocol values assigned to this class:  6(TCP)
   Police:
      None
   RED:
      WRED - Status: ON
              minth%   maxth%   mpd
      red       40       70      5
      yellow    50       80      5
      green     75      100      5
      EWF: 5
   CBQ:
      None
   PBR:
      None

SR4134/configure/qos/chassis/policy-map p2/class-map c1# no match protocol tcp
SR4134/configure/qos/chassis/policy-map p2/class-map c1# match protocol udp
SR4134/configure/qos/chassis/policy-map p2/class-map c1# show qos chassis policy-map p2 detail

Policy-map: p2
   Serviced Interfaces:
      Policy map is not attached to interface(s)

class-map: c1        parent class: root
---------------------------------------------------------------------

   Classification type:
      IP Protocol values assigned to this class:  17(UDP)

   Police:
      None
   RED:
      WRED - Status: ON
              minth%   maxth%   mpd
      red       40       70      5
      yellow    50       80      5
      green     75      100      5
      EWF: 5

   CBQ:
      None

   PBR:
      None
```

Packets are not getting classified

Symptom: Packet count can be '0' or very less for a class

Problem description: When a policy-map is attached to a interface, the user may perceive packet count is '0' or very less for a class. Giving the command **`show qos chassis [interface] [interface name]`** can see packet flow.

Prerequisite: Policy-map should be created and attached to an interface successfully.

Scenario 1:

```
SR4134/configure/interface/ethernet (0/1)/qos/chassis# show qos chassis ethernet 0/1
Interface: Ethernet 0/1 (Bandwidth: Interface = - ; QoS = 50000Kbps)
Auto QoS State: Disabled                                    QoS Status: Enabled
Service Policy Inbound: p1
Service Policy Outbound: p1
Interface Outbound Configuration & Statistics
-----------------------------------------
CBQ: OFF  Policing: OFF  MON: OFF
+--------------+--------------+--------------+--------------------+--------------------+
 CBQ-CR  CBQ-PR      Police     Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                         ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+--------------+--------------+--------------------+--------------------+
      0   50000       -       -       0       0          0          0 3.app-module-mpls(*)
      0   50000       -       -       0       0          0          0 2.app-module-default(*)
      0       0       -       -       0       0          0          0 9.c2(2)
     50      50       -       -       0       0          0          0 8.c1(2)
      0       0       -       -       0       0          0          0 10.c3(8)
    500   50000       -       -       0       0          0          0 1.outbound-default(*)
Interface Inbound Configuration & Statistics
-----------------------------------------
Policing: OFF  MON: OFF   PBR: OFF
+--------------+--------------+--------------+--------------------+--------------------+
 CBQ-CR  CBQ-PR      Police     Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                         ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+--------------+--------------+--------------------+--------------------+
      -       -       -       -       0       0          0          0 6.c2(*)
      -       -       -       -       0       0          0          0 5.c1(*)
      -       -       -       -       0       0          0          0 7.c3(5)
      -       -  500000       -       0       0          0          0 4.inbound-default(*)
```

Scenario 2:

```
SR4134/configure/interface/ethernet (0/1)/qos/chassis# show qos chassis ethernet 0/1
Interface: Ethernet 0/1 (Bandwidth: Interface = - ; QoS = 50000Kbps)
Auto QoS State: Disabled                                    QoS Status: Enabled
Service Policy Inbound: p1
Service Policy Outbound: p1
Interface Outbound Configuration & Statistics
-----------------------------------------
CBQ: OFF  Policing: OFF  MON: ON
+--------------+--------------+--------------+--------------------+--------------------+
 CBQ-CR  CBQ-PR      Police     Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                         ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+--------------+--------------+--------------------+--------------------+
      0   50000       -       -       0       0          0          0 3.app-module-mpls(*)
      0   50000       -       -       0       0          0          0 2.app-module-default(*)
      0       0       -       -       0       0          0          0 9.c2(2)
     50      50       -       -       0       0          0          0 8.c1(2)
      0       0       -       -       0       0          0          0 10.c3(8)
    500   50000       -       -   212.2   212.2     213311          0 1.outbound-default(*)
Interface Inbound Configuration & Statistics
-----------------------------------------
Policing: OFF  MON: ON    PBR: OFF
+--------------+--------------+--------------+--------------------+--------------------+
 CBQ-CR  CBQ-PR      Police     Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                         ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+--------------+--------------+--------------------+--------------------+
      -       -       -       -       0       0          0          0 6.c2(*)
      -       -       -       -       0       0          0          0 5.c1(*)
      -       -       -       -       0       0          0          0 7.c3(5)
      -       -  500000       -   212.2   212.2     213311          0 4.inbound-default(*)
```

Troubleshooting tips:

- Check whether any of the QoS feature like monitoring, policing, or CBQ is enabled.

Comments? infodev@avaya.com

```
SR4134/configure# interface ethernet 0/1
Configuring existing Ethernet interface
SR4134/configure/interface/ethernet (0/1)# qos
SR4134/configure/interface/ethernet (0/1)/qos# chassis
SR4134/configure/interface/ethernet (0/1)/qos/chassis# enable ?
  cbq                           Enable CBQ on the interface
  policing                      Enable policing on the interface
  monitoring                    Enable monitoring only
  pbr                           Enable Policy Based Routing

SR4134/configure/interface/ethernet (0/1)/qos/chassis# enable monitoring in
SR4134/configure/interface/ethernet (0/1)/qos/chassis# enable monitoring out
```

- QoS feature is enabled but packets are classified into interface default class as shown in Scenario 2. possible cause for this is the packet may not reach the leaf node. Follow the steps given below.
  - the MF tree configured. you can use '**`show qos chassis policy-map [policy-map name] detail`**' to get the details about the policy-map.
  - Ensure that packets are getting classified at the parent node. Then only it will reach the leaf node. For this check care fully the key values assigned the parents are appropriate.
  - If problem still persist then capture the packet by using "tcp dump" or Ethereal or any of the available packet capturing tools. Capture the packet and analyze it with the MF tree configured.

Not all the packets are classified

Symptom: The user can perceive less number of packets are getting classified than what he sent/incoming/outgoing packets.

Problem description: Sometimes the user may perceive not all packets are getting classified. He may find some of the packets which he sent/incoming/outgoing is classified under interface default class.

Prerequisite: Policy-map should be created and attached to an interface successfully.

Troubleshooting tips: Create a class-default class for each classification type. Then all the packets which aren't classified under the given classes won't go to interface default rather it goes to class-default.

```
SR4134/configure/qos/chassis/policy-map p1/class-map c3#
SR4134/configure/qos/chassis/policy-map p1#
SR4134/configure/qos/chassis# show qos chassis ethernet 0/1
Interface: Ethernet 0/1 (Bandwidth: Interface = - ; QoS = 50000Kbps)
Auto QoS State: Disabled                                    QoS Status: Enabled
Service Policy Outbound: p1
Interface Outbound Configuration & Statistics
----------------------------------------------
CBQ: OFF  Policing: OFF  MON: ON
+--------------+---------------+---------------+---------------------+---------------------+
 CBQ-CR  CBQ-PR      Police      Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                          ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+---------------+---------------+---------------------+---------------------+
      0   50000       -       -       0       0          0          0 3.app-module-mpls(*)
      0   50000       -       -       0       0          0          0 2.app-module-default(*)
      0       0       -       -    53.2    53.2          0          0 11.c3(2)
      0       0       -       -    51.5    51.6          0          0 9.c2(2)
    500   50000       -       -    53.3    53.3          0          0 8.c1(2)
    500   50000       -       -       0       0          0          0 1.outbound-default(*)

Interface Inbound Configuration & Statistics
----------------------------------------------
Policing: OFF  MON: ON   PBR: OFF
+--------------+---------------+---------------+---------------------+---------------------+
 CBQ-CR  CBQ-PR      Police      Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                          ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+---------------+---------------+---------------------+---------------------+
      -       -  500000       -       0       0          0          0 4.inbound-default(*)
```

Policy-map

Not able delete a policy-map

Symptom: The following error message will come 'Error! policy profile is mapped to one or more interfaces'

Problem description: Policy-map can be deleted only if it is not mapped to any of the interfaces.

Prerequisite: Policy-map should be created and attached to an interface successfully.

```
SR4134/configure/qos/chassis# no policy-map p1
Error! policy profile is mapped to one or more interfaces
```

Troubleshooting tips: To what are all the interfaces the policy-map is attached can be known by using the command **`show qos chassis policy-map [policy-map name]`**.

Comments? infodev@avaya.com

```
SR4134/configure/qos/chassis# show qos chassis policy-map p1

Policy-map: p1
   Serviced Interfaces:
      ethernet0/1   - output


Class-map Details
+--------------------+--------+----------------------+-----------------------------------+
         CBQ                                 Police          Class-map
   CR(%)       PR(%)    Priority       CIR          PIR   ID.<name>(<pID>)
+--------------------+--------+----------------------+-----------------------------------+
       0.1         0.1        8           -           - 1.c1(*)(+)
       0.0         0.0        8           -           - 2.c2(*)(+)
       0.0         0.0        8           -           - 4.c3(*)(+)
 (*) - Parent class-map is root. (+) - Leaf Class

SR4134/configure/qos/chassis#

SR4134/configure/interface/ethernet (0/1)/qos/chassis# no service-policy p1 out
```

We can alternatively remove the policy-map by using the 'force' option. This option will remove the policy-map force fully if it is attached to the interfaces.

```
SR4134/configure# qos
SR4134/configure/qos# chassis
SR4134/configure/qos/chassis# no policy-map p1 ?
  force                          Forcefully deletion of policy map
      <cr>
SR4134/configure/qos/chassis# no policy-map p1 force
```

Not able to modify the policy-map

Symptom 1: Modification fails

Problem description: If the policy-map is attached to a crypto interface and the modification is related to IPv6 then it fails since crypto interface won't support IPv6.

Prerequisite: Policy-map should be created and attached to a crypto interface successfully.

Troubleshooting tips: Remove the policy-map from the crypto if you want to do IPv6 related changes. But this policy-map can not be re attached to the crypto interface again.

Symptom 2: Modifying policing parameter for a class fails.

Problem description: Logical interfaces will accept policing parameters only in kbps. If you try to change the parameter in terms of percent, it is not accepted.

Prerequisite: Policy-map should be created successfully.

Example 1: policy-map is configured with policing parameter in percentage. It will fail in logical interface.

```
SR4134/configure#
SR4134/configure# qos
SR4134/configure/qos# chassis
SR4134/configure/qos/chassis# policy-map p1
Policy profile created successfully
SR4134/configure/qos/chassis/policy-map p1# class-map c1 root
SR4134/configure/qos/chassis/policy-map p1/class-map c1# match dscp 20
SR4134/configure/qos/chassis/policy-map p1/class-map c1# police
SR4134/configure/qos/chassis/policy-map p1/class-map
SR4134/configure/qos/chassis/policy-map p1/class-map c1/police# srtcm cir-percentage 20
SR4134/configure/qos/chassis/policy-map p1/class-map c1#
SR4134/configure/qos/chassis/policy-map p1#
SR4134/configure/qos/chassis#
SR4134/configure/qos#
SR4134/configure# interface tunnel tunnel1
configuring new tunnel interface
 tunnel1=======>
SR4134/configure/interface/tunnel tunnel1#
SR4134/configure/interface/tunnel tunnel1# qos
SR4134/configure/interface/tunnel tunnel1/qos# chassis
SR4134/configure/interface/tunnel tunnel1/qos/chassis# service-policy p1 in
Error! Cannot configure policing parameters(CIR/PIR in percenrage and Burst's in Msec's) to class
Mapc1 on this virtual
interface
Error! Cannot configure policing parameters to class Mapc1 on this interface
SR4134/configure/interface/tunnel tunnel1/qos/chassis#
```

Example 2: policy-map is configured with policing parameter in kbps. policy-map is attached to a logical interface. Try to reconfigure the policing parameters in percentage.

Comments? infodev@avaya.com

```
SR4134/configure# qos
SR4134/configure/qos# chassis
SR4134/configure/qos/chassis# policy-map p1
SR4134/configure/qos/chassis/policy-map p1# class-map c1
SR4134/configure/qos/chassis/policy-map p1/class-map c1# police
SR4134/configure/qos/chassis/policy-map p1/class-map c1/police# srtcm cir 50
SR4134/configure/qos/chassis# show qos chassis policy-map p1 de
Policy-map: p1
   Serviced Interfaces:
      Policy map is not attached to interface(s)
class-map: c1        parent class: root
---------------------------------------------------------------------
   Classification type:
      DiffServ Codepoints assigned to this Class:  af22
   Police:
      active, srTCM, color-blind, cir: 50 kbps, committed-burst-time: 1000 ms, excess-burst-time:
2000 ms, Green Action:
 Permit, Yellow Action: Permit, Red Action: Drop
   RED:
      WRED - Status: ON
              minth%   maxth%   mpd
      red       40       70      5
      yellow    50       80      5
      green     75      100      5
      EWF: 5
      DS RED - Status: OFF
   CBQ:
      None
   PBR:
      None

SR4134/configure/qos/chassis#
SR4134/configure/qos#
SR4134/configure# interface tunnel tunnel1
configuring existing tunnel interface
 tunnel1=======>
SR4134/configure/interface/tunnel tunnel1# qos
SR4134/configure/interface/tunnel tunnel1/qos# chassis
SR4134/configure/interface/tunnel tunnel1/qos/chassis# service-policy p1 in
SR4134/configure/interface/tunnel tunnel1/qos/chassis#
SR4134/configure/interface/tunnel tunnel1/qos#
SR4134/configure/interface/tunnel tunnel1#
SR4134/configure# qos
SR4134/configure/qos# chassis
SR4134/configure/qos/chassis# policy-map p1
SR4134/configure/qos/chassis/policy-map p1# class-map c1
SR4134/configure/qos/chassis/policy-map p1/class-map c1# police
SR4134/configure/qos/chassis/policy-map p1/class-map c1/police# srtcm cir-p 50
Error! Cannot configure policing parameters (CIR/PIR in percenrage and Burst's in Msec's) to class
Mapc1 on this virtual
interface
Error! Applying Policing failed for interface tunnel1. Configuration rejected.
Error! Cannot able to configure srtcm for mapped interface
SR4134/configure/qos/chassis/policy-map p1/class-map c1/police#
```

Troubleshooting tips: If a policy-map is attached to any of the logical interfaces then policing parameters should be kbps.

Symptom 3: Modification of CBQ parameter fails.

Problem description: When we modify the CBQ we should take of the interface bandwidth. Since the modification is in percentage sometimes the percentage value may lead to bandwidth allocation for a class as less than 1 kbps which cbq doesn't support.

Prerequisite: Policy-map should be created and attached to an interface successfully.

```
SR4134/configure# qos
SR4134/configure/qos# chassis
SR4134/configure/qos/chassis# policy-map p2
SR4134/configure/qos/chassis/policy-map p2# class-map c1
SR4134/configure/qos/chassis/policy-map p2/class-map c1# match dscp 20
Error! Invalid classification type requested
SR4134/configure/qos/chassis/policy-map p2/class-map c1#
SR4134/configure/qos/chassis/policy-map p2#
SR4134/configure/qos/chassis# no policy-map p2
SR4134/configure/qos/chassis# policy-map p2
Policy profile created succesfully
SR4134/configure/qos/chassis/policy-map p2# class-map c2 root
SR4134/configure/qos/chassis/policy-map p2/class-map c2# match dscp 30
SR4134/configure/qos/chassis/policy-map p2/class-map c2# cbq cr ?
  WORD                          Committed Rate as % of interface bandwidth
                                (E.g cbq cr-percent 45.689).

SR4134/configure/qos/chassis/policy-map p2/class-map c2# cbq cr 2
SR4134/configure/qos/chassis/policy-map p2/class-map c2#
SR4134/configure/qos/chassis/policy-map p2#
SR4134/configure/qos/chassis#
SR4134/configure/qos#
SR4134/configure# interface bundle wan
configuring existing WAN bundle interface wan
SR4134/configure/interface/bundle wan# qos
SR4134/configure/interface/bundle wan/qos# chassis
SR4134/configure/interface/bundle wan/qos/chassis# service-policy p2 out
```

Troubleshooting tips: Interfaces bandwidth should be taken into account while decide the CBQ CIR percentage. The percentage value should not lead to the bandwidth allocated for the class as less than 1 kbps, which CBQ doesn't support.

Not able to add a class to the policy-map

Symptom: The following error will come 'Error! Cannot add more than 750 classes per policy profile'

Problem description: Maximum number of classes that we can configure for policy-map is 750, beyond which current implementation is not supported.

Prerequisite: Policy-map with 750 classes is created successfully.

```
SR4134/configure/qos/chassis/policy-map p2# class-map c751 root
Error! Cannot add more than 750 classes per policy profile
```

Troubleshooting tips: Remove any of the existing unwanted class-map to add a new one.

Policing/Metering

Configuring policing mode as color aware/blind fails

Symptom: The following message will be popping up 'policing is not configured for this class'.

Comments? infodev@avaya.com

Problem description: Policing can be configured either in color aware or color blind mode. By default color blind will be enabled. Configuring color aware mode requires policing parameters to be configured first.

Prerequisite: Policy-map and class map should be created successfully.

```
SR4134/configure/qos/chassis/policy-map map1/class-map c1/police# color-aware

    policing is not configured for this class.
```

Troubleshooting tips: Configure the policing parameters (CIR/PIR and CBS/PBS) first before configuring color aware mode.

Not able to police the traffic

Symptom: Policing statistics at the class level are not getting updated while traffic is forwarded on that interface.

Problem description: srTCM or trTCM are the two models where either can be configured to meter a particular traffic. The command **`show qos chassis interface [interface-name] class [class-name]`** which will display class statistics on an interface will provide lot of information like policing parameters configured, actions associated with each conformance level and the statistics to display green, yellow, or red packets forwarded which are policed.

Troubleshooting tips: Following are the step-by-step troubleshooting procedure for policing in order to isolate the issue for further troubleshooting.

1. Ensure that the policing parameters are configured properly at the policy map level using the command **`show qos chassis policy-map [policy-name]`** and at the interface level after mapping with the above policy use **`show qos chassis interface [interface-name] class [class-name]`**.

```
SR4134# show qos chassis policy-map map

Policy-map: map
   Serviced Interfaces:
      ethernet0/1  - input


Class-map Details
+--------------------+--------+----------------------+-----------------------------------+
         CBQ                                 Police          Class-map
   CR(%)      PR(%)    Priority       CIR          PIR   ID.<name>(<pID>)
+--------------------+--------+----------------------+-----------------------------------+
      99.0      100.0        1           -           - 1.WAN(*)
       1.0        1.0        1        2000           - 2.voip(1)(+)
       1.0      100.0        7        2000           - 3.nonvoip(1)(+)
       0.0        0.0        8           -           - 4.c11(*)(+)
 (*) - Parent class-map is root. (+) - Leaf Class
```

2. Ensure that policing is enabled on the interface using **`show qos chassis interface [interface-name] class [class-name]`**.
3. Ensure that qos is enabled at the global level.

```
SR4134#show qos chassis system

  qos enabled, auto-qos disabled

Historical Statistics Configuration
-----------------------------------

Sample Interval       : 5 minutes
Uploading             : DISABLED

FTP parameters
```

4. Notice that the Policing statistics that corresponds to the class-map voip increases. If you do not see the statistics for the corresponding class-map, verify the class map in policy map which is attached to this interface.

Policing based marking not working

Symptom: User may see that marking is not working based on the conformance level assigned by the policer

Problem description: Three actions can be configured for different conformance level.

Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

1. Remark is not configured for the class
2. Policing is not enabled for the interface.

Comments? infodev@avaya.com

```
SR4134# show qos chassis policy-map map class voip

Policy-map: map
class-map: voip        parent class: WAN
------------------------------------------------------------------------

   Classification type:
      Source IP Addresses assigned to this Class:  4.4.4.2

   Police:
      active, srTCM, color-blind, cir: 2000 kbps, committed-burst-time: 1000 ms, excess-burst-
time: 2000 ms, Green Action: mark-dscp-20, Yellow Action: Permit, Red Action: Drop

   RED:

      WRED - Status: ON
              minth%   maxth%   mpd
      red       40       70      5
      yellow    50       80      5
      green     75      100      5
      EWF: 5

   CBQ:
      cr-percent: 1.000000, pr-percent: 1.000000, priority: 1

   PBR:
      None

SR4134#show qos chassis ethernet 0/1

Interface: Ethernet 0/1 (Bandwidth: Interface = - ; QoS = 50000Kbps)
Auto QoS State: Disabled                                    QoS Status: Enabled
Service Policy Inbound: map
Service Policy Outbound: map4

Interface Outbound Configuration & Statistics
---------------------------------------------
CBQ: OFF  Policing: ON  MON: OFF
+--------------+---------------+---------------+---------------------+--------------------+
 CBQ-CR  CBQ-PR      Police      Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                          ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+---------------+---------------+---------------------+--------------------+
      0   50000       -       -       0       0         7295        95 3.app-module-mpls(*)
      0   50000       -       -       0       0            0         0  2.app-module-default(*)
```

Shaping

Configuring CBQ fails on a Class-map

Symptom: An Error message will be thrown when CBQ is configured at policy-map level.

Problem description: Configuring CBQ parameters should adhere to the following conditions:

1. Sum of all leaf classes should not exceed 99 percent.
2. Parent-class should be configured with a valid Peak Rate that is greater than or equal to the requested Committed Rate of the child class.
3. Sum of CR of child classes to a parent class should not exceed the Parent class Peak rate.
4. Peak rate of child class should not exceed Parent class Peak rate.

Prerequisite: Policy-map should be successfully created

```
SR4134/configure/qos/chassis/policy-map map2# class-map c1 root
SR4134/configure/qos/chassis/policy-map map2/class-map c1#
SR4134/configure/qos/chassis/policy-map map2# class-map c2 c1
SR4134/configure/qos/chassis/policy-map map2/class-map c2# cbq cr-p 30 pr- 50
Error! Peak-rate(50.000000 %) cannot exceed parent class (c1) peak-rate of 0.000000 %
Error! Update of CBQ parameters failed for class map(c2)
SR4134/configure/qos/chassis/policy-map map2/class-map c2# show qos chassis policy-map map2 class
c1

Policy-map: map2
class-map: c1        parent class: root
------------------------------------------------------------------------
   Classification type:
      None
   Police:
      None

   RED:

      WRED - Status: ON
              minth%   maxth%   mpd
      red       40       70     5
      yellow    50       80     5
      green     75      100     5
      EWF: 5

   CBQ:
      None
```

Troubleshooting tips: Verify whether the configuration adhere to the conditions specified in problem description.

Configuring CBQ fails on a Class-map mapped to interfaces

Symptom: An Error message will be thrown when CBQ is configured at policy-map level.

Problem description: If configuring CBQ parameters fail for a policy-map, which is mapped to one or more interfaces then the following can be the reasons:

- Actual CR or PR value (not the percentage) for the interface should not be less than 1 Kbps. Example: CR percent of 1 for an interface with bandwidth of 9 Kbps will result in CR value of 0.9 Kbps.
- Buffers are not available for a particular interfaces. Buffers are allocated to interfaces based on the interface bandwidth. The CBQ configuration should not exceed the allocated buffers.

Prerequisite: Policy-map should be successfully created and mapped to interfaces.

Comments? infodev@avaya.com

```
SR4134/configure/interface/bundle wan1/qos/chassis# service-policy map11 out
SR4134/configure/interface/bundle wan1/qos/chassis# show qos chassis policy-map map11

Policy-map: map11
   Serviced Interfaces:
      ethernet0/2  - output
      bundle wan1  - output


Class-map Details
+--------------------+--------+----------------------+-----------------------------------+
         CBQ                                 Police          Class-map
   CR(%)       PR(%)    Priority       CIR          PIR   ID.<name>(<pID>)
+--------------------+--------+----------------------+-----------------------------------+
       0.0         0.0        8            -           - 1.c1(*)(+)
 (*) - Parent class-map is root. (+) - Leaf Class

SR4134/configure# qos
SR4134/configure/qos# chassis
SR4134/configure/qos/chassis# policy-map map11
SR4134/configure/qos/chassis/policy-map map11# class-map c1
SR4134/configure/qos/chassis/policy-map map11/class-map c1# cbq cr-percent .01
Error! Invalid committed-rate specified, the CR should be greater than or equal to 1kbps
Error! Applying cbq failed for interface wan1. Configuration rejected.
```

Troubleshooting tips:

1. Make sure that the configuration doesn't result in less than 1 Kbps in any of the mapped interfaces.
2. Verify that there will not be any buffer issues on any interface due to the new configuration.
3. If the configuration fails for only one interface and succeeds for other interfaces, then un-map the policy-map from that interface. Clone the policy-map and service it to that interface and modify the CBQ parameters in the actual policy-map.

Packets getting dropped for a class when CBQ enabled

Symptom: More number of packets will be dropped for a particular class.

Problem description: When CBQ is enabled, Class level RED will be functioning to ensure that the class won't exceed the allowed Committed Rate. RED values are calculated based on the CBQ values and the RED percentage values configured. If the values are not large enough to hold the traffic, then it may lead to excessive packet loss.

```
SR4134/configure/interface/bundle wan1# show qos chassis bundle wan1 class c1

Class: c1 (Outbound)
Parent Class: app-module-default (CR = 0 kbps (0.000000%); PR = 64 kbps (100.000000%))
Interface: Bundle wan1 (Bandwidth = 64Kbps)
Auto QoS State: Disabled                                    QoS Status: Enabled
CBQ OUT: ON, MON OUT: OFF,      Policing OUT: OFF)

Configuration
-------------
Committed Rate (CR): 6.4 Kbps(10.000000%)    Reserved Buffers: 4
Peak Rate (PR): 19.2 Kbps(30.000000%)        Max Buffers: 16 (Lo=16 Def=16 Hi=20)
Priority: 8                                  Bufs avail in comn pool: 12

WRED - Status: ON    ewf: 5   maxthHiBound: 15
   +---------+---------+----------+---------+-----+
        color       min       max  min  max  mpd
              threshold threshold    %    %
   +---------+---------+----------+---------+-----+
        green        11        15   75  100     5
       yellow         7        12   50   80     5
          red         6        10   40   70     5
```

Prerequisite: Policy-map should be successfully created and mapped to interfaces. CBQ parameters are configured and applied properly.

Troubleshooting tips:

1. Increase the CR configured to the class-map to handle more bandwidth for the class.
2. Tune the RED parameters such that not most of the packets will get dropped. Very-low match value for RED parameters is not advised, since it will lead to more packet loss.

PBR

PBR is not working

Symptom: Policy based redirection is not working for a policy-map attached to an interface.

Problem description: PBR is achieved through QoS. PBR is configured as one of the actions for all packets matching the rules of a class-map. Sometimes, user may see that PBR is not working i.e. packets are sent to the specified next-hop or outgoing interface.

Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

- Class map classification keys are not proper. For PBR to happens, first of all, the packets have to match the rules of the class-map to which PBR is configured. Make sure that rules are configured correctly using the following command and make sure the packets hit the class-map by enabling PBR.

Comments? infodev@avaya.com

```
SR4134# show qos chassis ethernet 0/2
Interface: Ethernet 0/2 (Bandwidth: Interface = 1000000Kbps ; QoS = 50000Kbps)
Auto QoS State: Disabled                                    QoS Status: Enabled
Service Policy Inbound: map4
Service Policy Outbound: map1

Interface Outbound Configuration & Statistics
---------------------------------------------
CBQ: OFF  Policing: OFF  MON: ON
+--------------+--------------+--------------+--------------------+--------------------+
 CBQ-CR  CBQ-PR      Police      Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                          ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+--------------+--------------+--------------------+--------------------+
      0   50000       -       -       0       0          0          0 3.app-module-mpls(*)
      0   50000       -       -       0       0          0          0 2.app-module-default(*)
  49500   50000       -       -       0       0          0          0 6.c1(2)
    500   50000       -       -       0       0          0          0 1.outbound-default(*)


Interface Inbound Configuration & Statistics
--------------------------------------------
Policing: OFF  MON: OFF   PBR: ON
+--------------+--------------+--------------+--------------------+--------------------+
 CBQ-CR  CBQ-PR      Police      Avg Out  Avg In    Packets  Packets     Traffic Class
                   CIR    PIR                                          ID.<name>(<pID>)
 (kbps)  (kbps)  (kbps)  (kbps)  (kbps)  (kbps)    (Fwded)  (Dropped)
+--------------+--------------+--------------+--------------------+--------------------+
      -       -       -       -       0       0        255          0 5.c1(*)
      -       -  500000       -       0       0          0          0 4.inbound-default(*)
```

- PBR configuration status is not up. Based on the correctness of the PBR configuration, the PBR status will be displayed. Make sure the PBR status is UP using the **`show qos chassis ethernet 0/2 class c1`** command.

