© 2013-2017, 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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of 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 Avaya hardware and software. 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service
The following applies only if you purchase an Avaya Hosted Service Subscription from Avaya or an Avaya Channel Partner (as applicable), The terms of use for hosted services are available on the Avaya website. https://support.avaya.com/licenseinfo under the link “Avaya Terms of Use for Hosted Services” or such successor site as designated by Avaya, and are applicable to anyone who accesses or uses the Hosted Service. By accessing or using the Hosted Service, or authorizing others to do so, you, on behalf of yourself and the entity for whom you are doing so (hereinafter referred to interchangeably as “you” and “end user”), agree to the terms of use. If you are accepting the terms of use on behalf of a company or other legal entity, you represent that you have the authority to bind such entity to these terms of use. If you do not have such authority, or if you do not wish to accept these terms of use, you must not access or use the hosted service or authorize anyone to access or use the hosted service.

Licenses
The software license terms available on the Avaya website, https://support.avaya.com/licenseinfo, under the link “Avaya Software License Terms (Avaya Products)” or such successor site as designated by Avaya, are applicable to anyone who downloads, uses and/or installs Avaya software, purchased from Avaya Inc., any Avaya Affiliate, or an Avaya Channel Partner (as applicable) under a commercial agreement with Avaya or an Avaya Channel Partner. Unless otherwise agreed to by Avaya in writing, Avaya does not extend this license if the software was obtained from Avaya, an Avaya Affiliate or an Avaya Channel Partner. 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

Licence types
Designated System(s) License (DS). End User may install and use each copy or an instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software
“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/licenseinfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the
documentation, Hosted Service, 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, publish, upload, post, transmit, distribute, store, modify, create derivative works of, publicly display, publicly perform, sublicense, sell, lease, loan, or transfer 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.

Virtualization
The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two instances of the same type of products, then two products of that type must be ordered.

Third Party Components
“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service 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”). As required, 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 products. Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights beneficial to You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws
You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities
Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Downloaded Documentation
For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support
See the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya, scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks
The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(s) 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.
Contents

Chapter 1: Introduction................................................................. 10
  Purpose.................................................................................. 10
  Related resources............................................................... 10
  Support................................................................................ 13

Chapter 2: Safety messages.................................................. 15
  Notices.................................................................................. 15

Chapter 3: New in this document.......................................... 17
  Features............................................................................... 17

Chapter 4: Data collection required for Technical Support cases.......................... 19
  Data collection for an outage................................................ 19
    Collecting data before you restart.................................... 19
    Collecting data after you restart...................................... 20
  Data collection for non outage problems.......................... 21
    Gathering critical information........................................ 21

Chapter 5: Troubleshooting planning fundamentals.................. 22
  Proper installation and routine maintenance...................... 22
  Network configuration........................................................ 22
  Normal behavior on the network...................................... 23

Chapter 6: Troubleshooting fundamentals................................. 25
  Connectivity problems....................................................... 25
  Routing table problems..................................................... 26
  LED indications of problems........................................... 26
  Cable connection problems.............................................. 27
  Alarm database.................................................................... 27

Chapter 7: Troubleshooting tool fundamentals............................. 28
  Troubleshooting overview................................................ 28
  Digital Diagnostic Monitoring.......................................... 29
  Flight Recorder.................................................................. 30
  Port mirroring.................................................................... 31
  General diagnostic tools................................................... 34

Chapter 8: Log and trap fundamentals......................................... 36
  Overview of traps and logs................................................ 36
  Secure syslog...................................................................... 38
  Simple Network Management Protocol.......................... 39
  Log message format.......................................................... 40
  Log files......................................................................... 43
  Log file transfer............................................................... 44

Chapter 9: Log configuration using ACLI...................................... 46
### Chapter 17: Software troubleshooting tool configuration using EDM

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flushing routing tables by VLAN</td>
<td>128</td>
</tr>
<tr>
<td>Flushing routing tables by port</td>
<td>128</td>
</tr>
<tr>
<td>Configuring port mirroring</td>
<td>129</td>
</tr>
<tr>
<td>Configuring ACLs for mirroring</td>
<td>130</td>
</tr>
<tr>
<td>Configuring ACEs for mirroring</td>
<td>132</td>
</tr>
<tr>
<td>Running a ping test</td>
<td>133</td>
</tr>
<tr>
<td>Viewing ping results</td>
<td>135</td>
</tr>
<tr>
<td>Viewing ping probe history</td>
<td>136</td>
</tr>
<tr>
<td>Running a traceroute test</td>
<td>137</td>
</tr>
<tr>
<td>Viewing traceroute results</td>
<td>139</td>
</tr>
<tr>
<td>Viewing the traceroute history</td>
<td>140</td>
</tr>
</tbody>
</table>

### Chapter 18: Layer 1 troubleshooting

Troubleshooting fiber optic links                                        | 142  |

### Chapter 19: Operations and Management

CFM fundamentals                                                        | 144  |
| Maintenance Domain (MD)                                               | 146  |
| Maintenance Association (MA)                                          | 146  |
| Maintenance association endpoints (MEP)                               | 147  |
| Fault verification                                                     | 148  |
| LBM message                                                           | 148  |
| l2ping                                                                | 148  |
| Fault isolation                                                       | 149  |
| Link trace message                                                    | 149  |
| l2traceroute                                                          | 150  |
| l2 tracetree                                                          | 151  |
| Maintenance domain intermediate points (MIP)                          | 151  |
| Layer 2 traceroute                                                    | 152  |
| Nodal MPs                                                             | 152  |
| Configuration considerations                                          | 153  |
| CFM configuration using ACLI                                          | 154  |
Contents

Troubleshooting IPv6 VRRP........................................................................................................... 231
VRRP transitions.......................................................................................................................... 231
Enabling trace messages for IPv6 VRRP troubleshooting............................................................... 232
Risks associated with enabling trace messages........................................................................ 233
VRRP with higher priority running as backup............................................................................... 234
Downgrading or upgrading from releases that support different key sizes......................... 234
Troubleshooting IPv6 connectivity loss....................................................................................... 235
Troubleshooting TACACS+........................................................................................................... 236
  Unable to log on using Telnet or rlogin....................................................................................... 236
  Unable to log on using SSH........................................................................................................ 240
  Unable to log on by any means (Telnet, rlogin, or SSH)............................................................. 242
  Administrator unable to obtain accounting information from the TACACS+ server............ 245
  Trap server cannot receive trap packets from the switch......................................................... 246
  Troubleshooting TACACS+ problems......................................................................................... 247
Troubleshooting RSMLT................................................................................................................ 249
  RSMLT peers not up.................................................................................................................... 249
  Enabling trace messages for RSMLT troubleshooting............................................................... 250
  Troubleshooting vlST failure...................................................................................................... 251

Chapter 21: Unicast routing troubleshooting................................................................................. 253
  Using BGP debugging commands............................................................................................. 253
  Troubleshooting licensed features............................................................................................ 255
  Viewing OSPF errors................................................................................................................ 256
  Viewing OSPF neighbor state problems.................................................................................... 257
  Troubleshooting OSPF Init state problems.............................................................................. 258
  Troubleshooting OSPF ExStart/Exchange problems................................................................. 259

Chapter 22: Multicast troubleshooting.......................................................................................... 261
  Multicast feature troubleshooting.............................................................................................. 261
    Troubleshooting IGMP Layer 2 Querier................................................................................ 261
    Troubleshooting IGMPv3 backwards compatibility................................................................. 265

Chapter 23: Multicast routing troubleshooting using ACLI........................................................ 267
  Viewing IGMP interface information.......................................................................................... 267
  Viewing multicast group trace information for IGMP snoop....................................................... 270
  Viewing IGMP group information.............................................................................................. 272
  Showing the hardware resource usage...................................................................................... 274
  Using PIM debugging commands............................................................................................. 275
  Determining the protocol configured on the added VLAN....................................................... 277
  Determining the data stream learned with IP Multicast over Fabric Connect on the VLAN.... 281
  Displaying the SPBM multicast database.................................................................................. 283
  Troubleshooting IP Multicast over Fabric Connect for Layer 2 VSNs......................................... 284
  Troubleshooting IP Multicast over Fabric Connect for Layer 3 VSNs......................................... 286
  Troubleshooting IP Multicast over Fabric Connect for IP Shortcuts........................................ 287
  Defining the IS-IS trace flag for IP multicast.......................................................................... 289

Chapter 24: Multicast routing troubleshooting using EDM.......................................................... 290
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing IGMP interface information</td>
<td>290</td>
</tr>
<tr>
<td>Viewing IGMP snoop trace information</td>
<td>292</td>
</tr>
<tr>
<td>Viewing IGMP group information</td>
<td>293</td>
</tr>
<tr>
<td>Viewing multicast group sources</td>
<td>294</td>
</tr>
<tr>
<td>Viewing multicast routes by egress VLAN</td>
<td>295</td>
</tr>
<tr>
<td>Enabling multicast routing process statistics</td>
<td>295</td>
</tr>
<tr>
<td>Determining the data stream learned when IP Multicast over Fabric Connect is configured on the VLAN</td>
<td>296</td>
</tr>
<tr>
<td>Showing the SPBM multicast database</td>
<td>297</td>
</tr>
<tr>
<td>Chapter 25: <strong>Transparent Port UNI</strong> feature troubleshooting using ACLI</td>
<td>298</td>
</tr>
<tr>
<td>Viewing all configured I-SIDs</td>
<td>298</td>
</tr>
<tr>
<td>Viewing C-MACs learned on T-UNI ports for an ISID</td>
<td>301</td>
</tr>
<tr>
<td>Viewing I-SID maximum MAC-limit</td>
<td>304</td>
</tr>
<tr>
<td>Chapter 26: <strong>Troubleshooting MACsec</strong></td>
<td>306</td>
</tr>
<tr>
<td>Viewing the MACsec connectivity association details</td>
<td>306</td>
</tr>
<tr>
<td>Viewing MACsec status</td>
<td>307</td>
</tr>
<tr>
<td>Chapter 27: <strong>Troubleshooting MACsec using EDM</strong></td>
<td>308</td>
</tr>
<tr>
<td>Viewing MACsec connectivity association details</td>
<td>308</td>
</tr>
<tr>
<td>Chapter 28: <strong>Troubleshooting Fabric Attach</strong></td>
<td>309</td>
</tr>
<tr>
<td>Troubleshooting Fabric Attach using the ACLI</td>
<td>309</td>
</tr>
<tr>
<td>Verify configuration of Fabric Attach</td>
<td>309</td>
</tr>
<tr>
<td>Verify LLDP port-level transmission and reception</td>
<td>312</td>
</tr>
<tr>
<td>Verify FA discovery and I-SID-to-VLAN mapping assignments</td>
<td>314</td>
</tr>
<tr>
<td>Troubleshooting Fabric Attach using the EDM</td>
<td>324</td>
</tr>
<tr>
<td>Verify configuration of Fabric Attach</td>
<td>324</td>
</tr>
<tr>
<td>Verify port-level transmission and reception</td>
<td>327</td>
</tr>
<tr>
<td>Verify FA discovery and I-SID-to-VLAN mapping assignments</td>
<td>332</td>
</tr>
<tr>
<td>Fabric Attach troubleshooting example</td>
<td>334</td>
</tr>
<tr>
<td>Troubleshooting FA Server rejection of I-SID-to-VLAN assignments using trace</td>
<td>334</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

Purpose

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Avaya Virtual Services Platform 4000 Series
- Avaya Virtual Services Platform 7200 Series
- Avaya Virtual Services Platform 8000 Series

This troubleshooting document describes common problems and error messages, provides information about traps and command logging, and provides techniques you can use to resolve common problems. This document provides troubleshooting information for Avaya Virtual Services Platform 4000 Series. This document also provides information about troubleshooting tools: for example, port mirroring.

For information on troubleshooting the Avaya Virtual Services Platform 7200 and Avaya Virtual Services Platform 8000, see Troubleshooting Avaya Virtual Services Platform 7200 Series and 8000 Series, NN47227-700.

Related resources

Documentation

See the Documentation Roadmap for Avaya Virtual Services Platform 4000 Series, NN46251-100 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, access the website at http://avaya-learning.com.
Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

• To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In Search, type Avaya Mentor Videos to see a list of the available videos.
  - In Search, type the product name. On the Search Results page, select Video in the Content Type column on the left.
• To find the Avaya Mentor videos on YouTube, go to 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 website.

  Note:

  Videos are not available for all products.

Subscribing to e-notifications

Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click Login.
3. Under My Information, select SSO login Profile.
4. Click E-NOTIFICATIONS.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click UPDATE.

6. Click OK.

7. In the PRODUCT NOTIFICATIONS area, click Add More Products.

8. Scroll through the list, and then select the product name.

9. Select a release version.

10. Select the check box next to the required documentation types.
11. Click **Submit**.

---

**Support**

Go to the Avaya Support website at [http://support.avaya.com](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.

---

**Searching a documentation collection**

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

**Before you begin**

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

**Procedure**

1. Extract the document collection zip file into a folder.

2. Navigate to the folder that contains the extracted files and open the file named `<product_name_release>.pdx`.
3. In the Search dialog box, select the option In the index named `<product_name_release>.pdx`.

4. Enter a search word or phrase.

5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments

6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.
Chapter 2: Safety messages

This section describes the different precautionary notices used in this document. This section also contains precautionary notices that you must read for the safe operation of Avaya Virtual Services Platform 4000 Series.

Notices

Notice paragraphs alert you about issues that require your attention. The following sections describe the types of notices.

Attention notice

⚠️ Important:

An attention notice provides important information regarding the installation and operation of Avaya products.

Caution ESD notice

⚠️ Electrostatic alert:

ESD

ESD notices provide information about how to avoid discharge of static electricity and subsequent damage to Avaya products.

⚠️ Electrostatic alert:

ESD (décharge électrostatique)

La mention ESD fournit des informations sur les moyens de prévenir une décharge électrostatique et d'éviter d'endommager les produits Avaya.

⚠️ Electrostatic alert:

ACHTUNG ESD

ESD-Hinweise bieten Information dazu, wie man die Entladung von statischer Elektrizität und Folgeschäden an Avaya-Produkten verhindert.

⚠️ Electrostatic alert:

PRECAUCIÓN ESD (Descarga electrostática)
Safety messages

El aviso de ESD brinda información acerca de cómo evitar una descarga de electricidad estática y el daño posterior a los productos Avaya.

⚠️ Electrostatic alert:

CUIDADO ESD
Os avisos do ESD oferecem informações sobre como evitar descarga de eletricidade estática e os consequentes danos aos produtos da Avaya.

⚠️ Electrostatic alert:

ATTENZIONE ESD
Le indicazioni ESD forniscono informazioni per evitare scariche di elettricità statica e i danni correlati per i prodotti Avaya.

Caution notice

⚠️ Caution:

Caution notices provide information about how to avoid possible service disruption or damage to Avaya products.

⚠️ Caution:

ATTENTION
La mention Attention fournit des informations sur les moyens de prévenir une perturbation possible du service et d'éviter d'endommager les produits Avaya.

⚠️ Caution:

ACHTUNG
Achtungshinweise bieten Informationen dazu, wie man mögliche Dienstunterbrechungen oder Schäden an Avaya-Produkten verhindert.

⚠️ Caution:

PRECAUCIÓN
Los avisos de Precaución brindan información acerca de cómo evitar posibles interrupciones del servicio o el daño a los productos Avaya.

⚠️ Caution:

CUIDADO
Os avisos de cuidado oferecem informações sobre como evitar possíveis interrupções do serviço ou danos aos produtos da Avaya.

⚠️ Caution:

ATTENZIONE
Le indicazioni di attenzione forniscono informazioni per evitare possibili interruzioni del servizio o danni ai prodotti Avaya.
Chapter 3: New in this document

The following section details what is new for this release in Troubleshooting of Avaya Virtual Services Platform 4000 Series, NN46251-700.

Features

Release 5.1.2
The following features are included in Release 5.1.2:

Secure syslog
This release introduces the Secure syslog feature that provides security for the communication path between a syslog server and a syslog client.

For more information, see:
- Secure syslog on page 38
- Configuring secure forwarding using ACLI on page 50
- Configuring cert-store with TLS using ACLI on page 52
- Configuring the system log table using EDM on page 64

SSH key sizes
This release updates SSH key sizes. This release accepts key sizes in multiples of 1024. The current key sizes are as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSA host key</td>
<td>1024</td>
</tr>
<tr>
<td>RSA host key</td>
<td>1024 or 2048</td>
</tr>
<tr>
<td>DSA user key</td>
<td>1024</td>
</tr>
</tbody>
</table>

Different releases can support different DSA host key, RSA host key, and DSA user key sizes. If you need to upgrade or downgrade to an earlier release that does not support the same key size, you must delete all of the keys from the .ssh directory and generate new keys for SSH. For more information about supported software, see Release Notes for VSP Operating System Software, NN47227-401.

For more information, see:
- Downgrading or upgrading from releases that support different key sizes on page 234.
Release 5.1.1
The following features are included in Release 5.1.1:

RMON1
This release supports RMON1 so the RMON alarm traps were added to Standard traps on page 87. RMON2 was already supported in a previous release.

Commands updates
The current release updates the following commands to add more modules and increase the module range.

<table>
<thead>
<tr>
<th>Command</th>
<th>Variables added</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config module</td>
<td>Adds the following modules: fa, fhs, ike, ipsec.</td>
</tr>
<tr>
<td>show trace modid-list</td>
<td>Updates the output to display more modules.</td>
</tr>
<tr>
<td>trace level</td>
<td>Expands the variable range to &lt;0–234&gt; to add new modules.</td>
</tr>
<tr>
<td>trace flags isis set</td>
<td>Adds the following trace flags: spf-intra, spf-inter, spf-extern, spbm-decide, debug, ip6–shortcut.</td>
</tr>
<tr>
<td>trace flags isis remove</td>
<td>Adds the following trace flags: spf-intra, spf-inter, spf-extern, spbm-decide, debug, ip6-shortcut.</td>
</tr>
</tbody>
</table>

• Using ACLI for troubleshooting on page 96.
• Using trace to diagnose problems on page 100.
• Using trace to examine IS-IS control packets on page 120.
• Using trace CFM to diagnose problems on page 178.
• Using trace SPBM to diagnose problems on page 181.
• Troubleshooting TACACS+ problems on page 247.
• Enabling trace messages for IGMP Layer 2 querier troubleshooting on page 263.
Chapter 4: Data collection required for Technical Support cases

Use the following sections to learn about how to gather information before you contact Avaya for technical support.

---

Data collection for an outage

Perform the following data collection procedures when Avaya Virtual Services Platform 4000 Series is in an outage condition and you require Avaya Technical Support to perform a root cause analysis.

---

Collecting data before you restart

**About this task**

Perform this procedure before you restart the chassis.

**Procedure**

1. Capture the current state of the chassis:
   
   ```
   terminal more disable
   show tech
   ```

2. Capture Flight Recorder trace information.
   
   ```
   flight-recorder all 1
   ```
   
   **This command executes three separate commands:** `flight-recorder snapshot`, `flight-recorder trace`, and `flight-recorder archive`.

3. Reset the chassis:
   
   ```
   reset -y
   ```

4. Continue with Collecting data after you restart on page 20.
Example

The following example shows output of the `flight-recorder all 1` command.

```
VSP-4850GTS-PWR+:1#flight-recorder all 1
Processing Flight-recorder snapshot for 1 ....
Flight-recorder snapshot for slot 1 complete, filename is /intflash/PMEM/1/pmem.20111019114431.1.bin.gz.
Processing Flight-recorder trace for 1 ....
Flight-recorder trace for slot 1 complete, filename is /intflash/flrec/1/trace.20111019114434.1.txt.
Processing Flight-recorder archive for slot 1 ....
Flight-recorder archive for slot 1 complete, filename is /intflash/archive/1/archive.20111019114446.1.tar.
```

Collecting data after you restart

About this task

Perform this procedure after you restart the affected chassis.

Procedure

1. Use FTP to transfer the following information:
   - configuration files from each chassis
     Configuration files are stored on the internal flash at /intflash/.
   - log files from each chassis
     Log files are stored on the internal flash at /intflash/.
   - generated archive files for slot
     The archive files are stored on the external flash at /intflash/archive/1. See Before You Restart The Chassis on page 19 for example output that shows how to identify the location and filename of the archive files.

2. Show core information:
   ```
   show core-files
   ```
   If the timestamp for an entry in the command output matches the time the outage first occurred, transfer the core files to an FTP server. Core files are stored on the internal flash at /intflash/coreFiles/.

3. Obtain the network diagram of the relevant nodes, down to the port level.
Data collection for non outage problems

Use the information in this section to collect data for problems that are less service-impacting than an outage.

Gathering critical information

This section identifies the critical information that you must gather before you contact Avaya Technical Support.

You must attempt to resolve the problem using this document. Contact Avaya as a final step taken only after you are unable to resolve the issue using the information and steps provided in this document.

Gather the following information before you contact Avaya Technical Support:

- a detailed description of the problem
- the date and time when the problem started
- the frequency of the problem
- if this is a new installation
- if there is information in the InSite Knowledge Base — Have you searched the InSite Knowledge Base? Were related problem solutions found? Is there currently a work around for this issue? You can search the InSite Knowledge Base on the Avaya Support site at www.avaya.com/support. Use the Advanced Search option to narrow your search to specific categories (products) and document types.
- if the system was recently upgraded — Have you recently changed or upgraded the system, the network, or a custom application? (For example, has configuration or code been changed?) When were these changes made? Provide the date and time. Who made these changes? Were the changes made by a partner or customer? Provide the names of the individuals who made the changes.
Chapter 5: Troubleshooting planning fundamentals

You can better troubleshoot the problems on the network by planning for these events in advance. To do this, you must know the following:

- that the system is properly installed and routinely maintained
- the configuration of the network
- the normal behavior of the network

Proper installation and routine maintenance

To prevent problems, follow proper maintenance and installation procedures. The following table lists the documents that provide maintenance and installation procedures.

Table 1: Maintenance and installation documentation

<table>
<thead>
<tr>
<th>Subject area</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation, environmental requirements</td>
<td>Installing Avaya Virtual Services Platform 4850GTS Series, NN46251-300</td>
</tr>
<tr>
<td>SFP and SFP+ installation and requirements</td>
<td>Installing Transceivers and Optical components on VSP Operating System Software, NN47227-301</td>
</tr>
</tbody>
</table>

Network configuration

To keep track of the network configuration, gather the information described in the following sections. This information, when kept up-to-date, is extremely helpful for locating information if you experience network or device problems.

Site network map

A site network map identifies where each device is physically located on site, which helps locate the users and applications that a problem affects. You can use the map to systematically search each part of the network for problems.
Logical connections
Avaya Virtual Services Platform 4000 Series supports virtual LANs (VLAN). With VLANs, you must know how the devices connect logically as well as physically.

Device configuration information
Maintain online and paper copies of the device configuration information. Store all online data with the regular data backup for the site. If the site does not use a backup system, copy the information onto an external storage device, and store the backup at an offsite location.

You can use the File Transfer Protocol (FTP) and Trivial FTP (TFTP) to store configuration files on a remote server.

Other important data about the network
For a complete picture of the network, have the following information available:

- all passwords
  Store passwords in a safe place. A good practice is to keep records of previous passwords in case you must restore a device to a previous software version and need to use the old password that was valid for that version.

- device inventory
  Maintain a device inventory, which lists all devices and relevant information for the network. The inventory allows you to easily see the device type, IP address, ports, MAC addresses, and attached devices.

- MAC address-to-port number list
  If you do not manage the hubs or switches, you must keep a list of the MAC addresses that correlate to the ports on the hubs and switches.

- change control
  Maintain a change control system for all critical systems. Permanently store change control records.

- contact details
  Store the details of all support contracts, support numbers, engineer details, and telephone and fax numbers.

Normal behavior on the network
If you are familiar with the network when it is fully operational, you can be more effective at troubleshooting problems that arise. To understand the normal behavior of the network, monitor the network over a long period of time. During this time you can see a pattern in the traffic flow, such as which devices users access most or when peak usage times occur.

To identify problems, you can use a baseline analysis, which is an important indicator of overall network health. A baseline serves as a useful reference of network traffic during normal operation, which you can then compare to captured network traffic while you troubleshoot network problems. A baseline analysis speeds the process of isolating network problems. By running tests on a healthy...
network, you compile normal data for your network. You can compare this normal data against the 
results that you get when the network experiences trouble.

For example, ping each node to discover how long it typically takes to receive a response from 
devices on your network. Capture and save each response time and you can use these baseline 
response times to help you troubleshoot. You can also use the **show tech** and **show khi 
performance {buffer-pool|cpu|memory|process|pthread|slabinfo}** commands to obtain baseline output for normal system behavior.

**Example**

```
VSP-4K-R1-BEB-5-HighTemp:1(config)#show khi performance memory
  Slot:1
    Used: 702380 (KB)
    Free: 1373656 (KB)
    Current utilization: 33 %
    5-minute average utilization: 33 %
    5-minute high water mark: 33 (02/10/15 13:03:25)

VSP-4K-R1-BEB-5-HighTemp:1#show tech
Sys Info:
--------------
General Info :
  SysDescr     : VSP-4450GTXHT-PWR+ (4.1.0.0)
  SysName      : VSP-4K-R1-BEB-5-HighTemp
  SysUpTime    : 0 day(s), 00:25:41
  SysContact   : http://support.avaya.com/
  SysLocation  : 211 Mt. Airy Road,Basking Ridge,NJ 0792
Chassis Info:
  Chassis            : 4450GTXHT-PWR+
  Serial#            : SDNIV44P0009
  H/W Revision       : R0A
  H/W Config         : none
  NumSlots           : 1
  NumPorts           : 50
  BaseMacAddr        : b0:ad:aa:54:d8:00
  MacAddrCapacity    : 256
  Temperature        : 31
  System MTU         : 9600
--More-- (q = quit)
```
Chapter 6: Troubleshooting fundamentals

This section provides conceptual information and helpful tips for common problems.

Connectivity problems

Use the following general tasks to isolate connectivity problems:

- Check physical connectivity. Verify if an alarm for link or port down exists.
- Check the link state by viewing the `show interface {gigabitEthernet|loopback|vlan}` command output.
- Use tools like ping or trace to verify if the connectivity issue is localized to an individual port or VLAN.
- Try to localize the affected range of ports and slot.

If you contact technical support staff to help troubleshoot connectivity problems, always provide source and destination IP pairs to facilitate in troubleshooting. Be sure to provide both working and non-working pairs for comparison.

Example

VSP-4850GTS:1#show interface vlan

```
===============================================================================================
Vlan Basic
===============================================================================================
VLAN ID   NAME             TYPE         MSTP INST_ID PROTOCOLID   SUBNETADDR      SUBNETMASK      VRFID
-----------------------------------------------------------------------------------------------
1  Default          byPort       0       none         N/A             N/A       0
16 VLAN-16         spbm-bvlan   62      none         N/A             N/A       0
32 VLAN-32         spbm-bvlan   62      none         N/A             N/A       0
50 VLAN-50         byPort       0       none         N/A             N/A       0
60 VLAN-60         byPort       0       none         N/A             N/A       0
70 VLAN-70         byPort       0       none         N/A             N/A       0
90 VLAN-90         byPort       0       none         N/A             N/A       0
100 VLAN-100        byPort       0       none         N/A             N/A       0
102 VLAN-102        byPort       0       none         N/A             N/A       0
All 9 out of 9 Total Num of Vlans displayed
===============================================================================================
Vlan Port
===============================================================================================
VLAN PORT ID MEMBER ACTIVE MEMBER STATIC MEMBER NOT_ALLOW MEMBER
-----------------------------------------------------------------------------------------------
1
```

Comments on this document? infodev@avaya.com
Routing table problems

Routing table problems include but are not limited to:

- inactive routes
- unnecessary routes
- black hole routes
- flapping links (links that go up and come down) that cause the routes to flap
- incorrect route tables
- invalid Address Resolution Protocol (ARP) cache that causes incorrect IP to MAC assignment
- problems with administrative distance or other parameters

Do not restart a device to clear a problem. In restarting the device, you also clear the logs. Logs are vital and can help determine many problems.

LED indications of problems

For information on LEDs on the chassis refer to:

- Installing Avaya Virtual Services Platform 4850GTS Series, NN46251-300
- Installing Avaya Virtual Services Platform 4450GTX-HT-PWR+ Switch, NN46251–304
- Installing Avaya Virtual Services Platform 4450GSX-PWR+ Switch, NN46251-307
Cable connection problems

You can usually trace port connection problems to a poor cable connection or to an improper connection of the port cables at either end of the link. To remedy such problems, make sure that the cable connections are secure and that the cables connect to the correct ports at both ends of the link. If you use homemade cables, ensure that the cables are wired correctly.

1000BASE-T cables

1 Gb/s ports operate using Category 5 UTP cabling only. Category 5 UTP cable is a two-pair cable. To minimize crosstalk noise, maintain the twist ratio of the cable up to the point of termination; untwist at termination cannot exceed 0.5 in. (1.27 cm).

SFP and SFP+ cables

Cables for the optical transceivers vary depending on the specific device type. For more information about the cable requirements for Small Form Factor Pluggable (SFP) and SFP plus (SFP+), see Installing Transceivers and Optical components on VSP Operating System Software, NN47227-301.

Alarm database

Avaya Virtual Services Platform 4000 Series contains a local alarms mechanism. Local alarms are raised and cleared by applications running on the switch. View active alarms by using the `show alarm database` command in the ACLI. Local alarms are an automatic mechanism run by the system that do not require additional configuration.

Check local alarms regularly to ensure no alarms require additional attention. The raising and clearing of local alarms also creates a log entry for each event. For more information about viewing logs, see Viewing Logs on page 58.

View the alarm database regularly to monitor alarm conditions, even if you do not observe a performance problem. Review the alarm messages to determine if the system performs as expected.

Not all alarm conditions indicate a problem so you must be familiar with expected behavior.

Example

The alarm database can show the following alarm text:

CP1 [01/01/70 00:03:06.796] 0x00010844 00000000 Global Router HW WARNING
USB found in slot 1 has VendorId 05dc ProductId a01a and Manufacturer Lexar and did not match supported devices

This alarm means that you have tried to insert an unsupported USB into the USB slot. Only the USB provided with your VSP 4000 system can be inserted into the USB slot.
Chapter 7: Troubleshooting tool fundamentals

This section provides conceptual information about the methods and tools that you can use to troubleshoot and isolate problems in the Avaya Virtual Services Platform 4000 Series network.

Troubleshooting overview

The types of problems that typically occur with networks involve connectivity and performance. Virtual Services Platform 4000 supports a diverse range of network architectures and protocols, some of which maintain and monitor connectivity and isolate connectivity faults.

In addition, Virtual Services Platform 4000 supports a wide range of diagnostic tools that you can use to monitor and analyze traffic, capture and analyze data packets, trace data flows, view statistics, and manage event messages.

Certain protocols and tools are tailored for troubleshooting specific Virtual Services Platform 4000 network topologies. Other tools are more general in their application and you can use them to diagnose and monitor ingress and egress traffic on Virtual Services Platform 4000.

If connectivity problems occur and the source of the problem is unknown, it is usually best to follow the Open Systems Interconnection (OSI) network architecture layers. Confirm that your physical environment, such as the cables and module connections, operates without failures before moving up to the network and application layers.

To gather information about a problem, consider the following information:

- Consider the OSI model when you troubleshoot. Start at Layer 1 and move upwards. The Address Resolution Protocol (ARP) can cause problems; ARP operates at Layer 2 to resolve MAC addresses to IP addresses (Layer 3).
- Device-specific tools and protocols can help you gather information. This document outlines Virtual Services Platform 4000-specific tools.
- You can use client- and server-based tools from Microsoft, Linux, and UNIX. For example, you can use Windows tools like ifconfig, ipconfig, winipcfg, and route print to obtain IP information and routing tables. Servers also maintain route tables.