```
SR4134# show qos chassis ethernet 0/2 class c1

Class: c1 (Inbound )
Parent Class: root-in (CR = 1000000 kbps ; PR = 1000000 kbps)
Interface: Ethernet 0/2 (Bandwidth = 1000000Kbps)
Auto QoS State: Disabled                                    QoS Status: Enabled
MON IN: OFF, Policing IN: OFF,  PBR Redirect IN: ON

Configuration
-------------
Policing - Not Configured
DiffServ Codepoints assigned to this Class:
Default af22
Packets redirected to -
Next hop: 3.3.3.2  Status: UP

Traffic Statistics
------------------
Avg Rate Out: 0 Kbps
Avg Rate In : 0 Kbps

Counters (since last boot/clear):       Packet drop details
---------------------------------       -------------------
Packets Forwarded:                    0 Queue overflow:                     0
Bytes Forwarded:                      0 No buffers:                         0
Packets Dropped:                      0 Policing pkts drop:                 0
Bytes Dropped:                        0 RED pkts dropped:                   0
PBR Class Statistics:
Matched: 256    Dropped: 0    Txed: 256
```

Auto QoS

Enabling AutoQos failed at interface

Symptom: An Error message will be thrown when auto-qos is enabled at the interface level.

Problem description: Auto-qos can be enabled for an interface by executing “enable-auto-qos” command at interface qos level. Enabling auto-qos will create pre-defined classes on the interface and enable Policing or CBQ functionality on the interface. There can be two reasons for auto-qos to fail on an interface: 1. Auto-qos is in manual state 2. Interface doesn’t have enough buffers

Case –1: Auto-qos will be applied in inbound direction for ethernet interfaces and outbound direction for bundle interfaces. So for applying auto-qos for an interface it should not have any manual configuration in the specific direction. For bundle interfaces: 1. No policy-map should be attached to outbound direction 2. No QoS features (policing, CBQ, monitoring) should be enabled on the outbound direction of the interface. For Ethernet interfaces: 1. No policy-map should be attached to inbound direction 2. No QoS features (policing, monitoring) should be enabled on the inbound direction of the interface If the above conditions are not met then applying auto-qos will fail for that interface.

Case – 2: For applying auto-qos on bundle interfaces, a minimum of 28 class buffers is needed. Buffers are calculated based on the interface bandwidth. So if the interface doesn’t have enough buffers then auto-qos will fail.

Prerequisite: Interface should be successfully created.

```
SR4134/configure/interface/bundle wan/qos# enable-auto-qos
Error! Auto-QoS: Auto-QoS state for this interface : Manual.
SR4134/configure/interface/bundle wan/qos# show qos chassis bundle wan

Interface: Bundle wan (Bandwidth = 1536Kbps)
Auto QoS State: Disabled                                    QoS Status: Enabled
Service Policy Inbound: map1
```

Troubleshooting tips:

- Remove all the manual configurations in the specified direction (outbound for bundle and inbound for ethernet). Use “**`show qos chassis [interface-type] [interface-name]`**” to verify the QoS configurations for that interface.
- Make sure that enough buffers are available in the interface. Use “**`show qos chassis [interface-type] [interface-name]`**” to verify the buffers available for that interface. If it is a bundle interface try adding more links to the bundle.

Enable or disable at global level does not change the auto-qos status at interface level

Symptom: • Interface auto-qos status will be shown as disabled in **`show qos chassis [interface-type] [interface-name]`**.

Problem description: Auto-qos can be enabled for all interfaces by executing “enable-auto-qos” command at global qos level. Enabling auto-qos will create predefined classes on all applicable interfaces and enable Policing or CBQ functionality on the interfaces. There can be

Comments? infodev@avaya.com

two reasons for auto-qos status to be in disabled for an interface even after enabling global auto-qos: 1. Auto-qos is in manual state 2. Interface is not applicable for that interface

Case – 1: Auto-qos will be applied in inbound direction for ethernet interfaces and outbound direction for bundle interfaces. So for applying auto-qos for an interface it should not have any manual configuration in the specific direction. For bundle interfaces: 1. No policy-map should be attached to outbound direction. 2. No QoS features (policing, CBQ, monitoring) should be enabled on the outbound direction of the interface For Ethernet interfaces: 1. No policy-map should be attached to inbound direction 2. No QoS features (policing, monitoring) should be enabled on the inbound direction of the interface If the above conditions are not met then applying auto-qos will fail for that interface.

Case – 2: Auto-qos is applicable only on bundle and ethernet interfaces. For all other interfaces auto-qos wont be enabled.

Prerequisite: Interface should be successfully created.

```
SR4134/configure/interface/bundle wan/qos# enable-auto-qos
Error! Auto-QoS: Auto-QoS state for this interface : Manual.
SR4134/configure/interface/bundle wan/qos# show qos chassis bundle wan

Interface: Bundle wan (Bandwidth = 1536Kbps)
Auto QoS State: Disabled                                    QoS Status: Enabled
Service Policy Inbound: map1
```

Troubleshooting tips:

- Remove all the manual configurations in the specified direction (outbound for bundle and inbound for ethernet). Use “show qos chassis [interface-type] [interface-name]” to verify the QoS configurations for that interface.
- Make sure that the interface is valid for auto-qos configuration.

Newly created interface is having Auto-qos configuration

Symptom: When an interface is created auto-qos configurations are automatically applied to the interface.

Problem description: This is not an issue. Instead it is the behavior of auto-qos functionality. When auto-qos is globally enabled, all the interfaces will be applied with auto-qos configurations. Also any new interface that is created will also be applied with auto-qos configurations. To view the global auto-qos status use “**`show qos chassis system`**” command.

Prerequisite: Interface should be successfully created and auto-qos is globally enabled.

Troubleshooting tips:

- Disable global auto-qos if auto-qos configurations are not needed for any for the interfaces.
- Disable auto-qos at the interface level, so that only the newly created bundle alone won’t be having the auto-qos configurations.

SLA

Unable to modify the SLA profile

Symptom: An Error message will be thrown when SLA is configured.

Problem description: SLA can take six SLA types. They are UDP-Echo, UDP-v6-Echo, UDP-Jitter, UDP-v6-Jitter, ICMP-Echo and ICMP-v6-Echo. A SLA profile can take only SLA type. When an SLA profile is in Process state (actively sending or receiving packets), then the configurations for that SLA cannot be modified. The “Transmit Status” in “show sla profile [id]” will give the status of the SLA profile. If the Transmit Status is “IN PROCESS” then the SLA profile cannot be modified. There can be two reasons for failure of SLA profile modification: 1. If a SLA profile is already configured with a SLA type, and a different SLA type configuration is requested for that SLA, it will not be accepted. 2. If a SLA profile is IN PROCESS state then the configuration cannot be modified.

Prerequisite: SLA profile has to be successfully configured with SLA type

Troubleshooting tips:

- Remove the previous configuration by executing “no” command and configure with the required SLA type.
- Wait till the SLA profile completes its execution and goes to “IN IDLE” state.

Unable to schedule the SLA

Symptom: An Error message will be thrown when SLA is scheduled.

Problem description: SLA profile will be scheduled to find out the SLA parameters such as jitter and delay. The reasons for this problem can be: 1. When an SLA profile is in Process state (actively sending or receiving packets), then the configurations for that SLA cannot be modified. Also it cannot be scheduled again. The “Transmit Status” in “**`show sla profile [id]`**” will give the status of the SLA profile. If the Transmit Status is “IN PROCESS” then the SLA profile cannot be modified. 2. If the SLA type is not configured for that SLA then it cannot be scheduled.

Prerequisite: SLA profile has to be successfully created.

Comments? infodev@avaya.com

```
Case 1:
SR4134/configure# sla schedule 1
SR4134/configure# sla schedule 1
Error! SLA set is in process. cannot accept the configuration for this set

Case 2:
SR4134/configure# sla schedule 66
Error! SLA Type is not configured for this Set
SR4134/configure#show sla profile 66

CONFIGURATION:
---------------
SLA Profile              : 66
Description              :
Destination Port         : 50001
Status                   : Enabled
Ready Status             : NOT ACTIVE
Transmit Status          : IN IDLE
Time to start            : 0 min
Time Out                 : 5 sec
```

Troubleshooting tips:

- Wait for the SLA profile to complete the process then try again.
- Configure a valid SLA type for the SLA profile before scheduling it.

Larger or negative time values in delay parameters

Symptom: "**`show sla profile [id]`**" will show large delay and jitter values.

Problem description: SLA calculates the delay and jitter values between two nodes by sending packets to the destination. The timestamps added by the two nodes are used for the delay and jitter calculations. One-way delay and jitter calculations depend on the time synchronization between the nodes. If the time at both the nodes are not synchronized then these calculations will not be accurate. Possible reasons for this problem are: 1. Time is not synchronized properly between the source and destination. 2. There is more network congestion between the two nodes. The interface, through which the SLA packets are sent, may be overloaded with more traffic.

Prerequisite: SLA should be properly configured and scheduled.

Troubleshooting tips:

- Synchronize the clock between the two nodes and reschedule the SLA.
- If the network is too congested, schedule the SLA after some time to get the exact values.

Response for the SLA packets sent is not received

Symptom: Receive count for the SLA profile will be less than transmit count.

Problem description: SLA sends out packets to the destination and wait for the response packets. Once it receives the response packets, it will calculate the delay and jitter values. If the packets have not reached within the timeout period then those packets are considered as loss. If twenty packets are sent to the destination and only 15 packets are received before the time out period, then 5 packets are considered as lost. "Remaining Time Out" value in the show sla profile command gives the time-out value remaining. The reasons for packet getting lost

can be: 1. Network unreachable. The destination may not be reachable. 2. Any of the two nodes is congested and drops the packets. 3. Packets get delayed and reach the source only after time-out period.

Prerequisite: SLA profile has to be successfully configured and scheduled.

Troubleshooting tips:

- Make sure that the destination is reachable. Ping to the destination and verify whether it is reachable.
- If the network is congested with heavy traffic, schedule the SLA after some time.
- If CBQ or any other features that can induce delay is enabled between the nodes, then disable that feature and reschedule the SLA profile.

Historical statistics

Statistics are not uploaded

Symptom: Historical statistics are not uploaded in the FTP server.

Problem description: The statistics that are collected for QoS on all the interfaces can be uploaded to a file server through historical statistics. To enable this feature some of the configurations like FTP server IP address, FTP username and password, and upload interval. The reasons for historical statistics not being uploaded are: a. Historical statistics is not enabled. By default historical statistics upload is not enabled. It has to be manually enabled by “upload” command. b. FTP parameters are not configured. The IP address of FTP server to which the statistics should be uploaded has to be configured. c. FTP server is not reachable or FTP username password is not valid.

Prerequisite: Historical statistics configured

```
SR4134/configure#
Error! FTP parameters not configured. Cannot upload QOS statistics.
        ----Or----
SR4134/configure#
06/23/2007-07:54:37 : alert : QOS
Error! Unable to upload QOS statistics...will retry in 10 seconds...
Error! QOS statistics upload failed

06/23/2007-07:54:47 : alert : QOS
Error! QOS statistics upload failed
```

Troubleshooting tips:

- Configure the upload interval and enable uploading historical statistics:

  ```
  Router/configure/qos/chassis/historical-stats# upload interval 1
  Uploading of Historical Statistics enabled Upload interval set to
  1 hours
  ```

- Configure the FTP parameters.

Comments? infodev@avaya.com

```
Router/configure/qos/chassis/historical-stats# ftp-parameters
Primary Ftp Server: 1.1.1.1 Secondary Ftp Server: 2.2.2.2 Ftp
user name: user Ftp password:
```

- Ping to the FTP server and verify that the connection is available to the FTP server.

Statistics are not uploaded for a particular interface

Symptom: Historical statistics are not uploaded for a particular interface.

Problem description: The statistics that are collected for QoS on all the interfaces can be uploaded to a file server through historical statistics. To enable this feature some of the configurations like FTP server IP address, FTP username and password, and upload interval. For an interface to get its statistics uploaded it should be a valid interface. The interface need not be up and running but it should be assigned with an IP address.

Prerequisite: Historical statistics configured

Troubleshooting tips: Configure a valid IP address to that interface.

Marking

Marking is not happening on the classes

Symptom: Packets passing through the class, with marking feature are not actually marked.

Problem description: Marking is a feature by which the user can mark all the packets that are passed through a class with desired dscp, IP precedence, priority and exp values. All the features such as CBQ, Policing or marking will be applied only for the leaf classes. These features will not have any effect on the parent classes which has child classes under it. When the Parent class is becoming a leaf class (its child classes are deleted), these features will be effective.

Prerequisite: Marking configuration is done on parent class and packets are forwarded through that class.

```
SR4134# show qos chassis policy-map map1 class-m
ap c1

Policy-map: map1
class-map: c1        parent class: root
-----------------------------------------------------------------------

   Classification type:
      DiffServ Codepoints assigned to this Class:  Default

   Police:
      None
   Mark DSCP: 30

SR4134# show qos chassis policy-map map1 class-map c2

Policy-map: map1
class-map: c2      parent class: c1   ➔ c1 is parent class
-----------------------------------------------------------------------

   Classification type:
      None
```

Troubleshooting tips: Configure marking parameters for the Leaf classes.

Module QoS troubleshooting

This section contains the basic step-by-step troubleshooting procedure for Module QoS in order to isolate the issue for further troubleshooting.

CoS marking:

CoS marking and remarking is supported at various stages during ingress QoS processing. Please note that the CoS marking at any stage will override any previous CoS marking done by the previous stages. For complete details on the CoS marking at different stages, refer to “QoS user guide”.

The **`show qos module system`** command shows the global user priority based CoS marking and output queue based CoS marking configuration. The user-priority based CoS marking is used to assign output queue and drop precedence for tagged packets based on user-priority value in the packet. The queue based CoS marking is used to assign user priority based on the default queue assigned to the packet.

Comments? infodev@avaya.com

```
SR4134# show qos module system

  qos enabled, auto-qos disabled, accounting enabled
  rate-monitoring stopped, 60 sec sampling-interval, 600 sec sampling-period

  user-priority-cos-map:

     user        output       drop
   priority      queue     precedence

       0           8          high
       1           7          high
       2           6          high
       3           5          high
       4           4          medium
       5           3          medium
       6           2          medium
       7           2          low

  queue-cos-map:

     output         user
     queue        priority

       1            7
       2            6
       3            5
       4            4
       5            3
       6            2
       7            1
       8            0
```

The **`show qos module ethernet`** command shows the default queue assignment and dscp, user-priority CoS markings for packets coming on the interface.

```
SR4134# show qos module ethernet 5/1

Interface ethernet5/1:
   default-queue 8
   tail-drop, congestion-profile 1
   345 ingress-buffers, 320 egress-buffers, 325 xon-limit, 342 xoff-limit
   0 packets-queued
   shaping:
      disabled

   Queue     Scheduling          Shaping          Buffers
          Mode Weight Group  Rate     Burst    Limit Used
                             kbps     KB

     1    SPQ   -       -    -        -        32    0
     2    SPQ   -       -    -        -        32    0
     3    SPQ   -       -    -        -        32    0
     4    SPQ   -       -    -        -        32    0
     5    WRR   2       1    -        -        48    0
     6    WRR   1       1    -        -        48    0
     7    WRR   2       0    -        -        48    0
     8    WRR   1       0    -        -        48    0

   qos enabled, auto-qos disabled
   mark-dscp 30, mark-user-priority disabled
   service-policy none
```

The **show qos module policy-map** command shows the CoS markings applied to packets classified by the rules specified in the class-map.

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      none                 none

   class-map: c1 (seq# 1)
      accounting disabled
      queue 7, drop-precedence medium, dscp af33, user-priority 4
      rate-monitoring:
         disabled
      rules:
         None
      police:
         disabled
      redirection:
         none
```

The **show qos module policing-cos-map ip** command shows the CoS markings based on previous DSCP value and the conformance level assigned to the packet by the Policer. This is used for IP packets.

Comments? infodev@avaya.com

```
SR4134# show qos module policing-cos-map ip

  Prev    Conformance    Mark    Mark      Mark
  DSCP       Level       DSCP    Drop      User
                                 Prec      Prio

   0        conform       0      low        0
   0        exceed        0      medium     0
   0        violate       0      high       0
   1        conform       1      low        0
```

The **show qos module policing-cos-map non-ip** command shows the CoS markings based on previous UP value and the conformance level assigned to the packet by the Policer. This is used for non-IP packets.

```
SR4134# show qos module policing-cos-map non-ip

  Prev    Conformance    Mark     Mark
  User       Level       Drop     User
  Prio                   Prec     Prio

   0        conform      low       0
   0        exceed       medium    0
   0        violate      high      0
   1        conform      low       1
```

Classification

Classification is used to classify packets into classes based on various fields in the packet header. A policy map contains one or more classes, which in turn, can have multiple classification rules. A policy map represents the complete set of classification rules that can be associated with one/more interfaces. A class represents a set of classification rules which can be associated with same set of actions. A packet is said to be classified into a class if it matches any of the classification rules in that class. The actions associated with the class will be applied for all packets that are classified into the class. The actions associated with a class can be CoS marking/re-marking, policing and policy based routing.

The **show qos module policy-map** command shows the policy-maps configured, the class-maps configured within the policy-map, the matching rules configured for each class-map, accounting status, different actions that are configured for each class-map, the sequence number of the class within the policy-map, and interface(s) the policy-map is servicing.

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet5/1         enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dscp af33
      police:
         disabled
      redirection:
         none

   class-map: c2 (seq# 2)
      accounting disabled
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv6 flow-label 30
      police:
         disabled
      redirection:
         none
```

The **show qos module service-policy** command shows all the policy-maps servicing different interface

```
SR4134# show qos module service-policy

   Interface            Serviced-policy            Qos-status
   ethernet5/1          m1                         enabled
```

The service policy of an interface can be seen in the **show qos module ethernet** command too.

Comments? infodev@avaya.com

```
SR4134# show qos module ethernet 5/1

Interface ethernet5/1:
   default-queue 8
   tail-drop, congestion-profile 1
   345 ingress-buffers, 320 egress-buffers, 325 xon-limit, 342 xoff-limit
   0 packets-queued
   shaping:
      disabled

   Queue     Scheduling          Shaping          Buffers
          Mode Weight Group  Rate     Burst    Limit Used
                             kbps     KB
     1    SPQ    -      -    -        -        32    0
     2    SPQ    -      -    -        -        32    0
     3    SPQ    -      -    -        -        32    0
     4    SPQ    -      -    -        -        32    0
     5    WRR    2      1    -        -        48    0
     6    WRR    1      1    -        -        48    0
     7    WRR    2      0    -        -        48    0
     8    WRR    1      0    -        -        48    0

   qos enabled, auto-qos disabled
   mark-dscp disabled, mark-user-priority disabled
   service-policy m1
```

Policing

Traffic policing provides the conformance metering, CoS re-marking and rate limiting functionality. The conformance metering functionality of the policer determines the conformance level of the packets (conforming, exceeding, and violating) and performs a configurable action based on the conformance level. The action configured could be re-marking CoS attributes based on conformance level and/or dropping of violating packets (rate-limit).

Policing can be enabled on the ingress Network Module interface. It can be configured for each class in the policy-map that is mapped to an ingress interface. If policing is configured and enabled for a class, it is applied to all the packets that are classified into the class.

The **`show qos module policy-map`** command shows the policing configuration (including accounting status, policing configuration, policing-based remarking configuration and the corresponding billing and conformance counters) for a class-map within a policy-map.

```
SR4134# show qos module policy-map m1 detail
policy-map: m1
   Serviced-interface    Qos-status
      ethernet5/1         enabled
   class-map: c1 (seq# 1)
      29866245920 bytes forwarded, 155631280 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dscp af33
      police:
         enabled, srtcm, color-aware
         10 Kbps cir
         10 Kbits (13 Kbits oper) committed-burst
         20 Kbits extended-burst
         remark on, drop-violate on
         3040 bytes conforming, 1520 bytes exceeding
         30021872640 bytes violating
      redirection:
         none
   class-map: c2 (seq# 2)
      accounting disabled
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv6 flow-label 30
      police:
         disabled
      redirection:
         none
```

The **`show qos module policy-map`** command (brief display) shows the policing configuration for a class-map within a policy-map

```
SR4134# show qos module policy-map m1

policy-map: m1

   Serviced-interface    Qos-status
      ethernet5/1         enabled

   seq#    class name           police mark PBR accnt rate  fwd/drop
                                                    mon     bytes

   1       c1                     Y      N   N   Y     N    29866245920 /
                                                            650249920
   2       c2                     N      N   N   N     N       -
```

The **`show qos module system`** command shows the global accounting status.

Comments? infodev@avaya.com

```
SR4134# show qos module system

  qos enabled, auto-qos disabled, accounting enabled
  rate-monitoring in-progress, 60 sec sampling-interval, 600 sec sampling-period

  user-priority-cos-map:

     user        output       drop
   priority      queue     precedence

       0           8          high
       1           7          high
       2           6          high
       3           5          high
       4           4          medium
       5           3          medium
       6           2          medium
       7           2          low

  queue-cos-map:

     output         user
     queue       priority

       1            7
       2            6
       3            5
       4            4
       5            3
       6            2
       7            1
       8            0
```

Congestion avoidance

The purpose of congestion avoidance is to identify the onset of congestion early enough and start dropping packets to avoid complete depletion of resources. RED monitors queue congestion and discards packets before they are admitted to the queue. The WRED algorithm is an extension to RED in the sense that it also incorporates the packet's conformance level (DP) into consideration, so that traffic with high DP is dropped first. Two packet dropping mechanisms namely the tail-drop and random-detect are supported

The **`show qos module congestion-profile`** command shows the WRED configuration for each outgoing queue and for each drop precedence value. There are 4 congestion profiles supported and one of these 4 profiles can be attached to an egress interface.

```
SR4134# show qos module congestion-profile 1

  Queue    Drop       Max Th    Min Th    Drop Prob    Exp Wt
           Prec                            Denom       Const

    1      low         4096      0           5           5
    1      medium      4096      0           4           5
    1      high        4096      0           3           5
    2      low         4096      0           5           5
    2      medium      4096      0           4           5
    2      high        4096      0           3           5
    3      low         4096      0           5           5
    3      medium      4096      0           4           5
    3      high        4096      0           3           5
    4      low         4096      0           5           5
    4      medium      4096      0           4           5
    4      high        4096      0           3           5
    5      low         4096      0           5           5
    5      medium      4096      0           4           5
    5      high        4096      0           3           5
    6      low         4096      0           5           5
    6      medium      4096      0           4           5
    6      high        4096      0           3           5
    7      low         4096      0           5           5
    7      medium      4096      0           4           5
    7      high        4096      0           3           5
    8      low         4096      0           5           5
    8      medium      4096      0           4           5
    8      high        4096      0           3           5

  Serviced-interfaces
    ethernet5/4
```

The congestion profile attached to an interface can be seen in **`show qos module ethernet`** command output too.

Comments? infodev@avaya.com

```
SR4134# show qos module ethernet 5/4

Interface ethernet5/4:
   default-queue 8
   random-detect, congestion-profile 1
   345 ingress-buffers, 320 egress-buffers, 325 xon-limit, 342 xoff-limit
   0 packets-queued
   shaping:
      disabled

   Queue     Scheduling         Shaping          Buffers
          Mode Weight Group  Rate     Burst    Limit Used
                             kbps     KB

     1    SPQ    -       -     -        -        32    0
     2    SPQ    -       -     -        -        32    0
     3    SPQ    -       -     -        -        32    0
     4    SPQ    -       -     -        -        32    0
     5    WRR    2       1     -        -        48    0
     6    WRR    1       1     -        -        48    0
     7    WRR    2       0     -        -        48    0
     8    WRR    1       0     -        -        48    0

   qos enabled, auto-qos disabled
   mark-dscp disabled, mark-user-priority disabled
   service-policy none
```

Output queuing and scheduling

Module QoS supports fixed set of eight egress queues on each port. When these queues have packet descriptors en-queued for transmission, the transmit scheduler is responsible for selecting one of the queues for transmission. Each of the queues in the Network Module ports can be scheduled using either Strict Priority (SP) or D-WRR (Deficit Weighted Round Robin).

The **`show qos module ethernet`** command shows the scheduling method and its configuration (including the weight and WRR group for queues with WRR scheduling) for each of the eight queues on that port.

```
SR4134# show qos module ethernet 5/4

Interface ethernet5/4:
   default-queue 8
   random-detect, congestion-profile 1
   345 ingress-buffers, 320 egress-buffers, 325 xon-limit, 342 xoff-limit
   0 packets-queued
   shaping:
      disabled

   Queue     Scheduling         Shaping          Buffers
          Mode Weight Group  Rate    Burst    Limit Used
                             kbps    KB

     1    SPQ    -       -    -       -        32    0
     2    SPQ    -       -    -       -        32    0
     3    SPQ    -       -    -       -        32    0
     4    SPQ    -       -    -       -        32    0
     5    WRR    2       1    -       -        48    0
     6    WRR    1       1    -       -        48    0
     7    WRR    2       0    -       -        48    0
     8    WRR    1       0    -       -        48    0

   qos enabled, auto-qos disabled
   mark-dscp disabled, mark-user-priority disabled
   service-policy none
```

Shaping

Traffic shaping smooths out traffic bursts by queuing packets for required amount of time. It limits a flow to any desired rate and burst. Module QoS supports shaping both at port level and at queue level. Shaping can be enabled independently for ports and queues.

The **`show qos module ethernet`** command shows the port and queue level shaping configuration.

Comments? infodev@avaya.com

```
SR4134# show qos module ethernet 5/4

Interface ethernet5/4:
   default-queue 8
   random-detect, congestion-profile 1
   345 ingress-buffers, 320 egress-buffers, 325 xon-limit, 342 xoff-limit
   0 packets-queued
   shaping:
      4557 kbps rate, 16 KB burst

   Queue     Scheduling         Shaping          Buffers
          Mode Weight Group  Rate    Burst    Limit Used
                             kbps    KB

     1    SPQ    -       -    -       -        32    0
     2    SPQ    -       -    -       -        32    0
     3    SPQ    -       -    2604    8        32    0
     4    SPQ    -       -    -       -        32    0
     5    WRR    2       1    -       -        48    0
     6    WRR    1       1    -       -        48    0
     7    WRR    2       0    -       -        48    0
     8    WRR    1       0    1302    4        48    0

   qos enabled, auto-qos disabled
   mark-dscp disabled, mark-user-priority disabled
   service-policy none
```

Buffer management

Module QoS provides a total of 4000 packet buffers in each line card. It supports per port buffer limits in the ingress direction (ingress buffers) and per-port packet descriptor limits in the egress direction (egress buffers) to avoid over-utilization of buffers by any specific port. Module QoS also supports buffer limits at the queue level to allow fair sharing of buffers and packet descriptors across the queues associated with a port.

Module QoS also supports flow control using 802.3x standards. Flow control prevents the buffer allocation limits (receive buffer limit) from being reached.

The **`show qos module ethernet`** command shows the port level ingress and egress buffers, port level xon and xoff limits and queue level buffer limits

```
SR4134# show qos module ethernet 5/4

Interface ethernet5/4:
   default-queue 8
   random-detect, congestion-profile 1
   345 ingress-buffers, 320 egress-buffers, 325 xon-limit, 342 xoff-limit
   0 packets-queued
   shaping:
      4557 kbps rate, 16 KB burst

   Queue     Scheduling        Shaping         Buffers
          Mode Weight Group  Rate    Burst    Limit Used
                             kbps    KB

     1    SPQ    -       -    -       -        32    0
     2    SPQ    -       -    -       -        32    0
     3    SPQ    -       -    2604    8        32    0
     4    SPQ    -       -    -       -        32    0
     5    WRR    2       1    -       -        48    0
     6    WRR    1       1    -       -        48    0
     7    WRR    2       0    -       -        48    0
     8    WRR    1       0    1302    4        48    0

   qos enabled, auto-qos disabled
   mark-dscp disabled, mark-user-priority disabled
   service-policy none
```

Flow rate monitoring

The network processor supports flow based packet statistics collection. These statistics serve as very useful tools for the operator to study the behavior of traffic flows/flow aggregates over any given period of time.

The **show qos module system** command shows the global sampling interval and sampling period configuration. It also shows if rate-monitoring is in progress or not.

Comments? infodev@avaya.com

```
SR4134# show qos module system

  qos enabled, auto-qos disabled, accounting enabled
  rate-monitoring in-progress, 60 sec sampling-interval, 600 sec sampling-period

  user-priority-cos-map:

     user       output      drop
   priority     queue    precedence

       0          8         high
       1          7         high
       2          6         high
       3          5         high
       4          4         medium
       5          3         medium
       6          2         medium
       7          2         low

  queue-cos-map:

     output        user
     queue       priority

       1            7
       2            6
       3            5
       4            4
       5            3
       6            2
       7            1
       8            0
```

The **`show qos module policy-map`** command shows if flow rate monitoring is enabled for a class-map or not and the rate-monitoring statistics.

```
SR4134# show qos module policy-map m1 detail
policy-map: m1
   Serviced-interface    Qos-status
      ethernet5/1         enabled
   class-map: c1 (seq# 1)
      29866245920 bytes forwarded, 104391683280 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         99760 Kbps input rate, 0 Kbps output rate
         99730 Kbps avg input rate, 0 Kbps avg output rate
      rules:
         match ipv4 dscp af33
      police:
         enabled, srtcm, color-aware
         10 Kbps cir
         10 Kbits (13 Kbits oper) committed-burst
         20 Kbits extended-burst
         remark on, drop-violate on
         3040 bytes conforming, 1520 bytes exceeding
         134257924640 bytes violating
      redirection:
         none
   class-map: c2 (seq# 2)
      accounting disabled
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv6 flow-label 30
      police:
         disabled
      redirection:
         none
```

Auto QoS

The Auto QoS feature allows user to configure default or basic QoS treatment in a system. It is supported at both interface and at global level.

The **`show qos module system`** command shows the global auto-qos configuration.

Comments? infodev@avaya.com

```
SR4134# show qos module system

  qos enabled, auto-qos disabled, accounting enabled
  rate-monitoring in-progress, 60 sec sampling-interval, 600 sec sampling-period

  user-priority-cos-map:

     user        output       drop
   priority      queue     precedence

       0           8          high
       1           7          high
       2           6          high
       3           5          high
       4           4          medium
       5           3          medium
       6           2          medium
       7           2          low

  queue-cos-map:

     output         user
     queue        priority

       1            7
       2            6
       3            5
       4            4
       5            3
       6            2
       7            1
       8            0
```

The **`show qos module ethernet`** command shows the interface level auto-qos configuration.

```
SR4134# show qos module ethernet 5/1

Interface ethernet5/1:
   default-queue 8
   tail-drop, congestion-profile 1
   345 ingress-buffers, 320 egress-buffers, 325 xon-limit, 342 xoff-limit
   0 packets-queued
   shaping:
      disabled

   Queue     Scheduling         Shaping          Buffers
          Mode Weight Group  Rate     Burst    Limit Used
                             kbps     KB

     1    SPQ    -       -     -        -        32    0
     2    SPQ    -       -     -        -        32    0
     3    SPQ    -       -     -        -        32    0
     4    SPQ    -       -     -        -        32    0
     5    WRR    2       1     -        -        48    0
     6    WRR    1       1     -        -        48    0
     7    WRR    2       0     -        -        48    0
     8    WRR    1       0     -        -        48    0

   qos enabled, auto-qos enabled (interface)
   mark-dscp disabled, mark-user-priority disabled
   service-policy AutoQoSPolicy
```

QoS status management

One of the important stages of Module QoS is the policy application stage (involving classification, policing and marking). The operator can choose to bypass the policy application stage completely, if required. The QoS enforcement stages (involving congestion management, scheduling, and so on) can also be managed by the operator. However every packet transiting the Ethernet will get subjected to QoS enforcement. It cannot be bypassed.

The **`show qos module system`** command shows the global qos status.

Comments? infodev@avaya.com

```
SR4134# show qos module system

  qos enabled, auto-qos disabled, accounting enabled
  rate-monitoring in-progress, 60 sec sampling-interval, 600 sec sampling-period

  user-priority-cos-map:

     user       output      drop
   priority     queue    precedence

       0          8         high
       1          7         high
       2          6         high
       3          5         high
       4          4         medium
       5          3         medium
       6          2         medium
       7          2         low

  queue-cos-map:

     output        user
     queue       priority

       1            7
       2            6
       3            5
       4            4
       5            3
       6            2
       7            1
       8            0
```

The **`show qos module ethernet`** command shows the interface level qos status.

```
SR4134# show qos module ethernet 5/1

Interface ethernet5/1:
   default-queue 8
   tail-drop, congestion-profile 1
   345 ingress-buffers, 320 egress-buffers, 325 xon-limit, 342 xoff-limit
   0 packets-queued
   shaping:
      disabled

   Queue     Scheduling         Shaping          Buffers
          Mode Weight Group  Rate    Burst    Limit Used
                             kbps    KB

     1    SPQ    -       -    -       -        32    0
     2    SPQ    -       -    -       -        32    0
     3    SPQ    -       -    -       -        32    0
     4    SPQ    -       -    -       -        32    0
     5    WRR    2       1    -       -        48    0
     6    WRR    1       1    -       -        48    0
     7    WRR    2       0    -       -        48    0
     8    WRR    1       0    -       -        48    0

   qos enabled, auto-qos enabled (interface)
   mark-dscp disabled, mark-user-priority disabled
   service-policy AutoQoSPolicy
```

Limitations, errors and warnings

TCAM limitation

The Ternary CAM (TCAM) is a specialized piece of memory designed for rapid table lookups performed by the ACL engine on Ethernet Modules. Module QoS users ACL based TCAM lookups for packet classification. ACLs are processed in hardware that is called TCAM. When you configure policy-map, configure matching rules for the class-maps within the policy-map and when you apply the QoS policy-map on the interface, the router programs the TCAM. If you have already utilized all of the available TCAM space on the Router for the QoS, you encounter this error message: PSL ERROR: TCAM usage reached the maximum limit

Currently there is no show command to display the TCAM usage.

Please note that TCAM is a shared resource used by Module QoS, ACL based firewall rules and for IPv6 Multicast.

Policer limitation

Module QoS Policing is done in the hardware. The number of policers that can be created is limited (300). If you have already utilized all policer entries on the Router, you encounter this error message: ERROR: Configured policers already reached the maximum limit: xxx

Please note that a policer entry is created in the hardware whenever accounting/policing is configured/enabled for a class-map.

Service Policy limitation

A policy-map with policer configuration (accounting/policing) cannot be mapped across line cards. If any policy-map is attempted to be mapped to interfaces across line cards, you encounter this error message: ERROR: Policy map (with policing/accounting enabled) is mapped across devices

CoS marking of output queue 1 (highest priority queue)

Module QoS supports eight queues on each port. The priorities assigned for these queues are fixed. Queue 1 is of highest priority and queue 8 is the lowest priority queue. In general, the control traffic generated by the CPU will go through the highest priority queue. So, if you attempt

Comments? infodev@avaya.com

to assign this high priority queue for user traffic, you encounter this warning message suggesting that the user traffic assigned to this queue will cause drop of the critical traffic. Warning!! This setting will make critical and data traffic treated with same priority. This will cause drops in critical traffic Please not that the configuration will still be successful after this warning.

Troubleshooting Module QoS - Error conditions

1. Packets are not getting classified to a class-map

   Symptom: Forwarded or dropped byte counters are not incrementing.

   Description: When a policy-map is configured and attached to an interface, user may see that the packets are not getting classified to the specified class-map in the “show qos module policy-map” command output.

   Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

   - Wrong rules are configured for the class-map. Traffic sent won’t be classified to a class-map unless the packets match the rules configured in that class-map. Make sure the rules configured for the class-map are proper. The classification field and the value assigned should be correct. Use the **`show qos module policy-map`** command to see the rules configured.

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

    Serviced-interface    Qos-status
       ethernet6/20        enabled

    class-map: c1 (seq# 1)
       0 bytes forwarded
       queue carry, drop-precedence carry, dscp carry, user-priority carry
       rate-monitoring:
          disabled
       rules:
          match ipv4 dscp af33
       police:
          disabled
       redirection:
          none
```

   - Wrong rule types are used. There are 3 types of classification rules supported in Module QoS 1. IPv4 rules - The ipv4 rules should be used only for IPv4 packets i.e. packets with IPv4 payload (any packets having ether-type value 0x0800). 2. IPv6 rules - The ipv6 rules should be used only for IPv6 packets i.e. packets with IPv6 payload (any packets having ether-type value 0x86dd) 3. Non IP rules - The non-ip rules should be used for non-ipv4 and non-ipv6

packets i.e. packets with no IPv4 or IPv6 payloads. For example, if you configure a non-ip rule using destination / source MAC address field for classification and you send IPv4 traffic with the specified destination / source MAC address, classification will not happen. Instead, use ipv4 rule to match packets based on MAC address since the packet payload contains IPv4 header.

```
SR4134# show qos module policy-map m1 detail
policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         disabled
      redirection:
         none
```

- Accounting not enabled for the class-map. For the user to see the classification counters, accounting needs to be enabled for the class-map.

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         disabled
      redirection:
         none
```

- Accounting disabled globally. Accounting is enabled globally by default. Verify that accounting is enabled globally.

Comments? infodev@avaya.com

```
SR4134# show qos module system

  qos enabled, auto-qos disabled, accounting enabled
  rate-monitoring stopped, 60 sec sampling-interval, 600 sec sampling-period

  user-priority-cos-map:

     user        output       drop
   priority      queue     precedence

       0           8          high
       1           7          high
       2           6          high
       3           5          high
       4           4          medium
       5           3          medium
       6           2          medium
       7           2          low

  queue-cos-map:

     output         user
     queue       priority

       1            7
       2            6
       3            5
       4            4
       5            3
       6            2
       7            1
       8            0
```

- Policy-map is not attached to the ingress interface. The policy-map to be serviced must be attached to the interface on which the traffic is sent. Verify that the policy-map is attached to the interface with one of the following commands: **`show qos module service-policy`** **`show qos module policy-map m1 detail`**

```
SR4134# show qos module service-policy

   Interface            Serviced-policy             Qos-status
   ethernet6/20         m1                          enabled

SR4134# show qos module policy-map m1 detail

policy-map: m1
   Serviced-interface    Qos-status
      ethernet6/20        enabled
      class-map: c1 (seq# 1)
      0 bytes forwarded
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         disabled
      redirection:
         none


SR4134# show qos module ethernet 6/20

Interface ethernet6/20:
   default-queue 8
   tail-drop, congestion-profile 1
   265 ingress-buffers, 256 egress-buffers, 245 xon-limit, 262 xoff-limit
   0 packets-queued
   shaping:
      disabled

   Queue     Scheduling         Shaping          Buffers
          Mode Weight Group  Rate     Burst    Limit Used
                             kbps     KB

     1    SPQ   -       -    -        -        32    0
     2    SPQ   -       -    -        -        32    0
     3    WRR   2       1    -        -        32    0
     4    WRR   1       1    -        -        32    0

   qos enabled, auto-qos disabled
   mark-dscp disabled, mark-user-priority disabled
   service-policy m1
```

- Classification works only in ingress direction. In Module QoS, policy-map can only be applied in the ingress direction i.e. the interface on which the packets are entering the DUT. Classification won't work if the service-policy interface is the egress interface.
- QoS not enabled on the interface. QoS must be enabled on the interface on which the service-policy is mapped. Verify that QoS is enabled on the interface using one of the following commands: **`show qos module ethernet 6/20`** **`show qos module service-policy`**

Comments? infodev@avaya.com

```
SR4134# show qos module ethernet 6/20

Interface ethernet6/20:
   default-queue 8
   tail-drop, congestion-profile 1
   265 ingress-buffers, 256 egress-buffers, 245 xon-limit, 262 xoff-limit
   0 packets-queued
   shaping:
      disabled

   Queue     Scheduling         Shaping          Buffers
          Mode Weight Group  Rate     Burst    Limit Used
                             kbps     KB

     1    SPQ   -       -    -        -        32    0
     2    SPQ   -       -    -        -        32    0
     3    SPQ   -       -    -        -        32    0
     4    SPQ   -       -    -        -        32    0
     5    WRR   2       1    -        -        32    0
     6    WRR   1       1    -        -        32    0
     7    WRR   2       0    -        -        32    0
     8    WRR   1       0    -        -        32    0

   qos enabled, auto-qos disabled
   mark-dscp disabled, mark-user-priority disabled
   service-policy m1


SR4134# show qos module service-policy

   Interface            Serviced-policy             Qos-status
   ethernet6/20         m1                          enabled

SR4134# show qos module policy-map m1 detail

policy-map: m1

    Serviced-interface    Qos-status
       ethernet6/20        enabled

    class-map: c1 (seq# 1)
       0 bytes forwarded
       queue carry, drop-precedence carry, dscp carry, user-priority carry
       rate-monitoring:
          disabled
       rules:
          match ipv4 dscp af33
          match ipv4 dest-mac 00:40:5c:00:00:01
       police:
          disabled
       redirection:
          none
```

2. Not able to delete a policy-map

   Symptom: User may not be able to delete a policy-map configured and an error message is displayed.

Description: In general, user should be able to delete a policy-map configured unless it is in use.

Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

- Policy-map is attached to one/more interfaces. The policy-map being deleted is already attached to one/more interfaces. The service-policy mappings need to be removed from all the interfaces to which it is attached before deleting the policy-map. Use the following command to see the service-policy-mappings: **show qos module service-policy**

```
SR4134# show qos module service-policy

    Interface             Serviced-policy             Qos-status
    ethernet6/20          m1                          enabled
    ethernet6/21          m1                          enabled
```

- Policy-map is auto-qos policy. User will not be able to delete an auto-qos policy map. If auto-qos needs to be disabled, use no enable-auto-qos command either globally or on the interface. Use the following command to see the service policy mappings: **show qos module service-policy**

```
SR4134# show qos module service-policy

    Interface             Serviced-policy             Qos-status
    ethernet6/20          AutoQoSPolicy               enabled
    ethernet6/21          m1                          enabled
```

3. Unable to map a policy-map to an interface

   Symptom: User may not be able to map a service-policy to an interface and error is reported.

   Description: User sometimes will not be able to map a policy-map to an interface and error will be reported.

   Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

   - Auto-qos is already enabled on the interface. If auto-qos is enabled on the interface, the default auto-qos policy will already be attached to the interface. To attach a user policy-map to the interface, remove auto-qos configuration on the interface first and then attempt to attach the user policy-map to the interface. Use the following command to see the service policy mappings: **show qos module service-policy**

Comments? infodev@avaya.com

```
SR4134# show qos module service-policy

   Interface            Serviced-policy            Qos-status
   ethernet6/20         AutoQoSPolicy              enabled
   ethernet6/21         m1                         enabled
```

- Interface is not a Module Ethernet interface. Module QoS policy-maps can be attached only on the Module Ethernet interfaces. They cannot be mapped to any other interface. If so, error will be reported to the user.

4. Policing not working

   Symptom: User may see that conformance counters are not incrementing or rate-limiting is not working.

   Description: Policing configuration should be properly configured on the interface on which policing is required. Otherwise policing may not work and rate-limiting may not happen.

   Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

   - Wrong policing configuration. Please verify that policing is properly configured for the class-map to which the traffic is classified to. This can be verified using the following command: **`show qos module policy-map m1 detail`**

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded, 0 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         enabled, srtcm, color-blind
         300 Kbps cir
         300 Kbits committed-burst
         600 Kbits extended-burst
         remark off, drop-violate off
         0 bytes conforming, 0 bytes exceeding
         0 bytes violating
      redirection:
         none
```

   - Class accounting is not enabled. For policing to work, the accounting should be enabled. Verify that accounting is enabled for the class-map and globally

using the following commands: **show qos module policy-map m1 detail show qos module system**

Comments? infodev@avaya.com

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded, 0 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         enabled, srtcm, color-blind
         300 Kbps cir
         300 Kbits committed-burst
         600 Kbits extended-burst
         remark off, drop-violate off
         0 bytes conforming, 0 bytes exceeding
         0 bytes violating
      redirection:
         none
SR4134# show qos module system

  qos enabled, auto-qos disabled, accounting enabled
  rate-monitoring stopped, 60 sec sampling-interval, 600 sec sampling-period

  user-priority-cos-map:

     user       output      drop
   priority     queue    precedence

        0          8         high
        1          7         high
        2          6         high
        3          5         high
        4          4         medium
        5          3         medium
        6          2         medium
        7          2         low

  queue-cos-map:

     output        user
     queue       priority

       1            7
       2            6
       3            5
       4            4
       5            3
       6            2
       7            1
       8            0
```

- Policing is disabled. By default, when policing configuration is configured for a class-map, policing will be enabled. However user can disable it anytime.

Verify that policing is enabled for the class-map using the following command: **show qos module policy-map m1 detail**

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

    Serviced-interface    Qos-status
       ethernet6/20        enabled

    class-map: c1 (seq# 1)
       0 bytes forwarded, 0 bytes dropped
       queue carry, drop-precedence carry, dscp carry, user-priority carry
       rate-monitoring:
          disabled
       rules:
          match ipv4 dscp af33
          match ipv4 dest-mac 00:40:5c:00:00:01
       police:
          enabled, srtcm, color-blind
          300 Kbps cir
          300 Kbits committed-burst
          600 Kbits extended-burst
          remark off, drop-violate off
          0 bytes conforming, 0 bytes exceeding
          0 bytes violating
       redirection:
          none
```

- No service policy. Policing is a configuration at class-map level. Hence the policy-map in which the class-map and its policing configuration is done should be properly attached to the ingress interface on which the traffic is coming into the DUT. Verify that the policy-map is attached to the interface using the following command: **show qos module policy-map m1 detail**

Comments? infodev@avaya.com

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded, 0 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         enabled, srtcm, color-blind
         300 Kbps cir
         300 Kbits committed-burst
         600 Kbits extended-burst
         remark off, drop-violate off
         0 bytes conforming, 0 bytes exceeding
         0 bytes violating
      redirection:
         none
```

- QoS is not enabled on the interface. QoS must be enabled on the interface on which the service-policy is mapped. Verify that QoS is enabled on the interface using one of the following commands: **`show qos module service-policy`**

```
SR4134# show qos module service-policy

   Interface            Serviced-policy            Qos-status
   ethernet6/20         m1                         enabled
```

5. Input and output rates are same even after configuring policing

   Symptom: User may see that rate-limiting is not working even after configuring policing for the class-map.

   Description: User may see that the conformance counters are incrementing but rate-limiting is not happening.

   Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

   - Drop violate is not configured. Drop-violate need to be enabled so that the packets violating the policing profile are dropped. By default, drop-violate is disabled. Verify that drop violate is enabled using the following command: **`show qos module policy-map m1 detail`**

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded, 0 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         enabled, srtcm, color-blind
         300 Kbps cir
         300 Kbits committed-burst
         600 Kbits extended-burst
         remark off, drop-violate on
         0 bytes conforming, 0 bytes exceeding
         0 bytes violating
      redirection:
         none
```

6. Policing based CoS marking not working.

   Symptom: User may see that CoS marking is not working based on the conformance level assigned by the policer.

   Description: There are two global tables for marking CoS attributes based on the conformance level. User may see that these CoS markings are not applied to the packets.

   Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

   - CoS remark is not configured for the class. Policing based CoS remarking needs to be enabled for these markings to take effect. By default, policing based CoS remarking is disabled. Verify that policing based CoS remarking is enabled using the following command: **`show qos module policy-map m1 detail`**

Comments? infodev@avaya.com

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded, 0 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         disabled
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         enabled, srtcm, color-blind
         300 Kbps cir
         300 Kbits committed-burst
         600 Kbits extended-burst
         remark on, drop-violate on
         0 bytes conforming, 0 bytes exceeding
         0 bytes violating
      redirection:
         none
```

7. Flow rate monitoring not working

   Symptom: User may see that the flow rate monitoring statistics are not shown

   Description: Flow rate monitoring can be enabled for any specified class-map by the user. User may see that flow rate monitoring statistics are not incrementing.

   Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

   - Enable flow rate monitoring for the class. User has to explicitly enable flow rate monitoring for the class-map. Verify that flow rate monitoring is enabled using the following command: **`show qos module policy-map m1 detail`**

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded, 0 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         0 Kbps input rate, 0 Kbps output rate
         0 Kbps avg input rate, 0 Kbps avg output rate
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         enabled, srtcm, color-blind
         10 Kbps cir
         10 Kbits (82 Kbits oper) committed-burst
         20 Kbits (82 Kbits oper) extended-burst
         remark off, drop-violate off
         0 bytes conforming, 0 bytes exceeding
         0 bytes violating
      redirection:
         none
```

- Configure and start rate monitoring globally. For flow rate monitoring to work for a class, the rate sampling has to be started from the global context. Verify that rate sampling is in progress using the following command: **show qos module system**

Comments? infodev@avaya.com

```
SR4134# show qos module system

  qos enabled, auto-qos disabled, accounting enabled
  rate-monitoring in-progress, 60 sec sampling-interval, 600 sec sampling-period

  user-priority-cos-map:

     user        output       drop
   priority      queue     precedence

       0           8          high
       1           7          high
       2           6          high
       3           5          high
       4           4          medium
       5           3          medium
       6           2          medium
       7           2          low

  queue-cos-map:

     output         user
     queue        priority

       1            7
       2            6
       3            5
       4            4
       5            3
       6            2
       7            1
       8            0
```

8. Not able to enable rate monitoring for a class-map

   Symptom: User may not be able to enable rate monitoring for a class-map.

   Description: Flow rate monitoring has to be enabled for any specified class-map by the user. User may sometimes not able to enable rate monitoring for a class-map.

   Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

   - Accounting is not enabled. Before enabling rate-monitoring, accounting for the class-map needs to be enabled. Verify that accounting is enabled using the following command: **`show qos module policy-map m1 detail`**

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      0 bytes forwarded, 0 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         0 Kbps input rate, 0 Kbps output rate
         0 Kbps avg input rate, 0 Kbps avg output rate
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         enabled, srtcm, color-blind
         10 Kbps cir
         10 Kbits (82 Kbits oper) committed-burst
         20 Kbits (82 Kbits oper) extended-burst
         remark off, drop-violate off
         0 bytes conforming, 0 bytes exceeding
         0 bytes violating
      redirection:
         none
```

- Global rate monitoring is in progress. User will not be able to enable rate-monitoring for a class-map when the rate-sampling is in progress. User has to stop the global rate-sampling before enabling the rate-monitoring for a class-map. Use the following command to verify that rate-sampling is in progress: **`show qos module system`**

Comments? infodev@avaya.com

```
SR4134# show qos module system

  qos enabled, auto-qos disabled, accounting enabled
  rate-monitoring in-progress, 60 sec sampling-interval, 600 sec sampling-period

  user-priority-cos-map:

     user       output      drop
   priority     queue    precedence

       0          8         high
       1          7         high
       2          6         high
       3          5         high
       4          4         medium
       5          3         medium
       6          2         medium
       7          2         low

  queue-cos-map:

     output        user
     queue       priority

       1           7
       2           6
       3           5
       4           4
       5           3
       6           2
       7           1
       8           0
```

9. Congestion Management doesn't seem to work

   Symptom: User may perceive that congestion management (RED) is not working.

   Description: In Module QoS same congestion profile is used for both tail drop and random drop. User may sometimes see that tail-drop is happening and not random drop.

   Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

   - Enable random-detect on the interface. User has to explicitly enable random drop even if a congestion profile is attached to an interface. Use the following command to verify that random drop is enabled on the interface. **`show qos module ethernet 6/10`**

```
SR4134# show qos module ethernet 6/10

Interface ethernet6/10:
   default-queue 8
   random-detect, congestion-profile 1
   265 ingress-buffers, 256 egress-buffers, 245 xon-limit, 262 xoff-limit
   0 packets-queued
   shaping:
      disabled

   Queue     Scheduling        Shaping          Buffers
          Mode Weight Group  Rate    Burst    Limit Used
                             kbps    KB

     1    SPQ    -      -    -       -        32    0
     2    SPQ    -      -    -       -        32    0
     3    SPQ    -      -    -       -        32    0
     4    SPQ    -      -    -       -        32    0
     5    WRR    2      1    -       -        32    0
     6    WRR    1      1    -       -        32    0
     7    WRR    2      0    -       -        32    0
     8    WRR    1      0    -       -        32    0

   qos enabled, auto-qos disabled
   mark-dscp disabled, mark-user-priority disabled
   service-policy none
```

10. Unable to map a policy-map to an interface

    Symptom: User may not be able map a policy-map to an interface with service-policy command.

    Description: In Module QoS, policy-map needs to be mapped to an ingress interface before it becomes operational. User may sometimes get an error while mapping a policy-map to an interface.

    Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

    - Another policy-map is already attached. At-most one policy-map can be attached to an interface. If a service policy already exists for an interface, remove the previous policy-map and attach the new policy-map to the interface. To verify if a service-policy exists for a policy-map, use the following command: **`show qos module service-policy`**

      ```
      SR4134# show qos module service-policy

         Interface            Serviced-policy            Qos-status
         ethernet6/23         AutoQoSPolicy              enabled
         ethernet6/20         m1                         enabled
      ```

    - Auto qos is already enabled on the interface. If auto qos is already enabled on the interface, the default auto-qos policy-map will be servicing the interface. To attach the new policy-map, disable auto-qos on the interface and then attach the new policy-map to the interface. To verify if a service-policy exists

Comments? infodev@avaya.com

for a policy-map, use the following command: **show qos module service-policy**

```
SR4134# show qos module service-policy

    Interface            Serviced-policy            Qos-status
    ethernet6/23         AutoQoSPolicy              enabled
    ethernet6/20         m1                         enabled
```

11. Enabling auto-qos fails on an interface

    Symptom: User may get an error if auto-qos is enabled on an interface either from the global context or from the interface context.

    Description: In Module QoS, when auto-qos is enabled on an interface, user might get an error and auto-qos configuration fails. This can happen when auto-qos is enabled either globally or from an interface context.

    Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

    - Service policy already exists. At-most one policy-map can be attached to an interface. When auto-qos is enabled on an interface, it attempts to attach default auto-qos profile to the interface. If a service policy already exists for an interface, remove the previous policy-map and then enable auto-qos. To verify if a service-policy exists for a policy-map, use the following command: **show qos module service-policy**

```
SR4134# show qos module service-policy

    Interface            Serviced-policy            Qos-status
    ethernet6/23         AutoQoSPolicy              enabled
    ethernet6/20         m1                         enabled
```

12. PBR is not working

    Symptom: Policy based redirection is not working for a policy-map attached to a Module Ethernet interface.

    Description: PBR is achieved through QoS. PBR over Module Ethernet interfaces is achieved through Module QoS. PBR is configured as one of the actions for all packets matching the rules of a class-map. Sometimes, user may see that PBR is not working i.e. packets are sent to the specified next-hop or outgoing interface.

    Troubleshooting tips: Some of the reasons that could result in the above behavior are described below:

    - Class map rules are not proper. For PBR to happens, first of all, the packets have to match the rules of the class-map to which PBR is configured. Make sure that rules are configured correctly using the following command and make sure the packets hit the class-map by enabling accounting: **show qos module policy-map m1 detail**

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      2323732 bytes forwarded, 0 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         0 Kbps input rate, 0 Kbps output rate
         0 Kbps avg input rate, 0 Kbps avg output rate
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         enabled, srtcm, color-blind
         10 Kbps cir
         10 Kbits (82 Kbits oper) committed-burst
         20 Kbits (82 Kbits oper) extended-burst
         remark off, drop-violate off
         0 bytes conforming, 0 bytes exceeding
         0 bytes violating
      redirection:
         ipv4 next-hop 20.1.1.2, up
```

- PBR configuration status is not up. Based on the correctness of the PBR configuration, the PBR status will be displayed. Make sure the PBR status is UP using the following command: **`show qos module policy-map m1 detail`**

```
SR4134# show qos module policy-map m1 detail

policy-map: m1

   Serviced-interface    Qos-status
      ethernet6/20        enabled

   class-map: c1 (seq# 1)
      2323732 bytes forwarded, 0 bytes dropped
      queue carry, drop-precedence carry, dscp carry, user-priority carry
      rate-monitoring:
         0 Kbps input rate, 0 Kbps output rate
         0 Kbps avg input rate, 0 Kbps avg output rate
      rules:
         match ipv4 dscp af33
         match ipv4 dest-mac 00:40:5c:00:00:01
      police:
         enabled, srtcm, color-blind
         10 Kbps cir
         10 Kbits (82 Kbits oper) committed-burst
         20 Kbits (82 Kbits oper) extended-burst
         remark off, drop-violate off
         0 bytes conforming, 0 bytes exceeding
         0 bytes violating
      redirection:
         ipv4 next-hop 20.1.1.2, up
```


Comments? infodev@avaya.com

- Qos is not enabled on the interface. QoS should be enabled on the interface on which the policy-map is attached. Verify that qos is enabled on the interface using the following command: **`show qos module service-policy`**

```
SR4134# show qos module service-policy

   Interface            Serviced-policy            Qos-status
   ethernet6/23         AutoQoSPolicy              enabled
   ethernet6/20         m1                         enabled
```

Comments? infodev@avaya.com

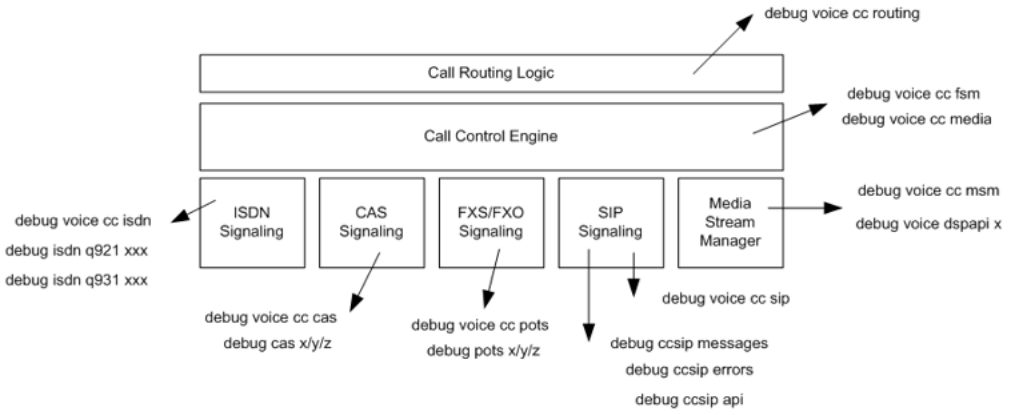
Chapter 16: Troubleshooting a SIP Media Gateway problem

The following sections provide information to help troubleshoot problems with SIP Media Gateway voice connections.