The following command output shows example output of the route print command.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\jsmith>route print
===============================================================================
Refer to page 28 for more information.
Interface List

0x1 ........................... MS TCP Loopback interface
0x2 ...00 12 f0 74 2a 87 ...... Broadcom NetLink (TM) Gigabit Ethernet - Packet Scheduler Miniport
0x3 ...00 14 38 08 19 c6 ...... Broadcom NetXtreme Gigabit Ethernet - Packet Scheduler Miniport
0x4 ...44 45 53 54 42 00 ...... Avaya IPSECSHM Adapter - Packet Scheduler Miniport

===============================================================================

Active Routes:

<table>
<thead>
<tr>
<th>Network</th>
<th>Destination</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.0.1</td>
<td>192.168.0.102</td>
<td>26</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>207.179.154.100</td>
<td>207.179.154.100</td>
<td>1</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>255.0.0.0</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.0</td>
<td>255.255.255.0</td>
<td>192.168.0.102</td>
<td>192.168.0.102</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.0</td>
<td>255.255.255.0</td>
<td>207.179.154.100</td>
<td>207.179.154.100</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.102</td>
<td>255.255.255.255</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>25</td>
</tr>
<tr>
<td>192.168.0.255</td>
<td>255.255.255.255</td>
<td>192.168.0.102</td>
<td>192.168.0.102</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.255</td>
<td>255.255.255.255</td>
<td>207.179.154.100</td>
<td>207.179.154.100</td>
<td>1</td>
</tr>
<tr>
<td>207.179.154.0</td>
<td>255.255.255.0</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>30</td>
</tr>
<tr>
<td>207.179.154.100</td>
<td>255.255.255.255</td>
<td>207.179.154.100</td>
<td>207.179.154.100</td>
<td>30</td>
</tr>
<tr>
<td>207.179.154.255</td>
<td>255.255.255.255</td>
<td>207.179.154.100</td>
<td>207.179.154.100</td>
<td>1</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>207.179.154.100</td>
<td>207.179.154.100</td>
<td>1</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>207.179.154.100</td>
<td>207.179.154.100</td>
<td>1</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>207.179.154.100</td>
<td>207.179.154.100</td>
<td>1</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>207.179.154.100</td>
<td>207.179.154.100</td>
<td>1</td>
</tr>
</tbody>
</table>

Default Gateway: 207.179.154.100

===============================================================================

Persistent Routes: None

- Other network problems can give the impression that a device has a problem. For instance, problems with a Domain Name Service (DNS) server, another switch, firewall, or access point can can appear to be routing problems.

---

Digital Diagnostic Monitoring

Use Digital Diagnostic Monitoring (DDM) to monitor laser operating characteristics such as temperature, voltage, current, and power. This feature works during active laser operation without affecting data traffic. Small Form Factor Pluggable (SFP) transceivers support DDM. Use the ACLI command `show pluggable-optical-modules {basic|config|detail|temperature|voltage}` to make use of DDM functionality.

An interface that supports DDM is a Digital Diagnostic Interface (DDI). These devices provide real-time monitoring of individual DDI SFPs on a variety of Avaya products. The DDM software provides warnings or alarms when the temperature, voltage, laser bias current, transmitter power or receiver power fall outside of vendor-specified thresholds during initialization.

For information about DDM and SFPs, see *Installing Transceivers and Optical components on VSP Operating System Software, NN47227-301*, and *Performance Management of Avaya Virtual Services Platform 4000 Series, NN46251-701.*
Example

VSP-4850GTS-PWR+:1#show pluggable-optical-modules config

================================================================================
Pluggable Optical Module Global Configuration
================================================================================
ddm-monitor : disabled
ddm-monitor-interval : 5
ddm-traps-send : enabled
ddm-alarm-portdown : disabled

Flight Recorder

The Flight Recorder is a high level term for the framework in place on Virtual Services Platform 4000 to store both history and current state information for various kernel, system, and application data with minimal overhead to execution. This data can later be accessed on-demand when debugging systems issues to give engineers the best possible troubleshooting information. Functionally, the Flight Recorder consists of two elements; Persistent Memory and Always-on Trace.

The Persistent Memory feature stores information in volatile memory outside of any process. This feature provides information on crashes, errors, and outages that are not the result of a power failure. Persistent Memory data not saved to non-volatile storage before a power failure will be lost. Persistent Memory snapshots are taken when:

- a critical process stops functioning
- a process stops responding
- the hardware watchdog activates
- the user initiates a snapshot in the ACLI

The Always-on Trace feature creates an ongoing, circular log of every trace call recently executed regardless of the trace level enabled by the user. The Always-On Trace feature uses circular logging, and therefore stores the most recent traces of the process.

Flight Recorder functionality is provided only through ACLI. The following commands are used to make use of this feature:

- **flight-recorder snapshot 1**
  This command takes a snapshot of all flight-recorder files, log files, and configuration files.
- **flight-recorder trace 1**
  This command takes snapshot of always-on-trace data.
- **flight-recorder all 1**
  The command creates a flight-recorder snapshot, trace and archive.
- **flight-recorder archive 1**
  This command creates a tarball of flight-recorder files, log files and configuration files.
Port mirroring

Virtual Services Platform 4000 has a port mirroring feature that helps you monitor and analyze network traffic. Port mirroring supports both ingress (incoming traffic) and egress (outgoing traffic) port mirroring. When you enable port mirroring, the system forwards ingress or egress packets normally from the mirrored (source) port, and sends a copy of the packet to the mirroring (destination) port.

Overview

Port mirroring causes the switch to make a copy of a traffic flow and send the copy to a device for analysis. Use port mirroring in diagnostic sniffing—use the mirror to view the packets in the flow without breaking the physical connection to place a packet sniffer inline. You can also use mirroring for security reasons.

You can use egress mirroring to monitor packets as they leave specified ports.

Use a network analyzer to observe and analyze packet traffic at the mirroring port. Unlike other methods that analyze packet traffic, the packet traffic is uninterrupted and packets flow normally through the mirrored port.

You can mirror to a port or list of ports or a MultiLink Trunking (MLT) group. Virtual Services Platform 4000 supports one-to-many, many-to-one, and many-to-many mirroring configurations.

Port mirroring and modules

You can use all module ports in the system to function as an ingress port for mirroring (mirrored port), an egress port for mirroring (mirrored port), or as a mirroring port (where all the mirrored traffic is redirected. The number of mirroring ports (also called destination ports) that you can configure is limited by the hardware. The hardware limitation is 4 ports simultaneously (where each mirroring direction counts as one). For example, if two mirroring ports are designated to mirror both ingress and egress traffic then all 4 mirroring ports are consumed.

The following table describes ingress mirroring functionality for modules. Only one type of mirroring destination is supported at a time. You cannot mirror the same port to multiple classes of destinations, for example, MLT. However, you can mirror to multiple physical destinations.

Table 2: Ingress mirroring functionality

<table>
<thead>
<tr>
<th>Function</th>
<th>Support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress port mirroring and ingress flow mirroring</td>
<td>Supported. Maximum of 4 mirror-to-ports per box.</td>
</tr>
<tr>
<td>One port to one port</td>
<td>Supported</td>
</tr>
<tr>
<td>One to MLT group [for threat protection system (TPS applications)]</td>
<td>Supported</td>
</tr>
<tr>
<td>One to many (multicast group ID/VLAN)</td>
<td>Not supported</td>
</tr>
<tr>
<td>One to one (remote mirrored destination)</td>
<td>Not supported</td>
</tr>
<tr>
<td>Many to one (multiple mirrored ports to one mirroring port)</td>
<td>Supported</td>
</tr>
<tr>
<td>Many to MLT group</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Function</th>
<th>Support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many to many (VLAN/multicast group ID) (multiple ports with several different destinations)</td>
<td>Not supported</td>
</tr>
<tr>
<td>Many to one (relation between Remote Mirror Source [RMS] and Remote Mirror Termination [RMT])</td>
<td>Not supported</td>
</tr>
<tr>
<td>VLAN and port combination as a mirroring destination</td>
<td>Not supported</td>
</tr>
<tr>
<td>Ingress flow mirroring</td>
<td>Supported</td>
</tr>
<tr>
<td>Allow filters to specify a separate destination for each access control entry</td>
<td>Supported</td>
</tr>
</tbody>
</table>

The following table describes egress mirroring functionality.

**Table 3: Egress mirroring functionality**

<table>
<thead>
<tr>
<th>Function</th>
<th>Support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress port mirroring and egress flow mirroring</td>
<td>Supported</td>
</tr>
<tr>
<td>One port to one port</td>
<td>Supported</td>
</tr>
<tr>
<td>One to MLT groups (for TPS applications)</td>
<td>Supported</td>
</tr>
<tr>
<td>One to many (multicast group ID/VLAN)</td>
<td>Not supported</td>
</tr>
<tr>
<td>Many to one (multiple mirrored ports to one mirroring port)</td>
<td>Supported</td>
</tr>
<tr>
<td>Many to MLT group</td>
<td>Supported</td>
</tr>
<tr>
<td>Many to many (multicast group ID) (multiple ports with several different destinations)</td>
<td>Supported</td>
</tr>
<tr>
<td>Many to one (relation between Remote Mirror Source [RMS] and Remote Mirror Termination [RMT])</td>
<td>Not supported</td>
</tr>
<tr>
<td>VLAN and port combination as mirroring destination</td>
<td>Not supported</td>
</tr>
<tr>
<td>Egress flow mirroring</td>
<td>Supported</td>
</tr>
<tr>
<td>Allow filter to specify a separate destination for each access control entry</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**Module configuration**

You can specify a destination multilink trunking (MLT) group, a destination port or set of ports.

Interface modules support two port mirroring modes: rx (ingress, that is, inPort) and tx (egress, that is, outPort). Configure the mirroring action globally in an access control list (ACL), or for a specific access control entry (ACE) by using the ACE mirror actions. Configure the mirroring destination by using an ACE.

In rx modes, when you configure the ACE mirror or ACL global options to mirror, use the ACE to configure the mirroring destination port.
To modify a port mirroring instance, first disable the instance. Also, to change a port or MLT entry, first remove whichever parameter is attached to the entry, and then add the required entry.

**ACLs, ACEs, and port mirroring**

You can configure an ACL or an ACE to perform the mirroring operation. To do so, you can configure the ACL global action to mirror, or you can configure the ACE action to mirror. If you use the global action, mirroring applies to all ACEs that match in an ACL.

To decouple flow-based mirrors from port-based mirrors, ACEs use a parameter called mirror, which you can configure to specific mirror to MLT ID, VLAN, port, or port list.

You can use filters to reduce the amount of mirrored traffic. To use filters with port mirroring, you must use an ACL-based filter. Apply an ACL to the mirrored port in the egress and ingress directions. Traffic patterns that match the ACL or ACE with an action of permit are forwarded to the destination and also to the mirroring port. Traffic patterns that match an ACE with an action of drop (deny) are not forwarded to the destination, but still reach the mirroring port. For example, for an ACL or ACE with a match action of permit and debug mirroring enabled, packets are mirrored to the specified mirroring destination on the ACE. If you enable a port or VLAN filter, that filter is the mirroring filter.

You can specify more than one mirroring destination by using multiple ACEs. Use each ACE to specify a different destination.

You can configure a port-based and a flow-based mirroring filter on the same port. If such a case occurs, then the flow-based mirror takes precedence.

For more information about how to configure ACLs and ACEs, see *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502.

**Port mirroring considerations and restrictions**

Although you can configure Virtual Services Platform 4000 to monitor both ingress and egress traffic, some restrictions apply:

- VSP 7000 and VSP 8000 do not support true egress mirroring. Of the VOSS platforms, only VSP 4000 supports true egress mirroring.

  On the VSP 7000 and VSP 8000, egress mirrored packets can differ from the packets egressing the port due to the hardware limitation.

- Mirrored traffic shares ingress queue and fabric bandwidth with normal traffic and therefore can impact normal traffic. Therefore, use these features with this potential consequence in mind and enable them only for troubleshooting, debugging, or for security purposes such as packet sniffing, intrusion detection, or intrusion prevention.

- You can configure as many ingress mirroring flows as you have filters.

- To avoid VLAN members from seeing mirrored traffic, you must remove mirroring (destination) ports from all VLANs.

- The MAC drops an errored packet, for example, packets that are too short or too long. Control packets consumed by the MAC (802.3x flow control) are also not mirrored.

- Certain control packets generated by the CP, such as CFM, STG BPDUs, SONMP, EAPOL, LACP, VLACP, TDP, and LLDP cannot be egress mirrored due to HW limitations.

- VSP 4000 supports a maximum of 256 IPv6 ingress port/vlan security ACL/filters. IPv6 ingress QoS ACL/Filters and IPv6 Egress Security and QoS ACL/Filters are not supported.
General diagnostic tools

Virtual Services Platform 4000 has diagnostic features available with Enterprise Device Manager (EDM) and Avaya command line interface (ACLI). You can use these diagnostic tools to help you troubleshoot operational and configuration issues. You can perform such tasks as configuring and displaying log files, viewing and monitoring port statistics, tracing a route, running loopback and ping tests, and viewing the address resolution table.

For more information about statistics, see Performance Management of Avaya Virtual Services Platform 4000 Series, NN46251-701.

Traceroute

Traceroute determines the path a packet takes to reach a destination by returning the sequence of hops (IP addresses) the packet traverses.

According to RFC1393, traceroute operates by: "sending out a packet with a time-to-live (TTL) of 1. The first hop then sends back an ICMP error message indicating that the packet could not be forwarded because the TTL expired. The packet is then resent with a TTL of 2, and the second hop returns the TTL expired. This process continues until the destination is reached. The purpose behind this is to record the source of each ICMP TTL exceeded message to provide a trace of the path the packet took to reach the destination."

Ping

Ping is a simple and useful diagnostic tool to determine reachability. When you use ping, the switch sends an ICMP echo request to a destination IP address. If the destination receives the packet, it responds with an ICMP echo response.

If a ping test is successful, the destination is alive and reachable. Even if a router is reachable, it could have improperly working interfaces or corrupted routing tables.

Trace

Use trace commands to provide detailed data collection about software modules on Virtual Services Platform 4000. The trace toolset can be used to trace multiple modules simultaneously and provides options to specify the verbosity level of the output.

You can enable trace logging through the boot config trace-logging flag.

⚠️ Caution:

Risk of traffic loss

Using the trace tool inappropriately can cause a CPU lockup conditions, loss of access to the switch, loss of protocols, and service degradation.

While these occurrences are uncommon, when using the trace level tool, minimize this risk. Avaya recommends:

- In situations where trace data is required concurrently from multiple modules, consider troubleshooting during a maintenance window if feasible. Consider a maintenance window period if the switch is stable but CPU utilization is high and CPU traces (example trace levels 9 and 11) are required to diagnose the cause.

- Run trace commands from the console port when the CPU utilization is already high. While you can enable or disable tracing when directly connected to the console port.
Activate tracing on one software module at a time.

• Initially activate tracing at lower verbosity settings (that is, 2 rather than 3). Increase to verbosity level 3 or 4 only if required, and after level 2 runs safely.

• Avoid leaving traces active for extended periods of time. For high CPU utilizations, a few seconds (typically less than 5 seconds) is generally sufficient to identify the cause for sustained high CPU utilization.
Chapter 8: Log and trap fundamentals

Use the information in this section to help you understand Simple Network Management Protocol (SNMP) traps and log files, available as part of Avaya Virtual Services Platform 4000 Series System Messaging Platform.

Overview of traps and logs

System log messaging

On a UNIX-based management platform, you can use system log (syslog) messaging to manage event messages. The switch syslog software communicates with a server software component named syslogd on the management workstation.

The UNIX daemon syslogd is a software component that receives and locally logs, displays, prints, and forwards messages that originate from sources internal and external to the workstation. For example, syslogd on a UNIX workstation concurrently handles messages received from applications that run on the workstation, as well as messages received from the switch that run in a network accessible to the workstation.

The remote UNIX management workstation performs the following actions:

- Receives system log messages from the switch.
- Examines the severity code in each message.
- Uses the severity code to determine appropriate system handling for each message.

Log consolidation

Virtual Services Platform generates a system log file and can forward that file to a syslog server for remote viewing, storage and analyzing.

The system log captures messages for the following components:

- Extensible Authentication Protocol (EAP)
- Remote Authentication Dial-in User Service (RADIUS)
- Remote Monitoring (RMON)
- Web
- hardware (HW)
- MultiLink Trunking (MLT)
- filter
Quality of Service (QoS)
Command line interface (CLI) log
software (SW)
Central Processing Unit (CPU)
Internet Protocol (IP)
Virtual Local Area Network (VLAN)
policy
Simple Network Management Protocol (SNMP) log

The switch can send information in the system log file, including ACLI command log and the SNMP operation log, to a syslog server.

View logs for CLILOG module to track all ACLI commands executed and for fault management purposes. The ACLI commands are logged to the system log file as CLILOG module.

View logs for SNMPLOG module to track SNMP logs. The SNMP operation log is logged to the system log file as SNMPLOG module.

The platform logs CLILOG and SNMPLOG as INFO. Normally, if you configure the logging level to WARNING, the system skips all INFO messages. However, if you enable CLILOG and SNMPLOG the system logs ACLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

System log client over IPv6 transport
You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration except in the following case. When you configure the system log table in EDM, under the System Log Table tab, you must select either IPv4 or IPv6.

Log messages with enhanced secure mode
Enhanced secure mode allows the system to provide role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use. If you enable enhanced secure mode, the system encrypts the entire log file.

With enhanced secure mode enabled, only individuals in the administrator or auditor role can view log files to analyze switch access and configuration activity. However, no access level role can modify the content of the log files, not even the administrator or the auditor access level roles. The administrator has access to the remove and delete commands.

If you enable enhanced secure mode, you cannot access the following commands for log files at any role-based access level:

- more
- edit
- rename
- copy

If someone attempts to access a log file with the preceding commands, an information and warning message displays on the screen.

The following table summarizes log file command access based on role-based access levels.
Table 4: Log commands accessible for various users

<table>
<thead>
<tr>
<th>Access level role</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>The remove and delete commands.</td>
</tr>
<tr>
<td>No user at any access level.</td>
<td>The following commands:</td>
</tr>
<tr>
<td></td>
<td>• more</td>
</tr>
<tr>
<td></td>
<td>• edit</td>
</tr>
<tr>
<td></td>
<td>• rename</td>
</tr>
<tr>
<td></td>
<td>• copy</td>
</tr>
<tr>
<td>Administrator</td>
<td>All configuration commands can only be accessed by the individual in the administrator role, other than the preceding commands.</td>
</tr>
<tr>
<td>Administrator and auditor</td>
<td>All show commands for log files.</td>
</tr>
<tr>
<td>All users (Administrator, auditor, security, privilege, operator.)</td>
<td>All show commands for log configurations.</td>
</tr>
</tbody>
</table>

With enhanced secure mode enabled, authorized users can use SFTP to transfer files to a remote server with the content encrypted.

**SNMP traps**

The SNMP trap is an industry-standard method used to manage events. You can set SNMP traps for specific types of log message (for example, warning or fatal), from specific applications, and send them to a trap server for further processing. For example, you can configure the switch to send SNMP traps to a server after a port is unplugged or if a power supply fails.

This document only describes SNMP commands related to traps. For more information about how to configure SNMP community strings and related topics, see *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601.

**Secure syslog**

Syslog is a standard used to send event log messages to devices within a network. The switch sends event messages to a logging server called syslog server. The syslog server stores the log messages and displays them for event reporting. Syslog messages are used for monitoring system activities and troubleshooting.

The secure syslog feature adds security and authenticated access to the plain text event log messages that are communicated between a remote syslog server and a syslog client. Secure syslog feature helps prevent unauthorized access to confidential data transmitted on an unsecured communication channel between a remote syslog server and client.

To implement the security, this feature employs port forwarding using the Secure Shell (SSH) cryptography protocol and Transport Layer Security (TLS) to provide the secure connection between syslog server and client.
After starting the syslog server, to ensure authentication, you must setup a remote port forwarding connection to connect the switch with the remote SSH client or the remote TLS server.

**Secure syslog using SSH:**

The syslog server is installed on a host that serves as SSH client. The SSH client requests a connection with the SSH server that resides on the switch. A remote port forwarding connection, called secure-forwarding, gets established between the syslog server and the switch. The syslog server now listens for the log messages on the port 601 at the end of the secure channel. The syslog server decrypts the received log messages and either stores or displays the messages.

**Secure syslog using TLS:**

The syslog server is installed on a host that serves as TLS server. The switch plays the role of a TLS client. A TLS handshake is initiated between the syslog server and the switch. The syslog server transmits a certificate which has subject common name and optional subject alternative name (SAN). Subject common name is always present in the certificate but SAN is optional. The server-cert-name must match with SAN name if present in the certificate else if SAN name is not present, it must match with the Subject Common Name else TLS negotiation fails and the connection to the server is closed. If the server-cert-name part is not configured, then the check is not done.

Once the TLS handshake is successful, the log messages sent from the switch to the syslog server are encrypted. The syslog server decrypts these messages using a private key. The server then stores the messages or forwards them to other servers.

**Supported syslog servers:**

This feature supports the following syslog servers:

- For SSH tunneling — WinSyslog, which is the Windows OS based syslog server.
- For TLS tunneling — Rsyslog, which is a Linux based open source syslog server.

---

**Simple Network Management Protocol**

The Simple Network Management Protocol (SNMP) provides facilities to manage and monitor network resources. SNMP consists of:

- **Agents**—An agent is software that runs on a device that maintains information about device configuration and current state in a database.
- **Managers**—An SNMP manager is an application that contacts an SNMP agent to query or modify the agent database.
- **The SNMP protocol**—SNMP is the application-layer protocol SNMP agents and managers use to send and receive data.
- **Management Information Bases (MIB)**—The MIB is a text file that specifies the managed objects by an object identifier (OID).
**Important:**

The switch does not reply to SNMP requests sent to the Virtual Router Redundancy Protocol (VRRP) virtual interface address; it does, however, reply to SNMP requests sent to the physical IP address.

An SNMP manager and agent communicate through the SNMP protocol. A manager sends queries and an agent responds; however, an agent initiates traps. Several types of packets transmit between SNMP managers and agents:

- Get request—This message requests the values of one or more objects.
- Get next request—This message requests the value of the next object.
- Set request—This message requests to modify the value of one or more objects.
- Get response—An SNMP agent sends this message in response to a get request, get next request, or set request message.
- Trap—SNMP trap is a notification triggered by events at the agent.

---

**Log message format**

The log messages for the switch have a standardized format. All system messages are tagged with the following information, except that alarm type and alarm status apply to alarm messages only:

- Avaya proprietary (AP) format—Provides encrypted information for debugging purposes
- CPU slot number—Indicates the CP slot where the command is logged.
- timestamp—Records the date and time at which the event occurred. The format is MM/DD/YY hh:mm:ss.uuu, where uuu is milliseconds. Example: [11/01/10 11:41:21.376].
- event code—Precisely identifies the event reported.
- alarm code—Specifies the alarm code.
- alarm type—identifies the alarm type (Dynamic or Persistent) for alarm messages
- alarm status—identifies the alarm status (set or clear) for alarm messages
- VRF name—Identifies the Virtual Routing and Forwarding (VRF) instance, if applicable.
- module name—Identifies the software module or hardware from which the log is generated.
- severity level—Identifies the severity of the message.
- sequence number—Identifies a specific CLI command.
- context—Specifies the type of the session used to connect to the switch. If the session is a remote session, the remote IP address is identified.
- user name—Specifies the user name used to login to the switch.
- ACLI command—Specifies the commands typed during the ACLI session. The system logs anything type during the ACLI session as soon as the user enters the Enter key.
The following messages are examples of an informational message for CLILOG:


CP1 [07/18/14 13:24:19.739] 0x002c0600 00000000 GlobalRouter CLILOG INFO 15 TELNET: 135.55.40.200 rwa term more en

CP1 [07/18/14 13:24:22.577] 0x002c0600 00000000 GlobalRouter CLILOG INFO 16 TELNET: 135.55.40.200 rwa show log

CP1 [01/12/70 15:13:59.056] 0x002c0600 00000000 GlobalRouter CLILOG INFO 5 TELNET: 47.17.170.108 rwa syslog host 4

CP1 [01/12/70 15:13:35.520] 0x002c0600 00000000 GlobalRouter CLILOG INFO 4 TELNET: 47.17.170.108 rwa syslog host enable

CP1 [01/12/70 15:13:14.576] 0x002c0600 00000000 GlobalRouter CLILOG INFO 3 TELNET: 47.17.170.108 rwa show syslog

CP1 [01/12/70 15:12:44.640] 0x002c0600 00000000 GlobalRouter CLILOG INFO 2 TELNET: 47.17.170.108 rwa show logging file tail

The following messages are examples of an informational message for SNMPLOG:

CP1 [05/07/14 10:24:05.468] 0x002c4600 00000000 GlobalRouter SNMPLOG INFO 1 ver=v2c  public rcVlanPortMembers.2 = [value]

CP1 [05/07/14 10:29:58.133] 0x002c4600 00000000 GlobalRouter SNMPLOG INFO 2 ver=v2c  public rcVlanPortMembers.2 = [value]

CP1 [05/07/14 10:30:20.466] 0x002c4600 00000000 GlobalRouter SNMPLOG INFO 3 ver=v2c  public rcVlanPortMembers.1 = [value]

The following messages are examples of an informational message for system logs:

CP1 [07/24/14 18:04:08.304] 0x00000670 00000000 GlobalRouter SW INFO Basic license supports all features on this device

CP1 [07/24/14 18:04:10.651] 0x00034594 00000000 GlobalRouter SW INFO System boot

CP1 [07/24/14 18:04:10.651] 0x00034595 00000000 GlobalRouter SW INFO VSP-8200 System Software Release 0.0.0.0_B553

CP1 [07/24/14 18:04:10.779] 0x00010774 00000000 GlobalRouter HW INFO Detected 8 284XSQ chassis

CP1 [07/24/14 18:04:10.779] 0x00010830 00000000 GlobalRouter HW INFO Detected 8242XSQ module (Serial#: SDNIV84Q2013) in slot 2

The system encrypts AP information before writing it to the log file. The encrypted information is for debugging purposes. Only an Avaya Customer Service engineer can decrypt the information. ACLI commands display the logs without the encrypted information. Avaya recommends that you do not edit the log file.

The following table describes the system message severity levels.
### Table 5: Severity levels

<table>
<thead>
<tr>
<th>Severity level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMERGENCY</td>
<td>A panic condition that occurs when the system becomes unusable. Usually a severity level of emergency is usually a condition where multiple applications or server are affected. You must correct a severity level of alert immediately.</td>
</tr>
<tr>
<td>ALERT</td>
<td>Any condition requiring immediate attention and correction. You must correct a severity level of alert immediately, but usually indicates failure of a secondary system, such as an Internet Service Provider connection.</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Any critical conditions, such as a hard drive error.</td>
</tr>
<tr>
<td>ERROR</td>
<td>A nonfatal condition occurred. You can be required to take appropriate action. For example, the system generates an error message if it is unable to lock onto the semaphore required to initialize the IP addresses used to transfer the log file to a remote host.</td>
</tr>
<tr>
<td>WARNING</td>
<td>A nonfatal condition occurred. No immediate action is needed. An indication that an error can occur if action is not taken within a given amount of time.</td>
</tr>
<tr>
<td>NOTIFICATION</td>
<td>Significant event of a normal and normal nature. An indication that unusual, but not error, conditions have occurred. No immediate action is required.</td>
</tr>
<tr>
<td>INFO</td>
<td>Information only. No action is required.</td>
</tr>
<tr>
<td>DEBUG</td>
<td>Message containing information useful for debugging.</td>
</tr>
<tr>
<td>FATAL</td>
<td>A fatal condition occurred. The system cannot recover without restarting. For example, a fatal message is generated after the configuration database is corrupted.</td>
</tr>
</tbody>
</table>

Based on the severity code in each message, the platform dispatches each message to one or more of the following destinations:

- workstation display
- local log file
- one or more remote hosts

You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration except in the following case. When you configure the system log table in EDM, under the **System Log Table** tab, you must select either IPv4 or IPv6.

Internally, the switch has four severity levels for log messages: INFO, WARNING, ERROR, and FATAL. The system log supports eight different severity levels:

- Debug
- Info
- Notice
- Warning
- Critical
- Error
The following table shows the default mapping of internal severity levels to syslog severity levels.

**Table 6: Default and system log severity level mapping**

<table>
<thead>
<tr>
<th>UNIX system error codes</th>
<th>System log severity level</th>
<th>Internal severity level</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency</td>
<td>Fatal</td>
</tr>
<tr>
<td>1</td>
<td>Alert</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>Error</td>
<td>Error</td>
</tr>
<tr>
<td>4</td>
<td>Warning</td>
<td>Warning</td>
</tr>
<tr>
<td>5</td>
<td>Notice</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>Info</td>
<td>Info</td>
</tr>
<tr>
<td>7</td>
<td>Debug</td>
<td>—</td>
</tr>
</tbody>
</table>

**Log files**

The log file captures hardware and software log messages, and alarm messages. Virtual Services Platform 4000 logs to internal flash.

The system saves internal log messages in a circular list in memory, which overwrite older log messages as the log fills. Unlike the log messages in a log file, the internal log messages in memory do not contain encrypted information, which can limit the information available during troubleshooting. Free up the disk space on the flash if the system generates the disk space 75% full alarm. After the disk space utilization returns below 75%, the system clears the alarm, and then starts logging to a file again.

**Log file naming conventions**

The following list provides the naming conventions for the log file:

- The log file is named as log.xxxxxxxx.sss format. The prefix of the log file name is log. The six characters after the log file prefix contain the last three bytes of the chassis base MAC address. The next two characters are 01. The last three characters (sss) denote the sequence number of the log file.
- The sequence number of the log file is incremented for each new log file created after the existing log file reaches the maximum configured size.
- At initial system start up when no log file exists, a new log file with the sequence number 000 is created. After a restart, the system finds the newest log file from internal flash based on file timestamps. If the newest log file is on the flash that is used for logging, the system continues to use the newest log file. And once the maximum configured size is reached, system continues to create a new log file with incremental sequence number on the internal flash for logging.
Log file transfer

The system logs contain important information for debugging and maintaining the switch. After the current log file reaches the configured maximum size, the system creates a new log file for logging. The system transfers old log files to a remote host. You can configure up to 10 remote hosts, which creates long-term backup storage of your system log files.

Of the 10 configured remote hosts, 1 is the primary host and the other 9 are redundant. Upon initiating a transfer, system messaging attempts to use host 1 first. If host 1 is not reachable, system messaging tries hosts 2 to 10.

If log file transfer is unsuccessful, the system keeps the old log files on internal flash. The system attempts to transfer old log files after the new log file reaches the configured maximum size. The system also attempts to transfer old log files periodically (once in one hundred log writes) if the disk space on the flash is more than 75% full.

You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration.

With enhanced secure mode enabled, authorized users can use SFTP to transfer files to a remote server with the content encrypted.

You can specify the following information to configure the transfer criteria:

- The maximum size of the log file.
- The IP address of the remote host.
- The name prefix of the log file to store on the remote host.

The system appends a suffix of .xxxxxxxx.sss to the file name. The first six characters of the suffix contain the last three bytes of the chassis base MAC address. The next two characters are 01. The last three characters (sss) denote the sequence number of the log file. For example, if you configure the name prefix as mylog, a possible file name is mylog.90000001.001.

- The user name and password, if using File Transfer Protocol (FTP) for file transfer. Use the following commands to configure the user name and password:

  boot config host user WORD<0–16>
  boot config host password WORD<0–16>

Be aware of the following restrictions to transfer log files to a remote host:

- The remote host IP address must be reachable.
- If you transfer a log file from a host to the system, (for example, to display it with a show command), rename the log file. Failure to rename the log file can cause the system to use the recently transferred file as the current log, if the sequence number in the extension is higher than the current log file. For example, if bf860005.002 is the current log file and you transfer bf860005.007 to the system, the system logs future messages to the bf860005.007 file. You can avoid this if you rename the log file to something other than the format used by system messaging.
- If your TFTP server is a UNIX-based machine, files written to the server must already exist. For example, you must create dummy files with the same names as your system logs. This action is commonly performed by using the touch command (for example, touch bf860005.001).
Three parameters exist to configure the log file:

- the minimum acceptable free space available for logging
- the maximum size of the log file
- the percentage of free disk space the system can use for logging

Although these three parameters exist, you can only configure the maximum size of the log file. The switch does not support the minimum size and percentage of free disk space parameters. The internal flash must be less than 75% full for the system to log a file. If the internal flash is more than 75% full, logging to a file stops to prevent exhausting disk space.

**Log file transfer using a wildcard filename**

Log files from VOSS Release 4.1 and earlier were created without access permissions. However, file transfers using SFTP require file permissions.

The command `attribute WORD<1-99> [+/-] R` allows you to change the permissions of a file. To change permissions for log files created in VOSS 4.1 and earlier, use the `attribute` command with the wildcard filename `log.*`. Using the command in the form `attribute log.* [+/-]R` changes permissions for log files with names that begin with the characters "log."

**Important:**

You cannot use a wildcard pattern other than `log.*` for this command.
Chapter 9: Log configuration using ACLI

Use log files and messages to perform diagnostic and fault management functions.

Configuring a UNIX system log and syslog host

Before you begin
• You must log on to the Global Configuration mode in ACLI.

About this task
Configure the syslog to control a facility in UNIX machines that logs SNMP messages and assigns each message a severity level based on importance.
You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration using ACLI.