- Debug command overview on page 303
- Common problems and solutions on page 309
- Troubleshooting the Mediation Server Module on page 359
- Re-imaging the Mediation Server Module on page 365

Debug command overview

The following diagram shows the Avaya Secure Router 2330/4134 telephony building blocks. The ISDN Signaling, CAS Signaling, FXS/FXO Signaling and SIP Signaling block take care of the corresponding protocol signaling. The Media Stream Manager is in charge of the digital signal processing (DSP). The Call Control Engine is the coordinating entity. The Call Routing Logic, an extension of the Call Control Engine, takes care of call routing and route table lookups.



The diagram also lists various debug commands associated with each of these modules. The syntax and functionality for the commands is explained in the following sections.

- debug cas on page 304
- debug ccsip all on page 304
- debug ccsip api on page 305

- debug ccsip errors on page 305
- debug ccsip media on page 305
- debug ccsip messages on page 306
- debug isdn q921 on page 306
- debug isdn q931 on page 307
- debug pots on page 307
- debug voice cc on page 307
- debug voip dial-peer on page 308

debug cas

Use this command to enable CAS related debugging. Use the no form of this command to disable the debug messages.

Syntax

```
[no] debug cas [slot <slot[/subslot/]port>] debug_identifier <debug-level>
```

Table 70: Variable definitions

Variable	Value
<slot/[<subslot/]port>	Specifies the port number of the voice card.
<debug-level>	Specifies the debug level: all, signal, or callcontrol.

Example

```
SR# debug cas slot 1/1
```

debug ccsip all

Use this command to enable SIP related call control debugging. Use the no form of this command to disable the debug messages.

Syntax

```
[no] debug ccsip all
```

Example

```
SR# debug ccsip all
```


Comments? infodev@avaya.com

debug ccsip api

Use this command to enable SIP application interface debugging. If no parameters are specified, all SIP application related debugs are output. Use the no form of this command to disable the debug messages.

Syntax

```
[no] debug ccsip api [ calling-num <calling-number> ] [called-num
<called-number> ]
```

Table 71: Variable definitions

Variable	Value
calling-num <calling-number>	Filters debugging information based on calling-number.
called-num <called-number>	Filters debugging information based on called-number.

Example

```
SR# debug ccsip api
```

debug ccsip errors

Use this command to enable output of SIP error messages. Use the no form of this command to disable the debug messages.

Syntax

```
[no] debug ccsip errors
```

Example

```
SR# debug ccsip errors
```

debug ccsip media

Use this command to enable SIP media interface debugging. If no parameters are specified, all SIP media related debug messages are output. Use the no form of this command to disable the debug messages.

Syntax

```
no debug ccsip media [calling-num <calling-number> ] [called-num
<called-number>]
```

Table 72: Variable definitions

Variable	Value
calling-num <calling-number>	Filters debugging information based on calling-number.
called-num <called-number>	Filters debugging information based on called-number.

Example

```
SR# debug ccsip media
```

debug ccsip messages

Use this command to enable SIP message debugging. If no parameters are specified, all SIP messages are output. Use the no form of this command to disable the debug messages.

Syntax

```
[no] debug ccsip messages [calling-num <calling-number>] [called-num <called-number> ]
```

Table 73: Variable definitions

Variable	Value
calling-num <calling-number>	Filters debugging information based on calling-number.
called-num <called-number>	Filters debugging information based on called-number.

Example

```
SR# debug ccsip messages
```

debug isdn q921

Use this command to enable Q921 related ISDN debugging. Use the no form of this command to disable the debug messages.

Syntax

```
[no] debug isdn q921 <bundle-name>
```

Table 74: Variable definitions

Variable	Value
<bundle-name>	Specifies the ISDN bundle name.

Comments? infodev@avaya.com

Example

```
SR# debug isdn q921 pri1
```

debug isdn q931

Use this command to enable Q931 related ISDN debugging. Use the no form of this command to disable the debug messages.

Syntax

```
[no] debug isdn q931 <bundle-name> [mon <1-3>]
```

Table 75: Variable definitions

Variable	Value
<bundle-name>	Specifies the ISDN bundle name.
[mon <1-3>]	Specifies the monitor level.

Example

```
SR# debug isdn q931 pri1
```

debug pots

Use this command to enable FXS /FXO (POTS) related debugging. Use the no form of this command to disable the debug messages.

Syntax

```
[no] debug pots slot <slot/subslot/port>
```

Table 76: Variable definitions

Variable	Value
<slot/[<subslot/]port>	Specifies the port number of the voice card.

Example

```
SR# debug pots slot 1/1
```

debug voice cc

Use this command to debug the VoIP call control engine. Use the no form of this command to disable the debug messages. If no parameters are specified, the router outputs all message types.

The most common option to use is **debug voice cc routing**, which acts as a type of trace command, displaying the dial-peer matching. Verify the status of the dial peer first using **show dial-peer voice**.

If debugging the routing does not identify the problem, then enable specific debugs. Enabling all debugs at once provides too much output to provide meaningful information.

Syntax

```
[no] debug voice cc [sip | isdn | cas | pots | fsm | media | routing
| msm | all]
```

Table 77: Variable definitions

Variable	Value
sip	Enables SIP adaptor specific debugs.
isdn	Enables ISDN adaptor specific debugs.
cas	Enables CAS adaptor specific debugs.
pots	Enables POTS adaptor specific debugs.
fsm	Enables state machine specific debugs.
media	Enables media specific debugs.
routing	Enables call routing specific debugs including dial peer matching.
msm	Enables call control and media manager specific debugs.
all	Enables all the above debugs.

Example

```
SR# debug voice cc routing
```

debug voip dial-peer

Use this command to debug VoIP dial peers. Use the no form of this command to disable the debug messages

Syntax

```
[no] debug voip dial-peer
```

Example

```
SR# debug voip dial-peer
```


Comments? infodev@avaya.com

Common problems and solutions

The following sections contain solutions for common SIP Media Gateway voice connectivity issues:

- No voice commands available on page 309
- New calls fail if more than 8 (or 16, 32, 64) simultaneous G.711 calls are attempted on page 313
- Port 2/2 on the SR4134 cannot be configured on page 316
- T1 Link: Amber or RED LED and alarms on page 316
- Remote T1 link reports clock slip or frame drop errors on page 319
- Configuration of BRI, T1, or PRI port as clock source produces error on page 322
- Module LEDs for T1 or BRI are off on page 323
- Creation of T1 CAS of addition of PRI link to bundle produces an error on the state of the slot on page 325
- Unable to make calls on T1 PRI on page 325
- Unable to make calls on T1 CAS on page 330
- FXS/FXO port status LEDs on page 332
- No dial tone on the analog FXS phones or ports on page 333
- Unable to make FXS calls on page 333
- FXS phones are not registered (Sylantro and BroadSoft only) on page 338
- Unable to make FXO calls on page 341
- Secure Router 2330/4134 not reachable from SIP Server on page 346
- Unable to make outbound calls to SIP endpoints on page 354
- Codec mismatch on page 356

No voice commands available

If the Secure Router 2330/4134 is not equipped for voice traffic, the CLI does not display voice commands.

To list the available commands, enter a **?** at the `configure#` prompt.

The following figure shows a sample output with some voice-related commands highlighted in red.

```
SR/configure# ?

      SYS_REM                   add comments to system related configuration
                                at the beginning
      SYS_REM_                  add comments to system related configuration
                                at the end
      aaa                       To configure AAA parameters
      access-list               Add An Access list Entry
      admin_name                Change the administrator account name
.
.
      console_timeout           configure console timeout
      date                      Set date
      dial-peer                 dial-peer
      dot1x                     IEEE 802.1X Port-Based Access Control
.
.
      mpls                      Configure MPLS specific attributes
      network-clock-select      Specify the selection priority for ports
                                that provide timing for network clock
      oam                       Configure OAM
.
.
      secure_passwords          encrypt all the passwords, while
                                saving/displaying the configuration
      sip-ua                    sip user agent configurations
      sla                       configure sla parameters
.
.
      tftp_server               enable/disable TFTP server
      time                      Set Time
      trunk                     Define or modify the definition of a trunk
                                group.
      user                      Configures user
      utc                       Set utc Time
      vlan                      Vlan commands
      voice                     Configure voice service settings
      voice-port                Configure the voice port on the given card.

SR/configure#
```

Figure 39: CLI help sample output

If the Secure Router 2330/4134 does not display voice commands, see the following sections for troubleshooting.

Voice-compatible software image not installed

The SIP Media Gateway features are only supported in release 10.1.0.0 and later. Verify that the Secure Router 2330/4134 is running the minimum release of software using the **`show version`** command.

Comments? infodev@avaya.com

```
SR4134# show version
  Kernel: WIND version 2.6.
    Boot: 0.0.0.29 (NORMAL Boot)
 Runtime: 10.1.0.0
 Created: Feb 22 2008, 07:45:23
 NorBoot: 0.0.0.29
 GolBoot: 0.0.0.29


Slot/SubSlot  Card-Type  Status   FPGA-Rev FPGA-Eng-Rev CPLD-Rev CPLD-Eng-Rev
-------------------------------------------------------------------------------
   0/-        MPU_A      NORMAL   0x1      0x3          ---      0xb
   6/-        SERVMOD    NORMAL   ---      ---          ---      0x1
   3/-        WTE_2M     NORMAL   ---      ---          0x1      0x5
   1/-        WTE_2M     NORMAL   ---      ---          0x1      0x5
```

Figure 40: show version sample output for software release

If the Secure Router 2330/4134 is not running 10.1.0.0 or later software, perform the required upgrade.

PVM or PVIM module not installed

The internal Packetized Voice Module (PVM) on the Secure Router 4134 or Packetized Voice Internal Module (PVIM) on the Secure Router 2330 must be installed for the Secure Router to support the SIP Media Gateway features. Ensure that the PVM or PVIM module is installed properly.

The following figure shows the installation location for the internal PVM in the Secure Router 4134.

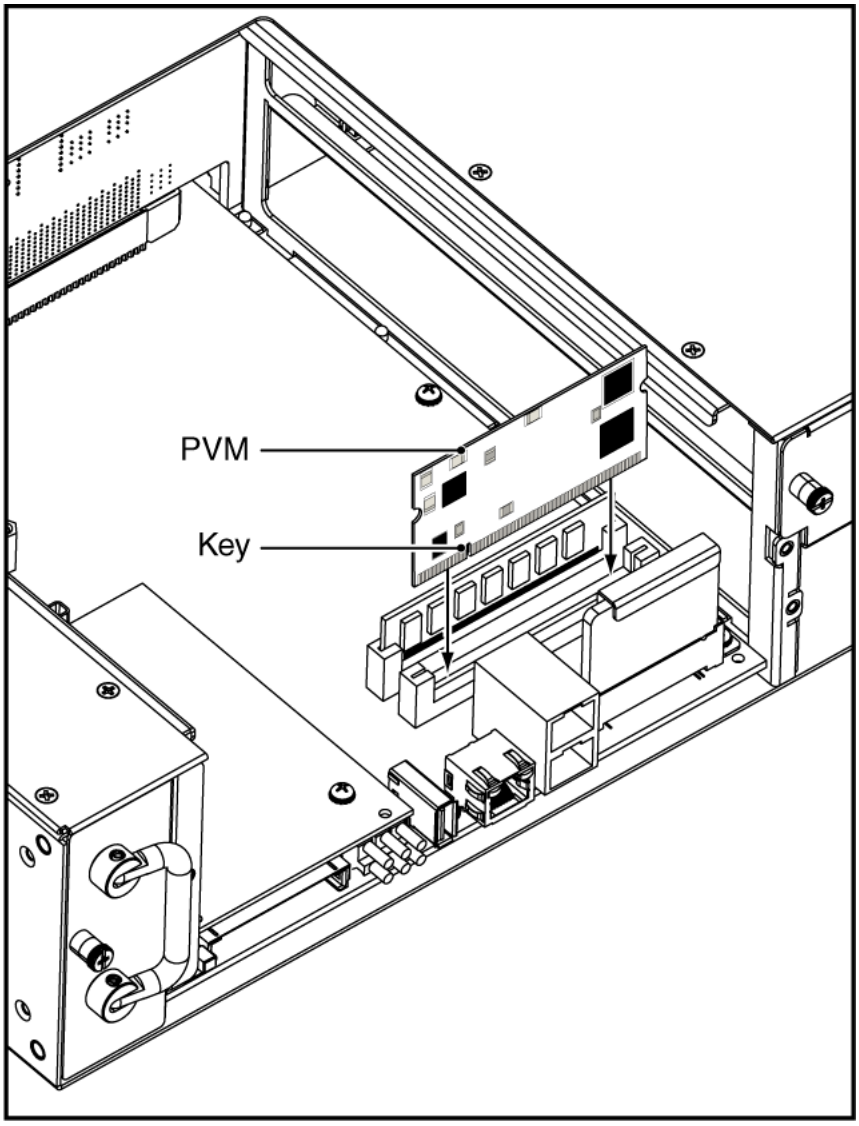


Figure 41: PVM installation in the Secure Router 4134

To display the presence of the internal PVM module (listed as VoIP_A card type), enter the **`show chassis`** command.

Comments? infodev@avaya.com

```
SR/configure# show chassis

Chassis Model: SR4134
Chassis Operational Status: NORMAL

Chassis Serial number: xxxxxxxxxxxxxxxx
Chassis Rev: 8

Slot/SubSlot    Card-Type       Status        Serial#
-----------------------------------------------------
   0            MPU_A           NORMAL        xxxxxxxxxxxxxxxx
   5            LMP_24          NORMAL        xxxxxxxxxxxxxxxx
   3            BRI_2U          NORMAL        xxxxxxxxxxxxxxxx
   4            WTE_1           NORMAL        xxxxxxxxxxxxxxxx
   1            WTE_2M          NORMAL        xxxxxxxxxxxxxxxx
   2            FXS_4M          NORMAL        xxxxxxxxxxxxxxxx
 INT            VOIP_A          NORMAL        ---

INT - Mainboard internal module.
SR/configure#
```

Figure 42: show chassis sample output for PVM module

If the PVM module is not listed, the PVM module is either not installed or installed improperly. You must verify that the module is installed properly. Ensure the PVM slot is clear of debris before you install the module. Protective tape is placed over the SO-DIMM and PVM slots during the manufacturing process; ensure you remove this tape if it is present. For details about PVM installation, see *Avaya Secure Router 2330/4134 Installation — Hardware Components* (NN47263-301).

The Secure Router 2330/4134 does not support hot swap for the internal PVM module. If the PVM module is inserted at run-time, this can damage the main board or the PVM module.

Electrostatic alert:

To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack when performing maintenance on a Secure Router 2330/4134. Ensure that the wrist strap makes contact with your skin.

New calls fail if more than 8 (or 16, 32, 64) simultaneous G.711 calls are attempted

The Secure Router 2330/4134 uses a DSP channel licensing mechanism. Each Secure Router 2330/4134 is configured with a given number of DSP channel licenses.

To verify the number of active DSP channels, use the **`show voice dsp status`** command.

```
SR/configure# show voice dsp status
DSP Status
MSP Version : v6_11_0_5 Rev E - HP
T38 Version : T38DDP_VER_5_1_7
PVDM Present : Present
MSP Status : Unknown
RTP port validation : Enabled
Max Channel : 8
Active VOIP Channels : 0
Active FOIP Channels : 0
Additional G.711 10ms Channels: 4
Additional G.711 20ms Channels: 8
Additional G.723 Channels: 4
Additional G.726 Channels: 4
Additional G.729 Channels: 4
Additional T.38 Channels: 2
SR/configure#
```

Figure 43: show voice dsp status sample output for active DSP channels

For any of the displayed codecs, if any of the additional channel capacity is 0, no more calls can be created using that codec.

You can use the same command to verify the licensed DSP channel capacity on the Secure Router 2330/4134.

```
SR/configure# show voice dsp status
DSP Status
MSP Version : v6_11_0_5 Rev E - HP
T38 Version : T38DDP_VER_5_1_7
PVDM Present : Present
MSP Status : Unknown
RTP port validation : Enabled
Max Channel : 8
Active VOIP Channels : 0
Active FOIP Channels : 0
Additional G.711 10ms Channels: 4
Additional G.711 20ms Channels: 8
Additional G.723 Channels: 4
Additional G.726 Channels: 4
Additional G.729 Channels: 4
Additional T.38 Channels: 2
SR/configure#
```

Figure 44: show voice dsp status sample output for maximum DSP channels

To upgrade the DSP channel capacity, contact Avaya customer support for a DSP license upgrade. You must provide Avaya customer support with the serial number of the Secure Router 2330/4134 motherboard and the maximum number of channels required.

To obtain the motherboard serial number (listed as MPU_A card type), enter the **`show chassis`** command.

Comments? infodev@avaya.com

```
SR/configure# show chassis

Chassis Model: SR4134
Chassis Operational Status: NORMAL

Chassis Serial number: xxxxxxxxxxxxxxxx
Chassis Rev: 8

Slot/SubSlot    Card-Type       Status        Serial#
-----------------------------------------------------
   0            MPU_A           NORMAL        LBabcdef12345678901
   5            LMP_24          NORMAL        xxxxxxxxxxxxxxxx
   3            BRI_2U          NORMAL        xxxxxxxxxxxxxxxx
   4            WTE_1           NORMAL        xxxxxxxxxxxxxxxx
   1            WTE_2M          NORMAL        xxxxxxxxxxxxxxxx
   2            FXS_4M          NORMAL        xxxxxxxxxxxxxxxx
 INT            VOIP_A          NORMAL        ---

INT - Mainboard internal module.
```

Figure 45: show chassis sample output for motherboard serial number

With the motherboard serial number and the number of required channels, Avaya customer support can provide you a license key that you must install on the router for the upgrade. (See *Avaya Secure Router 2330/4134 Configuration — SIP Media Gateway* (NN47263-508) for upgrade details.) You can load the license using the **`system licenses pvm_channels`** command.

```
SR/configure# system licenses pvm_channels 64
Enter License key: 04fedcba9876543101
Requested Change Is Done.
Please reboot the box for this change to take effect.
SR/configure#
```

Figure 46: system licenses pvm_channels sample response

After you load the license and reboot the chassis, you can verify that the licenses are upgraded successfully by entering the **`show voice dsp status`** command.

```
SR/configure# show voice dsp status
DSP Status
MSP Version : v6_11_0_5 Rev E - HP
T38 Version : T38DDP_VER_5_1_7
PVDM Present : Present
MSP Status : Unknown
RTP port validation : Enabled
Max Channel : 64
Active VOIP Channels : 0
Active FOIP Channels : 0
Additional G.711 10ms Channels: 32
Additional G.711 20ms Channels: 64
Additional G.723 Channels: 32
Additional G.726 Channels: 32
Additional G.729 Channels: 32
Additional T.38 Channels: 16
SR/configure#
```

Figure 47: show voice dsp status sample output for DSP channel upgrade

Port 0/0 cannot be configured

You cannot enable the management port on the rear of the Secure Router 4134 (Ethernet 0/0) if you have a PVM installed (this is related to hardware design). Ensure you use Ethernet 0/1, 0/2, 0/3, or 0/4 for management if you use a PVM in the router.

Port 2/2 on the SR4134 cannot be configured

Slot 2 of the Secure Router 4134 supports only one port of any WAN data Small Module. If you install a 2-port Small Module in Slot 2, and use the Small Module for data connections, one port only 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.

This limitation does not apply to FXS or FXO voice modules.

T1 Link: Amber or RED LED and alarms

The T1 link LED indicates the state of the physical layer of the module (not the D-channel status). An Amber or Red LED indicates that a local or remote T1 alarm is detected on the link.

To view the status of the physical layer of the module, enter the **`show module configuration t1`** command. The following figure shows a sample output with an example alarm received from a remote peer.

Comments? infodev@avaya.com

```
SR/configure# show module configuration t1 1/1
T1 1/1 is ENABLED
Alarm Hierarchy: TRUE,
Yellow Alarm: GENERATE & DETECT
Framing:ESF, LineCode:B8ZS, ClockSource: NET, LineMode:CSU, LBO:0 db
FDL: ANSI Unit Protocol enabled ,ATT Unit Protocol disabled ,
CsuDsuType:  CSU , Loopback Framing (In-band): Overwrite,
CIRCUIT-ID : Not Configured ,CONTACT-INFO : Not Configured ,
DESCRIPTION : Not Configured , LINK NAME : Not Configured ,

Line Status:
   RLOS:OFF,   RAIS: ON,   RLOF:OFF,   RRAI:OFF,   TAIS:OFF
   TRAI: ON,  TPtrn:OFF,   Loop:OFF

Timeslot Map:
  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
 _____________________________________________________________________
|0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |
|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|

SR/configure#
```

Figure 48: show module configuration t1 sample output with alarm

To troubleshoot a T1 alarm, see the following sections.

Configuration mismatch at opposite ends of the T1 connection

If the configuration at both ends of the T1 line does not match, this produces an alarm. The most common configuration mismatches include the framing format (ESF or D4/SF) and the linecoding format (B8ZS or AMI). Make sure these configurations match at both ends. The most common configuration for framing format is ESF and for linecode is B8ZS (the defaults for the Secure Router 2330/4134). The Secure Router 2330/4134 Media Gateway supports only ESF framing on T1 CAS; it does not support D4 framing.

The following figure shows a sample output of verifying the link configuration on the Secure Router 2330/4134.

```
SR/configure# show module configuration t1 1/1
T1 1/1 is ENABLED
Alarm Hierarchy: TRUE,
Yellow Alarm: GENERATE & DETECT
Framing:ESF, LineCode:B8ZS, ClockSource: NET, LineMode:CSU, LBO:0 db
FDL: ANSI Unit Protocol enabled ,ATT Unit Protocol disabled ,
CsuDsuType:  CSU , Loopback Framing (In-band): Overwrite,
CIRCUIT-ID : Not Configured ,CONTACT-INFO : Not Configured ,
DESCRIPTION : Not Configured , LINK NAME : Not Configured ,

Line Status:
   RLOS:OFF,   RAIS:OFF,   RLOF:OFF,   RRAI:OFF,   TAIS:OFF
   TRAI:OFF,  TPtrn:OFF,   Loop:OFF

Timeslot Map:
  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
 ___________________________________________________________________________
|0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |
|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|

SR/configure#
```

Figure 49: show module configuration t1 sample output for framing and linecode

Physical connection issue

The T1 link uses the standard 4 wire link on the RJ-45 connector. Ensure that the physical link is properly connected. Also make sure that the correct cable type is used: either crossover cable or straight cable. When connecting to a peer back-2-back, a crossover cable is typically required. When connecting to a channel-bank or patch-panel, a straight cable is typically required.

Peer configured as E1

Make sure that the peer you are connected to is a T1 source and not E1. Normally sources can be configured for both T1 and E1. The Secure Router 2330/4134 can also be configured for both T1 and E1, but for Release 10.1, voice is not supported on E1 links. Therefore, make sure both ends are configured for T1.

You can use the **`show module configuration all`** command to verify the configuration for multiple links.

Comments? infodev@avaya.com

```
SR/configure# show module configuration all

T1 #      Framing   Coding    ClkSrc    LBO-CableLength   State     Alarm
-------------------------------------------------------------------------
4/1       esf       ami       int       csu/0db           up        N/A

T1 #      Framing   Coding    ClkSrc    LBO-CableLength   State     Alarm
-------------------------------------------------------------------------
1/1       esf       b8zs      NET       csu/0db           up        N/A
1/2       esf       b8zs      NET       csu/0db           down      RLOS
SR/configure#
```

Figure 50: show module configuration all sample output

Remote T1 link reports clock slip or frame drop errors

If the remote T1 link reports a clock slip or that frames are being dropped, see the following section for troubleshooting.

Incorrect T1/E1 module version

Make sure that the T1/E1 module version is listed as CPLD version 5. Older version 4 cards can still be used for data links, but should not be used for voice. New version 5 cards support both data and voice links.

Use the **show version** command to display the module version. The following figure shows a sample output of the command displaying the T1/E1 module versions.

```
SR/configure# show version
  Kernel: WIND version 2.6.
    Boot: 0.0.0.29 (NORMAL Boot)
 Runtime: 10.1.0.98
 Created: Feb 14 2008, 10:01:02
 NorBoot: 0.0.0.29
 GolBoot: 0.0.0.29


Slot/SubSlot  Card-Type  Status   FPGA-Rev FPGA-Eng-Rev CPLD-Rev CPLD-Eng-Rev
-------------------------------------------------------------------------------
   0/-        MPU_A      NORMAL   0x1      0x3          ---      0xb
   5/-        LMP_24     NORMAL   ---      ---          0x1      0x5
   3/-        BRI_2U     NORMAL   ---      ---          0x1      0x6
   4/-        WTE_1      NORMAL   ---      ---          0x1      0x5
   1/-        WTE_2M     NORMAL   ---      ---          0x1      0x5
   2/-        FXS_4M     NORMAL   ---      ---          0x1      0x9

SR/configure#
```

Figure 51: show version sample output for T1/E1 module version

Network clock misconfigured, does not lock, or displays as bad clock

In some cases, the remote end of the link reports clock slip errors or frame drop errors on the physical link. In other cases, the clock source configured on the Secure Router 2330/4134 does not lock to the peer, or the clock state displays a bad clock.

To troubleshoot these problems, verify the clock configuration on the Secure Router 2330/4134.

Make sure that the Secure Router 2330/4134 is configured as the clock slave to the remote end and the remote end is configured as the clock master. If both the Secure Router 2330/4134 and the peer are configured as slaves, neither end of the link can lock to the external clock.

To display the clock configuration, enter the **show network-clocks** command.

```
SR/configure# show network-clocks
Network Clock Configuration
---------------------------
Priority | Clock Source | Clock Type | Clock State
   3     | Mainboard    | PLL        | GOOD

Current Clock Source
--------------------
Priority | Clock Source | Clock Type | Clock Status
   3     | Mainboard    | PLL        | GOOD

SR/configure#
```

Figure 52: show network-clocks sample output for clock source

In the preceding figure, there is no clock configured and the Secure Router 2330/4134 is free-running as the clock master.

The following figure shows an example of a bad clock source.

Comments? infodev@avaya.com

```
SR/configure# show network-clocks
Network Clock Configuration
---------------------------
Priority | Clock Source | Clock Type | Clock State
   1     | T1 1/1       | T1         | BAD
   3     | Mainboard    | PLL        | GOOD

Current Clock Source
--------------------
Priority | Clock Source | Clock Type | Clock Status
   3     | Mainboard    | PLL        | LOCKING

SR/configure#
```

Figure 53: show network-clocks sample output for bad clock source

To change the clock configuration on the Secure Router 2330/4134, use the **network-clock-select** command. Then use the **show network-clocks** command to verify that the Secure Router 2330/4134 locks to the clock from the remote peer.

```
SR/configure# network-clock-select 1 1/1
SR/configure# show network-clocks
Network Clock Configuration
---------------------------
Priority | Clock Source | Clock Type | Clock State
   1     | T1 1/1       | T1         | BAD
   3     | Mainboard    | PLL        | GOOD

Current Clock Source
--------------------
Priority | Clock Source | Clock Type | Clock Status
   3     | Mainboard    | PLL        | LOCKING

SR/configure#
```

Figure 54: show network-clocks sample output for locking clock source

As shown in the preceding figure, you must wait a period of time for the phase-locked loop (PLL) to lock to the external clock. It can take anywhere from 30 seconds up to 180 seconds for the PLL to detect a viable clock source and lock to it.

The following figure shows the clock in locked status.

```
SR/configure# show network-clocks
Network Clock Configuration
---------------------------
Priority | Clock Source | Clock Type | Clock State
   1     | T1 1/1       | T1         | GOOD
   3     | Mainboard    | PLL        | GOOD

Current Clock Source
--------------------
Priority | Clock Source | Clock Type | Clock Status
   1     | T1 1/1       | T1         | LOCKED

SR/configure#
```

Figure 55: show network-clocks sample output for locked clock source

Also, verify the status of the configured clock source by entering **show module configuration t1** for a T1 port and **show interface bundle** for an ISDN PRI or BRI port.

Finally, verify that the configuration at both ends of the link matches.

Configuration of BRI, T1, or PRI port as clock source produces error

To configure a BRI, T1, or PRI port as the network clock source, the port must be configured for voice. You cannot specify a data port as the clock source.

The following figure shows a T1 CAS port that can be used as the clock source.

```
SR/configure# show voice port summary

PORT   SIG-TYPE                  ADMIN OPER EC
====== ========================= ===== ==== ==
1/1    CAS wink-start            up    down y
1/2    CAS wink-start            up    down y
SR/configure#
```

Figure 56: show voice port summary sample output for CAS

The following figure shows a T1 PRI link in a voice bundle that can be used as the clock source.

Comments? infodev@avaya.com

```
SR/configure# show interface bundles
bundle    bw(kbps) description              contact         stat        IType
Link
------    -------- -----------              -------         ----        -----
----
pbx1      64       none                     none            Down
PRI_T1 (V) 4/1:1-23;


Link Usage Summary  :
---------------------
T1      4/1:1-23;

BRI     NONE

SR/configure#
```

Figure 57: show interface bundles sample output for PRI

The following figure shows a BRI port in a voice bundle that can be used as the clock source.

```
SR/configure# show interface bundles
bundle    bw(kbps) description              contact         stat        IType
Link
------    -------- -----------              -------         ----        -----
----
bri1      16       none                     none            Down        BRI
(V)     3/1:1-2;


Link Usage Summary  :
---------------------
T1      NONE
BRI     3/1:1-2;


SR/configure#
```

Figure 58: show interface bundles sample output for BRI

Module LEDs for T1 or BRI are off

The Secure Router 2330/4134 supports hot swap of identical external modules. If you boot up and the LEDs on a module are off, the module may be in the process of being hot swapped.

To determine if the module is being hot swapped, enter the **`show chassis`** command. The following figure shows a sample output when a module is being hot swapped.

```
SR/configure# show chassis

Chassis Model: SR4134
Chassis Operational Status: HOT-SWAP

Chassis Serial number: xxxxxxxxxxxxxxxx
Chassis Rev: 8

Slot/SubSlot    Card-Type       Status        Serial#
-------------------------------------------------------
   0            MPU_A           NORMAL        xxxxxxxxxxxxxxxx
   5            LMP_24          NORMAL        xxxxxxxxxxxxxxxx
   3            BRI_2U          NORMAL        xxxxxxxxxxxxxxxx
   4            WTE_1           ADMIN-DOWN    xxxxxxxxxxxxxxxx
   1            WTE_2M          NORMAL        xxxxxxxxxxxxxxxx
   2            FXS_4M          NORMAL        xxxxxxxxxxxxxxxx
 INT            VOIP_A          NORMAL        ---

HOT-SWAP under way for slot number 4.
Expected Card in slot 4 is : WTE_1

INT - Mainboard internal module.
SR/configure#
```

Figure 59: show chassis sample output during hot swap

To bring a module out of the hot swap state, use the **no shutdown** command and reboot the chassis.

```
SR/configure# chassis module 4
SR/configure/chassis/module (4)# no shutdown

Continue Configuring Module Administration Status: Are you sure? (y/n) : y
    1 : # SR4134 system configuration file (.CFG).
  2 : #
  3 : # Nortel Networks assumes no responsibility for product reliability,
  4 : # performance, or both if the user modifies the .CFG file.  Full
  5 : # responsibility for any modification made to the .CFG file, by
  6 : # the user, is assumed by the user.
  7 : #
  8 : # Version: 10.1.0.86
  9 : # File Created: 02/04/2008-20:19:34
 10 :
 11 :
 12 :
 13 : system logging
 14 :     console
.
.
```

Figure 60: module no shutdown sample output for hot swap

To verify that the card is in the normal state after the reboot, enter the **show chassis** command again.

Comments? infodev@avaya.com

Creation of T1 CAS of addition of PRI link to bundle produces an error on the state of the slot

The following figure shows sample errors when creating a CAS link or adding a PRI link to a bundle.

```
SR/configure# module t1 4/1
Error - Slot (4) not in NORMAL state.
Error! Invalid input for T1 Slot_Port No. Numeric value or range expected in
Slot/Port format.

SR/configure# interface bundle pbx2
configuring new WAN bundle interface pbx2
SR/configure/interface/bundle pbx2# link pri_t1 4/1 voice
Error - Slot (4) not in NORMAL state.
Error in specifying links
SR/configure/interface/bundle pbx2#
```

Figure 61: show module t1 sample output with error

The Secure Router 2330/4134 produces these errors when the port in question is on a module that is shutdown for a hot swap.

See Module LEDs for T1 or BRI are off on page 323 to troubleshoot a module in the hot swap state.

Unable to make calls on T1 PRI

If you cannot make calls on a T1 PRI port, see the following sections for troubleshooting instructions.

Verify the T1 PRI configuration

If you cannot make calls on a T1 PRI port, make sure that the PRI configuration is correct. The following is a typical configuration:

```
config term
interface bundle pri1
link pri_t1 1/1:1-23 voice
isdn
side USR
switch-type primary-5ess
activate
exit 2
```

Be sure to activate ISDN using the **`activate`** command under **`isdn`** (as shown above).

Verify ISDN timeslot configuration

Make sure that the ISDN timeslots are configured properly. If the **link** command under **interface bundle** is entered with partial channels, calls cannot be successful on the remaining channels. Furthermore, these remaining timeslots cannot be used in another bundle.

For example, in the following configuration, only timeslots 1 to 12 can be used for calls.

```
SR/configure# interface bundle pri1
SR/configure/interface/bundle pri1# link pri_t1 1/1:1-12 voice
```

Display the configuration status

You can display the configuration status using the **debug isdn isdn-status** command:

```
SR# debug isdn isdn-status pri1

  SAP Id          = 0
  Sap State       = 3   DCh State    = UP
  Interface       = PRI T1
  Side            = USER
  Switch Type     = primary-5ess
  Bundle          = pri1

  BChn   BStatus  Type     Id       Curr St          Curr Ev          Call Orig
   1     Free     --       --       --               --               --
   2     Free     --       --       --               --               --
   3     Free     --       --       --               --               --
   4     Free     --       --       --               --               --
   5     Free     --       --       --               --               --
   6     Free     --       --       --               --               --
   7     Free     --       --       --               --               --
   8     Free     --       --       --               --               --
   9     Free     --       --       --               --               --
  10     Free     --       --       --               --               --
  11     Free     --       --       --               --               --
  12     Free     --       --       --               --               --
  13     Free     --       --       --               --               --
  14     Free     --       --       --               --               --
  15     Free     --       --       --               --               --
  16     Free     --       --       --               --               --
  17     Free     --       --       --               --               --
  18     Free     --       --       --               --               --
  19     Free     --       --       --               --               --
  20     Free     --       --       --               --               --
  21     Free     --       --       --               --               --
  22     Free     --       --       --               --               --
  23     Free     --       --       --               --               --
```

Figure 62: debug isdn isdn-status sample output

Be sure that the far end also uses the same switch type (in this example, shown as primary 5ess).

Comments? infodev@avaya.com

Also, be sure that the other end is configured as network side. The current release only supports user side on the Secure Router 2330/4134.

Verify the D channel status

To verify that the D channel is up, use the **show interface bundle** command.

```
SR# show interface bundle pri1

bundle pri1
-----------
status                              up
number of links                     1
voice-port info                     1/1:23
switch-type                         primary-5ess
side                                USR

counters for 1/1:23 since last boot/clear
    Bytes Rx                     1152    Bytes Tx                     1453
    Packets Rx                    264    Packets Tx                    379
    All Err Pkt Rx                  0    All Err Pkt Tx                  0
    Pkt 2 Long Rx                   0    Failed Pkt Tx                   0
    Overrun Rx                      0    Underrun Tx                     0
    Pkt CRC Err Rx                  0
    Pkt Inv Len Rx                  0
    Abort Rx                        0
```

Figure 63: show interface bundle sample output to verify PRI D-channel

Verify Layer 2 status

When layer 2 is up, both sides continuously send RR messages to each other.

To verify that Layer 2 is up, use the **debug isdn q921** command.

```
SR# debug isdn q921 pri1

-- 0 --L2      T -> N  -- 20:03:16.67 --
 msg: SABME
 dat: 00 01 7f

-- 0 --L2      T -> N  -- 20:03:18.67 --
 msg: SABME
 dat: 00 01 7f

 -- 0 --L2      N -> T  -- 20:03:18.67 --
 msg: UA
 dat: 00 01 73

 -- 0 --L2      T -> N  -- 20:03:23.67 --
 msg: RR
 dat: 00 01 01 01

-- 0 --L2      N -> T  -- 20:03:23.67 --
 msg: RR
 dat: 00 01 01 01
```

Figure 64: debug isdn q921 sample output

Perform Layer 3 traces

For further ISDN troubleshooting, you can also perform Layer 3 traces using the **debug isdn q931** command. The following figures show sample Layer 3 traces for a successful ISDN call flow.

Comments? infodev@avaya.com

```
SR# debug isdn q931 pri1
```

SIP to ISDN:
Note that before CONNECT, gateway may receive PROGRESS or PROGRESS followed by ALERT message.

```
-- 0 --L3      T -> N  -- 20:57:05 --
 Msg:       SETUP
 MsgHdr: 08 02 00 01 05
 BC: 04 02 80 90
 CHID: 18 03 a9 83 82
 NSF: 20 02 00 e1
 CLNG: 6c 06 00 80 34 30 30 30
 CLED: 70 05 80 34 30 30 30

 -- 0 --L3      N -> T  -- 20:57:05 --

 Msg:  CALL PROC
 MsgHdr: 08 02 80 01 02
 CHID: 18 03 a9 83 82

 -- 0 --L3      N -> T  -- 20:57:05 --
 Msg:      ALERT
 MsgHdr: 08 02 80 01 01
 CHID: 18 03 a9 83 82

 -- 0 --L3      N -> T  -- 20:57:05 --
 Msg:    CONNECT
 MsgHdr: 08 02 80 01 07

 -- 0 --L3      T -> N  -- 20:57:05 -
 Msg:   CONN ACK
 MsgHdr: 08 02 00 01 0f
```

Figure 65: debug isdn q931 sample output

ISDN to SIP:

Note that gateway may send PROGRESS instead of ALERT depending on SIP messages.

```
-- 0 --L3      N -> T  -- 21:00:47 --
 Msg:      SETUP
 MsgHdr: 08 02 00 0a 05
 BC: 04 03 80 90 a2
 CHID: 18 03 a9 83 81
 PI: 1e 02 81 88
 CLNG: 6c 0c 21 80 34 30 38 37 35 34 31 37 34 37
 CLED: 70 07 a1 31 39 39 30 30 30

 -- 0 --L3      T -> N  -- 21:00:47 --
 Msg:  CALL PROC
 MsgHdr: 08 02 80 0a 02
 CHID: 18 03 a9 83 81

 -- 0 --L3      T -> N  -- 21:00:47 --
 Msg:      ALERT
 MsgHdr: 08 02 80 0a 01
 PI: 1e 02 80 81

-- 0 --L3      T -> N  -- 21:00:51 --

 Msg:    CONNECT
 MsgHdr: 08 02 80 0a 07
 CHID: 18 03 a1 83 81

 -- 0 --L3      N -> T  -- 21:00:51 --
 Msg:   CONN ACK
 MsgHdr: 08 02 00 0a 0f
```

Figure 66: debug isdn q931 sample output (continued)

Unable to make calls on T1 CAS

If you cannot make calls on a T1 CAS port, see the following sections for troubleshooting instructions.

Verify the T1 CAS configuration

If you cannot make calls on a T1 CAS port, make sure the T1 CAS configuration is correct. The following is a typical configuration:

```
config term
module t1 1/2
cas-group timeslots 1-24 em-wink-start
exit
voice-port 1/2
no shutdown
exit
```

Be sure to enter **`no shutdown`** under **`voice-port`**. (Note that ISDN ports are enabled by default.)

Comments? infodev@avaya.com

Also, make sure that the CAS protocol is the same on both ends of the link.

Verify that the CAS link is up

Make sure the CAS link is up. Use the **show module configuration all** command to check the state of the link for the CAS port.

```
SR# show module configuration all

T1 #      Framing   Coding    ClkSrc    LBO-CableLength   State     Alarm
-------------------------------------------------------------------------
1/2       esf       b8zs      NET       csu/0db           up        N/A
```

Figure 67: show module configuration all sample output

Perform call trace

For further CAS troubleshooting, you can also perform a call trace using the **debug voice cc cas** command. The following figures show a sample trace for a successful call using wink start.

```
SR# debug voice cc cas
MAR 10 2001 23:19:49:710:CAS [T1 1/2:--] rx rbs 000001 000001 000001 000001
MAR 10 2001 23:19:49:710:CAS [T1 1/2:00] Timer start event: CAS_WAIT_SEIZE_TIMER
MAR 10 2001 23:19:49:710-CAS [T1 1/2:00] state chg from: null to: call rcv ConnID:
unused
MAR 10 2001 23:19:49:800:CAS [T1 1/2:00] Timer event:CAS_WAIT_SEIZE_TIMER
MAR 10 2001 23:19:49:800:CAS [T1 1/2:00] Timer start event: CAS_WAIT_START_WINK_TIMER
MAR 10 2001 23:19:49:840:CAS [T1 1/2:00] Timer event:CAS_WAIT_START_WINK_TIMER
MAR 10 2001 23:19:49:840:CAS [T1 1/2:--] tx rbs 000001 000001 000001 000001
MAR 10 2001 23:19:49:840:CAS [T1 1/2:00] Timer start event: CAS_WAIT_SEND_WINK_TIMER
MAR 10 2001 23:19:50:050:CAS [T1 1/2:00] Timer event:CAS_WAIT_SEND_WINK_TIMER
MAR 10 2001 23:19:50:050:CAS [T1 1/2:--] tx rbs 000000 000000 000000 000000
MAR 10 2001 23:19:50:050:CAS [T1 1/2:00] Timer start event:
CAS_T1_END_OF_IN_DIALING_TIMER
MAR 10 2001 23:19:50:070:CAS [T1 1/2:00] Timer event:CAS_T1_END_OF_IN_DIALING_TIMER
MAR 10 2001 23:19:50:070:CAS [T1 1/2:00] Timer start event: CAS_WAIT_CONNECT_TIMER

(on answer from sip side)
ROOT/configure# MAR 10 2001 23:19:53:660:CAS [T1 1/2:00] Timer stop event:
CAS_WAIT_CONNECT_TIMER
MAR 10 2001 23:19:53:660:CAS [T1 1/2:--] tx rbs 000001 000001 000001 000001
MAR 10 2001 23:19:53:660:CAS [T1 1/2:00] Timer stop event: CAS_WAIT_DISC_TIMER
MAR 10 2001 23:19:53:660-CAS [T1 1/2:00] state chg from: call rcv to: ACTIVE ConnID:2
```

Figure 68: debug voice cc cas sample output

```
MAR 10 2001 23:28:00:800:CAS [T1 1/2:--] tx rbs 000002 000002 000002 000002
MAR 10 2001 23:28:00:800:CAS [T1 1/2:01] Timer start event: CAS_WINK_TIMEOUT_TIMER
MAR 10 2001 23:28:00:800-CAS [T1 1/2:01] state chg from: null to: wait rcv wink ConnID:3
MAR 10 2001 23:28:00:940:CAS [T1 1/2:--] rx rbs 000002 000002 000002 000002
MAR 10 2001 23:28:01:170:CAS [T1 1/2:--] rx rbs 000002 000002 000002 000002
MAR 10 2001 23:28:01:170:CAS [T1 1/2:01] Timer stop event: CAS_WINK_TIMEOUT_TIMER
MAR 10 2001 23:28:01:170:CAS [T1 1/2:01] Timer start event: CAS_INTER_DIGIT_TIMER
MAR 10 2001 23:28:01:170-CAS [T1 1/2:01] state chg from: wait rcv wink to: wait xmt
digit tone ConnID:3
MAR 10 2001 23:28:01:270:CAS [T1 1/2:01] Timer event:CAS_INTER_DIGIT_TIMER
MAR 10 2001 23:28:01:270:CAS [T1 1/2:01] Timer start event: CAS_INTER_DIGIT_TIMER
MAR 10 2001 23:28:01:690:CAS [T1 1/2:01] Timer event:CAS_INTER_DIGIT_TIMER
MAR 10 2001 23:28:01:690:CAS [T1 1/2:01] Timer start event: CAS_WAIT_CONNECT_TIMER
MAR 10 2001 23:28:01:690-CAS [T1 1/2:01] state chg from: wait xmt digit tone to: wait
remote connect ConnID:3
MAR 10 2001 23:28:01:890:CAS [T1 1/2:--] rx rbs 000002 000002 000002 000002
MAR 10 2001 23:28:01:890:CAS [T1 1/2:01] Timer stop event: CAS_WAIT_CONNECT_TIMER
MAR 10 2001 23:28:01:890:CAS [T1 1/2:01] Timer start event: CAS_WAIT_ANSWER_SIG_TIMER
MAR 10 2001 23:28:02:700:CAS [T1 1/2:01] Timer event:CAS_WAIT_ANSWER_SIG_TIMER
MAR 10 2001 23:28:02:700-CAS [T1 1/2:01] state chg from: wait remote connect to: ACTIVE
ConnID:3
```

Figure 69: debug voice cc cas sample output (continued)

FXS/FXO port status LEDs

The status LEDs on the front plate of the FXS/FXO cards can be used for debugging. If the LEDs are off, the card is not detected or is in hot swap shutdown mode. The following table describes how to interpret the other LED colors.

LED color	Description
Red	Not configured
Amber	Configured and idle

Comments? infodev@avaya.com

LED color	Description
Green	Busy; Call in Progress

No dial tone on the analog FXS phones or ports

The dial tone is only played on the FXS ports after the voice ports have been configured and enabled.

To display the status of the voice ports on the system, use the **show voice port summary** command.

```
SR/configure# show voice port summary

PORT   SIG-TYPE                  ADMIN OPER EC
====== ======================== ===== ==== ==
1/1    CAS wink-start            up    up   y
1/2    CAS wink-start            up    down y
2/1    FXS loop-start            up    up   y
2/3    FXS loop-start            up    up   y
SR/configure#
```

Figure 70: show voice port summary sample output

Unable to make FXS calls

If you are unable to make FXS calls, refer to the following sections for troubleshooting.

Verify that the port and dial peer are enabled

Make sure the port is not shut down using the **show voice port summary** command.

```
SR/configure# show voice port summary

PORT   SIG-TYPE                  ADMIN OPER EC
====== ======================== ===== ==== ==
1/1    CAS wink-start            up    up   y
1/2    CAS wink-start            up    down y
2/1    FXS loop-start            up    up   y
2/3    FXS loop-start            up    up   y
SR/configure#
```

Figure 71: show voice port summary sample output

Make sure the dial peer is configured with the appropriate destination pattern and is not shut down using the **show dial-peer voice summary** command.

```
SR# show dial-peer voice summary

                                                    PASS
TAG         TYPE ADMIN OPER PREFIX   DEST-PATTERN   THRU SESSION-TARGET/PORT
========== ==== ===== ==== ======== ============ ==== ====================
1           pots up    up           4087542006         1/1
2           pots up    up           4087542007         1/2
3           pots up    up           4087542008         1/3
4           pots up    up           4087542009         1/4
```

Figure 72: show dial-peer voice summary sample output

Verify that analog phones support DTMF

Make sure the analog phones support dual-tone multifrequency (DTMF). There is no support for pulse dialing in Release 10.1.

Perform call trace

For further FXS troubleshooting, you can perform a call trace using the **debug voice cc pots** command. The following figures show sample call traces of successful FXS calls: first from FXS to SIP, and then from SIP to FXS. The red text highlights the various steps of the call setup.

Comments? infodev@avaya.com

```
SR# debug voice cc pots

 POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=1 event=1
 POTS[    0]: slot=1 devNum=1 FXS:IDLE verify off-hook event
 POTS[-----]: event table = 0 category=1 event=1
 POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=9
 POTS[    0]: slot=1 devNum=1 FXS:IDLE valid off-hook event
 POTS[  868]: slot=1 devNum=-1 chanNum=1 Rcv Message msg=0 status=25
 POTS[  868]: call tcceSetupMedia
 POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
 POTS[-----]: slot=1 port=1
 POTS[  868]: slot=1 deviceNum=1 chanNum=0 category=2147483647 event=9
 POTS[  868]: slot=1 devNum=1 FXS:SETUP send dial tone event
 POTS[  868]: lssProcessTcceMsg:event=9 status=12
 POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 1
 POTS[  868]: fxs send create media response to TCCE
 POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
 POTS[-----]: slot=1 port=1
 POTS[  868]: slot=1 deviceNum=1 chanNum=0 category=2147483647 event=9
 POTS[  868]: lssProcessTcceMsg:event=9 status=18
 POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 15
 POTS[  868]: fxsPlaySignal signal=6
 POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
 POTS[-----]: slot=1 port=1
 POTS[  868]: slot=1 deviceNum=1 chanNum=0 category=2147483647 event=9
 POTS[  868]: slot=1 devNum=1 FXS:SETUP set SEND_RINGBACK sub state

 POTS[  868]: lssProcessTcceMsg:event=9 status=23
 POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 17

 SIP side Ringing, and goes off-hook

 POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 11
 POTS[  868]: fxsPlaySignal signal=7
 POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
 POTS[-----]: slot=1 port=1
 POTS[  868]: slot=1 deviceNum=1 chanNum=0 category=2147483647 event=9
 POTS[  868]: slot=1 devNum=1 FXS:SETUP batrev supervision config
 POTS[  868]: lssProcessTcceMsg:event=9 status=9
```

Figure 73: debug voice cc pots sample output

```
Call Connected, SIP side disconnects

POTS[  868]: fxsDisconnectMedia Log
POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 7
POTS[  868]:  TCCE_DISCONNECT_MEDIA_ACK
POTS[  868]: fxsPlaySignal signal=9
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=1 port=1
POTS[  868]: slot=1 deviceNum=1 chanNum=0 category=2147483647 event=9
POTS[  868]: slot=1 devNum=1 FXS:CONNECT terminate event
POTS[  868]: lssProcessTcceMsg:event=9 status=14
POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=16
POTS[    0]: slot=1 devNum=1 FXS:DISCONNECTING TM_SET_LCF
POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=15
POTS[    0]: slot=1 devNum=1 FXS:DISCONNECTING TM_SET_POWER_DENIAL
POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=18
POTS[    0]: slot=1 devNum=1 FXS:DISCONNECTING TM_GEN_APPLYTONE
POTS[  868]: slot=1 devNum=-1 chanNum=1 Rcv Message msg=9 status=11
POTS[  868]: LSS_SID_APPLYTONE cancelReason =200
POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 17

SIP Side Disconnected, FXS goes on-hook

POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=1 event=2
POTS[    0]: slot=1 devNum=1 FXS:DISCONNECTING verify on-hook event
POTS[-----]: event table = 0 category=1 event=2
POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=8
POTS[  868]: slot=1 devNum=-1 chanNum=1 Rcv Message msg=4 status=10
POTS[  868]: fxsPlaySignal signal=10
POTS[    0]: slot=1 devNum=1 FXS:DISCONNECTING  event
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=1 port=1
POTS[  868]: slot=1 deviceNum=1 chanNum=0 category=2147483647 event=7
POTS[  868]: slot=1 devNum=1 FXS:DISCONNECTING LSSRlsRq(LSSRlsCompInd)
POTS[  868]: lssProcessTcceMsg:event=7 status=0
POTS[  868]: slot=1 devNum=-1 chanNum=1 Rcv Message msg=2 status=25
POTS[  868]: fxsDestroyMedia Log
POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 13
```

Figure 74: debug voice cc pots sample output (continued)

Comments? infodev@avaya.com

```
FXS Incoming call from SIP, call terminated by FXS

SIP side calls FXS

POTS[  868]: fxsCreateMedia Log mType=5
POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 1
POTS[  868]: fxs send create media response to TCCE
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=1 port=1
POTS[  868]: slot=1 deviceNum=1 chanNum=0 category=2147483647 event=9
POTS[  868]: lssProcessTcceMsg:event=9 status=18
POTS[  868]: fxsPlaySignal signal=1
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=1 port=1
POTS[  868]: slot=1 deviceNum=1 chanNum=0 category=2147483647 event=6
POTS[  868]: slot=1 devNum=1 FXS:IDLE  ringindex:4
POTS[-----]: genTmEvent:352 slot=0 devNum=0 chNum=0 index=0
POTS[-----]: RDuration=2000: 2000 4000 0 0
POTS[  868]: slot=1 devNum=1 FXS:IDLE LSSSetupRq
POTS[  868]: lssProcessTcceMsg:event=6 status=0
POTS[  868]: slot=1 devNum=-1 chanNum=1 Rcv Message msg=9 status=0
POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 11
POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=0
POTS[-----]: genTmEvent:352 slot=0 devNum=0 chNum=0 index=1
POTS[-----]: RDuration=4000: 2000 4000 0 0

POTS[    0]: slot=1 devNum=1 FXS:SETUP TM_START_RINGING sendcallId=0 callertype1=0 current=1
caller=1

POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=1
POTS[    0]: slot=1 devNum=1 FXS:SETUP STOP RINGBACK
POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=0
POTS[-----]: genTmEvent:352 slot=0 devNum=0 chNum=0 index=0
POTS[-----]: RDuration=2000: 2000 4000 0 0
POTS[    0]: slot=1 devNum=1 FXS:SETUP TM_START_RINGING sendcallId=0 callertype1=0 current=1
caller=1
```

Figure 75: debug voice cc pots sample output (continued)

```
FXS Ringing and goes off-hook


POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=1 event=1
POTS[  868]: slot=1 devNum=-1 chanNum=1 Rcv Message msg=1 status=5
POTS[    0]: slot=1 devNum=1 sendCallId=0
POTS[    0]: slot=1 devNum=1 FXS:SETUP off-hook event
POTS[-----]: event table = 0 category=1 event=1

Call is connected, FXS goes on-hook

POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=1 event=2
POTS[-----]: disableOnHook
POTS[    0]: slot=1 devNum=1 FXS:CONNECT verify on-hook event
POTS[-----]: event table = 0 category=1 event=2
POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=11
POTS[    0]: slot=1 deviceNum=1 chanNum=0 category=7777 event=8
POTS[    0]: slot=1 devNum=1 FXS:CONNECT on-hook event
POTS[  868]: slot=1 devNum=-1 chanNum=1 Rcv Message msg=4 status=9
POTS[  868]: fxsDisconnectMedia Log
POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 7
POTS[  868]:  TCCE_DISCONNECT_MEDIA_ACK
POTS[  868]: fxsPlaySignal signal=10
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=1 port=1
POTS[  868]: slot=1 deviceNum=1 chanNum=0 category=2147483647 event=7
POTS[  868]: slot=1 devNum=1 FXS:DISCONNECTING LSSRlsRq(LSSRlsCompInd)
POTS[  868]: lssProcessTcceMsg:event=7 status=0
POTS[  868]: slot=1 devNum=-1 chanNum=1 Rcv Message msg=2 status=25
POTS[  868]: fxsDestroyMedia Log
POTS[  868]: slot=1 devNum=-1 chanNum=1 fxs Media response is 13
```

Figure 76: debug voice cc pots sample output (continued)

FXS phones are not registered (Sylantro and BroadSoft only)

With Sylantro and BroadSoft SIP servers, if no calls can be completed, the FXS phones might not be registered. To troubleshoot this issue, refer to the following sections.