Procedure
1. Enable the system log:
   syslog enable
2. Specify the IP header in syslog packets:
   syslog ip-header-type <circuitless-ip|default>
3. Configure the maximum number of syslog hosts:
   syslog max-hosts <1-10>
4. Create the syslog host:
   syslog host <1-10>
5. Configure the IP address for the syslog host:
   syslog host <1-10> address WORD <0–46>
6. Enable the syslog host:
   syslog host <1-10> enable

Configure optional syslog host parameters by using the variables in the following variable definition tables.
7. View the configuration to ensure it is correct:

```
show syslog [host <1–10>]
```

**Example**

Configure a UNIX system log host address to IPv4 address 47.17.143.52 and syslog host:

```
VSP-4850GTS-PWR+:1(config)#syslog enable
VSP-4850GTS-PWR+:1(config)#syslog host 7 address 1.1.1.1
VSP-4850GTS-PWR+:1(config)#syslog host 7 enable
```

```
VSP-4850GTS-PWR+:1(config)#show syslog host 7

    Id : 7  
    IpAddr : 1.1.1.1  
    UdpPort : 514  
    Facility : local7  
    Severity : info|warning|error|fatal  
    MapInfoSeverity : info  
    MapWarningSeverity : warning  
    MapErrorSeverity : error  
    MapMfgSeverity : notice  
    MapFatalSeverity : emergency  
    Enable : true  
    SecureForwardingMode: none  
    Tcp Port : 1025

VSP-4850GTS-PWR+:1(config)#show syslog

Enable : true  
Max Hosts : 5  
OperState : active  
header : default  
Total number of configured hosts : 3  
Total number of enabled hosts : 1  
Configured host : 7 8 9  
Enabled host : 7
```

**Variable definitions**

Use the data in the following table to use the `syslog` command.

**Table 7: Variable definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the sending of syslog messages on the device. The default is disabled. Use the no operator before this parameter, no syslog enable to disable the sending of syslog messages on the device. The default is enabled.</td>
</tr>
</tbody>
</table>

*Table continues...*
### Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
</table>
| **ip-header-type <circuitless-ip|default>|** Specifies the IP header in syslog packets to circuitless-ip or default.  
- If the value is default, the IP address of the VLAN is used for syslog packets that are transmitted in-band using input/output (I/O) ports.  
- If the value is circuitless-ip, then for all syslog messages (in-band or out-of-band), the circuitless IP address is used in the IP header. If you configure multiple circuitless IPs, the first circuitless IP configured is used. |
| **max-hosts <1-10>|** Specifies the maximum number of syslog hosts supported, from 1–10. The default is 5. |

Use the data in the following table to use the `syslog host` command.

### Table 8: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>**1–10</td>
<td>** Creates and configures a host instance. Use the no operator before this parameter, no syslog host to delete a host instance.</td>
</tr>
<tr>
<td>**address WORD &lt;0–46&gt;</td>
<td>** Configures a host location for the syslog host. WORD &lt;0–46&gt; is the IPv4 or IPv6 address of the UNIX system syslog host in the format A.B.C.D or x:x:x:x:x:x:x. You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration using ACLI.</td>
</tr>
<tr>
<td>**enable</td>
<td>** Enables the syslog host. Use the no operator before this parameter, no syslog host enable to disable syslog host. The default is disabled.</td>
</tr>
<tr>
<td>**facility {local0</td>
<td>local1</td>
</tr>
<tr>
<td>**maperror {emergency</td>
<td>alert</td>
</tr>
<tr>
<td>**mapfatal {emergency</td>
<td>alert</td>
</tr>
<tr>
<td>**mapinfo {emergency</td>
<td>alert</td>
</tr>
<tr>
<td>**mapwarning {emergency</td>
<td>alert</td>
</tr>
<tr>
<td>**secure-forwarding mode &lt;none</td>
<td>ssh</td>
</tr>
</tbody>
</table>
### Variable

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>secure-forwarding tcp-port &lt;1025–49151&gt;</td>
<td>Set tcp-port for secure forwarding of syslog for host. The default tcp-port is 1025.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>The tcp-port 6000 cannot be used, as it is used as an internal port for Internal Spanning Tree (IST).</td>
</tr>
<tr>
<td>severity &lt;info</td>
<td>warning</td>
</tr>
<tr>
<td>udp-port &lt;514-530&gt;</td>
<td>Specifies the User Datagram Protocol port number on which to send syslog messages to the syslog host. This value is the UNIX system syslog host port number from 514–530. The default is 514.</td>
</tr>
</tbody>
</table>

---

### Job aid

The following table describes the fields in the output for the `show syslog host` command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Specifies the ID for the syslog host. The range is 1–10.</td>
</tr>
<tr>
<td>IpAddr</td>
<td>Specifies the IP address of the syslog host. You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses.</td>
</tr>
<tr>
<td>UdpPort</td>
<td>Specifies the UDP port to use to send messages to the syslog host (514–530). The default is 514.</td>
</tr>
<tr>
<td>Facility</td>
<td>Specifies the syslog host facility used to identify messages (local0 to local7). The default is local7.</td>
</tr>
<tr>
<td>Severity</td>
<td>Specifies the message severity for which syslog messages are sent. The default is info</td>
</tr>
<tr>
<td>MapInfoSeverity</td>
<td>Specifies the syslog severity to use for INFO messages. The default is info.</td>
</tr>
<tr>
<td>MapWarningSeverity</td>
<td>Specifies the syslog severity to use for WARNING messages. The default is warning.</td>
</tr>
<tr>
<td>MapErrorSeverity</td>
<td>Specifies the syslog severity to use for ERROR messages. The default is error.</td>
</tr>
<tr>
<td>MapMfgSeverity</td>
<td>Specifies the syslog severity to use for Accelar manufacturing messages. The default is notice.</td>
</tr>
<tr>
<td>MapFatalSeverity</td>
<td>Specifies the syslog severity to use for FATAL messages. The default is emergency.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables or disables the sending of messages to the syslog host. The default is disabled.</td>
</tr>
<tr>
<td>SecureForwardingMode</td>
<td>Specifies the mode in which the syslog messages are securely forwarded. The supported values are ssh, tls, and none. The default is none, which means that secure forwarding is disabled.</td>
</tr>
<tr>
<td>TcpPort</td>
<td>Specifies the TCP port to use for secure forwarding for a particular host. The default is 1024.</td>
</tr>
</tbody>
</table>

## Configuring secure forwarding

Configuring secure forwarding includes setting the mode for the particular syslog host and setting the TCP port through which the logs are sent to the syslog server.

### Procedure

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. Create the syslog host:
   ```
   syslog host <1-10>
   ```
   Use the no operator before this parameter, that is, no syslog host to delete a host instance.
3. Configure an IP address for the syslog host:
   ```
   syslog host <1-10> address WORD<0-46>
   ```
4. Enable the syslog host:
   ```
   syslog host <1-10> enable
   ```
5. Enable syslog globally:
   ```
   syslog enable
   ```
6. Set the mode for secure forwarding on the host:
   ```
   syslog host <1-10> secure-forwarding mode [none] | [ssh] | [tls server-cert-name WORD<1-64>]
   ```
7. Set the TCP port:
   ```
   syslog host <1-10> secure-forwarding tcp-port <1025-49151>
   ```
8. Display the secure forwarding configured values:
show syslog host <1–10>

9.  
   (Optional) Remove the server certificate name:
   no syslog host <1–10> secure-forwarding mode tls server-cert-name

10. (Optional) Set secure-forwarding mode to none for a particular host:
    default syslog host <1–10> secure-forwarding mode

Next steps
After configuring secure forwarding on the switch, set the syslog server to be able to see the log messages on the interactive syslog viewer.

- For SSH secure syslog, on the winsyslog server, enter the host IP or the IP of the PC and set the port to 601 which is a default port for TCP and set the protocol type to RFC3195.
- For TLS secure syslog, on the rsyslog server, configure the server to use TLS method and install the root certificate on the server in the switch.

Variable definitions
Use the data in the following table to use the `syslog host` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host &lt;1–10&gt;</td>
<td>Specifies the ID for the syslog host. The range is 1–10.</td>
</tr>
<tr>
<td>address WORD&lt;0–46&gt;</td>
<td>Configures a host location for the syslog host. WORD &lt;0–46&gt; is the IPv4 or IPv6 address of the UNIX system syslog host in the format A.B.C.D or x:x:x:x:x:x:x:x. You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration using ACLI.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the syslog host. Use the no operator before this parameter, no syslog host enable to disable syslog host. The default is disabled.</td>
</tr>
<tr>
<td>secure-forwarding</td>
<td>Adds protected syslog using SSH remote port forwarding for host.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `syslog host secure-forwarding` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host &lt;1–10&gt;</td>
<td>Creates and configures a host instance. Use the no operator before this parameter, no syslog host to delete a host instance.</td>
</tr>
</tbody>
</table>
| mode [none | ssh | tls server-cert-name WORD<1-64>] | Specifies the mode of secure forwarding of syslog on the host. The default mode is none, that is, both ssh and tls modes are disabled by default.  

   Note:
   Certificate validation is done only if the server-cert-name is configured.
Variable | Value
---|---
tcp-port <1025–49151> | Set tcp-port for secure forwarding of syslog for host. The default tcp-port is 1025.

To set the TCP port to default value, use command `default syslog host <1–10> secure-forwarding tcp-port`.

⚠️ Important:
The tcp-port 6000 cannot be used, as it is used as an internal port for Internal Spanning Tree (IST).

#### Installing root certificate for syslog client

Use the following procedure to install a root certificate for a syslog client.

**Procedure**

1. Enter Global Configuration mode:
   ```
   enable
configure terminal
   ```

2. Install a root certificate on the store:
   ```
   syslog root-cert install-filename <file-name>
   ```
   The certificate is installed in folder: `/intflash/.cert/.syslogrootinstalledcert/`

   ✨ Note:
The offline root certificate for TLS syslog must be kept in folder: `/intflash/.cert/..syslogofflinerootcert/`

3. Uninstall a root certificate from the store:
   ```
   no syslog root-cert install-filename <file-name>
   ```

4. To display the installed syslog server root certificate file:
   ```
   show syslog root-cert-file
   ```

#### Variable definition

Use the data in the following table to use the `syslog root-cert` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>install-filename</td>
<td>WORD&lt;1–128&gt; Specifies the name of the root certificate to be installed on the store.</td>
</tr>
</tbody>
</table>
## Configuring logging

### Before you begin
- You must log on to the Global Configuration mode in ACLI.

### About this task
Configure logging to determine the types of messages to log and where to store the messages.

* **Note:**

   The platform logs CLILOG and SNMPLOG as INFO. Normally, if you configure the logging level to WARNING, the system skips all INFO messages. However, if you enable CLILOG and SNMPLOG the system logs ACLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

### Procedure
1. Define which messages to log:
   ```
   logging level <0-4>
   ```
2. Write the log file from memory to a file:
   ```
   logging write WORD<1-1536>
   ```
3. Show logging on the screen:
   ```
   logging screen
   ```

### Example
```
VSP-4850GTS-PWR+:1(config)#logging level 0
VSP-4850GTS-PWR+:1(config)#logging write log2
VSP-4850GTS-PWR+:1(config)#logging screen
```

### Variable definitions
Use the data in the following table to use the `logging` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level &lt;0-4&gt;</td>
<td>Shows and configures the logging level. The level is one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• 0: Information — all messages are recorded</td>
</tr>
<tr>
<td></td>
<td>• 1: Warning — only warning and more serious messages are recorded</td>
</tr>
<tr>
<td></td>
<td>• 2: Error — only error and more serious messages are recorded</td>
</tr>
</tbody>
</table>

*Table continues*
### Variable definitions

Use the data in the following table to use the `logging transferFile` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 3: Manufacturing — this parameter is not available for customer use&lt;br&gt;• 4: Fatal — only fatal messages are recorded</td>
</tr>
<tr>
<td>screen</td>
<td>Configures the log display on the screen to on. Use the no form of the command to stop the log display on the screen: <code>no logging screen</code></td>
</tr>
<tr>
<td>transferFile &lt;1–10&gt; address {A.B.C.D} filename-prefix WORD&lt;0–200</td>
<td>Transfers the syslog file to a remote FTP/TFTP server. <code>&lt;1–10&gt;</code> specifies the file ID. The <code>address {A.B.C.D}</code> option specifies the IP address. The <code>filename-prefix WORD&lt;0–200&gt;</code> option sets the filename prefix for the log file at the remote host.</td>
</tr>
<tr>
<td>write WORD&lt;1-1536&gt;</td>
<td>Writes the log file with the designated string. <code>WORD&lt;1-1536&gt;</code> is the string or command that you append to the log file. If the string contains spaces, you must enclose the string in quotation marks (&quot;.&quot;).</td>
</tr>
</tbody>
</table>

### Configuring the remote host address for log transfer

**Before you begin**

- The IP address you configure for the remote host must be reachable at the time of configuration.
- You must log on to the Global Configuration mode in ACLI.

**About this task**

Configure the remote host address for log transfer. The system transfers the current log file to a remote host after the log file size reaches the maximum size.

**Procedure**

Configure the remote host address for log transfer:

```
logging transferFile {1-10} address {A.B.C.D} [filename WORD<0-255>]
```

**Example**

```
VSP-4850GTS-PWR+:1(config)#logging transferFile 1 address 172.16.120.10
```
Configuring system logging to external storage

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

System logs are a valuable diagnostic tool.

You can change log file parameters at anytime without restarting the system. Changes made to these parameters take effect immediately.

Procedure

Configure the logfile parameters:

```
boot config logfile <64-500> <500-16384> <10-90>
```

Example

```
VSP-4850GTS-PWR+:1(config)#boot config logfile 64 600 10
```

Variable definitions

Use the data in the following table to use the `boot config` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>choice</td>
<td>Specifies runtime and configuration file choices.</td>
</tr>
<tr>
<td>flags</td>
<td>Commands to enable the boot flags</td>
</tr>
<tr>
<td>flags logging</td>
<td>Enables or disables logging to a file on external flash. The log file is named using the format <code>log.xxxxxxxx.sss</code>. The first six characters after the prefix of the file name log contain the last three bytes of the chassis base MAC address. The next two characters specify the slot number that generated</td>
</tr>
</tbody>
</table>
### Configuring system message control

**Before you begin**
- You must log on to the Global Configuration mode in ACLI.

**About this task**
Configure system message control to suppress duplicate error messages on the console, and to determine the action to take if they occur.

**Procedure**
1. Configure system message control action:
   ```
   sys msg-control action <both|send-trap|suppress-msg>
   ```
2. Configure the maximum number of messages:
   ```
   sys msg-control max-msg-num <2-500>
   ```
3. Configure the interval:
   ```
   sys msg-control control-interval <1-30>
   ```
4. Enable message control:
   ```
   sys msg-control
   ```

---

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>the logs. The last three characters denote the sequence number of the log file. Multiple sequence numbers are generated for the same chassis and same slot, if the maximum log file size is reached.</td>
<td></td>
</tr>
<tr>
<td>loadconfigtime</td>
<td>Configures the timeout for loading the configuration file in seconds. The values are 0 to 300 seconds.</td>
</tr>
<tr>
<td>multicast</td>
<td>Configures the system multicast scaling parameter. The multicast scaling values are 0 to 2147483647.</td>
</tr>
<tr>
<td>sio</td>
<td>Configures CPU serial port devices.</td>
</tr>
</tbody>
</table>
| logfile &lt;64-500&gt; &lt;500-16384&gt; &lt;10-90&gt; | Configures the logfile parameters  
   - &lt;64-500&gt; specifies the minimum free memory space on the external storage device from 64–500 KB. Virtual Services Platform 4000 does not support this parameter.  
   - &lt;500-16384&gt; specifies the maximum size of the log file from 500–16384 KB.  
   - &lt;10-90&gt; specifies the maximum percentage, from 10–90%, of space on the external storage device the logfile can use. Virtual Services Platform 4000 does not support this parameter. |
Example
VSP-4850GTS-PWR+:1(config)#sys msg-control action suppress-msg
VSP-4850GTS-PWR+:1(config)#sys msg-control max-msg-num 10
VSP-4850GTS-PWR+:1(config)#sys msg-control control-interval 15
VSP-4850GTS-PWR+:1(config)#sys msg-control

Variable definitions

Use the data in the following table to use the `sys msg-control` command.

Table 12: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>action &lt;both</td>
<td>send-trap</td>
</tr>
<tr>
<td>control-interval &lt;1-30&gt;</td>
<td>Configures the message control interval in minutes. The valid options are 1–30. The default is 5.</td>
</tr>
<tr>
<td>max-msg-num &lt;2-500&gt;</td>
<td>Configures the number of occurrences of a message after which the control action occurs. To configure the maximum number of occurrences, enter a value from 2–500. The default is 5.</td>
</tr>
</tbody>
</table>

Extending system message control

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

Use the force message control option to extend the message control feature functionality to the software and hardware log messages.

To enable the message control feature, you must specify an action, control interval, and maximum message number. After you enable the feature, the log messages, which get repeated and cross the maximum message number in the control interval, trigger the force message feature. You can either suppress the message or send a trap notification, or both.

Procedure

Configure the force message control option:

```
sys force-msg WORD<4-4>
```
Example

VSP-4850GTS-PWR+:1> enable
VSP-4850GTS-PWR+:1# configure terminal

Add a force message control pattern. If you use a wildcard pattern (****), all messages undergo message control.

VSP-4850GTS-PWR+:1(config)# sys force-msg ****

Variable definitions

Use the data in the following table to use the **sys force-msg** command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD&lt;4-4&gt;</td>
<td>Adds a forced message control pattern, where WORD&lt;4-4&gt; is a string of 4 characters. You can add a four-byte pattern into the force-msg table. The software and the hardware log messages that use the first four bytes that match one of the patterns in the force-msg table undergo the configured message control action. You can specify up to 32 different patterns in the force-msg table, including a wildcard pattern (****) as well. If you specify the wildcard pattern, all messages undergo message control.</td>
</tr>
</tbody>
</table>

Viewing logs

View log files by file name, category, or severity to identify possible problems.

**About this task**

View ACLI command and SNMP trap logs, which are logged as normal log messages and logged to the system log file.

**Procedure**

1. Enter Privileged EXEC mode:
   
   `enable`

2. Show log information:
   
   `show logging file [alarm] [event-code WORD<0–10>] [module WORD<0–100>] [name-of-file WORD<1–99>] [save-to-file WORD<1–99>] [severity WORD<0–25>] [tail] [vrf WORD<0–32>]`
Example

Display log file information:

Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#show logging file

Switch:1(config)#show logging file module SNMP

--More-- (q = quit)
Variable definitions

Use the data in the following table to use the `show logging file` command.

Table 14: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm</td>
<td>Displays alarm log entries.</td>
</tr>
<tr>
<td>CPU \texttt{WORD&lt;0-100&gt;}</td>
<td>Specifies the CPU event code and filename.</td>
</tr>
<tr>
<td>event-code \texttt{WORD&lt;0–10&gt;}</td>
<td>Specifies a number that precisely identifies the event reported.</td>
</tr>
<tr>
<td>module \texttt{WORD&lt;0-100&gt;}</td>
<td>Filters and lists the logs according to module. Specifies a string length of 0–100 characters. Categories include \texttt{SNMP}, \texttt{EAP}, \texttt{RADIUS}, \texttt{RMON}, \texttt{WEB}, \texttt{HW}, \texttt{MLT}, \texttt{FILTER}, \texttt{QOS}, \texttt{CLILOG}, \texttt{SW}, \texttt{CPU}, \texttt{IP}, \texttt{VLAN}, \texttt{IPMC}, \texttt{PIM}, \texttt{POLICY}, and \texttt{SNMPLOG}. To specify multiple filters, separate each category by the vertical bar (</td>
</tr>
<tr>
<td>name-of-file \texttt{WORD&lt;1-99&gt;}</td>
<td>Displays the valid logs from this file. For example, /intflash/logcopy.txt. You cannot use this command on the current log file—the file into which the messages are currently logged. Specify a string length of 1–99 characters. If you enable enhanced secure mode, the system encrypts the entire log file. After you use the <code>show log file name-of-file WORD&lt;1–99&gt;</code> command, the system takes the encrypted log file name as input, then decrypts it, and prints the output to the screen. You can then redirect the decrypted output to a file that you can store onto the flash. If enhanced secure mode is disabled, the system only encrypts the proprietary portion of the log file.</td>
</tr>
<tr>
<td>save-to-file \texttt{WORD&lt;1-99&gt;}</td>
<td>Redirects the output to the specified file and removes all encrypted information. You cannot use the \texttt{tail} option with the \texttt{save-to-file} option. Specify a string length of 1–99 characters.</td>
</tr>
<tr>
<td>severity \texttt{WORD&lt;0-25&gt;}</td>
<td>Filters and lists the logs according to severity. Choices include \texttt{INFO}, \texttt{ERROR}, \texttt{WARNING}, and \texttt{FATAL}. To specify multiple filters, separate each severity by the vertical bar (</td>
</tr>
<tr>
<td>tail</td>
<td>Shows the last results first.</td>
</tr>
<tr>
<td>vrf \texttt{WORD&lt;0–32&gt;}</td>
<td>Specifies the name of a VRF instance to show log messages that only pertain to that VRF.</td>
</tr>
</tbody>
</table>

Configuring ACLI logging

Use ACLI logging to track all ACLI commands executed and for fault management purposes. The ACLI commands are logged to the system log file as \texttt{CLILOG} module.
About this task

**Note:**

The platform logs CLILOG and SNMPLOG as INFO. Normally, if you configure the logging level to WARNING, the system skips all INFO messages. However, if you enable CLILOG and SNMPLOG the system logs ACLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

**Procedure**

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```

2. Enable ACLI logging:
   ```
   clilog enable
   ```

3. *(Optional)* Disable ACLI logging:
   ```
   no clilog enable
   ```

4. Ensure that the configuration is correct:
   ```
   show clilog
   ```

5. View the ACLI log:
   ```
   show logging file module clilog
   ```

**Example**

Enable ACLI logging, and view the ACLI log:

```plaintext
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#clilog enable
Switch:1(config)#show logging file module clilog
CP1 [02/13/13 17:27:25.956] 0x002c0600 00000000 GlobalRouter CLILOG INFO     1 CONSOLE
rwa show snmp-server host
CP1 [02/13/13 17:28:10.100] 0x002c0600 00000000 GlobalRouter CLILOG INFO     2 CONSOLE
rwa show snmp-server notif
CP1 [02/13/13 17:28:45.732] 0x002c0600 00000000 GlobalRouter CLILOG INFO     3 CONSOLE
rwa snmp-server force-trap
CP1 [02/13/13 17:29:30.628] 0x002c0600 00000000 GlobalRouter CLILOG INFO     4 CONSOLE
rwa show logging file modug
rwa ena
CP1 [02/14/13 19:39:11.648] 0x002c0600 00000000 GlobalRouter CLILOG INFO     5 CONSOLE
rwa conf t
CP1 [02/14/13 19:39:13.420] 0x002c0600 00000000 GlobalRouter CLILOG INFO     6 CONSOLE
rwa filter acl 2 enable
CP1 [02/14/13 19:49:21.044] 0x002c0600 00000000 GlobalRouter CLILOG INFO     7 CONSOLE
rwa filter acl 2 enable
CP1 [02/14/13 19:50:08.540] 0x002c0600 00000000 GlobalRouter CLILOG INFO     8 CONSOLE
rwa filter acl 2 type inpol
CP1 [02/14/13 19:50:38.444] 0x002c0600 00000000 GlobalRouter CLILOG INFO     9 CONSOLE
rwa filter acl 2 type inpol
CP1 [02/14/13 19:50:52.968] 0x002c0600 00000000 GlobalRouter CLILOG INFO    10 CONSOLE
rwa filter acl enable 2
CP1 [02/14/13 19:51:08.908] 0x002c0600 00000000 GlobalRouter CLILOG INFO    11 CONSOLE
rwa filter acl 2 enable
```

Comments on this document? infodev@avaya.com
Log configuration using ACLI

Variable definitions

Use the data in the following table to use the clilog commands.

Table 15: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Activates ACLI logging. To disable, use the no clilog enable command.</td>
</tr>
</tbody>
</table>
Chapter 10: Log configuration using EDM

Use log files and messages to perform diagnostic and fault management functions. This section provides procedures to configure and use the logging system in Enterprise Device Manager (EDM).

Configuring the system log

About this task

Configure the system log to track all user activity on the device. The system log can send messages of up to ten syslog hosts.

Procedure

1. In the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click System Log.
3. In the System Log tab, select Enable.
4. Configure the maximum number of syslog hosts.
5. Configure the IP header type for the syslog packet.
6. Click Apply.

System Log field descriptions

Use the data in the following table to use the System Log tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables or disables the syslog feature. If you select this variable, this feature sends a message to a server on a network that is configured to receive and store diagnostic messages from this device. You can configure the type of messages sent. The default is enabled.</td>
</tr>
<tr>
<td>MaxHosts</td>
<td>Specifies the maximum number of remote hosts considered active and can receive messages from the syslog service. The range is 0–10 and the default is 5.</td>
</tr>
</tbody>
</table>
OperState
- Specifies the operational state of the syslog service. The default is active.

Header
- Specifies the IP header in syslog packets to circuitlessIP, default, or managementVIP.
- If the value is circuitlessIP, the circuitless IP address is used in the IP header for all syslog messages (in-band or out-of-band). If you configure multiple circuitless IPs, the first circuitless IP configured is used.
- The default value is default.

Configuring the system log table

About this task
Use the system log table to customize the mappings between the severity levels and the type of alarms.

You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration except in the following case. When you configure the system log table, under the System Log Table tab, you must select ipv4 or IPv6 in the AddressType box. The Address box supports both IPv4 and IPv6 addresses.

Procedure
1. In the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click System Log.
3. Click the System Log Table tab.
4. Click Insert.
5. Configure the parameters as required.
6. Click Insert.
7. To modify mappings, double-click a parameter to view a list of options.
8. Click Apply.

System Log Table field descriptions
Use the data in the following table to use the System Log Table tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Specifies the ID for the syslog host. The range is 1–10.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>AddressType</strong></td>
<td>Specifies if the address is an IPv4 or an IPv6 address.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>Specifies the IP address of the syslog host. You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses.</td>
</tr>
<tr>
<td><strong>UdpPort</strong></td>
<td>Specifies the UDP port to use to send messages to the syslog host (514–530). The default is 514.</td>
</tr>
<tr>
<td><strong>Enable</strong></td>
<td>Enables or disables the sending of messages to the syslog host. The default is disabled.</td>
</tr>
<tr>
<td><strong>HostFacility</strong></td>
<td>Specifies the syslog host facility used to identify messages (LOCAL0 to LOCAL7). The default is LOCAL7.</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Specifies the message severity for which syslog messages are sent. The default is INFO, WARNING, ERROR, and FATAL.</td>
</tr>
<tr>
<td><strong>MapInfoSeverity</strong></td>
<td>Specifies the syslog severity to use for INFO messages. The default is INFO.</td>
</tr>
<tr>
<td><strong>MapWarningSeverity</strong></td>
<td>Specifies the syslog severity to use for WARNING messages. The default is WARNING.</td>
</tr>
<tr>
<td><strong>MapErrorSeverity</strong></td>
<td>Specifies the syslog severity to use for ERROR messages. The default is ERROR.</td>
</tr>
<tr>
<td><strong>MapFatalSeverity</strong></td>
<td>Specifies the syslog severity to use for FATAL messages. The default is EMERGENCY.</td>
</tr>
<tr>
<td><strong>MapMfgSeverity</strong></td>
<td>Specifies the syslog severity to use for Accelar manufacturing messages. There is no default value.</td>
</tr>
<tr>
<td><strong>SecureForwardingTcpPort</strong></td>
<td>Specifies the TCP port to use for secure forwarding for a particular host. The default is 1025.</td>
</tr>
<tr>
<td><strong>SecureForwardingMode</strong></td>
<td>Enables or disables secure forwarding of syslog over remote port forwarding. The supported values are ssh, tls, and none. The default is none, which means that secure forwarding is disabled.</td>
</tr>
<tr>
<td><strong>SecureForwardingServerCertName</strong></td>
<td>Specifies the server certificate name. Certificate validation is done only if the server certificate name is configured.</td>
</tr>
</tbody>
</table>
Chapter 11: SNMP trap configuration using ACLI

Use Simple Network Management Protocol (SNMP) traps and notifications to gather information about device activities, alarms, and other information on management stations.

For more information about how to configure SNMP community strings and related topics, see Security for Avaya Virtual Services Platform 4000 Series, NN46251-601.

Configuring an SNMP host

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

Configure an SNMP host so that the system can forward SNMP traps to a host for monitoring. You can use SNMPv1, SNMPv2c, or SNMPv3. You configure the target table parameters (security name and model) as part of the host configuration.

Procedure

1. Configure an SNMPv1 host:

   snmp-server host WORD<1-256> [port <1-65535>] v1 WORD<1-32> [filter WORD<1-32>]

2. Configure an SNMPv2c host:

   snmp-server host WORD<1-256> [port <1-65535>] v2c WORD<1-32> [inform [timeout <1-2147483647>] [retries <0-255>] [mms <0-2147483647>]] [filter WORD<1-32>]

3. Configure an SNMPv3 host:

   snmp-server host WORD<1-256> [port <1-65535>] v3 {noAuthNoPriv|authNoPriv|AuthPriv} WORD<1-32> [inform [timeout <1-2147483647>] [retries <0-255>]] [filter WORD<1-32>]

4. Ensure that the configuration is correct:

   show snmp-server host
Example

Configure the target table entry:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#snmp-server host 198.202.188.207 port 162 v2c ReadView inform timeout 1500 retries 3 mms 484
```

Variable definitions

Use the data in the following table to use the `snmp-server host` command.

**Table 16: Variable definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>inform [timeout &lt;1-2147483647&gt;] [retries &lt;0-255&gt;] [mms &lt;0-2147483647&gt;]</td>
<td>Sends SNMP notifications as inform (rather than trap). To use all three options in one command, you must use them in the following order: 1. timeout &lt;0-2147483647&gt; specifies the timeout value in seconds with a range of 0–214748364. 2. retries &lt;0-255&gt; specifies the retry count value with a range of 0–255. 3. mms &lt;0-2147483647&gt; specifies the maximum message size as an integer with a range of 0–214748364.</td>
</tr>
<tr>
<td>filter WORD&lt;1-32&gt;</td>
<td>Specifies the filter profile to use.</td>
</tr>
<tr>
<td>noAuthNoPriv</td>
<td>authNoPriv</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Specifies the host server port number.</td>
</tr>
<tr>
<td>WORD&lt;1-32&gt;</td>
<td>Specifies the security name, which identifies the principal that generates SNMP messages.</td>
</tr>
<tr>
<td>WORD&lt;1-256&gt;</td>
<td>Specifies either an IPv4 or IPv6 address.</td>
</tr>
</tbody>
</table>

**Note:**

The SNMP server host IPv6 format should be x:x:x:x:x:x:x:x. Avaya recommends you do not use :: in the IPv6 address. If you use :: the port number becomes part of the IPv6 address in the SNMP target address table.

Configuring SNMP interfaces

**Before you begin**

- You must log on to the Global Configuration mode in ACLI.
About this task
Configure an interface to send SNMP traps. If the Avaya Virtual Services Platform 4000 Series has multiple interfaces, configure the IP interface from which the SNMP traps originate.

Procedure
1. Configure the destination and source IP addresses for SNMP traps:
   ```
   snmp-server sender-ip {A.B.C.D} {A.B.C.D}
   ```

2. If required, send the source address (sender IP) as the sender network in the notification message:
   ```
   snmp-server force-trap-sender enable
   ```

3. If required, force the SNMP and IP sender flag to use the same value:
   ```
   snmp-server force-iphdr-sender enable
   ```

Example
VSP-4850GTSPWR+:1> enable
VSP-4850GTSPWR+:1# configure terminal
VSP-4850GTSPWR+:1(config)# snmp-server sender-ip 44.16.13.12 42.13.15.10
VSP-4850GTSPWR+:1(config)# snmp-server force-trap-sender enable
VSP-4850GTSPWR+:1(config)# snmp-server force-iphdr-sender enable

Enable the generation of authentication traps:
VSP-4850GTSPWR+:1(config)# snmp-server authentication-trap enable

Variable definitions
Use the data in the following table to use the `snmp-server` command.

Table 17: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication-trap enable</td>
<td>Activates the generation of authentication traps.</td>
</tr>
<tr>
<td>community WORD&lt;1–32&gt;</td>
<td>Specifies a community string to create a community to use in forming a relationship between an SNMP agent and one or more SNMP managers. You require SNMP community strings to access the system using an SNMP-based management software. Use the no option to delete the community string: no snmp-server community WORD&lt;1–32&gt;.</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>contact WORD&lt;0–255&gt;</td>
<td>Changes the sysContact information for Virtual Services Platform 4000. WORD&lt;0-255&gt; is an ASCII string from 0–255 characters (for example a phone extension or e-mail address).</td>
</tr>
<tr>
<td>force-iphdr-sender enable</td>
<td>Automatically configures the SNMP and IP sender to the same value. The default is no force-iphdr-sender enable.</td>
</tr>
<tr>
<td>force-trap-sender enable</td>
<td>Sends the configured source address (sender IP) as the sender network in the notification message.</td>
</tr>
<tr>
<td>group WORD&lt;1–32&gt; WORD&lt;0–32&gt; [auth-no-priv</td>
<td>auth-priv</td>
</tr>
<tr>
<td>host WORD&lt;1–256&gt; [port&lt;1–65535&gt;] [v1</td>
<td>v2c</td>
</tr>
<tr>
<td>location WORD&lt;0–255&gt;</td>
<td>Configures the sysLocation information for the system. &lt;WORD 0-255&gt; is an ASCII string from 0–255 characters.</td>
</tr>
<tr>
<td>login-success-trap enable</td>
<td>Enables the generation of login-success traps.</td>
</tr>
<tr>
<td>name WORD&lt;0–255&gt;</td>
<td>Configures the sysName information for the system. &lt;WORD 0-255&gt; is an ASCII string from 0–255 characters.</td>
</tr>
</tbody>
</table>

**Table continues…**
### Variable | Value
---|---
**notify-filter**<sup>WORD<1–32></sup> | Creates a new entry in the notify filter table. The first <sup>WORD<1-32></sup> specifies the filter profile name, and the second <sup>WORD<1-32></sup> specifies the subtree OID.

**sender-ip** <A.B.C.D> <A.B.C.D> | Configures the SNMP trap receiver and source IP addresses. Specify the IP address of the destination SNMP server that receives the SNMP trap notification in the first IP address. Specify the source IP address of the SNMP trap notification packet that is transmitted in the second IP address. If this address is 0.0.0.0, the system uses the IP address of the local interface that is closest (from an IP routing table perspective) to the destination SNMP server.

**user [engine-id WORD <16–97>] [group WORD <1–32>] [notify-view WORD<0–32>|read-view WORD<0–32>|write-view WORD<0–32>][WORD<1–32>][md5|sha Word<1–32>] [aes|des WORD<1–32>]** | Creates a new user in the USM table to authorize a user on a particular SNMP engine.  
  - [aes|des] WORD<1–32> – Specifies a privacy protocol. If no value is entered, no authentication capability exists. The choices are aes and des. WORD<1-32> assigns a privacy password. If no value is entered, no privacy capability exists. The range is 1 to 32 characters. You must set authentication before you can set the privacy option.  
  - engine-id WORD<1–32> – Assigns an SNMPv3 engine ID. Use the no operator to remove this configuration.  
  - group WORD<1–32> – Specifies the group access name.  
  - [md5|sha] WORD<1–32> – Specifies an authentication protocol. If no value is entered, no authentication capability exists. The protocol choices are: MD5 and SHA. WORD<1-32> specifies an authentication password. If no value is entered, no authentication capability exists. The range is 1 to 32 characters.  
  - notify-view WORD<0–32>|read-view WORD<0–32>|write-view WORD<0–32> – Specifies the view name.  

**view WORD<1–32>|WORD<1–32>** | WORD<1–32> — Specifies a new entry with this group name. The range is 1-32 characters. 

**view WORD<1–32>|WORD<1–32>** | WORD<1–32> — Specifies the prefix that defines the set of MIB objects accessible by this SNMP entity. The range is 1 to 32 characters.

---

**Enabling SNMP trap logging**

Use SNMP trap logging to send a copy of all traps to the syslog server.

**Before you begin**

- You must configure and enable the syslog server.
About this task

Note:

The platform logs CLILOG and SNMPLOG as INFO. Normally, if you configure the logging level to WARNING, the system skips all INFO messages. However, if you enable CLILOG and SNMPLOG the system logs ACLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

Procedure

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. Enable SNMP trap logging:
   ```
   snmplog enable
   ```
3. (Optional) Disable SNMP trap logging:
   ```
   no snmplog enable
   ```
4. View the contents of the SNMP log:
   ```
   show logging file module snmplog
   ```

Example

Enable SNMP trap logging and view the contents of the SNMP log:

```bash
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#snmplog enable
Switch:1(config-app)#show logging file module snmp
CP1 [02/06/15 22:39:58.530:UTC] 0x00004595 00000000 GlobalRouter SNMP INFO Booted with file
CP1 [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR GlobalRouter SNMP INFO 2k card up(CardNum=1 AdminStatus=1 OperStatus=1)
CP1 [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR GlobalRouter SNMP INFO 2k card up(CardNum=2 AdminStatus=1 OperStatus=1)
CP1 [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR GlobalRouter SNMP INFO 2k card up(CardNum=3 AdminStatus=1 OperStatus=1)
CP1 [02/06/15 22:40:45.839:UTC] 0x000045e5 00400005 DYNAMIC SET GlobalRouter SNMP INFO Sending Cold-Start Trap
```

Variable definitions

Use the data in the following table to use the `snmplog` command.

Table 18: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the logging of traps.</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Use the command <code>no snmplog enable</code> to disable the logging of traps.</td>
</tr>
<tr>
<td>file [grep WORD&lt;1–255&gt;[tail]]</td>
<td>The parameter only applies to log files generated by releases prior to Release 3.2:</td>
</tr>
<tr>
<td></td>
<td>Shows the trap log file stored on external flash. You can optionally specify search or display parameters:</td>
</tr>
<tr>
<td></td>
<td>• grep WORD&lt;1–255&gt; performs a string search in the log file. WORD&lt;1–255&gt; is the string, of up to 255 characters in length, to match.</td>
</tr>
<tr>
<td></td>
<td>• tail shows the last results first.</td>
</tr>
</tbody>
</table>
Chapter 12: SNMP trap configuration using EDM

Use Simple Network Management Protocol (SNMP) traps and notifications to gather information about device activities, alarms, and other information on management stations. This section provides procedures to configure and use SNMP traps in Enterprise Device Manager (EDM).

For information about how to configure SNMP community strings and related topics, see Security for Avaya Virtual Services Platform 4000 Series, NN46251-601.

Configuring an SNMP host target address

About this task
Configure a target table to specify the list of transport addresses to use in the generation of SNMP messages.

Procedure
1. In the navigation tree, expand the following folders: Configuration > Edit > SnmpV3.
2. Click Target Table.
3. In the Target Table tab, click Insert.
4. In the Name box, type a unique identifier.
5. In the TDomain box, select the transport type of the address. Select either ipv4Tdomain or ipv6Tdomain.
6. In the TAddress box, type the transport address and User Datagram Protocol (UDP) port.
7. In the Timeout box, type the maximum round trip time.
8. In the RetryCount box, type the number of retries to be attempted.
9. In the TagList box, type the list of tag values.
10. In the Params box, type the SnmpAdminString.
11. In the TMask box, type the mask.
12. In the MMS box, type the maximum message size.
13. Click Insert.
Target Table field descriptions

Use the data in the following table to use the **Target Table** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a unique identifier for this table. The name is a community string.</td>
</tr>
<tr>
<td>TDomain</td>
<td>Specifies the transport type of the address. <strong>ipv4Tdomain</strong> specifies the transport type of address is an IPv4 address. <strong>ipv6Tdomain</strong> specifies the transport type of address is IPv6. The default is ipv4Tdomain.</td>
</tr>
<tr>
<td>TAddress</td>
<td>Specifies the transport address in xx.xx.xx.xx:port format, for example: 10:10:10:10:162, where 162 is the trap listening port on the system 10.10.10.10.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specifies the maximum round trip time required to communicate with the transport address. The value is in 1/100 seconds from 0–2147483647. The default is 1500. After the system sends a message to this address, if a response (if one is expected) is not received within this time period, you can assume that the response is not delivered.</td>
</tr>
<tr>
<td>RetryCount</td>
<td>Specifies the maximum number of retries if a response is not received for a generated message. The count can be in the range of 0–255. The default is 3.</td>
</tr>
<tr>
<td>TagList</td>
<td>Contains the tag values used to select target addresses for a particular operation. A tag refers to a class of targets to which the messages can be sent.</td>
</tr>
<tr>
<td>Params</td>
<td>Contains SNMP parameters used to generate messages to send to this transport address. For example, to receive SNMPv2C traps, use TparamV2.</td>
</tr>
<tr>
<td>TMask</td>
<td>Specifies the mask. The value can be empty or in six-byte hex string format. Tmask is an optional parameter that permits an entry in the TargetAddrTable to specify multiple addresses.</td>
</tr>
<tr>
<td>MMS</td>
<td>Specifies the maximum message size. The size can be zero, or 484–2147483647. The default is 484. Although the maximum MMS is 2147483647, the device supports the maximum SNMP packet size of 8192.</td>
</tr>
</tbody>
</table>
Configuring target table parameters

About this task
Configure the target table to configure the security parameters for SNMP. Configure the target table to configure parameters such as SNMP version and security levels.

Procedure
1. In the navigation tree, expand the following folders: Configuration > Edit > SnmpV3.
2. Click Target Table.
3. Click the Target Params Table tab.
4. Click Insert.
5. In the Name box, type a target table name.
6. From the MPModel options, select an SNMP version.
7. From the Security Model options, select the security model.
8. In the SecurityName box, type readview or writeview.
9. From the SecurityLevel options, select the security level for the table.
10. Click Insert.

Target Params Table field descriptions
Use the data in the following table to use the Target Params Table tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifies the target table.</td>
</tr>
<tr>
<td>MPModel</td>
<td>Specifies the message processing model to use to generate messages: SNMPv1, SNMPv2c, or SNMPv3/USM.</td>
</tr>
<tr>
<td>SecurityModel</td>
<td>Specifies the security model to use to generate messages: SNMPv1, SNMPv2c, or USM. You can receive an inconsistentValue error if you try to configure this variable to a value for a security model that the implementation does not support.</td>
</tr>
<tr>
<td>SecurityName</td>
<td>Identifies the principal on whose behalf SNMP messages are generated.</td>
</tr>
<tr>
<td>SecurityLevel</td>
<td>Specifies the security level used to generate SNMP messages: noAuthNoPriv, authNoPriv, or authPriv.</td>
</tr>
</tbody>
</table>
Configuring SNMP notify filter profiles

About this task
Configure the SNMP table of filter profiles to determine whether particular management targets receive particular notifications.

Procedure
1. In the navigation tree, expand the following folders: Configuration > Edit > SnmpV3.
2. Click Notify Table.
3. Click the Notify Filter Table tab.
4. Click Insert.
5. In the NotifyFilterProfileName box, type a name for the notify filter profile.
6. In the Subtree box, type subtree location information in x.x.x.x.x.x.x.x.x.x format.
7. In the Mask box, type the mask location in hex string format.
8. From the Type options, select included or excluded.
9. Click Insert.

Notify Filter Table field descriptions
Use the data in the following table to use the Notify Filter Table tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotifyFilterProfileName</td>
<td>Specifies the name of the filter profile used to generate notifications.</td>
</tr>
<tr>
<td>Subtree</td>
<td>Specifies the MIB subtree that, if you combine it with the mask, defines a family of subtrees, which are included in or excluded from the filter profile. For more information, see RFC2573.</td>
</tr>
<tr>
<td>Mask</td>
<td>Specifies the bit mask (in hexadecimal format) that, in combination with Subtree, defines a family of subtrees, which are included in or excluded from the filter profile.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the family of filter subtrees are included in or excluded from a filter. The default is included.</td>
</tr>
</tbody>
</table>

Configuring SNMP notify filter profile table parameters

Before you begin
- The notify filter profile exists.
About this task
Configure the profile table to associate a notification filter profile with a particular set of target parameters.

Procedure
1. In the navigation tree, expand the following folders: Configuration > Edit > SnmpV3.
2. Click Notify Table.
3. Click the Notify Filter Profile Table tab.
4. Click Insert.
5. In the TargetParamsName box, type a name for the target parameters.
6. In the NotifyFilterProfileName box, type a name for the notify filter profile.
7. Click Insert.

Notify Filter Profile Table field descriptions
Use the data in the following table to use the Notify Filter Profile Table tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetParamsName</td>
<td>Specifies the unique identifier associated with this entry.</td>
</tr>
<tr>
<td>NotifyFilterProfileName</td>
<td>Specifies the name of the filter profile to use to generate notifications.</td>
</tr>
</tbody>
</table>

Enabling authentication traps

About this task
Enable the SNMP agent process to generate authentication-failure traps.

Procedure
1. In the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click General.
3. Click the Error tab.
4. Select AuthenticationTraps.
5. Click Apply.

Error field descriptions
Use the data in the following table to use the Error tab.
### SNMP Trap Configuration Using EDM

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthenticationTraps</td>
<td>Enables or disables the sending of traps after an error occurs. The default is disabled.</td>
</tr>
<tr>
<td>LastErrorCode</td>
<td>Specifies the last reported error code.</td>
</tr>
<tr>
<td>LastErrorSeverity</td>
<td>Specifies the last reported error severity:</td>
</tr>
<tr>
<td></td>
<td>0= Informative Information</td>
</tr>
<tr>
<td></td>
<td>1= Warning Condition</td>
</tr>
<tr>
<td></td>
<td>2= Error Condition</td>
</tr>
<tr>
<td></td>
<td>3= Manufacturing Information</td>
</tr>
<tr>
<td></td>
<td>4= Fatal Condition</td>
</tr>
</tbody>
</table>

Comments on this document? infodev@avaya.com
Chapter 13: Traps reference

The Virtual Services Platform 4000 generates alarms, traps, and logs. This section provides information about traps.

Proprietary traps

The following tables describe Avaya proprietary traps for Virtual Services Platform 4000. All of the following traps have a status of current.

**Table 19: 1.3.6.1.4.1.45.4.8.0.xx series**

<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.45.4.8.0.1</td>
<td>slaMonitorAgentExceptionDetected</td>
<td>slaMonitorAgentExceptionDetected</td>
<td>The SLA Monitor (SLA Mon™) agent process has terminated unexpectedly. You must reenable SLA Monitor to restart the SLA Monitor agent.</td>
</tr>
</tbody>
</table>

**Table 20: 1.3.6.1.4.1.2272.1.21.0.xx series**

<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.3</td>
<td>rcnErrorNotification</td>
<td>rcErrorLevel rcErrorCode rcErrorText</td>
<td>An rcnErrorNotification trap signifies that the SNMPv2 entity, acting in an agent role, has detected that an error condition has occurred.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.4</td>
<td>rcnStpNewRoot</td>
<td>rcStgId</td>
<td>An rcnStpNewRoot trap signifies that the SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has declared the device to be the new root of the spanning tree.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.5</td>
<td>rcnStpTopologyChange</td>
<td>rcStgId rcPortIndex</td>
<td>An rcnStpTopologyChange trap signifies that the SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has declared the device to be the new root of the spanning tree.</td>
</tr>
<tr>
<td>OID</td>
<td>Notification type</td>
<td>Objects</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.6</td>
<td>rcnChasPowerSupplyDown</td>
<td>rcChasPowerSupplyId, rcChasPowerSupplyOperStatus</td>
<td>An rcnChasPowerSupplyDown trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply unit is about to transition into the down state.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.7</td>
<td>rcnChasFanDown</td>
<td>rcChasFanId, rcChasFanOperStatus</td>
<td>An rcnChasFanDown trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcChasFanOperStatus object for one of its power supply units is about to transition into the down state.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.8</td>
<td>rcnLinkOscillation</td>
<td>rcPortIndex</td>
<td>An rcnLinkOscillation trap signifies that the SNMPv2 entity, acting in an agent role, has detected an excessive number of link state transitions on the specified port.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.9</td>
<td>rcnMacViolation</td>
<td>rcErrorText, rcPortIndex</td>
<td>An rcnMacViolation trap signifies that the SNMPv2 entity, acting in an agent role, has received a PDU with an invalid source MAC address.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.13</td>
<td>rcn2kTemperature</td>
<td>rc2kChassisTemperature</td>
<td>An rcn2kTemperature trap signifies that the SNMPv2 entity, acting in an agent role, has detected the chassis is overheating.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.14</td>
<td>rcnChasPowerSupplyUp</td>
<td>rcChasPowerSupplyId, rcChasPowerSupplyOperStatus</td>
<td>An rcnChasPowerSupplyUp trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply unit is about to transition into the up state.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.16</td>
<td>rcnStpTCN</td>
<td>rcStgId, rcPortIndex, rcStgBridgeAddress</td>
<td>An rcnStpTCN trap signifies that the SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has gone due to a topology change event.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.17</td>
<td>rcnSmltListLinkUp</td>
<td>—</td>
<td>An rcnSmltListLinkUp trap signifies that the split MLT link is from down to up.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.18</td>
<td>rcnSmltListLinkDown</td>
<td>—</td>
<td>An rcnSmltListLinkDown trap signifies that the split MLT link is from up to down.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.19</td>
<td>rcnSmltLinkUp</td>
<td>rcMltSmltId</td>
<td>An rcnSmltLinkUp trap signifies that the split SMLT link is up.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.20</td>
<td>rcnSmltLinkDown</td>
<td>rcmltSmltId</td>
<td>An rcnSmltLinkDown trap signifies that the split SMLT link is down.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.21</td>
<td>rcnChasFanUp</td>
<td>rcChasFanId, rcChasFanOperStatus</td>
<td>An rcnChasFanUp trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcChasFanOperStatus object for one of its power supply unit is about to transition into the up state.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.22</td>
<td>rcnPasswordChange</td>
<td>rcCliPasswordChange, rcCliPassChangeResult</td>
<td>An rcnPasswordChange trap signifies that the SNMPv2 entity, acting in an agent role, has detected that one of the ACLI passwords is changed.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.23</td>
<td>rcnEmError</td>
<td>rc2kCardIndex, rcChasEmModeError</td>
<td>An rcnEmError trap signifies that the SNMPv2 entity, acting in an agent role, has detected Em error.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.26</td>
<td>rcnSmartCpldTimerFired</td>
<td>rc2kCardIndex</td>
<td>An rcnSmartCpldTimerFired trap signifies that the CP ID timer fired.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.27</td>
<td>rcnCardCpldNotUpdate</td>
<td>rc2kCardIndex</td>
<td>An rcnCardCpldNotUpdate trap signifies that the CP ID is not up to date.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.28</td>
<td>rcnIgapLogFileFull</td>
<td></td>
<td>An rcnIgapLogFileFull trap signifies that the IGAP accounting time-out Log File has reached the maximum.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.30</td>
<td>rcnSshServerEnabled</td>
<td>rcSshGlobalPort</td>
<td>An rcnSshServerEnabled trap signifies that the SSH server is enabled.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.31</td>
<td>rcnSshServerDisabled</td>
<td>rcSshGlobalPort</td>
<td>An rcnSshServerDisabled trap signifies that the SSH server is disabled.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.37</td>
<td>rcnSaveConfigAction</td>
<td>rcSysActionL1</td>
<td>An rcnSaveConfigAction trap indicates the switch run time or boot configuration is being saved.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.38</td>
<td>rcnLoopDetectOnPort</td>
<td>rcVlanId, rcPortIndex</td>
<td>An rcnLoopDetectOnPort trap indicates that a loop has been detected on a port. The VLAN on that port will be disabled.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.41</td>
<td>rcnAggLinkUp</td>
<td>rcMltId</td>
<td>An rcnAggLinkUp trap is generated when the operational state of the aggregator changes from down to up.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.42</td>
<td>rcnAggLinkDown</td>
<td>rcMltId</td>
<td>An rcnAggLinkDown trap is generated when the operational state of the aggregator changes from up to down.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.59</td>
<td>rcnFdbProtectViolation</td>
<td>rcPortIndex, rcVlanId</td>
<td>The rcnFdbProtectViolation trap signifies that the has violated the user configured limit for total number of fdb-entries learned on that port.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.60</td>
<td>rcnLogMsgControl</td>
<td>rcSysMsgLogFrequency rcSysMsgLogText</td>
<td>An rcnLogMsgControl trap signifies whether the number of times of repetition of the particular Log message has exceeded the particular frequency/count or not.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.61</td>
<td>rcnSaveConfigFile</td>
<td>rcSysActionL1 rcSysConfigFileName</td>
<td>An rcnSaveConfigFile trap signifies that either the runtime config or the boot config has been saved on the switch.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.62</td>
<td>rcnDNSRequestResponse</td>
<td>rcSysDnsServerListIpAddress rcSysDnsRequestType</td>
<td>An rcnDNSRequestResponse trap signifies that the switch had sent a query to the DNS server or it had received a successful response from the DNS Server.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.63</td>
<td>rcnDuplicateIpAddress</td>
<td>ipNetToMediaNetAddress ipNetToMediaPhysAddress</td>
<td>An rcnDuplicateIpAddress trap signifies that a duplicate IP address is detected on the subnet.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.64</td>
<td>rcnLoopDetectPortDown</td>
<td>rcPortIndex ifAdminStatus ifOperStatus</td>
<td>An rcnLoopDetectPortDown trap signifies that a loop has been detected on a port and the port is going to shut down.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.65</td>
<td>rcnLoopDetectMacDiscard</td>
<td>rcPortIndex rcSysMacFlapLimitTime rcSysMacFlapLimitCount</td>
<td>An rcnLoopDetectMacDiscard trap signifies that a loop has been detected on a port and the MAC address will be discarded on all ports in that VLAN.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.66</td>
<td>rcnAutoRecoverPort</td>
<td>rcPortIndex</td>
<td>An rcnAutoRecoverPort trap signifies that autorecovery has reenabled a port disabled by link flap.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.67</td>
<td>rcnAutoRecoverLoopDetectedPort</td>
<td>rcVlanNewLoopDetectAction</td>
<td>An rcnAutoRecoverPort trap signifies that autorecovery has cleared the action taken on a port by loop detect.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.68</td>
<td>rcnVlacpPortDown</td>
<td>rcPortIndex</td>
<td>An rcnVlacpPortDown trap signifies that VLACP is down on the port specified.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.69</td>
<td>rcnVlacpPortUp</td>
<td>rcPortIndex</td>
<td>An rcnVlacpPortUp trap signifies that VLACP is up on the port specified.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.70</td>
<td>rcnEapMacIntrusion</td>
<td>rcSysIpAddr rcRadiusPaePortNumber rcRadiusEapLastAuthMac rcRadiusEapLastRejMac</td>
<td>An rcnEapMacIntrusion trap signifies that an EAP MAC intrusion has occurred on this port.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.71</td>
<td>rcnMaxRouteWarnClear</td>
<td>rcVrfName</td>
<td>An rcnMaxRouteWarnClear trap signifies that the number of routes in the routing...</td>
</tr>
</tbody>
</table>

**Table continues…**
<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.111</td>
<td>rcnMaxRouteWarnSet</td>
<td>rcVrfName</td>
<td>An rcnMaxRouteWarnSet trap signifies that the virtual router routing table is reaching its maximum size. Take action to prevent this.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.112</td>
<td>rcnMaxRouteDropClear</td>
<td>rcVrfName</td>
<td>An rcnMaxRouteDropClear trap signifies that the virtual router routing table is no longer dropping new routes as it is below the maximum size.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.113</td>
<td>rcnMaxRouteDropSet</td>
<td>rcVrfName</td>
<td>An rcnMaxRouteDropSet trap signifies that the virtual router routing table has reached the maximum size, and is now dropping all new nonstatic routes.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.117</td>
<td>rcnMstpNewCistRoot</td>
<td>rcStgBridgeAddress</td>
<td>An rcnMstpNewCistRoot trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the Multiple Spanning Tree Protocol has declared the device to be the new root of the common internal spanning tree.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.118</td>
<td>rcnMstpNewMstiRoot</td>
<td>rcStgBridgeAddress, rcStgId</td>
<td>An rcnMstpNewMstiRoot trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the Multiple Spanning Tree Protocol has declared the device to be the new root of the spanning tree instance.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.119</td>
<td>rcnMstpNewCistRegionalRoot</td>
<td>rcStgBridgeAddress</td>
<td>An rcnMstpNewCistRegionalRoot trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the Multiple Spanning Tree Protocol has declared the device to be the new regional root of the common internal spanning tree.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.120</td>
<td>rcnRstpNewRoot</td>
<td>rcStgBridgeAddress</td>
<td>An rcnRstpNewRoot trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the Rapid Spanning Tree Protocol has declared the device to be the new root of the spanning tree.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.124</td>
<td>rcnRsmltEdgePeerModified</td>
<td>rcVlanId</td>
<td>An rcnRsmltEdgePeerModified trap signifies that the RSMLT peer address is different from that of the stored address. You must save the configuration if EdgeSupport has to use this information on the next restart.</td>
</tr>
</tbody>
</table>

*Table continues*
<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.167</td>
<td>rcnChasPowerSupplyNoRedundancy</td>
<td>—</td>
<td>An rcnChasPowerSupplyNoRedundancy trap signifies that the chassis is running on power supply without redundancy.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.168</td>
<td>rcnChasPowerSupplyRedundancy</td>
<td>—</td>
<td>An rcnChasPowerSupplyRedundancy trap signifies that the chassis is running on power supply with redundancy.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.171</td>
<td>rcnLicenseTrialPeriodExpired</td>
<td>rcSysLicenseTrialDaysLeft</td>
<td>An rcnLicenseTrialPeriodExpired trap signifies that the Trial Period License has expired.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.172</td>
<td>rcnLicenseTrialPeriodExpiry</td>
<td>rcVrfName rcVrfOperStatus</td>
<td>An rcnLicenseTrialPeriodExpiry trap signifies the time remaining, in days, before the License Trial Period expires.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.173</td>
<td>rcnVrfUp</td>
<td>rcVrfName rcVrfOperStatus</td>
<td>This notification is generated when the operational status of the specified VRF is toggled from down to up.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.174</td>
<td>rcnVrfDown</td>
<td>rcVrfName rcVrfOperStatus</td>
<td>This notification is generated when the operational status of the specified VRF is toggled from up to down.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.175</td>
<td>rcnMrouteIngressThresholdExceeded</td>
<td>rclpResourceUsageGlo balIngressRecInUse rclpResourceUsageGlo balIngressThreshold</td>
<td>This notification is generated when the number of mroute ingress records exceeds the ingress threshold.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.176</td>
<td>rcnMrouteEgressThresholdExceeded</td>
<td>rclpResourceUsageGlo balEgressRecInUse rclpResourceUsageGlo balEgressThreshold</td>
<td>This notification is generated when the number of mroute egress records exceeds the egress threshold.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.185</td>
<td>rcnChasPowerSupplyRunningLow</td>
<td>—</td>
<td>An rcnChasPowerSupplyRunningLow trap signifies that the chassis is running on low power supply.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.192</td>
<td>rcnIsisPlsbMetricMismatchTrap</td>
<td>rclIsisLocalLspId rclIsisLocalL1Metric rclIsisNgbLspId rclIsisNgbL1Metric rclIsisPlsbTrapType rclIsisTrapIndicator rclIsisLocalHostName rclIsisNgbHostName</td>
<td>An rcnIsisPlsbMetricMismatchTrap signifies that an Link State Packet (LSP) with a different value of Level 1 metric is received.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.193</td>
<td>rcnIsisPlsbDuplicateSysidTrap</td>
<td>rclIsisLocalSysId rclIsisLocalInterface rclIsisPlsbTrapType rclIsisTrapIndicator</td>
<td>An rcnIsisPlsbDuplicateSysidTrap signifies that a Hello packet with a duplicate system ID is received.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.194</td>
<td>rcnIsisPlsbLsdbUpdateTrap</td>
<td>rcIsisPlsbTrapType</td>
<td>An rcnIsisPlsbLsdbUpdateTrap signifies that link state database (LSDB) information has changed.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.196</td>
<td>rcnChasFanCoolingLow</td>
<td>rcChasFanOperStatus rcChasFanType rcErrorLevel rcErrorText</td>
<td>An rcnChasFanCoolingLow trap signifies that the chassis is running on low fan cooling.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.278</td>
<td>rcnIsisPlsbBvidMismatchTrap</td>
<td>rcIsisLocalSysId rcIsisLocalPrimaryBvid rcIsisLocalPrimaryTieBreakAlg rcIsisLocalSecondaryBvid rcIsisLocalSecondaryTieBreakAlg rcIsisNgbSysId rcIsisNgbPrimaryBvid rcIsisNgbPrimaryTieBreakAlg rcIsisNgbSecondaryBvid rcIsisNgbSecondaryTieBreakAlg rcIsisLocalBvidCounter rcIsisNgbBvidCounter rcIsisPlsbTrapType rcIsisTrapIndicator rcIsisNgbHostName</td>
<td>An rcnIsisPlsbBvidMismatchTrap signifies when a backbone VLAN ID (BVID) Type-Length-Value (TLV) from a neighbor node does not match the local configuration.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.279</td>
<td>rcnIsisPlsbSmltVirtBmacMismatchTrap</td>
<td>rcIsisLocalVirtualBmac rcIsisPeerVirtualBmac rcIsisPlsbTrapType rcIsisTrapIndicator</td>
<td>An rcnIsisPlsbSmltVirtBmacMismatchTrap signifies that the virtual Backbone MAC (BMAC) configured in the switch is different from the virtual BMAC configured on the interswitch trunking (IST) peer.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.280</td>
<td>rcnIsisPlsbSmltPeerBmacMismatchTrap</td>
<td>rcIsisSysId rcIsisSmltPeerSysId rcIsisPlsbTrapType rcIsisTrapIndicator</td>
<td>An rcnIsisPlsbSmltPeerBmacMismatchTrap signifies that either the Split MultiLink Trunking (SMLT) peer Backbone MAC (BMAC) configured in the interswitch trunking (IST) peer is different from the Intermediate-System-to-Intermediate-System (IS-IS) System ID of the local switch or the SMLT peer BMAC configured on the local switch is different from the IS-IS System ID of the IST peer.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.281</td>
<td>rcnIsisPlsbAdjStateTrap</td>
<td>rcIsisNgbSysId, rcIsisLocalInterface, rcIsisPlsbTrapType, rcIsisAdjState, rcIsisNgbHostName</td>
<td>An rcnIsisPlsbAdjStateTrap signifies when IS-IS adjacency state changes.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.282</td>
<td>rcnIsisPlsbDuplicateNNameTrap</td>
<td>rcIsisNgbNickname, rcIsisPlsbTrapType, rcIsisTrapIndicator, rcIsisNgbSysId, rcIsisDuplicateNNameCounter, rcIsisNgbHostName</td>
<td>An rcnIsisPlsbDuplicateNNameTrap signifies that a Link State Packet (LSP) with a duplicate nickname is received. The trap should be generated by all the switches in the network.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.283</td>
<td>rcnIsisPlsbSplitBebMismatchTrap</td>
<td>rcIsisLocalSmltSplitBeb, rcIsisPeerSmltSplitBeb, rcIsisPlsbTrapType, rcIsisTrapIndicator</td>
<td>An rcnIsisPlsbSplitBebMismatchTrap signifies that the SMLT Split Backbone Edge Bridge (BEB) configured on the local switch and the IST peer are the same. One IST switch must be configured as the primary Split BEB and the other IST peer must be configured as the secondary Split BEB.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.284</td>
<td>rcnIsisPlsbMultiLinkAdjTrap</td>
<td>rcIsisNgbSysId, rcIsisLocalInterface, rcIsisPrevInterface, rcIsisPlsbTrapType, rcIsisNgbHostName, rcIsisTrapIndicator</td>
<td>An rcnIsisPlsbMultiLinkAdjTrap signifies when the Intermediate-System-to-Intermediate-System (IS-IS) protocol forms more than one adjacency with the same IS-IS.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.285</td>
<td>rcnA SSHSessionLogout</td>
<td>rcSshGlobalHostIpAddr</td>
<td>An rcnA SSHSessionLogout trap signifies a Secure Shell (SSH) session logout.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.286</td>
<td>rcnA UnauthorizedAccess</td>
<td>rcSshGlobalHostIpAddr</td>
<td>An rcnA UnauthorizedAccess trap signifies that an unauthorized access has occurred. It is deprecated by rcnA UnauthorizedAccess.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.287</td>
<td>rcnA AuthenticationSuccess</td>
<td>rcLoginUserName, rcLoginHostIpAddress</td>
<td>An rcnA AuthenticationSuccess trap signifies that a login is successful. The Trap includes the login username and the host IP address. It is deprecated by rcnA AuthenticationSuccess.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.288</td>
<td>rcnA SSHSessionLogin</td>
<td>rcSshGlobalHostIpAddr</td>
<td>An rcnA SSHSessionLogin trap signifies that there is a Secure Shell (SSH) session login.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.21.0.305</td>
<td>RcisIsIsPlsbSmltBmacMisconfigTrap</td>
<td>rcIsisSmltBmacNodeSysId, rcIsisPlsbTrapType</td>
<td>An SPBM ISIS trap signifies that SMLT virtual BMAC has been used by nodes other than the SMLT nodes as system-id or MAC.</td>
</tr>
</tbody>
</table>

Table continues…
### Table 21: 1.3.6.1.4.1.2272.1.206.x.x.x series

<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.2272.1.206.1.0.1</td>
<td>rcVrrpTmpTrapNewMaster</td>
<td>rcVrrpTmpOperationsMasterIpAddr&lt;br&gt;rcVrrpTmpNewMasterReason</td>
<td>This notification is generated when Virtual Router Redundancy Protocol (VRRP) transitions to the master.</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2272.1.206.2.2.1</td>
<td>rcVrrpExtTrapStateTransition</td>
<td>ifIndex&lt;br&gt;rcVrrpExtTrapStateTransitionType&lt;br&gt;rcVrrpExtTrapStateTransitionCause&lt;br&gt;rcVrrpExtOperationsVrid&lt;br&gt;rcVrrpTmpOperationsPrimaryIpAddr&lt;br&gt;rcVrrpTmpOperationsMasterIpAddr</td>
<td>This notification is generated when a transition happens in the state of Virtual Router Redundancy Protocol (VRRP), for instance, a transition from master to backup when shutdown is received.</td>
</tr>
</tbody>
</table>

### Standard traps

The following table describes standard traps that Virtual Services Platform 4000 can generate.

#### Table 22: Standard traps

<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.16.0.1</td>
<td>risingAlarm</td>
<td>alarmIndex&lt;br&gt;alarmVariable&lt;br&gt;alarmSampleType&lt;br&gt;alarmValue&lt;br&gt;alarmRisingThreshold</td>
<td>The SNMP trap that is generated after an alarm entry crosses the rising threshold and generates an event that is configured to send SNMP traps. TRAP TYPE ENTERPRISE rmon</td>
</tr>
<tr>
<td>1.3.6.1.2.1.16.0.2</td>
<td>fallingAlarm</td>
<td>alarmIndex&lt;br&gt;alarmVariable&lt;br&gt;alarmSampleType&lt;br&gt;alarmValue&lt;br&gt;alarmFallingThreshold</td>
<td>The SNMP trap that is generated after an alarm entry crosses the falling threshold and generates an event that is configured to send SNMP traps. TRAP TYPE ENTERPRISE rmon</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.46.1.3.0.3</td>
<td>vrrpTrapsStateTrans</td>
<td>ifIndex vrrpTrapsStateTransitionType vrrpTrapsStateTransitionCause vrrpOperVrId vrrpOperIpAddr ipAdEntAddr</td>
<td>A vrrpTrapsStateTransition trap signifies a state transition has occurred on a particular Virtual Router Redundancy Protocol (VRRP) interface. Implementation of this trap is optional. vrrpOperIpAddr contains the IP address of the VRRP interface while ipAdEntAddr contains the IP address assigned to the physical interface.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.68.0.1</td>
<td>vrrpTrapsNewMaster</td>
<td>vrrpOperMasterIpAddr</td>
<td>The newMaster trap indicates that the sending agent has transitioned to Master state.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.68.0.2</td>
<td>vrrpTrapsAuthFailure</td>
<td>vrrpTrapsPacketSrc vrrpTrapsAuthErrorType</td>
<td>A vrrpAuthFailure trap signifies that a packet has been received from a router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.80.0.1</td>
<td>pingProbeFailed</td>
<td>pingCtlTargetAddressType pingCtlTargetAddress pingResultsOperStatus pingResultsIpTargetAddressType pingResultsIpTargetAddress pingResultsMinRtt pingResultsMaxRtt pingResultsAverageRtt pingResultsProbeResponse pingResultsSentProbes pingResultsRttSumOfSquares pingResultsLastGoodProbe</td>
<td>This trap is generated after a probe failure is detected when the corresponding pingCtlTrapGeneration object is configured to probeFailure(0) subject to the value of pingCtlTrapProbeFailureFilter. The object pingCtlTrapProbeFailureFilter can specify the number of successive probe failures required before this notification can be generated.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.80.0.2</td>
<td>pingTestFailed</td>
<td>pingCtlTargetAddressType pingCtlTargetAddress pingResultsOperStatus pingResultsIpTargetAddressType pingResultsIpTargetAddress pingResultsMinRtt pingResultsMaxRtt</td>
<td>This trap is generated after a ping test fails when the corresponding pingCtlTrapGeneration object is configured to testFailure(1). In this instance pingCtlTrapTestFailureFilter specifies the number of probes in a test required to fail to consider the test as failed.</td>
</tr>
</tbody>
</table>

*Table continues...*
<table>
<thead>
<tr>
<th>OID</th>
<th>Notification type</th>
<th>Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>pingResultsAverageRtt pingResultsProbeResponses pingResultsSentProbes pingResultsRttSumOfSquares pingResultsLastGoodProbe</td>
<td>This trap is generated at the completion of a ping test when the corresponding pingCtlTrapGeneration object is configured to testCompletion(4).</td>
</tr>
<tr>
<td>1.3.6.1.2.1.80.0.3</td>
<td>pingTestCompleted</td>
<td>pingCtlTargetAddressType pingCtlTargetAddress pingResultsOperStatus pingResultsIpTargetAddressType pingResultsIpTargetAddress pingResultsMinRtt pingResultsMaxRtt pingResultsAverageRtt pingResultsProbeResponses pingResultsSentProbes pingResultsRttSumOfSquares pingResultsLastGoodProbe</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.2.1.81.0.1</td>
<td>traceRoutePathChanged</td>
<td>traceRouteCtlTargetAddressType traceRouteCtlTargetAddress traceRouteResultsIpTgtAddrType traceRouteResultsIpTgtAddr</td>
<td>This trap is generated after the path to a target changes.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.81.0.2</td>
<td>traceRouteTestFailed</td>
<td>traceRouteCtlTargetAddressType traceRouteCtlTargetAddress traceRouteResultsIpTgtAddrType traceRouteResultsIpTgtAddr</td>
<td>This trap is generated is traceroute cannot determine the path to a target (traceRouteNotifications 2).</td>
</tr>
<tr>
<td>1.3.6.1.2.1.81.0.3</td>
<td>traceRouteTestCompleted</td>
<td>traceRouteCtlTargetAddressType traceRouteCtlTargetAddress traceRouteResultsIpTgtAddr</td>
<td>This trap is generated after the path to a target is determined.</td>
</tr>
<tr>
<td>OID</td>
<td>Notification type</td>
<td>Objects</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1.3.6.1.6.3.1.1.5.1</td>
<td>coldStart</td>
<td>AddrType</td>
<td>traceRouteResultsIpTgt Addr</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing and that its configuration may have been altered.</td>
</tr>
<tr>
<td>1.3.6.1.6.3.1.1.5.2</td>
<td>warmStart</td>
<td>—</td>
<td>A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing such that its configuration is unaltered.</td>
</tr>
<tr>
<td>1.3.6.1.6.3.1.1.5.3</td>
<td>linkDown</td>
<td>—</td>
<td>A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent configuration. TRAP-TYPE ENTERPRISE snmp</td>
</tr>
<tr>
<td>1.3.6.1.6.3.1.1.5.4</td>
<td>linkUp</td>
<td>—</td>
<td>A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent configuration has come up. TRAP-TYPE ENTERPRISE snmp</td>
</tr>
<tr>
<td>1.3.6.1.6.3.1.1.5.5</td>
<td>authenticationFailure</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
Chapter 14: Hardware troubleshooting

The following sections provide troubleshooting information for common hardware problems.

Using trace to diagnose hardware problems

Before you begin

• You must log on to the Privileged EXEC mode in ACLI.

About this task

Use trace to observe the status of a hardware module at a given time.

Procedure

1. Begin the trace operation:
   ```
   line-card 1 trace level [{67–179} {0–4}]
   ```

2. Search the trace for a specific string value:
   ```
   line-card 1 trace grep [WORD<0–1024>]
   ```

Example

VSP-4850GTSPWR+:1>enable
Begin the trace operation:
VSP-4850GTSPWR+:1#line-card 1 trace level 67 1
Search the trace for a specific string value:
VSP-4850GTSPWR+:1#line-card 1 trace grep 00-1A-4B-8A-FB-6B

Variable definitions

Use the data in the following table to use the `line-card 1` command.
Table 23: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>{67–179} {0–4}</td>
<td>Starts the trace by specifying the module ID and level.</td>
</tr>
<tr>
<td></td>
<td>&lt;67-179&gt; specifies the module ID.</td>
</tr>
<tr>
<td></td>
<td>&lt;0-4&gt; specifies the trace level from 0–4, where 0 is disabled; 1 is</td>
</tr>
<tr>
<td></td>
<td>very terse; 2 is terse; 3 is very verbose, 4 is verbose.</td>
</tr>
<tr>
<td>WORD&lt;0–1024&gt;</td>
<td>Performs a string search in the trace.</td>
</tr>
</tbody>
</table>

Troubleshooting USB viewing problems

After you insert a USB device in the USB slot, the Linux system automatically detects and mounts the device. If you cannot view files on the device, perform this procedure.

* Note:

This procedure applies only to the VSP 4450 platform. It does not apply to the VSP 4850 platform.

**Procedure**

1. Enter Privileged EXEC mode:
   
   `enable`

2. Check the file system:
   
   `ls /usb/`

3. Remove a USB device:
   
   a. Unmount the USB device:
      
      `usb-stop`
   
   b. Wait for the response that indicates it is safe to remove the device.
   
   c. Physically remove the device.

4. Remove and then reinsert the device.

5. Check the device for errors:
   
   `dos-chkdsk /usb`

   Run the `dos-chkdsk /usb repair` command, if at the end of the `dos-chkdsk /usb` command output you see:
   
   1) Correct
   
   2) Don’t correct
6. If errors are detected, then you can reformat the device:

    dos-format /usb

⚠️ Caution:

If you format the device, you erase all data on the device.

Example

Check the file system:

Switch:1>enable
Switch:1#ls /usb/
Listing Directory /usb/:
drwxr-xr-x 4 0 0 4096 Jan 1 1970 ./
drwxrwxr-x 22 0 0 0 Sep 9 20:22 ../
drwxr-xr-x 2 0 0 4096 Mar 17 16:03 Photos-of-Flash-
drwxr-xr-x 2 0 0 4096 Jun 13 20:56 intflash/

Check the device for errors:

Switch:1#usb-stop
It is now safe to remove the USB device.
Switch:1#dos-chkdsk /usb
/usr/sbin/fsck.vfat /dev/usb1 -v > /dev/console
dosfsck 2.11a (05 Mar 2010)
dosfsck 2.11a, 05 Mar 2010, FAT32, LFN
Checking we can access the last sector of the filesystem
Boot sector contents:
System ID "mkdosfs"
Media byte 0xf8 (hard disk)
512 bytes per logical sector
4096 bytes per cluster
32 reserved sectors
First FAT starts at byte 16384 (sector 32)
2 FATs, 32 bit entries
389344 bytes per FAT (= 7612 sectors)
Root directory start at cluster 2 (arbitrary size)
Data area starts at byte 7811072 (sector 15256)
974240 data clusters (3990487040 bytes)
62 sectors/track, 124 heads
0 hidden sectors
7809178 sectors total
Checking for unused clusters.
Checking free cluster summary.
/dev/usb1: 17 files, 174804/974240 clusters

If errors are detected, reformat the disk:

Switch:1#dos-format /usb
Chapter 15: Software troubleshooting

This section contains general troubleshooting information for Avaya Virtual Services Platform 4000 Series software.

Failure to read failed configuration file

The device can fail to read and load a saved configuration file after it starts. This situation occurs if you enable the factorydefaults boot configuration flag. Configure the flag to false:

```
no boot config flags factorydefaults
```

**Example**

```
VSP-4850GTSPWR+:1> enable
VSP-4850GTSPWR+:1# configure terminal
VSP-4850GTSPWR+:1(config)# no boot config flags factorydefaults
```

No Web management interface access to a device

If the device and the PC that runs the Web browser are in the same network, you can find that even though other applications, for example, Telnet, can access a particular switch, the Web management interface cannot. This situation can occur if the Web browser has a proxy server that resolves the www path and returns the reachable IP address to the browser. If no route exists from the proxy server to the device, the HTTP query does not reach the device, and does not receive a response.

To prevent this problem, ensure that if the Web browser uses a proxy server, you specify a route from the proxy server to the device.

Cannot enable encryption

To enable encryption on the system, you must first download and install the necessary encryption module. If you do not download and install the module, you can enable the encryption method in the...

Comments on this document? infodev@avaya.com
software but it does not work. You must download and install the encryption modules separately from the software releases.

**Debug files**

Virtual Services Platform 4000 stores debug files in the intflash directory.

The debug file is in a zipped format and contains information to help debug the device, including:

- a memory snapshot
- logs
- traces

Avaya recommends you delete these files to ensure enough space exists in the internal flash on the CP module. New files do not overwrite old files. You must remove the files; otherwise, the internal flash may not have enough free space for necessary activities, for example, to store a core dump file if the switch fails, or you may not have the space to transfer a new release to the internal flash to upgrade your switch.

Virtual Services Platform 4000 stores a maximum of 32 files for each debug file for each slot, depending on the file size of each debug file. The internal flash provides 2 GB of storage. A message appears on the console to inform you when less than 700 MB is available.

The `debug-file remove` command can delete the following types of debug files:

- core
- archive
- PMEM
- dmalloc
- firec
- wd_stats

If you want to delete a specific file, you must use the `remove` command. For more information, see *Commands Reference for Avaya Virtual Services Platform 4000 Series*, NN46251-104.

**SNMP**

VSP 4000 does not support SNMP for the `show debug-file` or the `debug-file remove` commands.
Chapter 16: Software troubleshooting tool configuration using ACLI

Use the tools described in this section to perform troubleshooting procedures using ACLI.

Using ACLI for troubleshooting

Before you begin

- You must log on to at least Privileged EXEC mode in ACLI to use the `show running-config` and `show interfaces` commands in this procedure.

About this task

You can use ACLI to provide diagnostic information.

Procedure

1. Disable scrolling of the output display:
   
   `terminal more disable`

2. View configuration file information:
   
   `more WORD<1–99>`

3. Capture the output for the following command after you observe a problem with the device:
   
   `show running-config [verbose] [module <boot | cfm | cli | diag | fa | fhs | filter | ike | ip | ipsec | ipv6 | isis | i-sid | lACP | lldp | macsec | mlt | naap | nsna | ntp | poe | port | qos | radius | rmon | slamon | macsec | slpp | spbm | stg | sys | tacacs | vlan | web>]

4. Capture the output for the following command after you observe a problem with the device:
   
   `show tech`

5. Capture the output for the following command after you observe a problem with the device:
   
   `show interfaces gigabitEthernet statistics <bridging {slot/port[-slot/port][,..]}|dhcp-relay {slot/port[-slot/port][,..]} [vrf WORD<1-16>][vrfids WORD<0-512>]|lACP {slot/port[-slot/port][,..]}|...}`
Note:

This `show interfaces gigabitEthernet statistics rmon` command displays information only if you previously configured `rmon stats` or `rmon history`.

6. Capture the output for the following command after you observe a problem with the device:

   `show interfaces gigabitEthernet error <collision|verbose> {slot/port[-slot/port][,...]}`

Example

```
VSP-4850GTSPWR+:1>enable
```

Capture the output for the following command after you observe a problem with the device:

```
VSP-4K-R1-BEB-5-HighTemp:1#show running-config module cli
Preparing to Display Configuration...
#
# Tue Feb 10 13:21:12 2015 UTC
# box type             : VSP-4450GTXHT-PWR+
# software version     : 4.1.0.0
# cli mode             : ACLI
#
# config terminal
#
# # CLI CONFIGURATION
#
# cli timeout 65535
# prompt "VSP-4K-R1-BEB-5-HighTemp"
# password password-history 3
# cli log enable
```

Capture the output for the following command after you observe a problem with the device:

```
VSP-4K-R1-BEB-5-HighTemp:1#show tech
Sys Info:
---------
General Info :
   SysDescr   : VSP-4450GTXHT-PWR+ (4.1.0.0)
   SysName    : VSP-4K-R1-BEB-5-HighTemp
   SysUpTime  : 0 day(s), 00:25:41
   SysContact : http://support.avaya.com/
   SysLocation: 211 Mt. Airy Road,Basking Ridge,NJ 0792
Chassis Info:
   Chassis      : 4450GTXHT-PWR+
   Serial#      : SDNI44P009
   H/W Revision : R0A
   H/W Config   : none
   NumSlots     : 1
   NumPorts     : 50
```

Comments on this document? infodev@avaya.com
Software troubleshooting tool configuration using ACLI

BaseMacAddr : b0:ad:aa:54:d8:00
MacAddrCapacity : 256
Temperature : 31
System MTU : 9600

--More-- (q = quit)

Capture the output for the following command after you observe a problem with the device:

VSP-4850GTSPWR+:1#show interfaces gigabitethernet statistics

================================================================================
<table>
<thead>
<tr>
<th>Port Stats Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
</tr>
<tr>
<td>NUM</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>1/1</td>
</tr>
<tr>
<td>1/2</td>
</tr>
<tr>
<td>1/3</td>
</tr>
<tr>
<td>1/4</td>
</tr>
<tr>
<td>1/5</td>
</tr>
<tr>
<td>1/6</td>
</tr>
<tr>
<td>1/7</td>
</tr>
<tr>
<td>1/8</td>
</tr>
<tr>
<td>1/9</td>
</tr>
<tr>
<td>1/10</td>
</tr>
<tr>
<td>1/11</td>
</tr>
<tr>
<td>1/12</td>
</tr>
<tr>
<td>1/13</td>
</tr>
<tr>
<td>1/14</td>
</tr>
</tbody>
</table>

--More-- (q = quit)

Capture the output for the following command after you observe a problem with the device:

VSP-4850GTSPWR+:1#show interfaces gigabitEthernet error

================================================================================
<table>
<thead>
<tr>
<th>Port Ethernet Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
</tr>
<tr>
<td>NUM</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>1/1</td>
</tr>
<tr>
<td>1/2</td>
</tr>
<tr>
<td>1/3</td>
</tr>
<tr>
<td>1/4</td>
</tr>
<tr>
<td>1/5</td>
</tr>
<tr>
<td>1/6</td>
</tr>
<tr>
<td>1/7</td>
</tr>
<tr>
<td>1/8</td>
</tr>
<tr>
<td>1/9</td>
</tr>
<tr>
<td>1/10</td>
</tr>
<tr>
<td>1/11</td>
</tr>
<tr>
<td>1/12</td>
</tr>
<tr>
<td>1/13</td>
</tr>
<tr>
<td>1/14</td>
</tr>
</tbody>
</table>

--More-- (q = quit)
Variable definitions

Use the data in the following table to use the **more** command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD&lt;1–99&gt;</td>
<td>Specifies the file name to view. Provide the filename in one of the following formats: a.b.c.d:&lt;file&gt;, /intflash:&lt;file&gt;.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the **show running-config** command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>module &lt;boot</td>
<td>cfm</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the **show interfaces gigabitEthernet** command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridging {slot/port[-slot/port][,...]}</td>
<td>Displays ports bridging statistics.</td>
</tr>
<tr>
<td>dhcp-relay {slot/port[-slot/port][,...]} [vrf WORD&lt;1–16&gt;] [vRFids WORD&lt;0–512&gt;]</td>
<td>Displays port Dynamic Host Configuration Protocol (DHCP) statistics.</td>
</tr>
<tr>
<td>lACP {slot/port[-slot/port][,...]}</td>
<td>Displays Link Aggregation Control Protocol (LACP) statistics.</td>
</tr>
<tr>
<td>policer {slot/port[-slot/port][,...]}</td>
<td>Displays policer statistics.</td>
</tr>
<tr>
<td>rMON {slot/port[-slot/port][,...]} [history]</td>
<td>Displays Remote Network Monitoring (RMON) statistics.</td>
</tr>
<tr>
<td>verbose {slot/port[-slot/port][,...]}</td>
<td>Displays a complete list of all statistics.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the **show interfaces gigabitEthernet error** command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>collision</td>
<td>Displays port collision error information.</td>
</tr>
<tr>
<td>verbose</td>
<td>Displays all port error information.</td>
</tr>
<tr>
<td>{slot/port[-slot/port][,...]}</td>
<td>Specifies the port.</td>
</tr>
</tbody>
</table>
Using software record dumps

About this task
Capture a dump of the software records from ingress traffic to help troubleshoot performance problems. Generally, a verbosity level of 1 suffices.

Procedure
Dump software record information:

dump ar <1–12> WORD<1–1536> <0-3>

Example
VSP-4850GTSPWR+:1>enable
VSP-4850GTSPWR+:1(config)#dump ar 1 vlan 1

Variable definitions
Use the data in the following table to use the dump ar command.

Table 24: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1&gt;</td>
<td>Specifies the slot number.</td>
</tr>
<tr>
<td>WORD&lt;1-1536&gt;</td>
<td>Specifies a record type in the AR table. Options include vlan, ip_subnet, mac_vlan, mac, arp, ip, ipmc, protocol, all.</td>
</tr>
<tr>
<td>&lt;0-3&gt;</td>
<td>Specifies the verbosity from 0–3. Higher numbers specify more verbosity.</td>
</tr>
</tbody>
</table>

Using trace to diagnose problems

Before you begin
- You must log on to at least the Privileged EXEC mode in ACLI to clear or save trace information.

About this task
Use trace to observe the status of a software module at a given time.

For example, if you notice a CPU utilization issue (generally a sustained spike above 90%) perform a trace of the control plane activity.

Procedure
1. Clear the trace:
clear trace

2. Identify the module ID for which you want to use the trace tool:
   show trace modid-list

3. Begin the trace operation:
   trace level [<0-234>] [<0-4>]

4. Wait approximately 30 seconds.
   The default trace settings for CPU utilization are:
   - High CPU Utilization: 90%
   - High Track Duration: 5 seconds
   - Low CPU Utilization: 75%
   - Low Track Duration: 5 seconds

5. Stop tracing:
   trace shutdown

6. View the trace results:
   show trace file [tail]

7. Save the trace file to the Flash card for retrieval.
   save trace [file WORD<1-99>]
   If you do not specify a file name, the file name is systrace.txt.

8. Search trace results for a specific string value, for example, the word error:
   trace grep [WORD<0-128>]
   If you use this command and do not specify a string value, you clear the results of a previous search.

9. Stop tracing:
   trace shutdown

Example
Switch:1>enable
Clear the trace:
Switch:1#clear trace
Identify the module ID for which you want to use the trace tool:
Switch:1#show trace modid-list

<table>
<thead>
<tr>
<th>Module ID</th>
<th>Module Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>COMMON</td>
</tr>
<tr>
<td>1</td>
<td>SNMP</td>
</tr>
<tr>
<td>2</td>
<td>RMON</td>
</tr>
<tr>
<td>3</td>
<td>PORT_MGR</td>
</tr>
<tr>
<td>4</td>
<td>CHAS_MGR</td>
</tr>
<tr>
<td>119</td>
<td>ISIS</td>
</tr>
<tr>
<td>120</td>
<td>CFM</td>
</tr>
<tr>
<td>121</td>
<td>OERCD</td>
</tr>
<tr>
<td>122</td>
<td>PWE3</td>
</tr>
<tr>
<td>123</td>
<td>EXTENDED_PING</td>
</tr>
</tbody>
</table>
Variable definitions

Use the data in the following table to use the `trace` command.

Table 25: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
</table>
| cfm level [0-4] | Starts the trace by specifying the level.  
  • `<0-4>` specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose. |
| filter     | Configure a filter trace for a file or module. |
| flags      | Configure trace flags for ISIS or OSPF. |

Table continues…
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>grep [WORD&lt;0-128&gt;]</td>
<td>Search trace results for a specific string value, for example, the word error. Performs a comparison of trace messages.</td>
</tr>
</tbody>
</table>
| level [<0-234>] [<0-4>] | Starts the trace by specifying the module ID and level.  
  • <0-234> specifies the module ID.  
  • <0-4> specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose. |
| route-map        | Enables or disables the trace route-map. The values are on and off.  |
| screen {disable|enable} | Enables the display of trace output to the screen.  |
| shutdown         | Stops the trace operation.                                           |
| spbm isis level [<0-4>] | Starts the trace by specifying the level.  
  • <0-4> specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose.  
  The default is 1, very terse. |

Use the data in the following table to use the save trace command.

**Table 26: Variable definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
</table>
| file WORD<1–99>  | Specifies the file name in one of the following formats:  
  • a.b.c.d:<file> |

**Using trace to diagnose IPv6 problems**

Use trace to observe the status of IPv6 at a certain time.

**Before you begin**

• Confirm that trace level 99 is set to a value of 1 before you use trace to diagnose IPv6 problems. Trace level 1 is very terse.

⚠️ **Caution:**

**Risk of traffic loss**

Using the trace tool inappropriately can cause primary CPU lockup conditions, loss of access to the device, loss of protocols, and service degradation.

**About this task**

**Procedure**

1. Enter Privileged EXEC mode:
enable

2. Activate or deactivate the trace for the IPv6 base:
   trace ipv6 base <disable|enable> <all|debug|error|icmp|info|
ipclient|nbr|pkt|warn>

3. Activate or deactivate the trace for IPv6 forwarding:
   trace ipv6 forwarding <disable|enable> <all|debug|error|info|pkt|
   warn>

4. Activate or deactivate the trace for IPv6 neighbor discovery:
   trace ipv6 nd <disable|enable> <all|debug|error|info|nbr|pkt|
   redirect|warn>

5. Activate or deactivate the trace for IPv6 OSPF:
   trace ipv6 ospf <disable|enable> <adj|all|config|error|import|info|
   lsa|pkt|spf|warn>

6. Activate or deactivate the trace for the IPv6 routing table manager:
   trace ipv6 rtm <disable|enable> <all|change-list|debug|error|fib|
   info|redist|update|warn>

7. Activate or deactivate the trace for IPv6 transport:
   trace ipv6 transport <disable|enable> <all|common|tcp|udp>

8. Deactivate the trace to prevent service degradation:
   trace shutdown
   clear trace

Example
Switch:1>enable
Activate the trace for all the IPv6 base categories:
Switch:1#trace ipv6 base enable all
Activate the trace for all the IPv6 forwarding categories:
Switch:1#trace ipv6 forwarding enable all
Activate the trace for all the IPv6 neighbor discovery categories:
Switch:1#trace ipv6 nd enable all
Activate the trace for the all IPv6 routing table manager categories:
Switch:1#trace ipv6 rtm enable all
Activate the trace for all the IPv6 transport categories:
Switch:1#trace ipv6 transport enable all
Deactivate the trace:
Switch:1#trace shutdown
Switch:1#clear trace
Removed 5 files.

Variable definitions

Use the data in the following table to use the trace ipv6 command.

Table 27: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>base &lt;disable</td>
<td>enable&gt; &lt;all</td>
</tr>
<tr>
<td>forwarding &lt;disable</td>
<td>enable&gt; &lt;all</td>
</tr>
<tr>
<td>nd &lt;disable</td>
<td>enable&gt; &lt;all</td>
</tr>
<tr>
<td>ospf &lt;disable</td>
<td>enable&gt; &lt;adj</td>
</tr>
<tr>
<td>rtm &lt;disable</td>
<td>enable&gt; &lt;all</td>
</tr>
<tr>
<td>transport &lt;disable</td>
<td>enable&gt; &lt;all</td>
</tr>
</tbody>
</table>

Viewing and deleting debug files

Use this procedure to view and delete debug files.

Delete debug files to free space in the intflash, which has 2 GB of space. Avaya recommends you delete these files to ensure enough space exists in intflash. New debug files do not overwrite old debug files. You must remove the file; otherwise, enough free space may not exist in the intflash to store the core dump if the switch fails or enough space may not exist for you to transfer a new release to the intflash of the switch to upgrade your switch.

The debug-file remove command can delete the following types of files:

- core
- archive
- PMEM
- dmalloc
- firec
• **wd_stats**

If you want to delete a specific file, you must use the `remove` command. For more information, see *Commands Reference for Avaya Virtual Services Platform 4000 Series*, NN46251-104.

**Procedure**

1. Log on to the switch to enter User EXEC mode.
2. View debug files:
   
   ```
   show debug-file [all] [{slot[-slot]}[,...]]
   ```
3. Delete debug files:
   
   ```
   debug-file remove [all] [{slot[-slot]}[,...]]
   ```
4. Enter Privileged EXEC mode:
   
   ```
   enable
   ```
5. View core files:
   
   ```
   show core-files {slot[-slot]}[,...]
   ```

**Example**

The following example shows how you view all debug files for all slots, and then remove the debug files for slot 1.