Verify SIP registrar configuration

You can verify whether the SIP registrar is configured using the **`show sip-ua status`** command.

Comments? infodev@avaya.com

```
SR# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : DISABLED
SIP User Agent bind status(signaling): ENABLED
SIP max-forwards : 70
SIP server : ipv4:47.100.107.46:5060
Registrar server :
Authentication username : n/a
Authentication password : n/a
 SDP application configuration:
 Version line (v=) required
 Session name line (s=) required
 Timespec line (t=) required
 Network types supported: IN
 Address types supported: ipv4
 Transport types supported: RTP/AVP UDP
SR#
```

Figure 77: show sip-ua status sample output

If the registrar is not configured, then configure it using the **sip-ua registar** command. For example:

```
SR/configure# sip-ua registrar ipv4:47.100.107.46 expires 3600
```

Verify that registration is configured on the dial peer

If FXS phones are still not registered, then verify whether registration is enabled for the dial-peer corresponding to the FXS port using the **show dial-peer voice** command. The following figure shows the sample output for voice dial peer 3 that corresponds to the FXS phone.

```
SR/configure# show dial-peer voice 3

description : n/a
tag = 3, destination pattern : 3087771001
Admin state : Enabled, Operation state : Enabled
type : pots
prefix : n/a
port : 2/1
digit-strip : Disabled
trunkgroup : n/a
forward-digits : none
Register E.164 number : Disabled
clid : n/a
Translation Profile :
   Incoming : n/a
   Outgoing : n/a

Dial-Peer Statistics:

Successful calls  : 0
Failed calls: 0
Accepted calls: 0
Refused calls: 0
Connect Time : 0
Last Disconnect Reason : ""
SR/configure#
```

Figure 78: show dial-peer voice sample output

If the registration is not enabled, enter the following commands to enable the registration:

```
SR/configure# dial-peer voice pots 3 SR/configure/dial-peer-voice-pots 3# authentication 3087771001 3087771001 SR/configure/dial-peer-voice-pots 3# register e164
```

Note that the username and password specified in the **authentication** command must match to the username and password configured on the registrar.

To verify the FXS registration status, use the **show sip-ua register status** command.

```
SR# show sip-ua register status

Line      peer                          expires(sec)  registered
0         3087771001                    3600          yes
SR#
```

Figure 79: show sip-ua register status sample output

Ping

If the FXS phones are still not able to register, then verify whether the configured registrar can be reached from the Secure Router 2330/4134 using the **ping** command.

Comments? infodev@avaya.com

Unable to make FXO calls

If you are unable to make FXO calls, refer to the following sections for troubleshooting.

Verify that the port and dial peer are enabled

Make sure the port is not shut down using the **show voice port summary** command.

```
SR# show voice port summary

PORT    SIG-TYPE                  ADMIN OPER EC
======  ========================  ===== ==== ==
4/1:23  PRI primary-ni2           up    up   y
4/2     CAS wink-start            up    up   y
1/2     FXO loop-start            up    up   y
2/1     FXS loop-start            up    up   y
2/2     FXS loop-start            up    up   y
```

Figure 80: show voice port summary sample output

Make sure the dial peer is configured with the appropriate destination pattern and is not shut down using the **show dial-peer voice summary** command

```
SR# show dial-peer voice summary

                                                    PASS
TAG         TYPE ADMIN OPER PREFIX   DEST-PATTERN   THRU SESSION-TARGET/PORT
==========  ==== ===== ==== ======== ============== ==== ====================
1           pots up    up            4087542006          1/1
2           pots up    up            4087542007          1/2
3           pots up    up            4087542008          1/3
4           pots up    up            4087542009          1/4
```

Figure 81: show dial-peer voice summary sample output

Verify DTMF dialing on the FXO link

Pulse dialing not supported in this release. Make sure to use DTMF dialing on the FXO link.

Verify that PLAR is configured

Connection PLAR must be configured for FXO calls. Verify that it is configured using the **show voice port** command.

```
SR# show voice port 1/2

Type of VoicePort : FXO
Operation state : UP
Administrative State : UP
Description : n/a
In Gain : 0
Output Attenuation : 0
Echo Cancellation : enabled
Echo Cancel coverage : 64
Comfort noise : disabled
Compand type : G711 U-Law
Trunk group : n/a
Analog Info Follows
Region Tone : us
Voice Card Specific Info Follows
Ring number : 2
Connection plar : 96083000
ANI mapping table:
not configured
Signal Type : FXO loop-start
Battery Reversal : enabled (no answer)
Caller-id Enable : Disabled
Caller-id Block : disabled
Caller-id Alerting Ring : disabled
Interdigit Duration Timing : 10
Station Name : n/a
Station Number : 4444003
```

Figure 82: show voice port sample output

Perform call trace

For further FXO troubleshooting, you can perform a call trace using the **debug voice cc pots** command. The following figures show sample call traces of successful FXO calls.

Comments? infodev@avaya.com

FXO loop start incoming call

```
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=12
POTS[-----]: slot=12 port=0 data=0
POTS[-----]: slot=12 port=0 wdata=0 inputdata=0
POTS[    0]: slot=13 devNum=1 FXO:IDLE ringing ON event // First ring on
POTS[-----]: event table = 0 category=2147483647 event=12
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=0 status=25
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 1
POTS[ 1860]: fxo send create media response
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=13 // Ring off event
POTS[-----]: event table = 0 category=2147483647 event=13

POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=12
POTS[    0]: slot=13 devNum=1 FXO:IDLE ringing ON event // 2nd Ring on event
POTS[-----]: event table = 0 category=2147483647 event=12
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=9 status=5
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 11
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=7
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=9
POTS[ 1860]: slot=13 devNum=1 FXO:SETUP T:CONNECT event // FXO is connected after 2nd ring-on event
POTS[ 1860]: lssProcessTcceMsg:event=9 status=9
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=13
POTS[-----]: event table = 0 category=2147483647 event=13

POTS[ 1860]: fxoDisconnectMediaLog
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 7
POTS[ 1860]:  fxo send disconnect media response
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=9
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=7
POTS[ 1860]: slot=13 devNum=1 FXO/CAMA:CONNECT LSSRlsRq state=0
POTS[ 1860]: lssProcessTcceMsg:event=7 status=0
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=2 status=25
POTS[ 1860]: fxoDestroyMedia Log
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 13
POTS[ 1860]:  fxo send destroy media response
```

Figure 83: debug voice cc pots sample output

```
FXO loop start outgoing call

POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=25455700
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 1
POTS[ 1860]: fxo send create media response
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=1
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1 // Slot/port information
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=6
POTS[-----]: slot=12 port=0 data=0
POTS[-----]: slot=12 port=0 wdata=0 inputdata=0
POTS[ 1860]: slot=13 devNum=1 FXO:IDLE LSSSetupRq
POTS[ 1860]: lssProcessTcceMsg:event=6 status=0
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=3 status=1
POTS[ 1860]: called Number 4087544000 // Digits to be dialed on outgoing FXO

POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 27
POTS[ 1860]:  TCCE_OVERLAPSEND_MEDIA_ACK
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=9
POTS[ 1860]: slot=13 devNum=1 FXO:SETUP gd on tip or T:CONNECT event // Connect from FXO peer
POTS[ 1860]: lssProcessTcceMsg:event=9 status=8
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=9 status=9
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 11

POTS[ 1860]: fxoDisconnectMediaLog // Disconnect initiated by FXO
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 7
POTS[ 1860]:  fxo send disconnect media response
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=9
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=7
POTS[ 1860]: slot=13 devNum=1 FXO/CAMA:CONNECT LSSRlsRq state=0
POTS[ 1860]: lssProcessTcceMsg:event=7 status=0
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=2 status=25
POTS[ 1860]: fxoDestroyMedia Log
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 13
POTS[ 1860]:  fxo send destroy media response
```

Figure 84: debug voice cc pots sample output (continued)

Comments? infodev@avaya.com

FXO ground start incoming call
Note: For ground start straight cable is must

```
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=12
POTS[-----]: slot=12 port=0 data=0
POTS[-----]: slot=12 port=0 wdata=0 inputdata=0
POTS[    0]: slot=13 devNum=1 FXO:IDLE ringing ON event // 1st ring-on event
POTS[-----]: event table = 0 category=2147483647 event=12
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=0 status=25
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 1
POTS[ 1860]: fxo send create media response
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=13
POTS[-----]: event table = 0 category=2147483647 event=13 // 1st ring off-event


POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=12
POTS[    0]: slot=13 devNum=1 FXO:IDLE ringing ON event // 2nd ring-on event, fxo goes to connect
POTS[-----]: event table = 0 category=2147483647 event=12
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=9 status=5
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 11
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=7
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=9
POTS[ 1860]: slot=13 devNum=1 FXO:SETUP T:CONNECT event // connect from remote
POTS[ 1860]: lssProcessTcceMsg:event=9 status=9
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=13
POTS[-----]: event table = 0 category=2147483647 event=13


POTS[ 1860]: fxoDisconnectMediaLog // call disconnect
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 7
POTS[ 1860]:  fxo send disconnect media response
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=9
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=7
POTS[ 1860]: slot=13 devNum=1 FXO/CAMA:CONNECT LSSRlsRq state=0
POTS[ 1860]: lssProcessTcceMsg:event=7 status=0
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=2 status=25
POTS[ 1860]: fxoDestroyMedia Log
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 13
POTS[ 1860]:  fxo send destroy media response
```

Figure 85: debug voice cc pots sample output (continued)

```
FXO ground start outgoing call
Note: For ground start straight cable is must

POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=25455700
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 1
POTS[ 1860]: fxo send create media response
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=1
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=6
POTS[-----]: Enable =ee fxobase=d5018000
POTS[ 1860]: slot=13 devNum=1 FXO:IDLE set VP_LINE_FXO_RING_GND // Ring ground event
POTS[-----]: slot=12 port=0 data=c0
POTS[-----]: slot=12 port=0 wdata=c0 inputdata=c0
POTS[ 1860]: slot=13 devNum=1 FXO:IDLE LSSSetupRq
POTS[ 1860]: lssProcessTcceMsg:event=6 status=0
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=5 event=16
POTS[-----]: event table = 0 category=5 event=16
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=11
POTS[-----]: Disable =ff fxobase=1
POTS[    0]: slot=13 devNum=1 FXO:SETUP gd on tip // Tip ground event
POTS[-----]: event table = 0 category=2147483647 event=11
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=5 event=128
POTS[    0]: slot=13 devNum=1  FXO:SETUP L: invalid on-hook event
POTS[-----]: event table = 0 category=5 event=128
POTS[    0]: slot=13 deviceNum=1 chanNum=0 category=7777 event=14
POTS[    0]: slot=13 devNum=1  FXO:SETUP TM_SEND_RQRSP event
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=3 status=1
POTS[ 1860]: called Number 4087544000 // Digits to be dialed
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 27
POTS[ 1860]:  TCCE_OVERLAPSEND_MEDIA_ACK
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=9
POTS[ 1860]: slot=13 devNum=1 FXO:SETUP gd on tip or T:CONNECT event // Connect event
POTS[ 1860]: lssProcessTcceMsg:event=9 status=8
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=9 status=9
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 11

POTS[ 1860]: fxoDisconnectMediaLog // Media disconnect
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 7
POTS[ 1860]:  fxo send disconnect media response
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 signal=9
POTS[-----]: LSS MSG EVENT COMMING FROM TCCE
POTS[-----]: slot=7 subslot=1 port=1
POTS[ 1860]: slot=13 deviceNum=1 chanNum=0 category=2147483647 event=7
POTS[ 1860]: slot=13 devNum=1 FXO/CAMA:CONNECT LSSRlsRq state=0 // Call disconnect
POTS[ 1860]: lssProcessTcceMsg:event=7 status=0
POTS[ 1860]: slot=7 devNum=1 chanNum=1 Rcv Message msg=2 status=25
POTS[ 1860]: fxoDestroyMedia Log
POTS[ 1860]:  slot=7 devNum=1 chanNum=1 fxo Media response is 13
POTS[ 1860]:  fxo send destroy media response
```

Figure 86: debug voice cc pots sample output (continued)

Secure Router 2330/4134 not reachable from SIP Server

All Secure Router 2330/4134 call routing is performed by the central SIP Server. In cases where no calls can be completed, the Secure Router 2330/4134 may not be reachable from

Comments? infodev@avaya.com

the SIP Server. Use the **ping** command to verify that the SIP server can communicate with the Secure Router 2330/4134 SIP gateway.

Also, if the Secure Router 2330/4134 SIP Media Gateway is configured with FQDN, then verify whether the FQDN can be resolved. Be sure that the DNS server is specified using the **ip pname_server** command. Ensure that the DNS server is reachable.

There are several other potential reasons for call failures. You can debug many of these issues with information provided by routing traces.

To enable routing traces, enter the **debug voice cc routing** command.

Digit stripping enabled or digit forwarding disabled

To successfully terminate a call to a POTS dial peer, digit stripping must be disabled or digit forwarding must be enabled.

The following figure shows a sample output for the **debug voice cc routing** command. The output shows that, after the Secure Router 2330/4134 applies digit processing, there is no destination number for the call. In this case, the dial peer corresponding to the dialed number might have digit stripping enabled and digit forwarding disabled.

```
SR# debug voice cc routing
ROUTING[-----]: The destination number is 3087771001, lineId = -1
ROUTING[-----]: Call Limit is 128, active calls = 0
ROUTING[-----]: Outgoing DP found with tag = 3!!!
ROUTING[-----]: ERROR: No destination after digit processing
SR#
```

Figure 87: debug voice cc routing sample output

To display the dial peer configuration, enter **show dial-peer voice**.

The following figure shows a sample output for dial peer 3.

```
SR# show dial-peer voice 3

description : n/a
tag = 3, destination pattern : 3087771001
Admin state : Enabled, Operation state : Enabled
type : pots
prefix : n/a
port : 2/1
digit-strip : Enabled
trunkgroup : n/a
forward-digits : none
Register E.164 number : Enabled
clid : n/a
Translation Profile :
   Incoming : n/a
   Outgoing : n/a

Dial-Peer Statistics:

Successful calls  : 0
Failed calls: 9
Accepted calls: 31
Refused calls: 3
Connect Time : 0
Last Disconnect Reason : Not acceptable
SR#
```

Figure 88: show dial-peer voice sample output

The dial peer configuration shows that digit stripping is enabled and forward digits is disabled. As a solution, you must disable digit stripping or enable forward-digits all.

Dialed number not configured

If the dialed number is not configured on the Secure Router 2330/4134, the call cannot be completed.

The following figure shows a sample output for the **debug voice cc routing** command in which the dialed destination number is not found.

```
SR# debug voice cc routing
ROUTING[-----]: The destination number is 3087771004, lineId = -1
ROUTING[-----]: Call Limit is 128, active calls = 0
ROUTING[-----]: ERROR: Destination not found return CC Usr Not Found
ROUTING[-----]: TCCE finds line id = -1
ROUTING[-----]: Returning CC 404
SR#
```

Figure 89: debug voice cc routing sample output

To troubleshoot this issue, display all the configured dial peers in the Secure Router 2330/4134 using the **show dial-peer voice summary** command:

Comments? infodev@avaya.com

```
SR# show dial-peer voice summary

                                                    PASS
TAG         TYPE ADMIN OPER PREFIX   DEST-PATTERN  THRU SESSION-TARGET/PORT
========== ==== ===== ==== ======== ============ ==== ====================
3           pots up    up           3087771001        2/1
4           pots up    up           3087771002        2/2
6           pots up    up           4444000           1/2
5           pots up    up           4444001           1/1
1           pots up    up           50820000          4/1:23
11          pots up    up           5082.%            4/1:23
2           pots up    up           6083.%            4/2
10          pots up    up           8085552000        4/1:23
SR#
```

Figure 90: show dial-peer voice summary sample output

The display confirms that there are no dial peers configured with the dialed destination pattern of 3087771004.

If the number is expected to be handled by Secure Router 2330/4134, then you must configure a dial peer with a destination pattern of 3087771004.

Dialed number is busy

The following figure shows a sample output for the **`debug voice cc routing`** command in which the **`Returning CC 486`** message indicates that the dialed destination number is busy.

```
SR# debug voice cc routing
ROUTING[-----]: The destination number is 3087771002, lineId = -1
ROUTING[-----]: Call Limit is 128, active calls = 2
ROUTING[-----]: Outgoing DP found with tag = 4!!!
ROUTING[-----]: Destination is Port
ROUTING[-----]: Port Id = 33
ROUTING[-----]: Line id = -1, Go for channel hunt
ROUTING[-----]: ERROR: Channel not available: return
CAUSE_CODE_SERVICE_NOT_AVAIL OR BUSY
ROUTING[-----]: TCCE finds line id = -1
ROUTING[-----]: Returning CC 486
SR#
```

Figure 91: debug voice cc routing sample output

To display the active calls on the Secure Router 2330/4134, enter the **`show sip-ua calls`** command.

```
SR# show sip-ua calls

SIP UAC CALL INFO

Call 1
State of the call : ACTIVE
Calling Number : 3087771001
Called Number : 3087771002
Source IP Address (Sig ): 47.100.107.46
Destination Name :
Number of Media Streams : 1
Media Stream
Negotiated Codec : PCMU Bytes: 160
Codec Payload Type : 0
Media Source IP Addr:Port: 47.100.107.65:28000
Media Dest IP Addr:Port : 47.100.107.65:28002

Call 2
State of the call : ACTIVE
Calling Number : 1001
Called Number : 3087771002
Source IP Address (Sig ): sylantro.nortel.com
Destination Name :
Number of Media Streams : 1
Media Stream
Negotiated Codec : PCMU Bytes: 160
Codec Payload Type : 0
Media Source IP Addr:Port: 47.100.107.65:28002
Media Dest IP Addr:Port : 47.100.107.65:28000
SR#
```

Figure 92: show sip-ua calls sample output

The output confirms that an existing call is in progress on the destination.

ISDN PRI link down

The following figure shows a sample output for the **debug voice cc routing** command in which the **Returning CC 503** message indicates that a PRI T1 link is down.

```
SR# debug voice cc routing
ROUTING[-----]: The destination number is 5082000, lineId = -1
ROUTING[-----]: Call Limit is 128, active calls = 0
ROUTING[-----]: Outgoing DP found with tag = 11!!!
ROUTING[-----]: Destination is Port
ROUTING[-----]: Port Id = 24
ROUTING[-----]: Line id = -1, Go for channel hunt
ROUTING[-----]: ERROR: Channel not available: return
CAUSE_CODE_SERVICE_NOT_AVAIL OR BUSY
ROUTING[-----]: TCCE finds line id = -1
ROUTING[-----]: Returning CC 503
SR#
```

Figure 93: debug voice cc routing sample output

To display the T1 module status, enter the **show module configuration t1** command. The following figure shows that alarms have been detected on the module.

Comments? infodev@avaya.com

```
SR# show module configuration t1 4/1
T1 4/1 is ENABLED
Alarm Hierarchy: TRUE,
Yellow Alarm: GENERATE & DETECT
Framing:ESF, LineCode:B8ZS, ClockSource: NET, LineMode:CSU, LBO:0 db
FDL: ANSI Unit Protocol enabled ,ATT Unit Protocol disabled ,
CsuDsuType:  CSU , Loopback Framing (In-band): Overwrite,
CIRCUIT-ID : Not Configured ,CONTACT-INFO : Not Configured ,
DESCRIPTION : Not Configured , LINK NAME : Not Configured ,

Line Status:
   RLOS: ON,    RAIS:OFF,    RLOF:OFF,    RRAI:OFF,    TAIS:OFF
   TRAI: ON,     TPtrn:OFF,    Loop:OFF

Timeslot Map:
  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
 ___________________________________________________________________________
|0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |
|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|
```

Figure 94: show module configuration sample output

Alternatively, you can also enter the **show module configuration all** command.

```
SR# show module configuration all
T1 #      Framing   Coding    ClkSrc    LBO-CableLength   State     Alarm
-------------------------------------------------------------------------
4/1       esf       b8zs      NET       csu/0db           down      RLOS
4/2       esf       b8zs      NET       csu/0db           up        N/A
```

Figure 95: show module configuration all sample output

To display the ISDN PRI D channel status, enter the **show interface bundle** command. The following figure shows that the PRI bundle is down.

```
SR# show interface bundle pri1

bundle pri1
-----------
status                              down
number of links                     1
voice-port info                     4/1:23
switch-type                         primary-ni2
side                                USR

counters for 4/1:23 since last boot/clear
    Bytes Rx                    52727    Bytes Tx
53082
    Packets Rx                  13174    Packets Tx
13259
    All Err Pkt Rx                  0    All Err Pkt Tx
0
    Pkt 2 Long Rx                   0    Failed Pkt Tx
0
    Overrun Rx                      0    Underrun Tx
0
    Pkt CRC Err Rx                  0
    Pkt Inv Len Rx                  0
    Abort Rx                        0
```

Figure 96: show interface bundle sample output

You can also display the voice port status by entering the **show voice port** command. The following figure shows the operation state of the port as dormant.

```
SR# show voice port 4/1:23

Type of VoicePort : PRI
Operation state : DORMANT
Administrative State : UP
Description : n/a
In Gain : 0
Output Attenuation : 0
Echo Cancellation : enabled
Echo Cancel coverage : 64
Comfort noise : disabled
Compand type : G711 U-Law
Trunk group : n/a
Analog Info Follows
Region Tone : us
Voice Card Specific Info Follows
Timeslots : 1-23
Switch Type : PRI primary-ni2
SR#
```

Figure 97: show voice port sample output

To troubleshoot the issue, make sure that the T1 PRI cables are connected correctly. Also, verify the D channel and link status from the PBX side. Also, see Unable to make calls on T1 PRI on page 325 for further troubleshooting instructions.

T1 CAS link down

The following figure shows a sample output for the **debug voice cc routing** command which the **Returning CC 503** message indicates that the T1 CAS link is down.

```
SR# debug voice cc routing
ROUTING[-----]: The destination number is 6083000, lineId = -1
ROUTING[-----]: Call Limit is 128, active calls = 0
ROUTING[-----]: Outgoing DP found with tag = 2!!!
ROUTING[-----]: Destination is Port
ROUTING[-----]: Port Id = 25
ROUTING[-----]: Line id = -1, Go for channel hunt
ROUTING[-----]: ERROR: Channel not available: return
CAUSE_CODE_SERVICE_NOT_AVAIL OR BUSY
ROUTING[-----]: TCCE finds line id = -1
ROUTING[-----]: Returning CC 503
SR#
```

Figure 98: debug voice cc routing sample output

To display the T1 CAS status, enter the **show module configuration t1** command. The following figure shows that alarms have been detected on the module.

```
SR# show module configuration t1 4/2
T1 4/2 is ENABLED
Alarm Hierarchy: TRUE,
Yellow Alarm: GENERATE & DETECT
Framing:ESF, LineCode:B8ZS, ClockSource: NET, LineMode:CSU, LBO:0 db
FDL: ANSI Unit Protocol enabled ,ATT Unit Protocol disabled ,
CsuDsuType:  CSU , Loopback Framing (In-band): Overwrite,
CIRCUIT-ID : Not Configured ,CONTACT-INFO : Not Configured ,
DESCRIPTION : Not Configured , LINK NAME : Not Configured ,

Line Status:
   RLOS: ON,    RAIS:OFF,    RLOF:OFF,    RRAI:OFF,    TAIS:OFF
   TRAI: ON,   TPtrn:OFF,    Loop:OFF

Timeslot Map:
  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
 _____________________________________________________________________
|0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |
|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|
```

Figure 99: show module configuration sample output

To display the voice port status, enter the **show voice port** command. The following figure shows the operation state of the port as dormant.

```
SR# show voice port 4/2
Type of VoicePort : CAS
Operation state : DORMANT
Administrative State : UP
Description : n/a
In Gain : 0
Output Attenuation : 0
Echo Cancellation : enabled
Echo Cancel coverage : 64
Comfort noise : disabled
Compand type : G711 U-Law
Trunk group : n/a
Analog Info Follows
Region Tone : us
Voice Card Specific Info Follows
Interdigit Duration Timing : 3
Station Name : n/a
Station Number : n/a
Initial timeout : 10
Timeslots : 1-24
Signal Type : CAS wink-start
SR#
```

Figure 100: show voice port sample output

To troubleshoot the issue, make sure the CAS interface cables are connected correctly. Also, see Unable to make calls on T1 CAS on page 330for further troubleshooting instructions.

Unable to make outbound calls to SIP endpoints

In cases where no SIP calls can be completed, the SIP server may not be reachable from the Secure Router 2330/4134. Use the **ping** command to verify that the Secure Router 2330/4134 Media Gateway can communicate with the SIP server.

Also, if the SIP server is configured with FQDN, then verify whether the FQDN can be resolved. Be sure that the DNS server is specified on the Secure Router 2330/4134 using the **ip pname_server** command.

There are several other potential sources of call failures. You can debug many of these issues with information provided by routing traces.

To enable routing traces, enter the **debug voice cc routing** command

Neither SIP server nor VoIP dial peer are configured

If neither the SIP server or VoIP dial peer are configured on the Secure Router 2330/4134, then no calls can be routed to the SIP network.

Comments? infodev@avaya.com

The SIP server address can be configured on the Secure Router 2330/4134 using two methods:

- globally using the **sip-server** command under **voice service voip**
- for a particular destination pattern by configuring a VoIP Dial peer

You can verify whether the SIP server is configured using the **show sip-ua status** command.

```
SR# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : DISABLED
SIP User Agent bind status(signaling): ENABLED
SIP max-forwards : 70
SIP server :
Registrar server : ipv4:47.100.107.46 expires 3600
Authentication username : n/a
Authentication password : n/a
 SDP application configuration:
 Version line (v=) required
 Session name line (s=) required
 Timespec line (t=) required
 Network types supported: IN
 Address types supported: ipv4
 Transport types supported: RTP/AVP UDP
SR#
```

Figure 101: show sip-ua status sample output

In this case, no SIP server is configured.