```
VSP-4850GTS>show debug-file
================================================================================
Core Files
================================================================================
Directory: /intflash/coreFiles/1
1. File: core.logServer.20120611084204.1.tar
   Size: 60928 bytes
   Created: Mon Jun 11 08:42:04 2012
2. File: core.trcServer.20120611084213.1.tar
   Size: 60928 bytes
   Created: Mon Jun 11 08:42:13 2012
3. File: core.logServer.20120611164647.1.tar
   Size: 64000 bytes
4. File: core.trcServer.20120611164652.1.tar
   Size: 64000 bytes
   Created: Mon Jun 11 16:46:52 2012
5. File: core.dbgServer.20120611164700.1.tar
   Size: 64000 bytes
   Created: Mon Jun 11 16:47:01 2012
6. File: core.logServer.20120611164740.1.tar
   Size: 64000 bytes
   Created: Mon Jun 11 16:47:41 2012
Directory: /intflash/coreFiles/2
1. File: core.coreManager.x.20120611164740.1.tar
   Size: 1162240 bytes
   Created: Tue Jun 12 08:55:49 2012
2. File: core.coreManager.x.20120612085602.1.tar
   Size: 478208 bytes
   Created: Tue Jun 12 08:56:02 2012
3. File: core.coreManager.x.20120612085553.2.tar
   ```
<table>
<thead>
<tr>
<th>Directory</th>
<th>File Name</th>
<th>Size</th>
<th>Created Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>/intflash/archive/1</td>
<td>archive.20120611083021.1.tar</td>
<td>34296320   bytes</td>
<td>Mon Jun 11 08:30:22 2012</td>
</tr>
<tr>
<td></td>
<td>archive.2012061163454.1.tar</td>
<td>31108096   bytes</td>
<td>Mon Jun 11 16:34:54 2012</td>
</tr>
<tr>
<td></td>
<td>archive.20120611164507.1.tar</td>
<td>31881216   bytes</td>
<td>Mon Jun 11 16:45:08 2012</td>
</tr>
<tr>
<td></td>
<td>archive.20120611644008.2.tar</td>
<td>31314432   bytes</td>
<td>Mon Jun 11 16:44:09 2012</td>
</tr>
<tr>
<td></td>
<td>archive.2012061164521.2.tar</td>
<td>31367168   bytes</td>
<td>Mon Jun 11 16:45:21 2012</td>
</tr>
<tr>
<td>/intflash/archive/4</td>
<td>archive.2012061163515.4.tar</td>
<td>4725760    bytes</td>
<td>Mon Jun 11 16:35:18 2012</td>
</tr>
<tr>
<td></td>
<td>archive.2012061164416.4.tar</td>
<td>5639168    bytes</td>
<td>Mon Jun 11 16:44:20 2012</td>
</tr>
<tr>
<td></td>
<td>archive.2012061164529.4.tar</td>
<td>5760000    bytes</td>
<td>Mon Jun 11 16:45:33 2012</td>
</tr>
<tr>
<td>/intflash/archive/SF4</td>
<td>archive.2012061163536.SF4.tar</td>
<td>1550336    bytes</td>
<td>Mon Jun 11 16:35:40 2012</td>
</tr>
<tr>
<td></td>
<td>archive.2012061164549.SF4.tar</td>
<td>1811968    bytes</td>
<td>Mon Jun 11 16:45:53 2012</td>
</tr>
<tr>
<td>/intflash/PMEM/4</td>
<td>pmem.20120607194023.4.bin.gz</td>
<td>571048     bytes</td>
<td>Thu Jun 17 19:40:23 2012</td>
</tr>
</tbody>
</table>
Software troubleshooting tool configuration using ACLI

DMalloc Files

Flrec Files

WdStats Files

Directory: /intflash/wd_stats/4
1. File:    wd_stats.log.backup
   Size:    2311 bytes
   Created: Mon Jun 11 09:25:07 2012

VSP-4850GTS1>debug-file remove 1
VSP-4850GTS>show debug-file

Core Files

Remote CP Directory: /intflash/coreFiles/2
1. File:    core.coreManager.x.20120612085548.2.tar
   Size:    1162240 bytes
   Created: Tue Jun 12 08:55:49 2012
2. File:    core.coreManager.x.20120612085602.2.tar
   Size:    478208 bytes
   Created: Tue Jun 12 08:56:02 2012
3. File:    core.coreManager.x.20120612085553.2.tar
   Size:    1170432 bytes
   Created: Tue Jun 12 08:55:56 2012
4. File:    core.coreManager.x.20120612085558.2.tar
   Size:    1883136 bytes
   Created: Tue Jun 12 08:56:00 2012

Archive Files

Remote CP Directory: /intflash//archive/2
1. File:    archive.20120611163507.2.tar
   Size:    30903296 bytes
   Created: Mon Jun 11 16:35:08 2012
2. File:    archive.20120611164408.2.tar
   Size:    3134432 bytes
   Created: Mon Jun 11 16:44:09 2012
3. File:    archive.20120611164521.2.tar
   Size:    31367168 bytes
   Created: Mon Jun 11 16:45:21 2012

Directory: /intflash/archive/4
1. File:    archive.20120611163515.4.tar
   Size:    4725760 bytes
   Created: Mon Jun 11 16:35:18 2012
2. File:    archive.20120611164416.4.tar
   Size:    5639168 bytes
   Created: Mon Jun 11 16:44:20 2012
3. File:    archive.20120611164529.4.tar
   Size:    5760000 bytes
   Created: Mon Jun 11 16:45:33 2012

Directory: /intflash/archive/SF4
1. File:    archive.20120611163536.SF4.tar
The following example shows how to view only core files on the switch.

VSP-4850GTS#show core-files

Directory: /intflash/coreFiles/1
1. File: core.1353113115.lifecyle.CP.1.gz
   Size: 139406 bytes
   Created: Fri Nov 16 19:45:15 2012
2. File: core.cbcp-main.x.20121114043335.1.tar
   Size: 14059520 bytes
   Created: Wed Nov 14 04:35:36 2012
3. File: core.cbcp-main.x.20121114045202.1.tar
   Size: 12809728 bytes
   Created: Wed Nov 14 04:54:03 2012
4. File: core.cbcp-main.x.20121114050825.1.tar
   Size: 12638720 bytes
   Created: Wed Nov 14 05:10:26 2012
5. File: core.cbcp-main.x.20121114122506.1.tar
   Size: 13020160 bytes
   Created: Wed Nov 14 12:27:07 2012
6. File: core.1353336274.lifecyle.CP.1.gz
   Size: 139390 bytes
   Created: Mon Nov 19 09:44:34 2012
7. File: core.1353319337.lifecyle.CP.1.gz
   Size: 139404 bytes
   Created: Mon Nov 19 05:02:17 2012
8. File: core.cbcp-main.x.20130122182946.1.tar
   Size: 13683712 bytes
   Created: Tue Jan 22 18:32:08 2013
Variable definitions

Use the data in the following table to use the show core-files command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>{slot[-slot]...,}</td>
<td>Displays the core files for the slot that you select.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the show debug-file command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all types of debug files</td>
</tr>
<tr>
<td>{slot[-slot]...,}</td>
<td>Displays debug files for the slot that you select. If you do not select a slot number, the device displays all types of the archived debug files present in a slot by slot basis. If you select a slot number, the device only displays archived files for the slot you select.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the debug-file remove command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Removes all types of debug files in all slots. If you use the option all with the remove debug-file command, then the device deletes all types of debug files, including the latest debug files.</td>
</tr>
<tr>
<td>{slot[-slot]...,}</td>
<td>Removes debug files for the slot that you select. When you clear archived files, if you do not select a slot number, the device deletes all types of archived debug files except the latest file in each slot. Valid slots are 1–12, SF1–SF6, and all.</td>
</tr>
</tbody>
</table>

Configuring port mirroring

Before you begin

• You must log on to Global Configuration mode in ACLI.
About this task

Use port mirroring to aid in diagnostic and security operations.

Use port mirroring to make a copy of a traffic flow and send that copy to a device for analysis, for example, for diagnostic sniffing. Use the mirror to see the packets in the flow without breaking into the physical connection to place a packet onto the sniffer inline. You can also use port mirroring for security. You can send flows to inspection engines for post processing.

Connect the sniffer (or other traffic analyzer) to the output port you specify in this procedure.

Procedure

1. Create a port mirroring instance:
   ```plaintext
   mirror-by-port <1-479> in-port {slot/port[-slot/port][,...]} {monitor-mlt <1-512>|out-port {slot/port[-slot/port][,...]}
   ```
2. Configure the mode:
   ```plaintext
   mirror-by-port <1-479> mode <both|rx|tx>
   ```
3. Enable the mirroring instance:
   ```plaintext
   mirror-by-port <1-479> enable
   ```
4. Modify existing mirroring entries as required:
   ```plaintext
   mirror-by-port mirror-port <1-479> {slot/port[-slot/port][,...]}
   OR
   mirror-by-port monitor-mlt <1-479> <1-512>
   OR
   mirror-by-port monitor-port <1-479> {slot/port[-slot/port][,...]}
   OR
   ```
   **Note:**
   Before you can modify an existing entry, you must disable the entry: 
   ```plaintext
   no mirror-by-port <1-479> enable.
   ```
5. Verify the configuration:
   ```plaintext
   show mirror-by-port
   ```

Example

```plaintext
VSP-4850GTSPWR+:1>enable
VSP-4850GTSPWR+:1#configure terminal

Create the port mirroring instance. Traffic passing port 1/15 is mirrored to port 1/16:
VSP-4850GTSPWR+:1(config)# mirror-by-port 8 in-port 1/15 out-port 1/16
The analyzer connects to port 1/16.
Disable the entry:
```
No command output is displayed.

The following example shows sample command output; it does not necessarily reflect the preceding examples.

```
VSP-4850GTSPWR+:1(config)# show mirror-by-port

16 out of 24 Total Num of MirIds displayed
VSP-4850GTS(config)# show mirror-by-port 1
```

## Variable definitions

Use the data in the following table to use the `mirror-by-port` command.

**Table 28: Variable definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-479&gt;</code></td>
<td>Specifies the entry ID.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables or disables a mirroring instance already created in the mirror-by-port table.</td>
</tr>
</tbody>
</table>
| `in-port {slot/port[-slot/port][,...]}` | Creates a new mirror-by-port table entry.  
| `monitor-mlt <1-512>`     | Specifies the mirrored port.                                          |
| `out-port {slot/port[-slot/port][,...]}` | Specifies the mirroring port.                                       |
| `mirror-port <1-479> {slot/port[-slot/port][,...]}` | Modifies the mirrored port.                                      |
| `monitor-ip <1-479> {A.B.C.D} [dscp <0-63>] [ttl <2-255>]` | Creates a mirroring instance for Layer 3 mirroring. The destination must be an IP address (A.B.C.D). The default DSCP is 0 and the default TTL is 255. |
| `monitor-mlt <1-479> <1-512>` | Modifies the monitoring MLT.<1-512> specifies the mirroring MLT ID.   |

Table continues…
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Before you can modify an existing entry, you must disable the entry: no mirror-by-port &lt;1-479&gt; enable.</td>
</tr>
<tr>
<td>monitor-port &lt;1-479&gt;</td>
<td>Modifies the monitoring ports.</td>
</tr>
<tr>
<td></td>
<td>Before you can modify an existing entry, you must disable the entry: no mirror-by-port &lt;1-479&gt; enable.</td>
</tr>
<tr>
<td></td>
<td>Modifies the monitoring VLAN.</td>
</tr>
<tr>
<td></td>
<td>Before you can modify an existing entry, you must disable the entry: no mirror-by-port &lt;1-479&gt; enable.</td>
</tr>
<tr>
<td>mode &lt;both</td>
<td>rx</td>
</tr>
<tr>
<td></td>
<td>• both mirrors both egress and ingress packets.</td>
</tr>
<tr>
<td></td>
<td>• rx mirrors ingress packets.</td>
</tr>
<tr>
<td></td>
<td>• tx mirrors egress packets.</td>
</tr>
</tbody>
</table>

## Configuring global mirroring actions with an ACL

### Before you begin

- The ACL exists.
- You must log on to Global Configuration mode in ACLI.

### About this task

Configure the global action to mirror packets that match an access control list (ACL).

### Procedure

Configure the global action for an ACL:

```bash
filter acl set <1-2048> global-action {monitor-dst-mlt <1-512>|monitor-dst-ports {slot/port[-slot/port ][,...]}}
```

### Example

```
VSP-4850GTSPWR+:1>enable
VSP-4850GTSPWR+:1#configure terminal

Configure the global action for an ACL:

VSP-4850GTSPWR+:1(config)#filter acl set 200 global-action monitor-dst-mlt 20
```

### Variable definitions

Use the data in the following table to use the `filter acl set` command.
Table 29: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-2048&gt;</td>
<td>Specifies an ACL ID from 1–2048.</td>
</tr>
<tr>
<td>default-action &lt;deny</td>
<td>permit&gt;</td>
</tr>
</tbody>
</table>
| global-action {monitor-dst-mlt PT_MLT<1–512>|monitor-dst-ports {slot/port[-slot/port ][,...]}} | Specifies the global action to take for matching ACLs:  
• monitor destination MLT—Configures mirroring to a destination MultiLink Trunking (MLT) group.  
• monitor destination ports—Configures mirroring to a destination port or ports. |

Configuring ACE actions to mirror

Before you begin

• The access control entry (ACE) exists.
• You must log on to Global Configuration mode in ACLI.

About this task

Configure actions to use filters for flow-based mirroring. If you use the mirror action, ensure that you specify the mirroring destination: MLTs or ports.

Procedure

1. Configure actions for an ACE:

   filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-mlt <1-512>
   
   OR
   
   filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-ports {slot/port[-slot/port ][,...]}

2. Ensure the configuration is correct:

   show filter acl action [<1-2048>] [<1-2000>]

Example

VSP-4850GTSPWR+:1>enable
VSP-4850GTSPWR+:1#configure terminal
VSP-4850GTSPWR+:1(config)#filter acl ace action 901 1 permit monitor-dst-mlt 5
Variable definitions

Use the data in the following table to use the `filter acl ace action` command.

Table 30: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2048</td>
<td>Specifies the ACL ID from 1–2048</td>
</tr>
<tr>
<td>1-2000</td>
<td>Specifies the ACE ID from 1–2000.</td>
</tr>
<tr>
<td>monitor-dst-mlt &lt;1–512&gt;</td>
<td>Configures mirroring to a destination MLT group.</td>
</tr>
<tr>
<td>monitor-dst-ports {slot/port[-slot/port [...]]}</td>
<td>Configures mirroring to a destination port or ports.</td>
</tr>
<tr>
<td>{permit</td>
<td>deny}</td>
</tr>
</tbody>
</table>

Clearing ARP information for an interface

Before you begin

- You must log on to at least Privileged EXEC mode in ACLI.

About this task

Clear the Address Resolution Protocol (ARP) cache as part of ARP problem resolution procedures.

Procedure

Clear ARP information:

`clear ip arp interface gigabitethernet {slot/port[-slot/port][,...]}`

OR

`clear ip arp interface vlan <1-4059>`

Example

VSP-4850GTSPWR+:1> enable
VSP-4850GTSPWR+:1# clear ip arp interface gigabitethernet 1/1

Variable definitions

Use the data in the following table to use the `clear ip arp interface` command.
Table 31: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4059&gt;</td>
<td>Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.</td>
</tr>
<tr>
<td>slot/port[-slot/port][,...]</td>
<td>Identifies the slot and port in one of the following formats: a slot and port (1/1), a range of ports (1/2-1/4), or a series ports (1/2,1/3).</td>
</tr>
</tbody>
</table>

Flush routing, MAC, and ARP tables for an interface

Before you begin
• You must log on to the Interface Configuration mode in ACLI.

About this task
Flush or clear the routing tables for administrative and troubleshooting purposes. The clear and flush commands perform the same function; they remove the contents of the table.

Procedure

1. Flush IP routing tables by port:
   action flushIp

2. Flush the MAC address tables:
   action flushMacFdb

3. Flush ARP tables:
   action flushArp

4. Flush all tables with one command:
   action flushAll

5. Exit to Global Configuration mode:
   exit

6. Clear a routing table:
   clear ip route gigabitethernet {slot/port}
   OR
   clear ip route vlan <1-4059>

Comments on this document? infodev@avaya.com
Example

VSP-4850GTSPWR+:1> enable
VSP-4850GTSPWR+:1# configure terminal
VSP-4850GTSPWR+:1(config)# interface gigabitethernet 1/1
VSP-4850GTSPWR+:1(config-if)# action flushAll
VSP-4850GTSPWR+:1(config-if)# exit
VSP-4850GTSPWR+:1(config)# clear ip route gigabitethernet 1/1

Variable definitions

Use the data in the following table to use the clear ip route command.

Table 32: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4059&gt;</td>
<td>Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.</td>
</tr>
<tr>
<td>{slot/port}</td>
<td>Specifies a port number.</td>
</tr>
</tbody>
</table>

Pinging an IP device

About this task

Ping a device to test the connection between the Avaya Virtual Services Platform 4000 Series and another network device. After you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. After the switch receives the reply, a message appears that indicates traffic can reach the specified IP address. If the switch does not receive a reply, the message indicates the address does not respond.

Ping and traceroute can fail for VRF routes if you use large packet sizes for the operation. Do not use packet sizes larger than the following:

- Traceroute for VRF: 1444 bytes

**Note:**

Pinging a device over VRF using its IP address is successful only when the source IP address is specified.
Procedure

Ping an IP network connection:

ping WORD<0–256> [-d] [-I <1–60>] [-s] [-t <1–120>] [count <1–9999>]
[datasize <28–9216|28–51200>] [interface WORD<1–256>|gigabitEthernet|tunnel|vlan] [scopeid <1–9999>] [source WORD<1–256>] [vrf WORD<1–16>]

Variable definitions

Use the data in the following table to use the ping command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>count &lt;1–9999&gt;</td>
<td>Specifies the number of times to ping (1–9999).</td>
</tr>
<tr>
<td>-d</td>
<td>Configures the ping debug mode. This variable detects local software failures (ping related threads creation or write to sending socket) and receiving issues (icmp packet too short or wrong icmp packet type).</td>
</tr>
<tr>
<td>datasize &lt;28–9216</td>
<td>28–51200&gt;</td>
</tr>
<tr>
<td></td>
<td>The datasize for IPv4 addresses is 28-9216.</td>
</tr>
<tr>
<td></td>
<td>The datasize for IPv6 addresses is 28-51200.</td>
</tr>
<tr>
<td></td>
<td>The default is 0.</td>
</tr>
<tr>
<td>-I &lt;1–60&gt;</td>
<td>Specifies the interval between transmissions in seconds (1–60).</td>
</tr>
<tr>
<td>interface WORD&lt;1–256&gt;</td>
<td>gigabitEthernet</td>
</tr>
<tr>
<td></td>
<td>• gigabitEthernet: {slot/port} gigabitethernet port</td>
</tr>
<tr>
<td></td>
<td>• tunnel: tunnel ID as a value from 1 to 2147277248</td>
</tr>
<tr>
<td></td>
<td>• vlan: VLAN ID as a value from 2 to 4059</td>
</tr>
<tr>
<td>-s</td>
<td>Configures the continuous ping at the interval rate defined by the [-I] parameter.</td>
</tr>
<tr>
<td>scopeid &lt;1–9999&gt;</td>
<td>Specifies the circuit ID for IPv6.</td>
</tr>
<tr>
<td>source WORD&lt;1–256&gt;</td>
<td>Specifies the source IP address for the ping command.</td>
</tr>
<tr>
<td>-t &lt;1–120&gt;</td>
<td>Specifies the no-answer timeout value in seconds (1–120).</td>
</tr>
<tr>
<td>WORD&lt;0–256&gt;</td>
<td>Specifies the host name or IPv4 (a.b.c.d) or IPv6 (x:x:x:x:x:x:x) address (string length 0–256).</td>
</tr>
<tr>
<td>vrf WORD&lt;1–16&gt;</td>
<td>Specifies the virtual router and forwarder (VRF) name from 1–16 characters.</td>
</tr>
</tbody>
</table>
Running a traceroute test

Use traceroute to determine the route packets take through a network to a destination.

Before you begin

- You must log on to at least Privileged EXEC mode in ACLI.

About this task

Ping and traceroute can fail for VRF routes if you use large packet sizes for the operation. Do not use packet sizes larger than the following:

- Ping for VRF: 1480 bytes
- Traceroute for VRF: 1444 bytes

Procedure

Run a traceroute test:

```
traceroute WORD<0-256> [<1-1176>] [-m <1-255>] [-p <1-65535>] [-q <1-255>] [-v] [-w <1-255>] [source <WORD 1-256>] [vrf <WORD 1-16>]
```

Example

```
VSP-4850GTSPWR+:1> enable
Run traceroute test, with a probe packet size of 200 and a max time to live of 60:
VSP-4850GTSPWR+:1# traceroute 46.11.10.33 200 -m 60
Run a traceroute test for IPv6 address 2001:db8::
VSP-4850GTSPWR+:1# traceroute 2001:db8::
```

Variable definitions

Use the data in the following table to use the `traceroute` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD&lt;0-256&gt;</td>
<td>Specifies the destination IPv4 or IPv6 address, or hostname.</td>
</tr>
<tr>
<td>-m &lt;1-255&gt;</td>
<td>Specifies the maximum time-to-live (TTL).</td>
</tr>
<tr>
<td>-p &lt;1-65535&gt;</td>
<td>Specifies the base UDP port number.</td>
</tr>
<tr>
<td>-q &lt;1-255&gt;</td>
<td>Specifies the number of probes per TTL.</td>
</tr>
<tr>
<td>-v</td>
<td>Specifies verbose mode (detailed output).</td>
</tr>
<tr>
<td>-w &lt;1-255&gt;</td>
<td>Specifies the wait time for each probe.</td>
</tr>
<tr>
<td>&lt;1-1176&gt;</td>
<td>Specifies the size of the probe packet.</td>
</tr>
<tr>
<td>source &lt;WORD 1-256&gt;</td>
<td>Specifies the source IP address.</td>
</tr>
<tr>
<td>vrf &lt;WORD 1-16&gt;</td>
<td>Specifies the VRF instance by VRF name for IPv4 addresses only.</td>
</tr>
</tbody>
</table>
Showing SNMP logs

Before you begin

• You must log on to the Global Configuration mode in ACLI.

About this task

Show the full SNMP logs. SNMP logs display the alarms and events that have been registered on the device.

Procedure

Show the logs:

```
show fulltech file WORD<1-99>
```

Variable definitions

Use the data in the following table to use the `show fulltech` command.

Table 33: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>file WORD&lt;1-99&gt;</td>
<td>This variable represents the log file to be opened and displayed. It is displayed in the following format:</td>
</tr>
<tr>
<td></td>
<td>• /intflash/&lt;file&gt;</td>
</tr>
</tbody>
</table>

Using trace to examine IS-IS control packets

Use trace as a debug tool to examine the code flow and Intermediate-System-to-Intermediate-System (IS-IS) control packets. When you enable IS-IS trace flags, only trace information about the set flag appears.

Before you begin

• You must know what you want to trace before you enable trace.

• You must log on to at least Privileged EXEC mode in ACLI to clear or save trace information.

Procedure

1. Enable the Intermediate-System-to-Intermediate-System trace flags:

```
trace flags isis set {none | tx-hello | rx-hello | tx-pkt | rx-pkt | adj | opt | tx-lsack | rx-lsack | tx-lsp | rx-lsp | pkt-err | nbr-mismatch | flood | spf-intra | spf-inter | spf-extern | prefix | nbr-change | intf-change | decide | fdb | dr | auth-fail | config | purge | policy | redist | tx-snp | rx-snp | timer | spbm-global |
```
Using trace to examine IS-IS control packets

2. Identify the module ID for which you want to use the trace tool:
   show trace modid-list

3. Clear the trace:
   clear trace

4. Begin the trace operation:
   trace level [<0-215>] [<0-4>]
   OR
   trace spbm isis level [<0-4>]
   OR
   trace cfm level [<0-4>]

   ✷ Note:
   Module ID 119 represents the IS-IS module.

5. Wait approximately 30 seconds.
   The default trace settings for CPU utilization are:
   • High CPU Utilization: 90%
   • High Track Duration: 5 seconds
   • Low CPU Utilization: 75%
   • Low Track Duration: 5 seconds

6. Stop tracing:
   trace shutdown

7. View the trace results:
   trace screen enable

   ⚠ Important:
   If you use trace level 3 (verbose) or trace level 4 (very verbose), Avaya recommends you do not use the screen to view commands due to the volume of information the system generates and the effect on the system.

8. Save the trace file.
   save trace [file WORD<1-99>]
   If you do not specify a file name, the file name is systrace.txt.

9. Display trace lines saved to a file:
   show trace file [tail]
10. Search trace results for a specific string value:

```
trace grep [WORD<0-128>]
```

If you use this command and do not specify a string value, you clear the results of a previous search.

11. Stop tracing:

```
trace shutdown
```

12. Disable the Intermediate-System-to-Intermediate-System trace flags:

```
trace flags isis remove { none | tx-hello | rx-hello | tx-pkt | rx-pkt | adj | opt | tx-lsack | rx-lsack | tx-lsp | rx-lsp | pkt-err | nbr-mismatch | flood | spf-intra | spf-inter | spf-extern | prefix | nbr-change | intf-change | decide |fdb | dr | auth-fail | config | purge | policy | redist | tx-snp | rx-snp | timer | spbm-global | global | perf | ucast-fib | node | mcast-fib | isid | ip-shortcut | debug | ip6-shortcut }
```

**Example**

Switch:1>enable

Clear prior trace information:

Switch:1#clear trace

Enable IS-IS trace flags for received IS-IS hello packets:

Switch:1#trace flags isis set rx-hello

Enable IS-IS trace flags for transmitted IS-IS hello packets:

Switch:1#trace flags isis set tx-hello

Configure the module ID to 119 (IS-IS module) and the trace to 4 (very verbose):

Switch:1#trace level 119 4

Enable the display of trace output to the screen:

Switch:1#trace screen enable

Switch:1# Screen tracing is on

Disable the display of trace output to the screen:

Switch:1#trace screen disable

Switch:1# Screen tracing is off

---

**Variable definitions**

Use the data in the following table to use the `trace flags isis` command.
Table 34: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>remove { none</td>
<td>Removes the Intermediate-System-to-Intermediate-System (IS-IS) trace flags for the specified option.</td>
</tr>
<tr>
<td>tx-hello</td>
<td>tx-hello</td>
</tr>
</tbody>
</table>

Using trace to examine IS-IS control packets

January 2017

Troubleshooting

Comments on this document? infodev@avaya.com
### Table: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-fail</td>
<td>Authorization failed</td>
</tr>
<tr>
<td>config</td>
<td>Configuration</td>
</tr>
<tr>
<td>purge</td>
<td>Link State Packet purge</td>
</tr>
<tr>
<td>redist</td>
<td>Redistribute</td>
</tr>
<tr>
<td>tx-snp</td>
<td>Transmitted Sequence Number PDU (CSNP and PSNP)</td>
</tr>
<tr>
<td>rx-snp</td>
<td>Received Sequence Number Packet (CSNP and PSNP)</td>
</tr>
<tr>
<td>timer</td>
<td>Timer</td>
</tr>
<tr>
<td>spbm-decide</td>
<td>SPBM decide flag</td>
</tr>
<tr>
<td>global</td>
<td>Global flag</td>
</tr>
<tr>
<td>perf</td>
<td>SPBM performance</td>
</tr>
<tr>
<td>ucast-fib</td>
<td>Unicast Forwarding Information Base</td>
</tr>
<tr>
<td>node</td>
<td>Node</td>
</tr>
<tr>
<td>isid</td>
<td>I-SID</td>
</tr>
<tr>
<td>ip-shortcut</td>
<td>IP Shortcut</td>
</tr>
<tr>
<td>debug</td>
<td>Debug</td>
</tr>
<tr>
<td>ip6-shortcut</td>
<td>IPv6 shortcut flag</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `show trace` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Displays the current configuration for the automatic trace function.</td>
</tr>
<tr>
<td>file</td>
<td>Displays the trace results saved to a file.</td>
</tr>
<tr>
<td>level</td>
<td>Displays the current trace level for all modules.</td>
</tr>
<tr>
<td>modid-list</td>
<td>Specifies the module ID list.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `trace` command.

**Table 35: Variable definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>grep [WORD&lt;0-128&gt;]</td>
<td>Specifies the search keyword. You can use a specific MAC address. You can search for errors, using the command, <code>trace grep error</code>.</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cfm level [&lt;0-4&gt;]</td>
<td>Starts tracing by CFM.</td>
</tr>
<tr>
<td></td>
<td>• 0-4 specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose.</td>
</tr>
<tr>
<td>spbm isis level [&lt;0-4&gt;]</td>
<td>Specifies exactly which IS-IS component to display.</td>
</tr>
<tr>
<td></td>
<td>• 0-4 specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose.</td>
</tr>
<tr>
<td>level [&lt;0-234&gt;] [&lt;0-4&gt;]</td>
<td>Starts the trace by specifying the module ID and level.</td>
</tr>
<tr>
<td></td>
<td>&lt;0-234&gt; specifies the module ID. Module ID 119 represents the IS-IS module.</td>
</tr>
<tr>
<td></td>
<td>Specifies the trace level:</td>
</tr>
<tr>
<td></td>
<td>• 0 — Disabled</td>
</tr>
<tr>
<td></td>
<td>• 1 — Very terse</td>
</tr>
<tr>
<td></td>
<td>• 2 — Terse</td>
</tr>
<tr>
<td></td>
<td>• 3 — Verbose</td>
</tr>
<tr>
<td></td>
<td>• 4 — Very verbose</td>
</tr>
<tr>
<td>shutdown</td>
<td>Stops the trace operation.</td>
</tr>
<tr>
<td>screen {disable</td>
<td>enable}</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>Avaya recommends you avoid using the screen to view commands if you use trace level 3 (verbose) or trace level 4 (very verbose) due to the volume of information generated and the effect on the system.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `save trace` command.

**Table 36: Variable definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>file WORD&lt;1–99&gt;</td>
<td>Specifies the file name in one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• a.b.c.d: &lt;file&gt;</td>
</tr>
<tr>
<td></td>
<td>WORD&lt;1–99&gt; is a string of 1–99 characters.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>If you do not specify a file name, the file name is systrace.txt.</td>
</tr>
</tbody>
</table>
Viewing the metric type of IS-IS route in TLVs – detailed

About this task

Use the following procedure to view the detailed information about metric type of IS-IS routes in TLVs in Link State Packets (LSP).

Procedure

1. Display the detail view of TLV 135:
   ```
   show isis lsdb tlv 135 detail
   ```
2. Display the detail view of TLV 184:
   ```
   show isis lsdb tlv 184 detail
   ```

Example

Viewing the metric type of IS-IS route in TLV 135

Switch:1#show isis lsdb tlv 135 detail

```
================================================================================
ISIS LSDB (DETAIL)
================================================================================
--------------------------------------------------------------------------------
Level-1 LspID: 4072.0000.0000.00-02     SeqNum: 0x00000009      Lifetime:  1110
Chksum: 0x31ce  PDU Length: 46
Host_name: evp4k
Attributes:     IS-Type 1
TLV:135 TE IP Reachability: 2
   Metric: 1 Metric Type:Internal  Prefix Length: 32
     UP/Down Bit: FALSE              Sub TLV Bit: FALSE
   IP Address: 15.15.15.72
   Metric: 1 Metric Type:External  Prefix Length: 24
     UP/Down Bit: FALSE              Sub TLV Bit: FALSE
   IP Address: 10.139.99.0
```

Viewing the metric type of IS-IS route in TLV 184

Switch:1#show isis lsdb tlv 184 detail

```
================================================================================
ISIS LSDB (DETAIL)
================================================================================
--------------------------------------------------------------------------------
Level-1 LspID: 4072.0000.0000.00-03     SeqNum: 0x00000008      Lifetime:  1103
Chksum: 0x3ce6  PDU Length: 72
Host_name: evp4k
Attributes:     IS-Type 1
TLV:184 SPBM IPVPN Reachability: 2
   Metric: 1 Metric Type:External   Prefix Length:32
     Vrf ISID:100
     Metric:1 Metric Type:Internal   Prefix Length:32
       IP Address: 100.1.1.1
       IP Address: 15.15.15.72
```
### Viewing the metric type of IS-IS route in TLVs – summarized

**About this task**

Use the following procedure to view the summarized information about metric type of IS-IS routes in TLVs. You can also view the metric type of the prefix.

**Procedure**

Display the summarized view of TLVs 135 and 184:

```
show isis lsdb ip-unicast
```

**Example**

Display the summarized view of TLVs.