You can also verify whether any VoIP dial peers are configured using the **show dial-peer voice summary** command

```
SR# show dial-peer voice summary

                                                    PASS
TAG         TYPE ADMIN OPER PREFIX   DEST-PATTERN   THRU SESSION-TARGET/PORT
========== ==== ===== ==== ======== ============ ==== ==================
3           pots up    up            3087771001        2/1
4           pots up    up            3087771002        2/2
6           pots up    up            4444000           1/2
5           pots up    up            4444001           1/1
1           pots up    up            50820000          4/1:23
11          pots up    up            5082.%            4/1:23
2           pots up    up            6083.%            4/2
10          pots up    up            8085552000        4/1:23
SR#
```

Figure 102: show dial-peer voice summary sample output

In this case, no VoIP dial peer is configured.

To fix the problem, configure either the SIP server or a VoIP dial peer.

You can configure the SIP server globally by entering the following commands

```
config term
sip-ua sip-server ipv4:47.100.107.46:5060
exit
```

Alternatively, you can configure a VoIP dial peer by entering the following commands

```
config term
dial-peer voice voip 100
session target ipv4:47.100.107.46:5060

destination-pattern 408.%T
no shutdown
exit
exit
```

Codec mismatch

To troubleshoot a potential codec mismatch, enable SIP debugging using the **debug ccsip message** command.

Comments? infodev@avaya.com

```
SR# debug ccsip message

 [TCCE-TRACE]:1204055450.900 Msg-IN            Call-IN           SIP
Interface                     SIP Messa
ge PDU
INVITE sip:3087771001@47.100.107.65:5060 SIP/2.0
From: "phone1,polycom" <sip:3087771003@sylantro.nortel.com>;tag=64ffaa18-
1dd2-11b2-89b2-b03162323164+6509c5
e8
To: <sip:3087771001@sylantro.nortel.com>
Call-ID: 1329018-12778397 2@47.100.107.46
CSeq: 1 INVITE
Max-Forwards: 67
Allow: INVITE,BYE,ACK,CANCEL,PRACK,REFER,OPTIONS,REGISTER,NOTIFY
Content-Type: application/sdp
Supported: 100rel,timer
Min-SE: 1800
P-Asserted-Identity:  "phone1,polycom" <sip:1003@sylantro.nortel.com>
Via: SIP/2.0/UDP
47.100.107.46:5060;branch=z9hG4bK3de1edc97f17c319b0efe614bdab7b4c.1,SIP/2.0/U
DP 47.100.107
.46:5075;branch=z9hG4bK1321634306362724
Contact: <sip:3087771003@47.100.107.46:5075;transport=udp>
Content-Length: 251

v=0
o=- 1489631476 1489631476 IN IP4 47.100.107.46
s=Polycom IP Phone
c=IN IP4 47.100.107.66
t=0 0
m=audio 2228 RTP/AVP 0 8 18 101
a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/80
[TCCE-TRACE]:1204055450.910 Msg-OUT           Call-IN           SIP Interface
SIP Messa
ge PDU
SIP/2.0 100 Trying
Via: SIP/2.0/UDP
47.100.107.46:5060;branch=z9hG4bK3de1edc97f17c319b0efe614bdab7b4c.1,SIP/2.0/U
DP 47.100.107
.46:5075;branch=z9hG4bK1321634306362724
From: "phone1,polycom"<sip:3087771003@sylantro.nortel.com>;tag=64ffaa18-1dd2-
11b2-89b2-b03162323164+6509c5e
8
To: <sip:3087771001@sylantro.nortel.com>;tag=SR4134_3785172608-460
Call-ID: 1329018-12778397 2@47.100.107.46
CSeq: 1 INVITE
Supported: timer
Contact: <sip:3087771001@47.100.107.65:5060;transport=udp>
Content-Length: 0
```

Figure 103: debug ccsip message sample output

```
[TCCE-TRACE]:1204055450.930 Msg-OUT          Call-IN          SIP Interface
SIP Messa
ge PDU
SIP/2.0 488 Not Acceptable Here
Via: SIP/2.0/UDP
47.100.107.46:5060;branch=z9hG4bK3de1edc97f17c319b0efe614bdab7b4c.1,SIP/2.0/U
DP 47.100.107
.46:5075;branch=z9hG4bK1321634306362724
From: "phone1,polycom"<sip:3087771003@sylantro.nortel.com>;tag=64ffaa18-1dd2-
11b2-89b2-b03162323164+6509c5e
8
To: <sip:3087771001@sylantro.nortel.com>;tag=SR4134_3785172608-460
Call-ID: 1329018-12778397 2@47.100.107.46
CSeq: 1 INVITE
Supported: timer
Contact: <sip:3087771001@47.100.107.65:5060;transport=udp>
Content-Length: 0


[TCCE-TRACE]:1204055450.940 Msg-IN           Call-IN          SIP Interface
SIP Messa
ge PDU
ACK sip:3087771001@47.100.107.65:5060 SIP/2.0
From: "phone1,polycom" <sip:3087771003@sylantro.nortel.com>;tag=64ffaa18-
1dd2-11b2-89b2-b03162323164+6509c5
e8
To: <sip:3087771001@sylantro.nortel.com>;tag=SR4134_3785172608-460
Call-ID: 1329018-12778397 2@47.100.107.46
CSeq: 1 ACK
Max-Forwards: 69
Via: SIP/2.0/UDP
47.100.107.46:5060;branch=z9hG4bK3de1edc97f17c319b0efe614bdab7b4c.1,SIP/2.0/U
DP 47.100.107
.46:5075;branch=z9hG4bK1321634306362724
Content-Length: 0
```

Figure 104: debug ccsip message sample output (continued)

In the preceding figures, the codecs offered in the INVITE message are not configured on the Secure Router 2330/4134, and the call is therefore rejected.

Verify the configured codec by entering the **`show voice service voip`** command.

Comments? infodev@avaya.com

```
SR# show voice service voip
call limit : 128
codec preference : 1, g723r53, bytes 20
dtmf relay rtp nte : Disabled
emergency-number : n/a
fax rate : 9600
fax protocol : none
modem passthrough : none
pass through call prefix : 9
comfort noise negotiate : Enabled
rtp port-validation : Enabled
Configured bind IP address : all ipv4:47.100.107.65:5060
Bound IP address : all ipv4:47.100.107.65:5060
rel1xx : Disabled
SR#
```

Figure 105: show voice service voip sample output

As the solution, configure Secure Router 2330/4134 to support the G.711 a-law codec offered by the endpoint.

```
config term
voice service voip
codec 1 g711alaw
exit 2
```

Troubleshooting the Mediation Server Module

The procedures in this section assume that you have installed and configured the Microsoft Office Communications Server (OCS) components in your network according to the *Microsoft Office Communications Server 2007 Deployment Guide*. It also assumes that Microsoft OCS Mediation Server has been installed in the Mediation Server module of the Secure Router 4134 along with the OCS 2007 Resource Kit. For details on configuring the Mediation Server module, see *Avaya Secure Router 2330/4134 Configuration — SIP Media Gateway* (NN47263-508).

After you have assigned in IP address to the Mediation Server module, you can use the central OCS GUI to connect to the Mediation Server.

You can also use Remote Desktop to connect to the Mediation Server Module IP address. This provides access to the Windows 2003 server running on the module as well as the OCS GUI on the module.

If you experience connectivity issues or a non-responding Mediation Server Module, you can connect directly to the module using a monitor and USB-based keyboard and mouse for debugging.

Problem scenario 1

The OCS Mediation Server installed in the Mediation Server module of the Secure Router 4134 does not show up in the OCS GUI.

Solution

The Mediation Server in the Mediation Server module of the Secure Router 4134 has not been activated with the OCS setup for your system. Please refer to the Microsoft Mediation Server for Hybrid Gateways document for steps to activate the Mediation Server. Once activated this Mediation Server should appear in the Mediation Server section under the given OCS forest domain in the GUI.

Problem scenario 2

Mediation Server in the Mediation Server module does not come up.

Solution

1. Verify that Mediation Server module has a valid IP address configured. See *Avaya Secure Router 2330/4134 Configuration — SIP Media Gateway* (NN47263-508) for details to configure the IP address of the Mediation Server module.
2. Verify that Mediation Server module has been joined to the Active Directory of OCS 2007.
3. Verify that the Mediation Server properties namely Communication Server Listen IP address, Default Location Profile, Office Communication Server next hop, PSTN Gateway next hop and Certificate have been configured.

Problem scenario 3

Calls from OCS Client to PSTN numbers are not going through.

Solution

The following checklist needs to be verified in the given order.

1. Verify that the Mediation Server is running. If not refer to Problem scenario 2.
2. Check whether you are able to ping the OCS Communication Server and PSTN Gateway IP address from the Mediation Server module. If not, see *Avaya Secure Router 2330/4134 Configuration — SIP Media Gateway* (NN47263-508) to configure the required network interfaces.
3. Verify that the PSTN Gateway next hop Media Gateway is listening on transport TCP on the configured listen port for SIP signaling packets.

Comments? infodev@avaya.com

4. Check whether you have the TDM trunks configured and the TDM links up on the Secure Router 4134. If not, see *Avaya Secure Router 2330/4134 Configuration — SIP Media Gateway* (NN47263-508) to configure the required network interfaces.
5. If all the above is working, enable the logging of the OCS Mediation Server on the Mediation Server module and collect the logs.

Collecting the OCS Mediation Server logs on the Secure Router 4134 Mediation Server module

To collect the OCS Mediation Server logs on the Secure Router 4134 Mediation Server module, perform the following procedure.

Procedure steps

1. From the OCS GUI, right click on the Mediation Server running in the Mediation Server module, and select **Logging Tool > New Debug Session**.

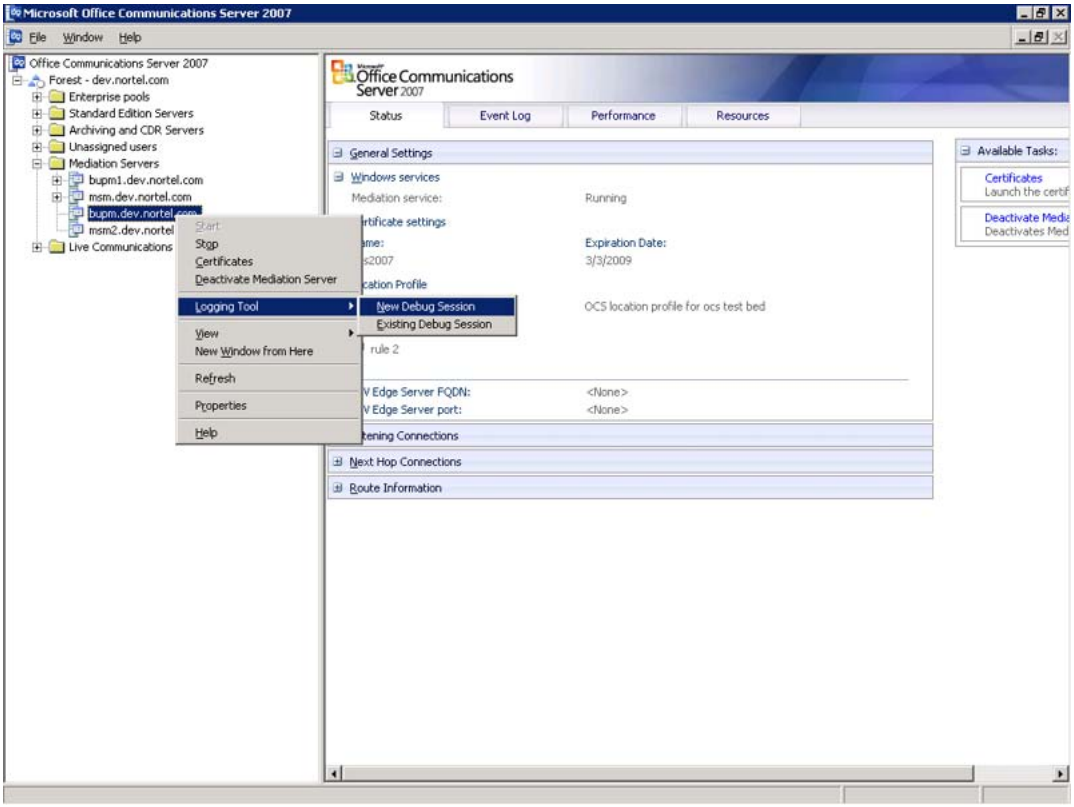


Figure 106: OCS GUI

2. From the OCS 2007 Logging tool dialog box, in the Components window, select **Mediation Server** and then click on **Start Logging**.

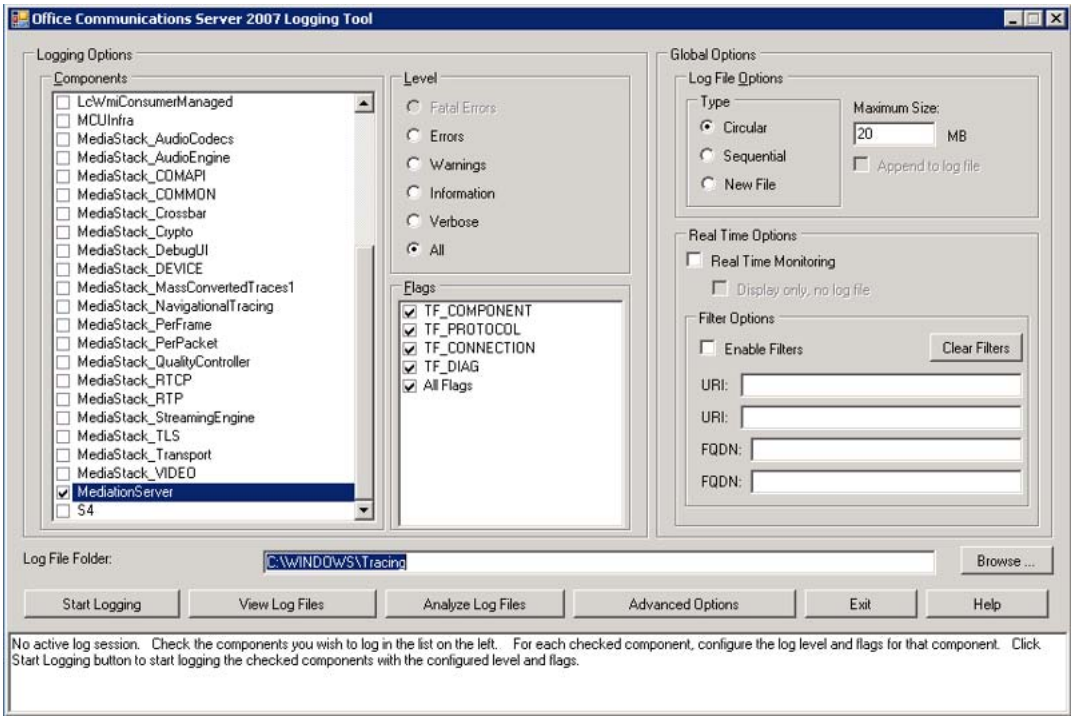


Figure 107: OCS Logging Tool dialog box

3. Initiate a call between an OCS Client and a PSTN user. When the call is completed (successfully or not) click **Stop Logging**.

Comments? infodev@avaya.com

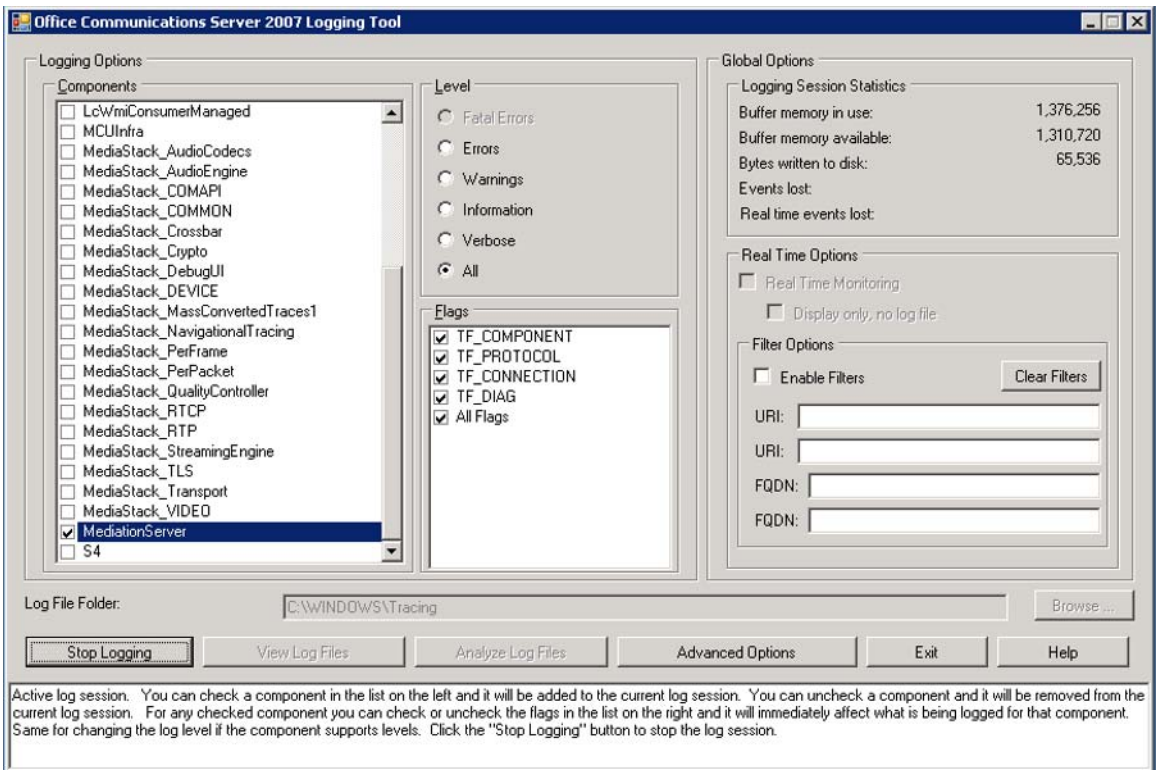


Figure 108: OCS Logging Tool window with active log session

After you stop the logging, the log file MediationServer.etl is created in the Log File Folder, and the **View Log Files** button becomes active on the OCS Logging Tool window.

4. Click **View Log Files** to view the Mediation Server logs in Notepad.
5. Click **Analyze Log Files** to view the Mediation Server logs in the Snooper window.

Network packet capture

You can use third-party packet capture tools to capture the network packets flowing in and out of the Mediation Server. The Mediation Server module has the Wireshark network protocol analyzer software pre-installed for capturing the network traces.

To use Wireshark for VoIP traffic monitoring, perform the following procedure.

Procedure steps

1. Launch Wireshark.
2. To open the Capture Options dialog box, select Capture > Options.

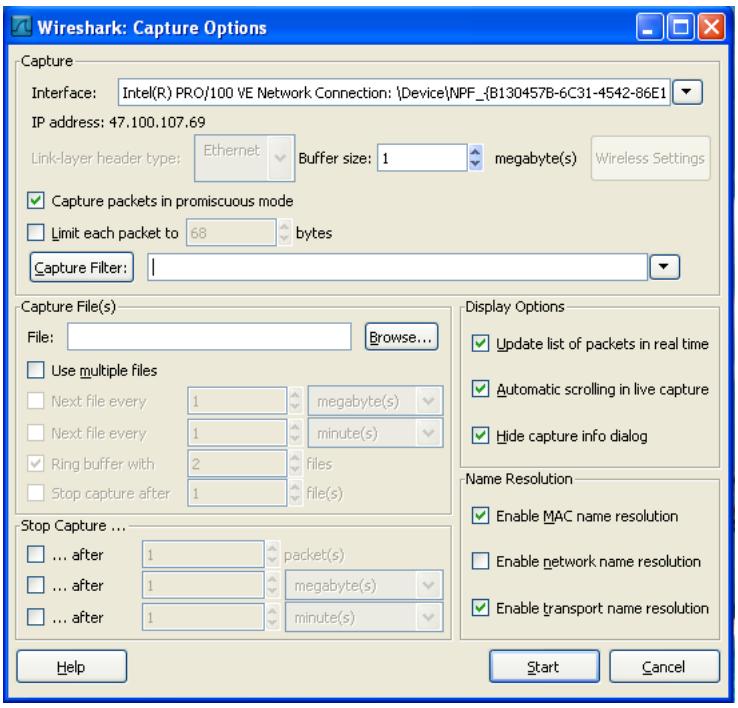


Figure 109: Capture Options dialog box

3. In the Interface box, ensure that the correct interface is specified. In this example, traffic is captured on the Mediation Server module backplane Ethernet interface.
4. When the correct interface is specified, click Start.
5. In the Filter window, you have the option of specifying a filter to limit the number of packets you want to filter. Select sip to capture the voice signaling traffic (SIP) and rtp to capture the voice media traffic (RTP).

Comments? infodev@avaya.com

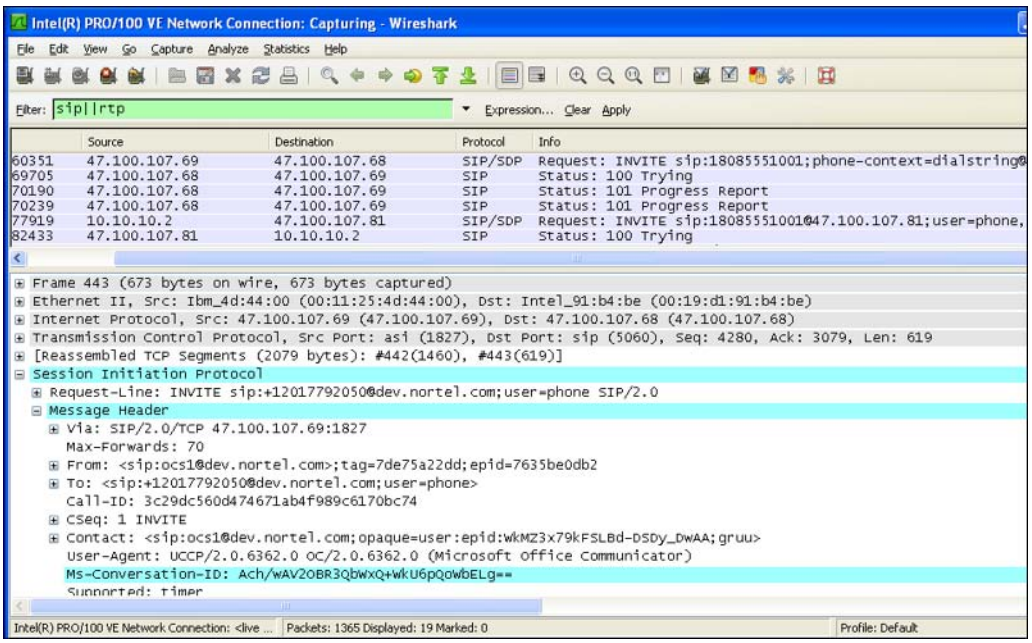


Figure 110: Sample packet capture output

The preceding figure shows the packet list. The first four columns show the packet number, time and the addresses of the hosts involved. Because Wireshark understands SIP, it is able to identify the packets as SIP in the Protocol column and give detailed information in the Info column.

A cursory examination of the information in this figure shows that the same three packets repeat themselves five times. First, the Mediation Server sends a SIP INVITE message to the Media Gateway, which is used to open a conversation. Next, the Media Gateway responds with “404 Not Found” to which the Mediation Server responds with an ACK. From this trace it is likely that the OCS Client through the Mediation Server is trying to reach a non-existent user or the Secure Router 4134 is not configured to handle this number.

Re-imaging the Mediation Server Module

If you lose the administrator password for your Mediation Server Module (and have no other account with administrator privileges), or if the software image becomes corrupt on the module, you must re-image the module.

Avaya strongly recommends the following procedures to protect the software on the Mediation Server Module:

- Create at least one additional user account with administrator privileges on the Microsoft Windows Server 2003 running on the Mediation Server Module for OCS. If you lose or

forget the administrator password, you can log in using another user account. Similar to other Operating Systems, the administrator password cannot be recovered.

- Enable auto updates on Windows Server 2003 and the Mediation server running on the Mediation Server Module.

  "High Priority" updates for Windows Server 2003 and the Mediation Server are automatically downloaded and auto-installed (identical to the Windows updates process) when you enable the Microsoft auto update feature on each. "Optional" updates must be done manually—you are only alerted to their availability. You must go to the Microsoft update Web site (http://www.update.microsoft.com) to get a description of the optional updates. You can then decide if the update is necessary for your system.

- Make a backup copy of the Mediation Server Module software and configuration using a third-party application such as Ghost software from Symantec Corporation.

Cloning the Mediation Server Module image to a USB drive

Use the procedure in this section to create a backup copy of the image and configuration on the Mediation Server Module.

Prerequisites

- Ensure you have an application available with which to create a clone of your Mediation Server Module image and configuration.
- Ensure the Secure Router 4134 is powered down.

Procedure steps

1. Insert a USB drive into the USB slot of the Mediation Server Module.
2. Connect a display monitor and a USB keyboard to the Mediation Server Module.
3. Power up the Secure Router 4134.
4. Launch the software you use to clone images, if necessary (the software may launch automatically, depending on the software and the version you run).
5. Follow the prompts on your screen to create a backup of the Mediation Server Module image. Refer to instructions that ship with the application you use if you require additional information about the prompts.

   It takes approximately 30 minutes to create a backup image if you use Ghost software.
6. Close the cloning application.
7. Remove the USB drive from the Mediation Server Module.

8. Insert the USB drive into a desktop PC.
9. Verify that the cloned image has been successfully created. If you use Ghost software, ensure that the cloned image is created in the correct path and that the following three files exist:
    - two files with the .GHS file extension
    - one file with the .GHO file extension

Restoring the Mediation Server Module image from the backup on a USB drive

Use the procedure in this section to restore the image on the Mediation Server Module.

Prerequisites

- Ensure you have a backup (cloned image) of your Mediation Server Module image and configuration.
- Ensure you have an application available with which to restore the cloned Mediation Server Module image.
- Ensure the Secure Router 4134 is powered down.

Procedure steps

1. Insert the USB drive that contains the cloned image into the USB slot of the Mediation Server Module.
2. Connect a display monitor and a USB keyboard to the Mediation Server Module.
3. Power up the Secure Router 4134.
4. Launch the software you use to clone and restore images, if necessary (the software may launch automatically, depending on the software and the version you run).
5. Follow the prompts on your screen to restore the image to the Mediation Server Module. Refer to instructions that ship with the application you use if you require additional information about the prompts.

   It takes approximately 30 minutes to restore the backup image to the Mediation Server Module if you use Ghost software.
6. Reboot the Mediation Server Module at the end of the restoration (cloning) process and remove the USB drive from the Mediation Server Module.

   The Mediation Server Module initializes using the cloned image that you restored to the module.

Comments? infodev@avaya.com

Chapter 17: Troubleshooting high CPU utilization

Use the commands in this section to troubleshoot high CPU utilization.

The CPU Utilization feature provides data about CPU usage by the processes running on Secure Router 2330/4134. You can view CPU utilization information for the past 10 seconds (s), 1 minute (min), 5 minutes (min), or since system startup. The router displays CPU utilization as a percentage. The CPU utilization information allows you to see how the CPU was used during a specific time interval. This feature helps you to channelize traffic through the secure router to make efficient use of available CPU time. As a result you can reduce data loss due to sufficient CPU time not being available.

You can configure three levels of CPU utilization threshold:

- Green threshold – indicates that CPU utilization is below optimum range. Specified by the user.
- Yellow threshold – indicates that CPU utilization is in optimum range. This is the range between green and red threshold.
- Red threshold – indicates that CPU utilization is above optimum range. Specified by the user.

To configure the CPU utilization threshold and enable threshold notification, see configure process cpu threshold total notify on page 369.

When you receive a notification that the CPU utilization is in the red threshold, reduce the traffic flow to the CPU until the CPU utilization returns to the yellow or green threshold range.

To reduce the traffic flow to the CPU, redirect the traffic to another router by reducing the number of Ethernet and WAN interfaces on the affected router.

configure process cpu threshold total notify

Use this command to configure the threshold notification for total CPU utilization.

You can configure the system to generate an event notification for total system CPU utilization. This notification provides data regarding the peak and average CPU utilization in percentages as well as the color (green/yellow/red) of the entire system. Notifications can be generated either only once when the corresponding threshold is breached or periodically at regular intervals.

Note:

To receive these notifications, ensure the following:

- Enable console logging and also change the event-log priority to info. See Configuring the system for console logging on page 381.
- Enable system logging and also change the sys-log priority to info. See Configuring the system for syslog reporting on page 376.

Syntax

```
threshold total red <%red> green <%green> interval <interval> notify
<type>
```

Table 78: Variable definitions

Variable	Value
<%red>	Red threshold in percentage. (Default: 85)
<%green>	Green threshold in percentage. (Default: 70)
<interval>	Duration in seconds for which the CPU utilization is measured. You can enter multiples of 10 up to a maximum of 300 seconds. (Default: 30)
<type>	• cont - this type generates notification periodically at the interval specified. • once - this type generates notification once when the utilization changes from one threshold to another threshold. (Default: once)

Example

- `SR/configure/process cpu#` **`threshold total red 90 green 50 interval 10 notify cont`**
- `SR/configure/process cpu#` **`threshold total red 90 green 50 interval 10 notify once`**

CPU utilization debug commands

This section provides the CPU utilization debug commands.

Related topics:

debug process start-history on page 371
debug process stop-history on page 371

Comments? infodev@avaya.com

debug process start-history

Use this command to start the history collection for a process.

Syntax

```
start-history <WORD>
```

Table 79: Variable definitions

Variable	Value
<WORD>	Name of the process

Example

```
SR/debug/process# start-history rxPoll
```

debug process stop-history

Use this command to stop the history collection for a process.

Syntax

```
stop-history <WORD>
```

Table 80: Variable definitions

Variable	Value
<WORD>	Name of the process

Example

```
SR/debug/process# stop-history rxPoll
```

CPU utilization show commands

This section provides the CPU utilization show commands.

Related topics:

show processes cpu color on page 372
show processes cpu history format on page 372
show processes cpu history process on page 373

show processes cpu show-config on page 373
show processes cpu utilization format on page 373

show processes cpu color

Use this command to view the CPU utilization color.

Syntax

```
show processes cpu color
```

Example

```
SR# show processes cpu color
```

show processes cpu history format

Use this command to view the history graph of the total CPU utilization.

Syntax

```
show processes cpu history format <display format>
```

Table 81: Variable definitions

Variable	Value
<display format>	• seconds - displays CPU utilization history in seconds (maximum 300 seconds for total and maximum 60 seconds for individual process) • minutes - displays CPU utilization history in minutes (maximum 60 minutes) • hours - displays CPU utilization history in hours (maximum 24 hours) • days - displays CPU utilization history in days (maximum 30 days) • all - displays CPU utilization history in seconds, minutes, hours, and days

Example

- `SR# show processes cpu history format seconds`
- `SR# show processes cpu history format minutes`

show processes cpu history process

Use this command to view the history graph of the CPU utilization of processes.

Syntax

```
show processes cpu history process <WORD>
```

Table 82: Variable definitions

Variable	Value
<WORD>	Name of the process

Example

```
SR# show processes cpu history process rxPoll
```

show processes cpu show-config

Use this command to view the configuration of the CPU utilization monitor.

Syntax

```
show processes cpu show-config
```

Example

```
SR# show processes cpu show-config
```

show processes cpu utilization format

Use this command to view the CPU utilization of all the processes.

Syntax

```
show processes cpu utilization format <display format>
```

Table 83: Variable definitions

Variable	Value
<display format>	• brief - displays CPU utilization of processes with 1% or more CPU utilization • invoked - displays CPU utilization of processes that were invoked at least once • all - displays full information

Example

- SR# **show processes cpu utilization format brief**
- SR# **show processes cpu utilization format invoked**
- SR# **show processes cpu utilization format all**

Comments? infodev@avaya.com

Chapter 18: Secure Router 2330/4134 system error messages

Use syslog error messages to assist you in troubleshooting errors or issues in the Avaya Secure Router 2330/4134 system.

Important:

Syslog and console reporting can generate a substantial amount of output and can use a substantial amount of system resources. Use the syslog and console reporting features with caution in any production network to avoid adversely affecting other activities on the network. Ensure you configure syslog and console reporting for the specific options you are troubleshooting.

Message severity levels

The Secure Router 2330/4134 sorts syslog error messages based on the following levels of severity:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notification
- Informational
- Debugging

The following table describes the severity levels.

Table 84: Syslog error message severity levels

Level	Description
Emergency	System is unusable
Alert	Immediate action required
Critical	Critical condition
Error	Error condition

Level	Description
Warning	Warning condition
Notification	Normal but significant condition
Informational	Informational only
Debugging	Message that appears only during debugging

Configuring the system for syslog reporting

Use the commands in this section to enable and disable syslog reporting and to define parameters for syslog messages.

Enabling and disabling syslog messages

Use the commands in this section to enable and disable syslog messages.

Procedure steps

1. To access configuration mode, enter:

   ```
   configure terminal
   ```

2. To enable or disable syslog messages, enter:

   ```
   system logging syslog {enable|disable}
   ```

Specifying the device to which the Secure Router 2330/4134 sends syslog messages

Use the commands in this section to specify the host IP address to which the Secure Router 2330/4134 sends syslog messages

Procedure steps

1. To access configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the host IP address (IPv4 address) to which the Secure Router 2330/4134 sends syslog messages, enter:

Comments? infodev@avaya.com

```
system logging syslog host_ipaddr <ipaddr> udp_portno <udp
port>
```

3. To specify the host IP address (IPv6 address) to which the Secure Router 2330/4134 sends syslog messages, enter:

```
system logging syslog host_ipaddrv6 <ipaddr> udp_portno <udp
port>
```

Table 85: Variable definitions

Variable	Value
<ipaddr>	The IP address of the host to which the Secure Router 2330/4134 sends the syslog messages. Enter the IP address in the proper format for your network (that is, in IPv4 or IPv6 format).
<udp_portno>	The UDP port used for communication. The default UDP port number is 514.

Configuring multiple Syslog servers

Several devices in a network can be configured to generate Syslog messages. A Syslog Server monitors the incoming Syslog messages on UDP ports and decodes the messages for logging purposes. The Secure Router supports the configuration of up to five Syslog Servers. Because the Syslog servers are logged simultaneously, they all contain the same Syslog records.

To achieve backward compatibility with the existing Syslog implementation, the provision of a port number during configuration of the host IP address remains optional. If a user does not specify a port during CLI configuration, UDP port 514 is used by default. In addition, the enabling of message logging remains unchanged.

As a limitation, all enable or disable functions apply to all configured servers. Configuration of Syslog message logging on selected servers is not supported.

When viewing Syslog Server information, the SNMP interface can only display information for one server at a time.

Use the following steps to configure multiple Syslog servers.

Procedure steps

1. To configure multiple Syslog servers, enter Configuration Mode.

```
configuration terminal
```

2. Enter the **`system logging`** command tree.

```
system logging
```

3. Access the Syslog command tree.

```
syslog
```

4. Specify a host IP address and UDP port. If a port number is not specified, port 514 is used by default.

   ```
   host_ipaddr <A.B.C.D> [port]
   ```

5. To add another Syslog server address, repeat step 4 until up to 5 Syslog servers are added.
6. Enable Syslog.

   ```
   enable
   ```

Table 86: Variable definitions

Variable	Value
<A.B.C.D>	Specifies the host IP address.
[port]	Specifies (optionally) the UDP port. If not specified, port 514 is used by default.

Specifying the syslog messages to report

Use the commands in this section to specify the syslog messages that the Secure Router 2330/4134 reports.

Procedure steps

1. To access configuration mode, enter:

   ```
   configure terminal
   ```

2. To specify the syslog messages that the Secure Router 2330/4134 reports, enter:

   ```
   system logging syslog module <module> <facility> <priority>
   ```

Table 87: Variable definitions

Variable	Value
<facility>	The source of the message. Valid values are the following: • local0 • local1 • local2 • local3 • local4 • local5 • local6

Comments? infodev@avaya.com

Variable	Value
	• local7 • sys9 • sys10 • sys11 • sys12 • sys13 • sys14 The default value is "local0".
<module>	The type of event to report. Valid values are the following: • auth – events related to the authorization facility • bundle – interface bundle • crypto – cryptographic library or hardware • fr – frame relay • fwl-alg – firewall Application Layer Gateway • fwl-atk – firewall attack • fwl-conn – firewall connection • fwl-rsm – firewall reassembly • hdlc – hdlc protocol on wan links • ike – Internet Key Exchange • ipsec – IP security protocol (AH or ESP) • ipsl2tp – IPSEC + L2TP (for L2TP server) • isdn – ISDN • ntp – events related to the Network Time Protocol facility • pki – Public Key Infrastructure (certificate management) • ppp – point-to-point protocol on wan links • pppoe – point-to-point over ethernet • qos – Quality of Service system • radius – radius logging • routing – routing protocols

Variable	Value
	• security – events related to the security facility • system – events related to the system facility • userdb – user database • vif – virtual interface (for PPPoE and L2TP server) • vifppp – PPP events for virtual interfaces • xauth – extended authentication for IKE • alarms – alarms • command-parser – command parser • dos – DoS • forwarding – forwarding • mfr – MFR • mlppp – MLPPP • os – OS • mpls – MPLS system logging • mstp – MSTP system logging • L2-CTRL – L2 Control Packets logging • cfm – CFM
<priority>	The severity level of the message. Valid values are the following: • emerg – log emergency messages only • alert – log alert messages and above • crit – log critical messages and above • err – log error messages and above • warn – log warning messages and above • notice – log notification messages and above • info – log informational messages and above • debug – log all messaes • none – log no messages The default value is "none".

Comments? infodev@avaya.com

Configuring the Syslog source address

Use the following procedure to configure the Syslog server source address for all services.

Procedure Steps

1. To configure source addresses for a service, enter Configuration Mode.

   ```
   configuration terminal
   ```

2. Enter the **system logging** subtree.

   ```
   system logging
   ```

3. Enter the **syslog** subtree.

   ```
   syslog
   ```

4. Configure the source address.

   ```
   source-address <[ip-address]|[interface-name]>
   ```

Table 88: Variable definitions

Variable	Value
[ip-address]	Specifies the source address by IP address.
[interface-name]	Specifies the source address by interface name.

Configuring the system for console logging

Use the commands in this section to enable console logging and to define parameters for console messages.

Procedure steps

1. To access configuration mode, enter:

   ```
   configure terminal
   ```

2. To enable or disable console logging, enter:

   ```
   system logging console {enable|disable}
   ```

3. To specify the messages to log to the console based on severity level, enter:

   ```
   system logging console priority <priority>
   ```

Table 89: Variable definitions

Variable	Value
{enable | disable}	Enables or disables console logging. The default value is "enable".
<priority>	The severity level of the message. Valid values are the following: • emerg – log emergency messages only • alert – log alert messages and above • crit – log critical messages and above • err – log error messages and above • warn – log warning messages and above • notice – log notification messages and above • info – log informational messages and above • debug – log all messages • none – log no messages The default value is "critical".

Syslog error messages that indicate a possible fault in the system

The following table provides a list of Secure Router 2330/4134 syslog error messages that indicate a possible fault condition in the Secure Router 2330/4134. If you receive one of the following error messages, contact Technical Support.

Table 90: Syslog error messages that require Avaya Technical Support assistance

Security Level	Module	Message
ALERT	FORWARDING	RouteCacheInit: Warning:Unable to allocate complete pool of cache entries.
ALERT	FORWARDING	Error : Failed init UAM event queue
ALERT	FORWARDING	Error : Failed init ARP event queue
CRITICAL	FORWARDING	ipOutput: invalid interface <x>

Comments? infodev@avaya.com

Security Level	Module	Message
CRITICAL	FORWARDING	ipOutput: queue pointer NULL for interface <x>:if_type :<y>
CRITICAL	FORWARDING	ipOutput: queue pointer NULL for interface <x>
CRITICAL	FORWARDING	ip6Output: invalid interface <x>
CRITICAL	FORWARDING	ip6Output: queue pointer NULL for interface <x>
CRITICAL	FORWARDING	ip6Moutput: invalid interface <x>
CRITICAL	FORWARDING	ip6Moutput: queue pointer NULL for interface <x>
CRITICAL	FORWARDING	Equal cost routes out of synch = <x>, <y>
CRITICAL	FORWARDING	Error starting route cache timer
CRITICAL	FORWARDING	Error getting route cache timer information
CRITICAL	FORWARDING	Cache hold_down timer_create error
CRITICAL	FORWARDING	Cache hold_down timer_connect error
CRITICAL	FORWARDING	Error starting route6 cache timer
CRITICAL	FORWARDING	error bringing down static route <ip address> <mask>
CRITICAL	FORWARDING	error bringing up static route <ip address> <mask>
CRITICAL	FR	ioctl FR_GET_VC_CONFIG failed
CRITICAL	HDLC	close l2Fd failed
CRITICAL	HDLC	I_UNLINK failed
CRITICAL	HDLC	failed to add driver /dev/ghdlc
CRITICAL	HDLC	open failure: /dev/ghdlc
CRITICAL	HDLC	ioctl GHDLC_SET_LINK failed
CRITICAL	HDLC	Ioctl failed: I_LINK
CRITICAL	HDLC	ioctl GHDLC_BIND_LINK failed
CRITICAL	HDLC	ioctl GHDLC_UNBIND_LINK failed
CRITICAL	HDLC	ioctl GHDLC_SET_CONFIG failed
CRITICAL	HDLC	ioctl GHDLC_CONNECT_LINK failed

Security Level	Module	Message
CRITICAL	HDLC	ioctl GHDLC_RECONNECT_LINK failed
CRITICAL	HDLC	ioctl GHDLC_DISCONNECT_LINK failed
CRITICAL	HDLC	GHDLC_GET_STAT failed
CRITICAL	HDLC	ioctl GHDLC_CLR_MIB failed
CRITICAL	HDLC	ioctl GHDLC_CLR_STAT failed
CRITICAL	MLFR	ioctl FR_STOP/ START_TRAFFIC_ON_LINK failed
CRITICAL	MLPPP	ioctl PPP_GET_CONFIG failed for local lcp –MRU mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_SET_CONFIG failed for local lcp –MRU mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_GET_CONFIG failed for remote lcp –MTU mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_SET_CONFIG failed for remote lcp –MTU mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_GET_CONFIG failed for local MLP –mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_SET_CONFIG failed for MLP –mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_GET_CONFIG failed for local ipcp –mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_SET_CONFIG failed for local ipcp –mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_GET_CONFIG failed for local lcp –mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_GET_CONFIG failed for MLP –mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_SET_CONFIG failed for mlp –mlppp config for bundle <name>

Comments? infodev@avaya.com

Security Level	Module	Message
CRITICAL	MLPPP	ioctl PPP_GET_CONFIG failed for MLP –discriminator mlppp config for bundle <name>
CRITICAL	MLPPP	ioctl PPP_SET_CONFIG failed for mlp in setting discriminator mlppp config for bundle <name>
CRITICAL	OS	Error: In route_ouput:ENOBUFS
CRITICAL	PPP	ioctl PPP_GET_CONFIG failed for local BCP for bundle <name>
CRITICAL	PPP	ioctl PPP_SET_CONFIG failed for local BCP for bundle <name>
CRITICAL	PPP	ioctl PPP_GET_CONFIG failed for remote lcp- ppp config for bundle <name>
CRITICAL	PPP	ioctl PPP_SET_CONFIG failed for local lcp –MRU ppp config for bundle <name>
CRITICAL	PPP	ioctl PPP_GET_CONFIG failed for local lcp –MTU ppp config for bundle <name>
CRITICAL	PPP	ioctl PPP_SET_CONFIG failed for local lcp –MTU ppp config for bundle <name>
CRITICAL	PPP	ioctl PPP_GET_CONFIG failed for local ipcp- ppp config for bundle <name>
CRITICAL	PPP	ioctl PPP_SET_CONFIG failed for local ipcp – ppp config for local ipcp when configuring pp for bundle <name>
CRITICAL	PPP	ioctl PPP_GET_CONFIG failed for remote lcp- ppp config for bundle <name>
CRITICAL	PPP	ioctl PPP_GET_CONFIG failed for remote lcp-MTU ppp config for bundle <name>
CRITICAL	PPP	ioctl PPP_SET_CONFIG failed for remote lcp-MTU ppp config for bundle <name>
CRITICAL	PPP	ioctl PPP_GET_STAT failed: for bundle <name>

Security Level	Module	Message
CRITICAL	PPP	ioctl PPP_GET_CONFIG failed for local lcp –get ppp config for bundle <name>
ERROR	DOS	Memory Allocation Failure. Report Error
ERROR	DOS	Error in clearing incomplete tcp connection
ERROR	FORWARDING	ip6MuxScanIPv6AddrLstAcrossIntf: unit <x> out of range
ERROR	FORWARDING	Error adding interface route
ERROR	FORWARDING	Error deleting interface route
ERROR	FORWARDING	Interface <name> keepalive timer no memory error
ERROR	FORWARDING	Error keepalive timer not initialized, interface = <name>
ERROR	FORWARDING	Start timer gives an error for interface <name>
ERROR	FORWARDING	Error keepalive timer not initialized for interface = <name> timer
ERROR	FORWARDING	Sending keepalive packet gives an error for interface = <name>
ERROR	FORWARDING	ipMuxIfProxyArpSet: unit <x> out of range
ERROR	FORWARDING	ipMuxIfProxyArpSet: unit <x> not ethernet
ERROR	FORWARDING	ipMuxIfDown: unit <x> out of range
ERROR	FORWARDING	ip4MuxIfDown: unit <x> out of range
ERROR	FORWARDING	ip6MuxIfDown: unit <x> out of range
ERROR	FORWARDING	ipMuxIfUp: unit <x> out of range
ERROR	FORWARDING	ip6MuxInet6Up: unit <x> out of range
ERROR	FORWARDING	ip6MuxInet6Down: unit <x> out of range
ERROR	FORWARDING	Error <name> peer route
ERROR	FORWARDING	Error <name> peer route invalidaddress or mask
ERROR	FORWARDING	Error bringing down staticroute <ip_address> <mask>

Comments? infodev@avaya.com

Security Level	Module	Message
ERROR	FORWARDING	Error bringing up staticroute <ip_address> <mask>
ERROR	FR	ERR:Fr_Dequeue failed: Report Error
ERROR	OS	Error: unable to add 32 bit interface route, could not delete conflicting routes
ERROR	OS	rtinit: wrong ifa (<x>) was(<y>)
ERROR	OS	Error: In route_ouput <x>
ERROR	PPPOE	PPPoE(<name>): address <ip_address> from server overlaps
ERROR	PPPOE	PPPoE(%s): address %s from server is invalid or overlaps
ERROR	PPPOE	PPPoE(<name>):peer address <ip_address> from server overlaps
ERROR	PPPOE	PPPoE(<name>): peer address <ip_address> from server is invalid or overlaps
NOTIFCATION	ALARMS	Modem service is off
NOTIFCATION	ALARMS	terminate Remote Modem/cli service
NOTIFCATION	ALARMS	Remote Modem/cli service is up
NOTIFCATION	ALARMS	Remote Modem/cli service is down
NOTIFCATION	ALARMS	Modem Answer failed
NOTIFCATION	ALARMS	Modem Answer Setup is turned off
NOTIFCATION	ALARMS	Modem Answer Setup failed: line is connected already
NOTIFCATION	ALARMS	Modem Answer Setup Success
NOTIFCATION	ALARMS	Modem Answer Setup Failed
NOTIFCATION	FORWARDING	MPLS_L2_VPN up on <interface name>
NOTIFCATION	FORWARDING	Bridge protocol up on <interface name>
NOTIFCATION	FORWARDING	MPLS_L2_VPN down on <interface name>
NOTIFCATION	FORWARDING	Bridge protocol down on <interface name>

Security Level	Module	Message
NOTIFCATION	FORWARDING	Ipv6 is activated on bundle <name> PVC <x>
NOTIFCATION	FORWARDING	Ipv6 is deactivated on bundle <name> PVC <x>
NOTIFCATION	FR	bundle UP: <name>
NOTIFCATION	FR	bundle DOWN: <name>
NOTIFCATION	FR	<type>VC UP:<name><dlci>
NOTIFCATION	FR	<type>VC DOWN:<name><dlci>
NOTIFCATION	FR	MFR ind: Bundle <name>, Link UP:<interface>
NOTIFCATION	FR	MFR ind: Bundle <name>, Link DOWN:<interface> cause <str>
NOTIFCATION	FR	Got request from FR stack to verify the status of PVC
NOTIFCATION	HDLC	bundle UP: <name>
NOTIFCATION	HDLC	bundle DOWN: <name>
NOTIFCATION	L2-CTRL	hsl_af_eapol_l2_sock_queue_length_ exceeded: EAPOL Socket buffer
NOTIFCATION	L2-CTRL	hsl_af_garp_l2_sock_queue_length_e xceeded: GARP Socket buffer Queue Count Exceeded, Dropping packets
NOTIFCATION	L2-CTRL	hsl_af_igs_l2_sock_queue_length_ex ceeded: IGS Socket buffer Queue Count Exceeded, Dropping packets
NOTIFCATION	L2-CTRL	hsl_af_lacp_l2_sock_queue_length_e xceeded: LACP Socket buffer Queue Count Exceeded, Dropping packets
NOTIFCATION	L2-CTRL	hsl_af_stp_l2_sock_queue_length_ex ceeded: STP Socket buffer Queue Count Exceeded, Dropping packets
NOTIFCATION	PPP	bundle UP: <name>
NOTIFCATION	PPP	bundle Down: <name>
NOTIFCATION	PPP	Ipv6 is activated on bundle <name> PVC <dlci>
NOTIFCATION	PPP	Ipv6 is de-activated on bundle <name> PVC < dlci>

Comments? infodev@avaya.com

Security Level	Module	Message
DEBUGGING	FORWARDING	sfSendToStack2(): sfSendToStack() failed !
DEBUGGING	FORWARDING	ipMuxIfReset: (unit): <x>
DEBUGGING	FR	frReserveAtEnd(): Enter!-n=<x>
DEBUGGING	FR	frReserveAtEnd(): Found the last bp
DEBUGGING	FR	frReserveAtEnd(): Allocating new buf
DEBUGGING	FR	frReserveAtEnd(): Alloc new buf failed
DEBUGGING	FR	frReserveAtEnd(): Alloc new buf OK
DEBUGGING	FR	frReserveAtEnd(): BP = NULL
DEBUGGING	FR	fr_uwput():msize:<x>
DEBUGGING	FR	frPhreceive():Rcvd ACTIVATE IND
DEBUGGING	FR	frPhreceive(): Rcvd DEACTIVATE IND
DEBUGGING	FR	frPhreceive():Rcvd DEFAULT IND
DEBUGGING	FR	frPhreceive():rc=<x>
DEBUGGING	HDLC	GHDLC open successful:/dev/ghdlc fd=<x>
DEBUGGING	ISDN	Sending SETUP messageon bundle :<name> slot/port :<x>/<y> channel :<z> and called number is :<string>"
DEBUGGING	ISDN	Incoming call on bundle :<name> slot/port :<x>/<y> channel :<z> and calling number:<string>
DEBUGGING	ISDN	Call is ACTIVE on bundle :<name> slot/port :<x>/<y> channel :<z>
DEBUGGING	ISDN	Call is DISCONNECTED on bundle :<name> slot/port :<x>/<y> and channel :<z>
DEBUGGING	MLFR	MFR Indication: Link num:<x>, Event: DATA
DEBUGGING	MLFR	MFR Msg received: Link num:<x>
DEBUGGING	MLFR	Mfr_LinkTransmit:Sending Data. link
DEBUGGING	MLPPP	ioctl PPP_GET_CONFIG successful for local lcp - MRU mlppp config for bundle:<name>

Security Level	Module	Message
DEBUGGING	MLPPP	ioctl PPP_SET_CONFIG successful for local lcp - MRU mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_GET_CONFIG successful for remote lcp - MTU mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_SET_CONFIG successful for remote lcp - MTU mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_GET_CONFIG successful for MLP – mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_GET_CONFIG successful for local lcp - MRU mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_SET_CONFIG successful for local lcp - MRU mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_GET_CONFIG successful for remote lcp - MTU mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_SET_CONFIG successful for remote lcp - MTU mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_GET_CONFIG successful for MLP - mlppp config for bundle: <name>
DEBUGGING	MLPPP	ioctl PPP_SET_CONFIG successful for MLP - mlppp config for bundle: <name>
DEBUGGING	MLPPP	ioctl PPP_GET_CONFIG successful for local ipcp - mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_SET_CONFIG successful for local ipcp - mlppp config for bundle:<name>
DEBUGGING	MLPPP	ioctl PPP_SET_CONFIG successful for mlp - mlppp config for bundle: <name>

Comments? infodev@avaya.com

Security Level	Module	Message
DEBUGGING	PPP	ioctl PPP_GET_CONFIG successful for local lcp - MRU ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_SET_CONFIG successful for local lcp - MRU ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_GET_CONFIG successful for local lcp - MTU ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_SET_CONFIG successful for local lcp - MTU ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_GET_CONFIG successful for local ipcp - ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_SET_CONFIG successful for local ipcp - ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_GET_CONFIG successful for remote lcp – get ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_GET_CONFIG successful for local lcp - MRU ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_SET_CONFIG successful for local lcp - MRU ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_GET_CONFIG successful for remote lcp - MTU ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_SET_CONFIG successful for remote lcp - MTU ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_GET_CONFIG successful for local ipcp - ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_SET_CONFIG successful for local ipcp - ppp config for bundle: <name>
DEBUGGING	PPP	ioctl PPP_GET_CONFIG successful for local BCP for bundle:<name>

Security Level	Module	Message
DEBUGGING	PPP	ioctl PPP_SET_CONFIG successful for local BCP for bundle:<name>

Comments? infodev@avaya.com

Chapter 19: Emergency Recovery Procedure

In the event the Avaya Secure Router 2330/4134 becomes unstable or unresponsive, follow the steps in this section.

Note:

Avaya strongly recommends that you save the Secure Router 2330/4134 configuration both locally and to a location on the network in the event it is required for system restoration in the future.

Procedure steps

1. Save the configuration locally and to a network location. See Saving the config file on page 46
2. Verify the unit has power. See Power problem on page 52 and Power supply on page 40
   - Check system and power supply LEDs. If LEDs are off, verify there is power to the unit.
   - Verify that power cords are attached and secure.
   - Verify that the power switch is on.
   - Verify that the power source has current.

   If LEDs are still off, replace Secure Router 4134 power supply modules.
3. Check interface module LEDs. If any LEDs are red, the module may need to be replaced. See Interpreting LEDs on page 38
4. If unit has power, but is unresponsive, try to telnet to the router. If Telnet is successful, show the running configuration to obtain more information that could be useful for a diagnosis. If telnet is not successful, verify you can ping the router. If ping is unsuccessful, troubleshoot ping. See Ping does not work on page 56
5. Enter the show tech-support command and save the file for use in diagnosis. See Using the show tech-support command on page 44
6. If you feel there is an issue with Secure Router 2330/4134 configuration, restore with a known good configuration. If still unresponsive, reboot the router. See Importing a saved configuration on page 49
7. If the router remains unresponsive, restore the unit to factory defaults. It is very important to have a configuration file saved locally and to a network location for backup prior to this step. Specifically, it is likely you will need to have Telnet and/or SSH enabled for remote access. See Resetting to factory defaults on page 48 The default settings after a factory restore are:
   - Telnet server is disabled
   - Telnet client is enabled

- TFTP server is disabled
- FTP server is disabled
- SSH server is disabled
- SNMP is disabled

After the restore, reapply the saved configuration from the network.

8. If a console or telnet session is unresponsive, you can recover access without having to reboot. See Obtaining Configuration Mode access when occupied by an inactive or unresponsive session on page 21