```
evp4k:1#show isis lsdb ip-unicast
```

<table>
<thead>
<tr>
<th>I-SID</th>
<th>ADDRESS</th>
<th>METRIC</th>
<th>TYPE</th>
<th>TLV</th>
<th>TYPE</th>
<th>FRAG</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>15.15.15.72</td>
<td>32</td>
<td>1</td>
<td>Internal</td>
<td>135</td>
<td>0x2</td>
<td>evp4k</td>
</tr>
<tr>
<td>-</td>
<td>10.139.99.0</td>
<td>24</td>
<td>1</td>
<td>External</td>
<td>135</td>
<td>0x2</td>
<td>evp4k</td>
</tr>
<tr>
<td>100</td>
<td>100.1.1.1</td>
<td>32</td>
<td>1</td>
<td>External</td>
<td>184</td>
<td>0x3</td>
<td>evp4k</td>
</tr>
<tr>
<td>100</td>
<td>15.15.15.72</td>
<td>32</td>
<td>1</td>
<td>Internal</td>
<td>184</td>
<td>0x3</td>
<td>evp4k</td>
</tr>
<tr>
<td>-</td>
<td>15.0.60.4</td>
<td>32</td>
<td>1</td>
<td>Internal</td>
<td>135</td>
<td>0x2</td>
<td>esp1</td>
</tr>
</tbody>
</table>

5 out of 5 Total Num of Entries
Chapter 17: Software troubleshooting tool configuration using EDM

Use the tools described in this section to perform troubleshooting procedures using Enterprise Device Manager (EDM).

Flushing routing tables by VLAN

About this task
For administrative and troubleshooting purposes, sometimes you must flush the routing tables. You can use EDM to flush the routing tables by VLAN or flush them by port. Perform this procedure to flush the IP routing table for a VLAN.

Procedure
1. In the navigation tree, expand the following folders: Configuration > VLAN.
2. Click VLANs.
3. Click the Advanced tab.
4. In the Vlan Operation Action box for the VLAN you want to flush, double-click, and then select a flush option from the list.
   In a VLAN context, all entries associated with the VLAN are flushed. You can also flush the Address Resolution Protocol (ARP) entries and IP routes for the VLAN.
5. Click Apply.

Flushing routing tables by port

About this task
For administrative and troubleshooting purposes, sometimes you must flush the routing tables. You can use EDM to flush the routing tables by VLAN or flush them by port. Perform this procedure to flush the IP routing table for a port.
**Procedure**

1. On the Device Physical View, select a port.
2. In the navigation tree, expand the following folders: **Configuration > Edit > Port**.
3. Click **General**.
4. Click the Interface tab.
5. In the **Action** section, select **flushAll**.
   
   In a port context, all entries associated with the port are flushed. You can flush the ARP entries and IP routes for a port. After you flush a routing table, it is not automatically repopulated. The repopulation time delay depends on the routing protocols in use.
6. Click **Apply**.

---

**Configuring port mirroring**

**Before you begin**

- To change a port mirroring configuration, first disable mirroring.

**About this task**

Use port mirroring to aid in diagnostic and security operations.

Use port mirroring to make a copy of a traffic flow and send that copy to a device for analysis, for example, for diagnostic sniffing. Use the mirror to see the packets in the flow without breaking into the physical connection to place a packet onto the sniffer inline. You can also use port mirroring for security. You can send flows to inspection engines for post processing.

Connect the sniffer (or other traffic analyzer) to the output port you specify in this procedure.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **General**.
3. Click the **Port Mirrors** tab.
4. Click **Insert**.
5. To enable port mirroring for the instance, select the **Enable** check box.
6. Configure mirroring as required.

**Note:**

When you configure **tx** mode port mirroring on T-UNI and SPBM NNI ports, unknown unicast, broadcast and multicast traffic packets that ingress these ports appear on the mirror destination port, although they do not egress the mirror source port. This is
because tx mode port mirroring happens on the mirror source port before the source port squelching logic drops the packets at the egress port.

7. Click **Insert**.

### Port Mirrors field descriptions

Use the data in the following table to use the **Port Mirrors** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Specifies an assigned identifier for the configured port mirroring instance.</td>
</tr>
<tr>
<td>MirroredPortList</td>
<td>Specifies a port to be mirrored (the source port).</td>
</tr>
<tr>
<td>Enable</td>
<td>Enables or disables this port mirroring instance. The default value is Enable.</td>
</tr>
<tr>
<td>Mode</td>
<td>Specifies the traffic direction of the packet being mirrored:</td>
</tr>
<tr>
<td></td>
<td>• tx mirrors egress packets.</td>
</tr>
<tr>
<td></td>
<td>• rx mirrors ingress packets.</td>
</tr>
<tr>
<td></td>
<td>• both mirrors both egress and ingress packets.</td>
</tr>
<tr>
<td></td>
<td>The default is rx.</td>
</tr>
<tr>
<td>MirroringPortList</td>
<td>Specifies a destination port (the port to which the mirrored packets are forwarded). Configures the mirroring port.</td>
</tr>
<tr>
<td>MirroringMultId</td>
<td>Specifies the destination MultiLink trunking ID.</td>
</tr>
</tbody>
</table>

### Configuring ACLs for mirroring

Configure the access control list (ACL) to mirror packets for an access control entry (ACE) that matches a particular packet.

**Before you begin**

- The ACL exists.

**About this task**

To modify an ACL parameter, double-click the parameter you wish to change. Change the value, and then click Apply. You cannot change a parameter that appears dimmed; in this case, delete the ACL, and then configure a new one.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > Security > Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Double-click the parameter **MirrorVlanId** to configure mirroring to a destination VLAN.
5. Double-click the parameter **MirrorMltId** to configure mirroring to a destination MLT group.
6. Double-click the parameter **MirrorDstPortList** to configure mirroring to a destination port or ports.

---

**ACL field descriptions**

Use the data in the following table to use the **ACL** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AclId</td>
<td>Specifies a unique identifier for the ACL from 1–2048.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the ACL is VLAN- or port-based. Valid options are</td>
</tr>
<tr>
<td></td>
<td>• inVlan</td>
</tr>
<tr>
<td></td>
<td>• inPort</td>
</tr>
<tr>
<td></td>
<td>• outPort</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> The inVlan ACLs drop packets if you add a VLAN after ACE</td>
</tr>
<tr>
<td></td>
<td>creation.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies a descriptive user-defined name for the ACL.</td>
</tr>
<tr>
<td>VlanList</td>
<td>For inVlan type, specifies all VLANs to associate with the ACL.</td>
</tr>
<tr>
<td>PortList</td>
<td>For inPort and outPort ACL types, specifies the ports to associate with the</td>
</tr>
<tr>
<td></td>
<td>ACL.</td>
</tr>
<tr>
<td>DefaultAction</td>
<td>Specifies the action taken when no ACEs in the ACL match. Valid options are</td>
</tr>
<tr>
<td></td>
<td>• deny and permit. Deny means the system drops the packets; permit means</td>
</tr>
<tr>
<td></td>
<td>• the system forwards packets. The default is permit.</td>
</tr>
<tr>
<td>ControlPktAction</td>
<td>Specifies the action for control packets, if you configure DefaultAction</td>
</tr>
<tr>
<td></td>
<td>to deny. If DefaultAction is permit, this value is ignored.</td>
</tr>
<tr>
<td>State</td>
<td>Enables or disables all of the ACEs in the ACL. The default value is</td>
</tr>
<tr>
<td></td>
<td>enable.</td>
</tr>
<tr>
<td>PktType</td>
<td>Indicates the packet type that this ACL is applicable to. The default is</td>
</tr>
<tr>
<td></td>
<td>IPv4.</td>
</tr>
<tr>
<td>MirrorVlanId</td>
<td>Configures mirroring to a destination VLAN.</td>
</tr>
<tr>
<td>MirrorMltId</td>
<td>Configures mirroring to a destination MLT group.</td>
</tr>
<tr>
<td>MirrorDstPortList</td>
<td>Configures mirroring to a destination port or ports.</td>
</tr>
</tbody>
</table>
Configuring ACEs for mirroring

**Before you begin**
- The ACL exists.
- The ACE exists.

**About this task**
Configure actions to use filters for flow mirroring. Use an ACE to define the mirroring actions the filter performs.

If you use the mirror action, ensure that you specify the mirroring destination: IP address, MLTs, ports, or VLANs.

**Procedure**
1. In the navigation tree, expand the following folders: **Configuration > Security > Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the ACL for which to modify an ACE.
5. Click **ACE**.
6. Select an ACE, and then click **Action**.
7. Configure one of: **DstPortList**, **DstMltId**, or **DstIp**.
8. Click **Apply**.

**Action field descriptions**
Use the data in the following table to use the **Action** tab.

*Note:* The table lists the options for both Security ACEs and QoS ACEs. Dependent upon the ACE different options appear on the EDM interface.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AclId</td>
<td>Specifies the ACL ID.</td>
</tr>
<tr>
<td>AceId</td>
<td>Specifies a unique identifier and priority for the ACE.</td>
</tr>
<tr>
<td>Mode</td>
<td>Indicates the operating mode associated with this ACE. Valid options are deny, permit and none. The default is none.</td>
</tr>
<tr>
<td>RemarkDscp</td>
<td>Specifies the new Per-Hop Behavior (PHB) for matching packets: phbs0, phbs1, phbf11, phbf12, phbf13, phbs2, phbf21, phbf22, phbf23, phbs3, phbf31, phbf32, phbf33, phbs4, phbf41, phbf42, phbf43, phbs5, phbf, phbs6, phbs7.</td>
</tr>
</tbody>
</table>

Table continues…

January 2017  
Troubleshooting  
Comments on this document? infodev@avaya.com
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>RemarkDot1Priority</td>
<td>Specifies the new 802.1 priority bit for matching packets: zero, one, two, three, four, five, six, or seven. This action is a QoS action. The ACE ID must be in the range of 1001–2000. The default is disable.</td>
</tr>
<tr>
<td>InternalQoS</td>
<td>This variable is a QoS action. The ACE ID must be in the range of 1001–2000. The default value is 1.</td>
</tr>
<tr>
<td>RedirectNextHop</td>
<td>Redirects matching IP traffic to the next hop. The default is 0.0.0.0.</td>
</tr>
<tr>
<td>RedirectUnreach</td>
<td>Configures the desired behavior for redirected traffic when the specified next-hop is not reachable. The default value is deny.</td>
</tr>
<tr>
<td>Count</td>
<td>Enables the ability to count matching packets. Use this parameter with either a security or QoS ACE. The default is disabled.</td>
</tr>
<tr>
<td>Log</td>
<td>This action logs to the switch. Use this parameter with either a security or QoS ACE. The default is disabled.</td>
</tr>
<tr>
<td>DstPortList</td>
<td>Specifies the ports to which to mirror traffic.</td>
</tr>
<tr>
<td>DstMltId</td>
<td>Specifies the Multilink Trunking (MLT) group to which to mirror traffic.</td>
</tr>
<tr>
<td>DstIp</td>
<td>Configures mirroring to a destination IP address for flow-based mirroring.</td>
</tr>
<tr>
<td>DstIpDscp</td>
<td>Optionally, configures the DSCP value. The default is 256 (disabled).</td>
</tr>
<tr>
<td>DstIpTtl</td>
<td>Optionally, configures the time-to-live value. The default TTL is 64.</td>
</tr>
</tbody>
</table>

**Running a ping test**

**About this task**

Use ping to determine if an entity is reachable.

⚠️ **Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software*, NN47227-401. As an alternative, use the ACLI.

**Procedure**

1. From the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **Ping/Trace Route**.
3. Click the **Ping Control** tab.
4. Click **Insert**.
5. In the **OwnerIndex** box, type the owner index.
6. In the **TestName** box, type the name of the test.
7. In the **TargetAddress** box, type the host IP address.
8. From the **AdminStatus** options, select **enabled**.
9. In the remainder of the option boxes, type the desired values.
10. Click **Insert**.
11. Select an entry, and then click **Start**.
    Let the test run for several seconds.
12. Select an entry, and then click **Stop**.
13. View the Ping results.

### Ping Control field descriptions

Use the data in the following table to use the **Ping Control** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OwnerIndex</strong></td>
<td>Provides access control by a security administrator using the View-Based Access Control Model (VACM) for tables in which multiple users need to independently create or modify entries. This is a string of up to 32 characters.</td>
</tr>
<tr>
<td><strong>TestName</strong></td>
<td>Specifies the name of the ping test.</td>
</tr>
<tr>
<td><strong>TargetAddress</strong></td>
<td>Specifies the host address to use at a remote host to perform a ping operation.</td>
</tr>
<tr>
<td><strong>DataSize</strong></td>
<td>Specifies the size of the data portion (in octets) to transmit in a ping operation. The default is 16.</td>
</tr>
<tr>
<td><strong>TimeOut</strong></td>
<td>Specifies the timeout value, in seconds, for a remote ping operation. The default is 3 seconds.</td>
</tr>
<tr>
<td><strong>ProbeCount</strong></td>
<td>Specifies the number of times to perform a ping operation at a remote host. The default is 1.</td>
</tr>
<tr>
<td><strong>AdminStatus</strong></td>
<td>Specifies the state of the ping control entry: enabled or disabled. The default is disabled.</td>
</tr>
<tr>
<td><strong>DataFill</strong></td>
<td>Determines the data portion of a probe packet.</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>Specifies the number of seconds to wait before repeating a ping test. The default is 0.</td>
</tr>
<tr>
<td><strong>MaxRows</strong></td>
<td>Specifies the maximum number of entries allowed in the PingProbeHistory table. The default is 50.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrapGeneration</td>
<td>Specifies when to generate a notification. The options are:</td>
</tr>
<tr>
<td></td>
<td>• ProbeFailure—Generates a PingProbeFailed notification subject to the value of TrapProbeFailureFilter. The object TrapProbeFailureFilter can specify the number of successive probe failures that are required before a pingProbeFailed notification is generated.</td>
</tr>
<tr>
<td></td>
<td>• TestFailure—Generates a PingTestFailed notification. The object TrapTestFailureFilter can determine the number of probe failures that signal when a test fails.</td>
</tr>
<tr>
<td></td>
<td>• TestCompletion—Generates a PingTestCompleted notification. The value of this object defaults to zero, indicating that none of the above options have been selected.</td>
</tr>
<tr>
<td>TrapProbeFailureFilter</td>
<td>Specifies the number of successive probe failures that are required before a pingProbeFailed notification is generated. The default is 1.</td>
</tr>
<tr>
<td>TrapTestFailureFilter</td>
<td>Determines the number of probe failures that signal when a test fails. The default is 1.</td>
</tr>
<tr>
<td>Descr</td>
<td>Describes the remote ping test. The default is 0x00.</td>
</tr>
<tr>
<td>SourceAddress</td>
<td>Specifies the IP address (a.b.c.d) as the source address in outgoing probe packets.</td>
</tr>
<tr>
<td>ByPassRouteTable</td>
<td>Enables (optionally) the bypassing of the route table. The default is disabled.</td>
</tr>
</tbody>
</table>

**Viewing ping results**

**About this task**

View ping results to view performance-related data.

**Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software, NN47227-401*. As an alternative, use the ACLI.

**Procedure**

1. From the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **Ping/Trace Route**.
3. Click the **Ping Control** tab.
4. Select a ping test entry.
5. Click **Ping Result**.
### Ping Result field descriptions

Use the data in the following table to use the Ping Result tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OwnerIndex</td>
<td>Specifies the ping test owner.</td>
</tr>
<tr>
<td>TestName</td>
<td>Specifies the test name.</td>
</tr>
<tr>
<td>OperStatus</td>
<td>Indicates the operational status of the test. The default is disabled.</td>
</tr>
<tr>
<td>IpTargetAddressType</td>
<td>Specifies the IP address type of the target. The default is unknown.</td>
</tr>
<tr>
<td>IpTargetAddress</td>
<td>Specifies the IP address of the target.</td>
</tr>
<tr>
<td>MinRtt</td>
<td>Specifies the minimum ping round-trip-time (RTT) received. A value of 0 means that no RTT is received.</td>
</tr>
<tr>
<td>MaxRtt</td>
<td>Specifies the maximum ping RTT received. A value of 0 means that no RTT is received.</td>
</tr>
<tr>
<td>AverageRtt</td>
<td>Specifies the current average ping RTT.</td>
</tr>
<tr>
<td>ProbeResponses</td>
<td>Specifies the number of responses to probes.</td>
</tr>
<tr>
<td>SentProbes</td>
<td>Specifies the number of sent probes.</td>
</tr>
<tr>
<td>RttSumOfSquares</td>
<td>Specifies the sum of squares of RTT for all probes received.</td>
</tr>
<tr>
<td>LastGoodProbe</td>
<td>Specifies the date and time when the last response is received for a probe.</td>
</tr>
</tbody>
</table>

### Viewing ping probe history

**About this task**

View the ping probe history to view the history of ping tests performed by the switch.

**Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see Release Notes for VSP Operating System Software, NN47227-401. As an alternative, use the ACLI.

**Procedure**

1. From the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click Ping/Trace Route.
3. Select a ping entry.
4. Click Ping Probe History.
Ping Probe History field descriptions

Use the data in the following table to use the Ping Probe History tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OwnerIndex</td>
<td>Specifies the owner index</td>
</tr>
<tr>
<td>TestName</td>
<td>Indicates the name given to the test.</td>
</tr>
<tr>
<td>Index</td>
<td>Specifies the index number</td>
</tr>
<tr>
<td>Response</td>
<td>Indicates the amount of time, measured in milliseconds, between request (probe) and response, or when the request timed out. Response is reported as 0 when it is not possible to transmit a probe.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the status of the response; the result of a particular probe done by a remote host.</td>
</tr>
<tr>
<td>LastRC</td>
<td>Indicates the last implementation-method-specific reply code (RC) received. If ICMP Echo is used, then a successful probe ends when an ICMP response is received that contains the code ICMP_ECHOREPLY(0).</td>
</tr>
<tr>
<td>Time</td>
<td>Indicates the timestamp for this probe result.</td>
</tr>
</tbody>
</table>

Running a traceroute test

About this task

Run a traceroute test to determine the route packets take through a network to a destination.

⚠ Note:

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see Release Notes for VSP Operating System Software, NN47227-401. As an alternative, use the ACLI.

Procedure

1. From the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click Ping/Trace Route.
3. Click the Trace Route Control tab.
4. Click Insert.
5. Configure the instance as required.
6. Click Insert.
7. Select an entry, and then click Start.
Let the test run for several seconds.
8. Select an entry, and then click Stop.
9. View the traceroute test results.

**Trace Route Control field descriptions**

Use the data in the following table to use the Trace Route Control tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OwnerIndex</strong></td>
<td>Provides access control by a security administrator using the VACM for tables in which multiple users need to independently create or modify entries.</td>
</tr>
<tr>
<td><strong>TestName</strong></td>
<td>Specifies the name of the traceroute test.</td>
</tr>
<tr>
<td><strong>TargetAddressType</strong></td>
<td>Specifies the type of host address to use on the traceroute request at the remote host. The default is IPv4.</td>
</tr>
<tr>
<td><strong>TargetAddress</strong></td>
<td>Specifies the host address used on the traceroute request at the remote host.</td>
</tr>
<tr>
<td><strong>ByPassRouteTable</strong></td>
<td>Enables bypassing of the route table. If you enable this variable, the remote host bypasses the normal routing tables and sends directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. You can use this variable to perform the traceroute operation to a local host through an interface that has no route defined. The default is disabled.</td>
</tr>
<tr>
<td><strong>DataSize</strong></td>
<td>Specifies the size of the data portion of a traceroute request in octets. The default is 1.</td>
</tr>
<tr>
<td><strong>TimeOut</strong></td>
<td>Specifies the timeout value, in seconds, for a traceroute request. The default is 3.</td>
</tr>
<tr>
<td><strong>ProbesPerHop</strong></td>
<td>Specifies the number of times to reissue a traceroute request with the same time-to-live (TTL) value. The default is 3.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Specifies the UDP port to which to send the traceroute request. Specify a port that is not in use at the destination (target) host. The default is the IANA assigned port 33434.</td>
</tr>
<tr>
<td><strong>MaxTtl</strong></td>
<td>Specifies the maximum time-to-live from 1–255. The default is 30.</td>
</tr>
<tr>
<td><strong>DSField</strong></td>
<td>Specifies the value to store in the Differentiated Services (DS) field in the IP packet used to encapsulate the traceroute probe. The default is 0.</td>
</tr>
<tr>
<td><strong>SourceAddressType</strong></td>
<td>Specifies the type of the source address to use at a remote host.</td>
</tr>
<tr>
<td><strong>SourceAddress</strong></td>
<td>Uses the specified IP address (which must be an IP number, not a hostname) as the source address in outgoing probe packets.</td>
</tr>
<tr>
<td><strong>IfIndex</strong></td>
<td>Directs the traceroute probes to be transmitted over the specified interface. The default is 0.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiscOptions</td>
<td>Enables an application to specify implementation-dependent options.</td>
</tr>
<tr>
<td>MaxFailures</td>
<td>Indicates the maximum number of consecutive timeouts allowed before terminating a remote traceroute request. The default is 5.</td>
</tr>
<tr>
<td>DontFragment</td>
<td>Enables setting of the do not fragment (DF) flag in the IP header for a probe. The default is disabled.</td>
</tr>
<tr>
<td>InitialTtl</td>
<td>Specifies the initial time-to-live (TTL) value to use. The default is 1.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Specifies the number of seconds to wait before repeating a traceroute test as defined by the value of the various objects in the corresponding row. The default is 0.</td>
</tr>
<tr>
<td>StorageType</td>
<td>Specifies the storage type for this row.</td>
</tr>
<tr>
<td>AdminStatus</td>
<td>Specifies the desired state for TraceRouteCtlEntry. The options are enabled or disabled. The default is disabled.</td>
</tr>
<tr>
<td>MaxRows</td>
<td>Specifies the maximum number of entries allowed in the TraceRouteProbeHistoryTable. The default is 50.</td>
</tr>
<tr>
<td>TrapGeneration</td>
<td>Determines when to generate a notification for this entry. The options are</td>
</tr>
<tr>
<td></td>
<td>• pathChange — Generates a TraceRoutePathChange notification after the current path varies from a previously determined path.</td>
</tr>
<tr>
<td></td>
<td>• testFailure — Generates a TraceRouteTestFailed notification after the full path to a target cannot be determined.</td>
</tr>
<tr>
<td></td>
<td>• testCompletion — Generates a TraceRouteTestCompleted notification after the path to a target has been determined.</td>
</tr>
<tr>
<td>Descr</td>
<td>Describes the remote traceroute test.</td>
</tr>
<tr>
<td>CreateHopsEntries</td>
<td>Stores the current path for a traceroute test in the TraceRouteHopsTable on an individual hop basis when the value of this object is true. The default is false.</td>
</tr>
<tr>
<td>Type</td>
<td>Reports or selects the implementation method to use for performing a traceroute operation.</td>
</tr>
</tbody>
</table>

**Viewing traceroute results**

**About this task**

View traceroute results to view performance-related data.

**Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software*, NN47227-401. As an alternative, use the ACLI.
Procedure

1. From the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click Ping/Trace Route.
3. Click the Trace Route Control tab.
4. Select a traceroute entry.
5. Click Trace Route Result.

Trace Route Result field descriptions

Use the data in the following table to use the Trace Route Result tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OwnerIndex</td>
<td>Specifies the index of the owner.</td>
</tr>
<tr>
<td>TestName</td>
<td>Specifies the name of the test.</td>
</tr>
<tr>
<td>OperStatus</td>
<td>Specifies the operational status of the test. The default is disabled.</td>
</tr>
<tr>
<td>CurHopCount</td>
<td>Specifies the current count of hops.</td>
</tr>
<tr>
<td>CurProbeCount</td>
<td>Specifies the current count of probes.</td>
</tr>
<tr>
<td>IpTgtAddressType</td>
<td>Specifies the IP target address type</td>
</tr>
<tr>
<td>IpTgtAddr</td>
<td>Specifies the IP target address.</td>
</tr>
<tr>
<td>TestAttempts</td>
<td>Specifies the number of test attempts.</td>
</tr>
<tr>
<td>TestSuccesses</td>
<td>Specifies the number of successful test attempts.</td>
</tr>
<tr>
<td>LastGoodPath</td>
<td>Specifies the date and time when the last response is received for a probe.</td>
</tr>
</tbody>
</table>

Viewing the traceroute history

About this task

View the traceroute history to view the history of traceroute tests performed by the switch.

The traceroute probe history contains probe information for the hops in the routing path.

Note:

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see Release Notes for VSP Operating System Software, NN47227-401. As an alternative, use the ACLI.

Procedure

1. From the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click Ping/Trace Route.
3. Click the Trace Route Control tab.
4. Select an entry.
5. Click Trace Route Probe History.

---

**Route Probe History field descriptions**

Use the data in the following table to use the Trace Route Probe History tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OwnerIndex</td>
<td>Identifies the Trace Route entry to which a probe result belongs.</td>
</tr>
<tr>
<td>TestName</td>
<td>Specifies the test name.</td>
</tr>
<tr>
<td>Index</td>
<td>Specifies the Index.</td>
</tr>
<tr>
<td>HopIndex</td>
<td>Indicates for which hop in a traceroute path the probe results are intended.</td>
</tr>
<tr>
<td>ProbeIndex</td>
<td>Specifies the index of a probe for a particular hop in a traceroute path.</td>
</tr>
<tr>
<td>HAddrType</td>
<td>Specifies the IP address type of the hop to which this probe belongs.</td>
</tr>
<tr>
<td>HAddr</td>
<td>Specifies the IP address of the hop to which this probe belongs.</td>
</tr>
<tr>
<td>Response</td>
<td>Specifies the cumulative results at any time.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the status of the probe.</td>
</tr>
<tr>
<td>LastRC</td>
<td>When a new entry is added, the old entry is purged if the total number of entries exceeds the specified maximum number of entries in the Control Table Entry.</td>
</tr>
<tr>
<td>Time</td>
<td>Specifies the response time of the probe.</td>
</tr>
</tbody>
</table>
Chapter 18: Layer 1 troubleshooting

Use this section to help you troubleshoot Layer 1 (physical layer) problems.

Troubleshooting fiber optic links

About this task

You can troubleshoot fiber optic links to ensure that the optical transmitters and receivers operate correctly, and to determine if a receiver is saturated, or does not receive enough power.

To troubleshoot optical links and devices, you can use Digital Diagnostic Monitoring (DDM), as well as published optical specifications.

For more information about Small Form Factor Pluggable (SFP) transceivers and SFP plus (SFP+) transceivers, see Installing Transceivers and Optical components on VSP Operating System Software, NN47227-301.

Important:

Avaya recommends the use of Avaya branded SFP and SFP+ transceivers as they have been through extensive qualification and testing. Avaya will not be responsible for issues related to non-Avaya branded SFP and SFP+ transceivers.

Procedure

1. Measure the SFP or SFP+ transmit power.
2. Compare the measured transmit power with the specified launch power.
   The values are similar. If the measured power is far below the specified value, a faulty transmitter is a possible cause.
3. Compare the measured transmit power for the near-end optical device to the measured transmit power for the far-end device.
   Large differences can mean that the optical devices are mismatched (that is, -SX versus -LX).
4. Measure the receive power at each end of the link.
5. Compare the receive power to the transmit power.
   • For short fiber links, the transmit and received power are similar (after taking into consideration connection losses).
For long fiber links, the transmit and received power are similar (after taking into consideration connection losses and fiber attenuation).

Large differences can mean a damaged fiber or dirty or faulty connectors. Large differences can also mean that the link does not use the right type of fiber (single mode or multimode). If the receiver power is measured to be zero, and the link worked previously, it is probable that the far-end transmitter is not operating or the fiber is broken.

6. Compare the measured receive power for the near-end optical device to the measured receive power for the far-end device.

Large differences could mean that the optical devices are mismatched (that is, -SX versus -LX). If optical devices are mismatched, the receiver can be saturated (overdriven).

7. If a receiver is saturated but still operable, install a suitable attenuator.

For long-haul optical devices, the receive power must be significantly less that the transmit power.

8. To help debug the link, loop back the local transmit and receive ports, and use the DDM parameters to help determine the fault.
Chapter 19: Operations and Management

CFM fundamentals

The Shortest Path Bridging MAC (SPBM) network needs a mechanism to debug connectivity issues and to isolate faults. This is performed at Layer 2, not Layer 3. Connectivity Fault Management (CFM) operates at Layer 2 and provides an equivalent of ping and traceroute. To support troubleshooting of the SPBM cloud, the Avaya Virtual Services Platform switch supports a subset of CFM functionality. Configure CFM on all SPBM VLANs.

CFM is based on the IEEE 802.1ag standard.

IEEE 802.1ag Connectivity Fault Management (CFM) provides OAM tools for the service layer, which allows you to monitor and troubleshoot an end-to-end Ethernet service instance. CFM is the standard for Layer 2 ping, Layer 2 traceroute, and the end-to-end connectivity check of the Ethernet network.

The 802.1ag feature divides or separates a network into administrative domains called Maintenance Domains (MD). Each MD is further subdivided into logical groupings called Maintenance Associations (MA). A single MD can contain several MAs.

Each MA is defined by a set of Maintenance Points (MP). An MP is a demarcation point on an interface that participates in CFM within an MD. Two types of MP exist:

- Maintenance End Point (MEP)
- Maintenance Intermediate Point (MIP)

CFM supports three kinds of standard CFM messages: Continuity Check Message (CCM), Loopback Message (LBM), and Linktrace Message (LTM). Messages are sent between Maintenance Points (MP) in the system.

On the switch, CFM is implemented using the LBM and LTM features only to debug SPBM. CCM messages are not required or supported in the current release.

You can assign maintenance levels for each CFM SPBM MEP and MIP to each SPBM B-VLAN individually or you can assign maintenance levels and global MEPs for all SPBM VLANs.
Autogenerated CFM and explicitly configured CFM

The Avaya Virtual Services Platform switch simplifies CFM configuration with autogenerated CFM. With autogenerated CFM, you use the commands `cfm spbm enable` and `cfm cmac enable` and the switch creates default MD, MA, MEPs, and MIPs for SPBM B-VLANs and C-VLANs respectively.

If you choose to configure CFM explicitly, you must configure an MD, MA, MEPs, and MIPs.

- For SPBM B-VLANs, the switch provides two methods to configure CFM, namely, autogenerated and explicitly configured. You cannot use both.
- For C-VLANs, you can only use autogenerated CFM.

⚠️ Important:

Only the VSP 4000 Series switch supports CFM configuration on C-VLANs.

Autogenerated CFM

You can use autogenerated CFM at a global level to create a MEP and a MIP at a specified level for every SPBM B-VLAN and C-VLAN on the chassis. If you use autogenerated CFM commands, you do not have to configure explicit MDs, MAs, MEPs, or MIPs, and associate them with multiple VLANs.

If you do not want to use autogenerated CFM commands, you can choose to configure explicit MDs, MAs, MEPs, and MIPs for SPBM B-VLANs. However, you cannot use both an autogenerated CFM configuration and an explicit CFM configuration together.

⚠️ Note:

Previous explicit CFM configurations of MDs, MAs, and MEPs on SPBM B-VLANs continue to be supported. However, if you want to enable the new autogenerated commands you must first remove the existing MEP and MIP on the SPBM B-VLANs. The switch only supports one type of MEP or MIP for each SPBM B-VLAN.

For information on autogenerated CFM configuration using the ACLI see:

- Configuring autogenerated CFM on SPBM B-VLANs on page 155
- Configuring autogenerated CFM on C-VLANs on page 157

For information on autogenerated CFM configuration using the EDM see:

- Configuring autogenerated CFM on SPBM B-VLANs on page 184
- Configuring autogenerated CFM on C-VLANs on page 186

Explicitly configured CFM

If you choose to explicitly configure CFM, you must configure an MD, MA, MEPs, and MIPs. You can configure explicit CFM only on SPBM B-VLANs.

For explicit configuration information for ACLI see Configuring explicit mode CFM on page 159.

For explicit configuration information for EDM see Configuring explicit CFM in EDM on page 187.
Using CFM

For SPBM B-VLANs, the autogenerated MEPs and MIPs respond to **12 ping**, **12 traceroute**, and **12 tracetree** in the same manner as the MEPs and MIPs created explicitly. For C-VLANs, the autogenerated MEPs and MIPs respond to **12 ping** and **12 traceroute**, but not to **12 tracetree** because no multicast trees exist on C-VLANs. The CFM show commands that display MD, MA, and MEP information work for both autogenerated and explicitly configured CFM MEPs.

You can use CFM to troubleshoot networks and hosts that support the CFM protocol. Once you configure CFM, CFM works in the network whether or not SPBM is in use.

You cannot use CFM to troubleshoot networks and hosts that do not support the CFM protocol, such as a customer domain that does not support CFM. Only devices that support the CFM protocol respond to **12 ping** and **12 traceroute** requests.

---

**Maintenance Domain (MD)**

A Maintenance Domain (MD) is the part of a network that is controlled by a single administrator. For example, a customer can engage the services of a service provider, who, in turn, can engage the services of several operators. In this scenario, there can be one MD associated with the customer, one MD associated with the service provider, and one MD associated with each of the operators.

You assign one of the following eight levels to the MD:

- 0–2 (operator levels)
- 3–4 (provider levels)
- 5–7 (customer levels)

The levels separate MDs from each other and provide different areas of functionality to different devices using the network. An MD is characterized by a level and an MD name (optional).

A single MD can contain several Maintenance Associations (MA).

---

**Maintenance Association (MA)**

An MA represents a logical grouping of monitored entities within its Domain. It can therefore represent a set of Maintenance association End Points (MEPs), each configured with the same Maintenance Association ID (MAID) and MD Level, established to verify the integrity of a single service instance.

The following figure shows MD level assignment in accordance with the 802.1ag standard. As shown in the figure, MIPs can be associated with MEPs. However, MIPs can also function independently of MEPs.
A Maintenance Endpoint (MEP) represents a managed CFM entity, associated with a specific Domain Service Access Point (DoSAP) of a service instance, which can generate and receive CFM Protocol Data Units (PDU) and track any responses. A MEP is created by MEP ID under the context of an MA. MEP functionality can be divided into the following functions:

- Fault Detection
- Fault Verification
- Fault Isolation
- Fault Notification

Figure 1: MD level assignment
Fault detection and notification are achieved through the use of Continuity Check Messages (CCM). CCM messages are not supported in the current release.

---

**Fault verification**

Fault verification is achieved through the use of Loopback Messages (LBM). An LBM is a unicast message triggered by the operator issuing an operational command. LBM can be addressed to either a MEP or Maintenance Intermediate Point (MIP) but only a MEP can initiate an LBM. The destination MP can be addressed by its MAC address. The receiving MP responds with a Loopback Response (LBR). LBM can contain an arbitrary amount of data that can be used to diagnose faults as well as performance measurements. The receiving MP copies the data to the LBR.

---

**LBM message**

The LBM packet is often compared to a ping. A MEP transmits the LBM packet. This packet can be addressed to another MEP or to the MAC address of the MP; in the case of SPBM, this is the SPBM system ID or its virtual SMLT MAC. Only the MP for which the packet is addressed responds with an LBR message.

- Provides “ICMP ping like” functionality natively at Layer-2.
- DA is the MAC address of the target.
- Includes a transaction identifier that allows the corresponding LBR to be identified when more than one LBM request is waiting for a response.
- Bridges forward the frame using the normal FDB rules.
- Only the target (MIP or MEP) responds.
- Initiator can choose the size and contents data portion of the LBM frame.
- Can be used to check the ability of the network to forward different sized frames.

---

**l2ping**

The `l2 ping` command is a proprietary command that allows a user to trigger an LBM message.

For B-VLANs, specify either the destination MAC address or node name.

This provides a simpler command syntax than the standard LBM commands, which require the user to specify the MD, MA, and MEP ID information. The `l2 ping` command provides a ping equivalent at Layer 2 for use with nodes on the SPBM B-VLAN in the customer domain. SPBM B-VLANs support the SMLT virtual option for the source mode.
Fault isolation

Fault isolation is achieved through the use of Linktrace Messages (LTM). LTM is intercepted by all the MPs on the way to the destination MP. Avaya Virtual Services Platform 8000 Series supports two types of LTM.

The first type, the unicast LTM, can be addressed to either MEP or MIP MAC address. Each MP on the way decrements the TTL field in the LTM frame, sends Linktrace Reply (LTR), and forwards the original LTM to the destination. The LTM is forwarded until it reaches its destination or the TTL value is decremented to zero. LTR is a unicast message addressed to the originating MEP.

The second type, the proprietary LTM, is used to map the MAC addresses of the SPBM network; in this case the target MAC is not an MP, but rather a service instance identifier (I-SID).

Link trace message

Connectivity Fault Management offers link trace messaging for fast fault detection. Link trace messages allow operators, service providers and customers to verify the connectivity that they provide or use and to debug systems.

Link trace message — unicast

The link trace message (LTM) is often compared to traceroute. A MEP transmits the LTM packet. This packet specifies the target MAC address of an MP which is the SPBM system id or the virtual SMLT MAC. MPs on the path to the target address respond with an LTR.

- Trace the path to any given MAC address.
- DA is unicast
- LTM contains:
  - Time to live (TTL)
  - Transaction Identifier
  - Originator MAC address
  - Target MAC address
- CFM unaware entities forward the frame as is like any other data frame.
- MIP or MEP that is not on the path to the target discards the LTM and does not reply.
- MIP that is on the path to the target
  - Forwards the LTM after decrementing the TTL and replacing the SA with its own address.
  - Sends a reply (LTR) to the originator.
  - Identifies itself in the forwarded LTM and LTR by modifying TLV information.
- If the MIP or MEP is a target
  - Sends an LTR to the originator.
  - Identifies itself in the forwarded LTM and LTR by modifying TLV information.
• A MEP that is not the target but is on the path to the target
  - Generates a reply as described above.
  - It also sets one of the flags fields in the reply to indicate that it is the terminal MEP.

**Link trace message — multicast**

The multicast link trace message (LTM) can be used to trace the multicast tree from any node on any I- SID using the nickname MAC address and the I-SID multicast address.

Specifying a multicast target address for an LTM allows for the tracing of the multicast tree corresponding to that destination address (DA). With a multicast target every node that is in the active topology for that multicast address responds with a Linktrace reply and also forwards the LTM frame along the multicast path. Missing Linktrace replies (LTRs) from the nodes in the path indicate the point of first failure.

This functionality allows you to better troubleshoot I-SID multicast paths in a SPBM network.

---

**l2traceroute**

The `l2 traceroute` command is a proprietary command that allows you to trigger an LTM message. Use this command as follows:

- For B-VLANs, specify either the destination MAC address or node name.
- For C-VLANs, specify the destination MAC address.

This command provides a simpler command syntax than the standard LTM commands, which require the user to specify the MD, MA, and MEP ID information. The `l2 traceroute` command provides a trace equivalent at Layer 2 for use with nodes on the SPBM B-VLAN in the customer domain.

⚠️ **Important:**

Only the VSP 4000 Series switch supports CFM configuration on C-VLANs.

⚠️ **Note:**

You can use CFM to troubleshoot networks and hosts that support the CFM protocol. After you configure CFM, CFM works in the network whether or not SPBM is in use.

You cannot use CFM to troubleshoot networks and hosts that do not support the CFM protocol, such as a customer domain that does not support CFM. Only devices that support the CFM protocol respond to `l2 ping` and `l2 traceroute` requests.

**l2 traceroute with IP address**

The `l2 traceroute` command allows you to specify an IP address as the destination address. In this case, the IP address can be either a C-VLAN or a B-VLAN in the SPBM cloud.

The `l2 traceroute` command converts Layer 3 IP information to an appropriate Layer 2 VLAN and MAC combination. The system can also target IP addresses that are not SPBM derived routes.

If ECMP is enabled, `l2 traceroute` runs internally for each of the VLAN paths returned, and displays a summary of the results. If ECMP is disabled, the results display only one path.
Destination addresses for C-VLAN \texttt{l2 traceroute} and \texttt{linktrace} messages

For C-VLANs, CFM uses the following destination MAC addresses for the corresponding maintenance domain (MD) levels for \texttt{l2 traceroute} and \texttt{linktrace} messages.

The Avaya Virtual Services Platform switch supports both \texttt{l2 traceroute} and \texttt{linktrace} for C-VLANs, but Avaya prefers you use \texttt{l2 traceroute}.

Table 37: MD levels and corresponding destination addresses for CFM for C-VLANs

<table>
<thead>
<tr>
<th>CFM MD Level</th>
<th>Destination MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>01:80:c2:00:00:38</td>
</tr>
<tr>
<td>1</td>
<td>01:80:c2:00:00:39</td>
</tr>
<tr>
<td>2</td>
<td>01:80:c2:00:00:3a</td>
</tr>
<tr>
<td>3</td>
<td>01:80:c2:00:00:3b</td>
</tr>
<tr>
<td>4</td>
<td>01:80:c2:00:00:3c</td>
</tr>
<tr>
<td>5</td>
<td>01:80:c2:00:00:3d</td>
</tr>
<tr>
<td>6</td>
<td>01:80:c2:00:00:3e</td>
</tr>
<tr>
<td>7</td>
<td>01:80:c2:00:00:3f</td>
</tr>
</tbody>
</table>

\textbf{l2 tracetree}

The \texttt{l2 tracetree} command is a proprietary command that allows a user to trigger a multicast LTM message by specifying the B-VLAN and I-SID. This command allows the user to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID.

\textbf{Note:}

The Avaya Virtual Services Platform 4000 Series does not support the \texttt{l2 tracetree} command on C-VLANs because no multicast tree exists on C-VLANs.

Maintenance domain intermediate points (MIP)

MIPs do not initialize any CFM messages. MIPs passively receive CFM messages, process the messages received and respond back to the originating MEP. By responding to received CFM messages, MIPs can support discovery of hop-by-hop path among MEPs, allow connection failures to be isolated to smaller segments of the network to help discover location of faults along the paths. MIPs can be created independent of MEPs. MIP functionality can be summarized as:

- Respond to Loopback (ping) messages at the same level as itself and addressed to it.
- Respond to Linktrace (traceroute) messages.
- Forward Linktrace messages after decrementing the TTL.
Layer 2 tracemroute

The 12tracemroute command is a proprietary command that allows the user to trace the multicast tree for a certain multicast flow. The user specifies source, group, and service context (either VLAN or VRF) for the multicast flow to trace.

CFM sends a multicast LTM using an internal calculation to map the source, group, and context to the corresponding target address. The LTR comes from all leaves of the multicast tree for that flow, as well as transit nodes. The target MAC used in the LTM is a combination of the data I-SID and the nickname and the packet is sent on the appropriate SPBM B-VLAN. The user can see the generated multicast tree for that flow, which includes the data I-SID and nickname.

Nodal MPs

Nodal MPs provide both MEP and MIP functionality for SPBM deployments. Nodal MPs are associated with a B-VLAN and are VLAN encapsulated packets. The Nodal MEP provides traceability and troubleshooting at the system level for a given B-VLAN. Each node (chassis) has a given MAC address and communicates with other nodes. The SPBM instance MAC address is used as the MAC address of the Nodal MP. The Nodal B-VLAN MPs supports eight levels of CFM and you configure the Nodal B-VLAN MPs on a per B-VLAN basis. Virtual SMLT 10 MAC addresses are also able to respond for LTM and LBM.

Nodal B-VLAN MEPs

The Nodal B-VLAN MEPs created on the CP and function as if they are connected to the virtual interface of the given B-VLAN. Because of this they are supported for both port and MLT based B-VLANs. To support this behavior a MAC Entry is added to the FDB and a new CFM data-path table containing the B-VLAN and MP level are added to direct CFM frames to the CP as required.

Nodal B-VLAN MIPs

The Nodal MIP is associated with a B-VLAN. VLAN and level are sufficient to specify the Nodal MIP entity. The Nodal MIP MAC address is the SPBM system ID for the node on which it resides. If the fastpath sends a message to the CP, the MIP responds if it is not the target and the MEP responds if it is the target.

Nodal B-VLAN MIPs with SMLT

When Nodal MEPS or MIPs are on SPBM B-VLANs the LTM code uses a unicast MAC DA. The LTM DA is the same as the target MAC address, which is the SPBM MAC address or the SMLT MAC address of the target node.

Avaya Virtual Services Platform 8000 Series supports SMLT interaction with SPBM. This is accomplished by using two B-VIDs into the core from each pair of SMLT terminating nodes. Both nodes advertise the Nodal B-MAC into the core on both B-VIDS. In addition each node advertises the SMLT virtual B-MAC on one of the two B-VLANs.
The Nodal MEP and MIP are expanded to respond to both the Nodal MAC address as well as the Virtual SMLT MAC address if both MACs are being advertised on its B-VLAN. In addition a source mode is added to the LTM and LBM command to use either the Nodal MAC or the SMLT virtual MAC address as the source MAC in the packet.

Configuration considerations

When you configure CFM, be aware of the following configuration considerations.

**General CFM**

- A single switch has a limit of one MEP and one MIP on a C-VLAN or B-VLAN.
- The maintenance level for MEPs and MIPs on a given B-VID (in a network) must be configured to the same level for them to respond to a given CFM command.
- You can configure global CFM at only one MD level for each switch for each VLAN type.
- All nodal MEPs and MIPs are restricted to SPBM B-VIDs.
- SMLT Virtual MAC for C-VLAN does not exist, so the switch does not support this option for the `l2 ping` and `l2 traceroute` commands.

**Autogenerated CFM**

- Autogenerated MEPs are not unique across the entire network unless you configure the global MEP ID on each switch to a different value. You must configure a unique MEP ID at a global level, for CFM.
- A single switch can have only one autogenerated MEP or MIP for each B-VLAN or C-VLAN.

**Explicit CFM**

- Previous explicit CFM configurations of MDs, MAs and MEPs on SPBM B-VLANs continue to be supported. However, if you want to enable autogenerated CFM you must first remove the existing MEP and MIP on the SPBM B-VLAN.
- You can assign maintenance levels for each CFM SPBM MEP and MIP to each SPBM B-VLAN individually or you can assign maintenance levels and global MEPs for all SPBM VLANs by following the appropriate procedure:
  - Assigning a MEP MIP level to an SPBM B-VLAN on page 163
  - Assigning MEP MIP levels to SPBM B-VLANs globally on page 165
  - Configuring CFM nodal MEP on page 190

**C-VLAN versus SPBM B-VLAN considerations**

**Important:**

Only VSP 4000 Series supports CFM configuration on C-VLANs.

CFM breaks the network into sections, called MEPS, so you can determine exactly where the problem exists.

The MEPS and MIPs configured for SPBM VLANs do not respond to CFM messages sent from C-MAC VLANs because the VLAN and packet encapsulation are different.

To forward customer traffic across the core network backbone, SPBM uses IEEE 802.1ah Provider Backbone Bridging (PBB) MAC-in-MAC encapsulation, which hides the customer MAC (C-MAC)
addresses in a backbone MAC (B-MAC) address pair. MAC-in-MAC encapsulation defines a B-MAC destination address (BMAC-DA) and a B-MAC source address (BMAC-SA). In SPBM, each node populates its forwarding database (FDB) with the B-MAC information derived from the IS-IS shortest path tree calculations.

Typically the SPBM Backbone Core Bridges (BCBs) in the SPBM cloud only learn the B-MAC addresses. The Backbone Edge Bridges (BEBs) know the Customer MACs on the appropriate BEBs that terminate the virtual services networks (VSNs). As such, the nodes within the SPBM cloud have no knowledge of the C-MAC addresses in the VSNs.

Important:

To trace a route to a MAC address, the MAC address must be in the VLAN FDB table.

• For C-VLANs, you have to trigger an **12 ping** to learn the C-MAC address.
• For B-VLANs, you do not have to trigger an **12 ping** to learn the C-MAC address because IS-IS populates the MAC addresses in the FDB table.

In both cases, linktrace traces the path up to the closest device to that MAC address that supports CFM in the SPBM cloud.

C-VLAN source addresses

CFM uses either the VLAN MAC or the CFM C-MAC for the BMAC-SA for the C-VLANs. The CFM C-MAC is the value of the management base MAC, which ends in 0x64. The system creates the VLAN MAC after a user adds an IP address to a VLAN.

If a VLAN has a MAC address, the system uses the VLAN MAC as the BMAC-SA by default. If a VLAN does not have a MAC address, the system uses the CFM C-MAC for the BMAC-SA. You may also configure the system to use the CFM C-MAC, even if a VLAN MAC exists.

CFM configuration using ACLI

This section provides procedures to configure and use Connectivity Fault Management (CFM) using Avaya Command Line Interface (ACLI). The Shortest Path Bridging MAC (SPBM) network needs a mechanism to debug connectivity issues and to isolate faults. This is performed at Layer 2, not Layer 3. To support troubleshooting of the SPBM cloud, Virtual Services Platform 4000 supports a subset of CFM functionality.

Note:

When you enable CFM in an SBP network, Avaya recommends that you enable CFM on the Backbone Edge Bridges (BEB) and on all Backbone Core Bridges (BCB). If you do not enable CFM on a particular node, you cannot obtain CFM debug information from that node.

CFM is configured by using the following two ways:

• **Explicit**: In the explicit way of configuring CFM, you can configure an MD, MA, MEP and then associate the MEP to a B-VLAN and MIP level to a B-VLAN.
• **Simplified:** In the simplified way of configuring CFM, you can use the simplified command `cfm spbm enable` which automatically creates the MD, MA, MEP and associates it with the B-VLAN and the MIP level with the B-VLAN.

---

### Autogenerated CFM

CFM provides two methods for configuration; autogenerated and explicit. You cannot use both. You must choose one or the other. Use the procedures in this section to configure autogenerated MEPs that eliminate the need to configure a MD, MA, and MEP ID to create a MEP.

- For SPBM B-VLANs, you can use either autogenerated or explicitly configured CFM MEPs.
- For C-VLANs, you can only use autogenerated CFM MEPs.

ℹ️ **Important:**

Only the VSP 4000 Series switch supports configuring autogenerated CFM on C-VLANs.

The CFM show commands that display MD, MA, and MEP information work for both autogenerated and explicitly configured CFM MEPs.

Previous explicit CFM configurations of MDs, MAs and MEPs on SPBM B-VLANs continue to function in this release. However, if you want to enable the new autogenerated commands you must first remove the existing MEP and MIP on the SPBM B-VLAN.

The switch only supports one MEP and one MIP, either autogenerated or explicitly configured, on the SPBM B-VLAN. Similarly, the switch only supports one MEP and one MIP on the C-VLAN. This means that if you want to use these autogenerated MEPs, you cannot use your existing CFM configuration. You must first remove the existing MEP or MIP on the SPBM B-VLAN.

For information on configuring autogenerated CFM using the ACLI, see:

- [Configuring autogenerated CFM on SPBM B-VLANs](#) on page 155
- [Configuring autogenerated CFM on C-VLANs](#) on page 157

### Configuring autogenerated CFM on SPBM B-VLANs

Use this procedure to configure the autogenerated CFM MEP and MIP level for every SPBM B-VLAN on the chassis. This eliminates the need to explicitly configure an MD, MA, and MEP ID, and to associate the MEP and MIP level to the SPBM B-VLAN.

When you enable this feature, the device creates a global MD (named spbm) for all the SPBM Nodal MEPs. This MD has a default maintenance level of 4, which you can change with the level attribute. All the MEPs that the device creates use the MEP ID configured under the global context, which has a default value of 1.

The nodal MEPs are automatically associated with the SPBM B-VLANs configured. The MIP level maps to the global level. When you enable the feature, the device automatically associates the MIP level with the SPBM B-VLANs configured. The feature is disabled by default.
Important:

CFM supports one MEP or MIP for each SPBM B-VLAN only. This means that if you want to use these autogenerated MEPs, you cannot use your existing CFM configuration. You must first remove the existing MEP or MIP on the SPBM B-VLAN. If you want to continue configuring MEPs manually, skip this procedure.

Procedure

1. Enter Global Configuration mode:
   
enable
cfg-term

2. Configure the maintenance level for every CFM SPBM MEP and MP level on all the SPBM B-VLANs:
   
cfm spbm level <0-7>
   
You can change this level from the default of 4 either before or after the feature is enabled. Only configure global CFM at one MD level for each chassis for each VLAN type.

3. Assign a global CFM MEP ID for all CFM SPBM MEPs:
   
cfm spbm mepid <1-8191>

4. Enable the autogenerated CFM for SPBM B-VLANs globally:
   
cfm spbm enable

5. (Optional) Configure the maintenance level for every CFM SPBM MEP and MP level on all the SPBM B-VLANs to the default:
   
default cfm spbm level

6. (Optional) Assign a global CFM MEP ID for all CFM SPBM MEPs to the default:
   
default cfm spbm mepid

7. (Optional) Disable the global CFM MEPs and MIPs:
   
no cfm spbm enable

8. Display the global CFM MEP configuration:
   
show cfm spbm

Example

Configure autogenerated CFM MEPs and MIPs:

```
VSP-4850GTS>enable
VSP-4850GTS#configure terminal
VSP-4850GTS(config)#cfm spbm level 6
VSP-4850GTS(config)#cfm spbm mepid 4
VSP-4850GTS(config)#cfm spbm enable
VSP-4850GTS(config)#show cfm spbm
LEVEL ADMIN    MEPID    MAC
```
Variable definitions

Use the data in the following table to use the `cfm spbm` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level&lt;0-7&gt;</td>
<td>Specifies the global SPBM CFM maintenance level for the chassis within the range of 0 to 7. The default is 4. Only configure global CFM at one MD level for each chassis for each VLAN type.</td>
</tr>
<tr>
<td>mepid&lt;1-8191&gt;</td>
<td>Specifies the global MEP ID within the range of 1–8191. Select a unique ID for each switch to ensure that the MEPs are unique across the network. The default is 1.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables autogenerated CFM on all SPBM B-VLANs.</td>
</tr>
</tbody>
</table>

Job aid

The following table describes the fields for the `show cfm spbm` command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL</td>
<td>Specifies the global SPBM CFM maintenance level for the chassis. The default is 4.</td>
</tr>
<tr>
<td>ADMIN</td>
<td>Specifies if CFM MEPs and MIPs are globally enabled.</td>
</tr>
<tr>
<td>MEP ID</td>
<td>Specifies the global MEP ID. The default is 1.</td>
</tr>
<tr>
<td>MAC</td>
<td>Specifies the MAC address.</td>
</tr>
</tbody>
</table>

Configuring autogenerated CFM on C-VLANs

Use this procedure to configure the autogenerated CFM MEP and MIP level for every C-VLAN on the chassis.

**Important:**

For C-VLANs, you can only use autogenerated CFM MEPs. Only the VSP 4000 Series switch supports configuring autogenerated CFM on a C-VLAN.

**Important:**

CFM supports one MEP or MIP for each C-VLAN. Only autogenerated CFM provides support for configuring MEP and MIPs on C-VLANs. You cannot explicitly configure C-VLANs.

About this task

When you enable this feature, you create a global MD (named cmac) for all the customer MAC (C-MAC) MEPs. This global MD has a default maintenance level of 4, which you can change with the
level attribute. The autogenerated CFM commands also create an MA for each C-VLAN, a MEP for each C-VLAN, associate the MEP with the corresponding C-VLAN, and a MIP with the C-VLAN.

All the MEPs that the device creates use the MEP ID configured under the global context, which has a default value of 1. The device automatically associates the MEPs with the C-VLANs configured. The MIP level maps to the global level. The device automatically associates the MIP level with the C-VLANs configured when you enable the feature.

The feature is disabled by default.

Procedure

1. Enter Global Configuration mode:
   ```
   enable
configure terminal
   ```

2. Configure the maintenance level for every CFM C-MAC MEP and MP level on all the C-VLANs:
   ```
cfm cmac level <0-7>
```
   Only configure global CFM at one MD level for each chassis for each VLAN type.

3. Assign a global CFM MEP ID for all CFM C-MAC MEPs:
   ```
cfm cmac mepid <1-8191>
   ```

4. Enable the autogenerated CFM for C-VLANs:
   ```
cfm cmac enable
   ```

5. (Optional) Configure the maintenance level for every CFM C-MAC MEPs and MP level on all the C-VLANs to the default:
   ```
default cfm cmac level
   ```

6. (Optional) Assign a global CFM MEP ID for all CFM C-MAC MEPs to the default:
   ```
default cfm cmac mepid
   ```

7. (Optional) Disable the global CFM MEPs and MIPs:
   ```
   no cfm cmac enable
   ```

8. Display the global CFM MEP configuration:
   ```
   show cfm cmac
   ```

Example

Configure autogenerated CFM MEPs and MIP level:

```
VSP-4850GTS>enable
VSP-4850GTS#configure terminal
VSP-4850GTS(config)#cfm cmac level 0
VSP-4850GTS(config)#cfm cmac mepid 4
VSP-4850GTS(config)#cfm cmac enable
VSP-4850GTS(config)#show cfm cmac
```

```plaintext
LEVEL ADMIN  MEPID  MAC
```
Variable definitions

Use the data in the following table for the `cfm cmac` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level&lt;0-7&gt;</td>
<td>Specifies the global C-MAC CFM maintenance level for the chassis within the range of 0 to 7. The default is 4. Only configure global CFM at one MD level for each chassis for each VLAN type.</td>
</tr>
<tr>
<td>mepid&lt;1-8191&gt;</td>
<td>Specifies the global MEP ID within the range of 1–8191. Select a unique ID for each switch to ensure that the MEPs are unique across the network. The default is 1. <strong>Note:</strong> The MA takes its name from this value for autogenerated CFM. For example, if you specify 500 as the MEP ID, the MA will also be 500.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables autogenerated CFM for all C-MAC VLANs.</td>
</tr>
</tbody>
</table>

Job aid

The following table describes the fields for the `show cfm cmac` command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL</td>
<td>Specifies the global C-VLAN CFM maintenance level for the chassis. The default is 4.</td>
</tr>
<tr>
<td>ADMIN</td>
<td>Specifies if CFM C-VLAN MEPs and MIPs are globally enabled.</td>
</tr>
<tr>
<td>MEP ID</td>
<td>Specifies the global MEP ID. The default is 1.</td>
</tr>
<tr>
<td>MAC</td>
<td>Specifies the MAC address.</td>
</tr>
</tbody>
</table>

Configuring explicit mode CFM

In the explicit mode of configuring CFM, you can manually configure an MD, MA, MEP and then associate the MEP to a B-VLAN and assign a MIP level to a B-VLAN.

**Note:**

If you use autogenerated CFM, these steps are unnecessary.
Configuring CFM MD

Use this procedure to configure the Connectivity Fault Management (CFM) Maintenance Domain (MD). An MD is the part of a network that is controlled by a single administrator. A single MD can contain several Maintenance Associations (MA).

Procedure

1. Log on to Global Configuration mode:
   
   ```
   enable
   configure terminal
   ```

2. Create the CFM MD:
   
   ```
   cfm maintenance-domain WORD<0–22> [index <1–2147483647>] [maintenance-level <0–7>] [level <0–7>]
   ```

3. Display the CFM MD configuration:
   
   ```
   show cfm maintenance-domain
   ```

4. Delete the CFM MD:
   
   ```
   no cfm maintenance-domain WORD<0–22>
   ```

Example

VSP-4850GTS> enable
VSP-4850GTS# configure terminal
VSP-4850GTS(config)# cfm maintenance-domain md1 index 99 maintenance-level 3
VSP-4850GTS(config)# show cfm maintenance-domain

<table>
<thead>
<tr>
<th>Maintenance Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
</tr>
<tr>
<td>md1</td>
</tr>
</tbody>
</table>

Total number of Maintenance Domain entries: 1.

VSP-4850GTS(config)# no cfm maintenance-domain md1
VSP-4850GTS(config)# show cfm maintenance-domain

<table>
<thead>
<tr>
<th>Maintenance Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Total number of Maintenance Domain entries: 0.

Variable definitions

Use the data in the following table to use the `cfm maintenance-domain` command.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD&lt;0–22&gt;</td>
<td>Specifies the maintenance domain name.</td>
</tr>
<tr>
<td>index &lt;1–2147483647&gt;</td>
<td>Specifies a maintenance domain entry index.</td>
</tr>
<tr>
<td>maintenance-level &lt;0–7&gt;</td>
<td>Specifies the MD maintenance level when creating the MD. The default is 4.</td>
</tr>
<tr>
<td>level &lt;0–7&gt;</td>
<td>Modifies the MD maintenance level for an existing MD. The default is 4.</td>
</tr>
</tbody>
</table>

Configuring CFM MA

Use this procedure to configure the CFM Maintenance Association (MA). An MA represents a logical grouping of monitored entities within its domain. It can therefore represent a set of Maintenance Association End Points (MEPs), each configured with the same Maintenance Association ID (MAID) and MD Level, established to verify the integrity of a single service instance.

Procedure

1. Log on to Global Configuration mode:
   ```
   enable
   configure terminal
   ```

2. Create the CFM MA:
   ```
   cfm maintenance-association WORD<0–22> WORD<0–22> [index <1–2147483647>]
   ```

3. Display the CFM MA configuration:
   ```
   show cfm maintenance-association
   ```

4. Use the following command, if you want to delete the CFM MA:
   ```
   no cfm maintenance-association WORD<0–22> WORD<0–22>
   ```

Example

```
VSP-4850GTS> enable
VSP-4850GTS# configure terminal
VSP-4850GTS(config)# cfm maintenance-association md1 ma1 index 98
VSP-4850GTS(config)# show cfm maintenance-association
```

```
================================================================================
<table>
<thead>
<tr>
<th>Maintenance Association Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>md1</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>Total number of Maintenance Association entries: 1.</td>
</tr>
</tbody>
</table>
```

Comments on this document? infodev@avaya.com
Variable definitions

Use the data in the following table to use the `cfm maintenance-association` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD&lt;0–22&gt; WORD&lt;0–22&gt;</td>
<td>Creates the CFM MA. The first parameter, specifies the MD name. The second parameter, specifies the MA name.</td>
</tr>
<tr>
<td>index &lt;1–2147483647&gt;</td>
<td>Specifies a maintenance association entry index.</td>
</tr>
</tbody>
</table>

Configuring CFM MEP

Use this procedure to configure the CFM Maintenance Endpoint (MEP). A MEP represents a managed CFM entity, associated with a specific Domain Service Access Point (DoSAP) of a service instance, which can generate and receive CFM Protocol Data Units (PDU) and track any responses. A MEP is created by MEP ID under the context of an MA.

Procedure

1. Log on to Global Configuration mode:
   
   enable
   
   configure terminal

2. Create the CFM MEP:

   cfm maintenance-endpoint WORD<0–22> WORD<0–22> <1–8191> [state <enable>]

3. Enable an existing CFM MEP:

   cfm maintenance-endpoint WORD<0–22> WORD<0–22> <1–8191> enable

4. Disable an existing CFM MEP:

   no cfm maintenance-endpoint WORD<0–22> WORD<0–22> <1–8191> enable

5. Display the CFM MEP configuration:

   show cfm maintenance-endpoint

6. Delete an existing CFM MEP:

   no cfm maintenance-endpoint WORD<0–22> WORD<0–22> <1–8191>

Example

VSP-4850GTS> enable
VSP-4850GTS# configure terminal
VSP-4850GTS(config)# cfm maintenance-endpoint md1 mal 1 state enable
show cfm maintenance-endpoint

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>ASSOCIATION</th>
<th>MEP</th>
<th>ADMIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>md1</td>
<td>ma1</td>
<td>1</td>
<td>enable</td>
</tr>
</tbody>
</table>

Total number of MEP entries: 1.

Variable definitions

Use the data in the following table to use the cfm maintenance-endpoint command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD&lt;0–22&gt;</td>
<td>The first parameter, specifies the MD name.</td>
</tr>
<tr>
<td>WORD&lt;0–22&gt;</td>
<td>The second parameter, specifies the MA name.</td>
</tr>
<tr>
<td>&lt;1–8191&gt;</td>
<td>Specifies the MEP ID.</td>
</tr>
<tr>
<td>state {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>enable</td>
<td>Enables an existing MEP. Use this parameter with the no option to disable an existing MEP.</td>
</tr>
</tbody>
</table>

Assigning a MEP/MIP level to an SPBM B-VLAN

Use this procedure to assign a nodal MEP to an SPBM B-VLAN. The Nodal MEP provides traceability and troubleshooting at the system level for a given B-VLAN. The Nodal B-VLAN MEPs created on the CP and function as if they are connected to the virtual interface of the given B-VLAN. Because of this they are supported for both port and MLT based B-VLANs.

Nodal MPs provide both MEP and MIP functionality for SPBM deployments. Nodal MPs are associated with a B-VLAN and are VLAN encapsulated packets. Each node (chassis) has a given MAC address and communicates with other nodes. The SPBM instance MAC address is used as the MAC address of the Nodal MP.

Before you begin

- You must configure a CFM MD, MA, and MEP.

Procedure

1. Add nodal MEPs to the B-VLAN:

   vlan nodal-mep <1-4059> WORD<0-22> WORD<0-22> <1-8191>
2. Display the nodal MEP configuration:
   show vlan nodal-mep <1-4059>

3. Remove the nodal MEPs from the B-VLAN:
   no vlan nodal-mep <1-4059> WORD<0-22> WORD<0-22> <1-8191>

4. Add nodal MIP level to the B-VLAN:
   vlan nodal-mip-level <1-4059> WORD<0-15>

5. Display the nodal MIP level configuration:
   show vlan nodal-mip-level [<1-4059>]

6. Remove the nodal MIP level from the B-VLAN:
   no vlan nodal-mip-level <1-4059> WORD<0-15>

Example
Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# vlan nodal-mep 100 md1 ma1 2
Switch:1(config)# show vlan nodal-mep

<table>
<thead>
<tr>
<th>VLAN_ID</th>
<th>DOMAIN_NAME.ASSOCIATION_NAME.MEP_ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>spbm.100.6</td>
</tr>
<tr>
<td>200</td>
<td>spbm.200.6</td>
</tr>
</tbody>
</table>

Switch:1(config)# vlan nodal-mip 100 6
Switch:1(config)# show vlan nodal-mip

<table>
<thead>
<tr>
<th>VLAN_ID</th>
<th>NODAL_MIP_LEVEL_LIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>100</td>
<td>6</td>
</tr>
<tr>
<td>216</td>
<td></td>
</tr>
<tr>
<td>304</td>
<td></td>
</tr>
<tr>
<td>41000</td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td></td>
</tr>
</tbody>
</table>

Variable definitions
Use the data in the following table to use the **vlan nodal-mep** command.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4059&gt;</td>
<td>Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.</td>
</tr>
<tr>
<td>WORD&lt;0–22&gt;</td>
<td>The first parameter, specifies the Maintenance Domain name.</td>
</tr>
<tr>
<td>WORD&lt;0–22&gt;</td>
<td>The second parameter, specifies the Maintenance Association name.</td>
</tr>
<tr>
<td>&lt;1–8191&gt;</td>
<td>Specifies the nodal MEPs to add to the VLAN.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `vlan nodal-mip-level` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4059&gt;</td>
<td>Adds the nodal MIP level.</td>
</tr>
<tr>
<td></td>
<td>Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.</td>
</tr>
<tr>
<td>WORD&lt;0–15&gt;</td>
<td>Adds the nodal MIP level, which has up to eight levels, ranging from 0 to 7.</td>
</tr>
</tbody>
</table>

**Assigning MEP/MIP levels to SPBM B-VLANs globally**

⚠️ **Note:**

If you enable the `cfm spbm enable` command, you cannot assign a MEP/MIP level to an individual SPBM B-VLAN or configure CFM MD maintenance levels individually.

**About this task**

Enables the global CFM MEP and MIPs for all SPBM B-VLANs.

**Procedure**

1. Enter Global Configuration mode:
   
   ```
   enable
   configure terminal
   ```

2. Enable simplified CFM configuration for SPBM VLANs:
   
   ```
   cfm spbm enable
   ```

3. Enter the CFM SPBM level:
   
   ```
   cfm spbm level <0–7>
   ```

4. Enter the CFM SPBM MEPID level:
   
   ```
   cfm spbm mepid <1–8191>
   ```
Example
Switch:1(config)# cfm spbm level 7
Switch:1(config)# cfm spbm mepid 12
Switch:1(config)# cfm spbm enable

Variable definitions
Use the data in the following table to use the simplified CFM commands.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>spbm level &lt;0–7&gt;</td>
<td>Configures the maintenance level for every CFM SPBM MEP and MIP level on all SPBM B-VLANs. The default is 4.</td>
</tr>
<tr>
<td>mepid &lt;1–8191&gt;</td>
<td>Assigns a global MEP ID for all CFM SPBM MEPs. The default is 1.</td>
</tr>
<tr>
<td>no cfm spbm enable</td>
<td>Disables global configuration of CFM SPBM MEP and MIP levels on all SPBM B-VLANs.</td>
</tr>
<tr>
<td>default cfm spbm level</td>
<td>Returns maintenance level to default for all CFM SPBM MEP and MIP level on all SPBM B-VLANs.</td>
</tr>
<tr>
<td>default cfm spbm mepid</td>
<td>Returns MEP ID for all CFM SPBM MEPS to default.</td>
</tr>
<tr>
<td>show cfm spbm</td>
<td>Displays the global CFM MEP configuration for SPBM B-VLANs.</td>
</tr>
</tbody>
</table>

Displaying SPBM nodal configuration
Use this procedure to view the nodal MEP and nodal MIP level configuration for SPBM B-VLANs.

Procedure
1. Display the nodal MEP configuration:
   
   ```
   show vlan nodal-mep <1-4059>
   ```

2. Display the nodal MIP level configuration:

   ```
   show vlan nodal-mip-level [<1-4059>]
   ```

Example
VSP-4850GTS> show vlan nodal-mep
VSP-4850GTS> show vlan nodal-mip

================================================================================
Vlan Nodal Mip Level
=================================================================================
VLAN_ID  NODAL_MIP_LEVEL_LIST
=================================================================================
1 6
216
304
404
500
616
716
Configuring simplified CFM SPBM

Use this procedure to configure CFM for the Shortest Path Bridging Mac (SPBM) VLANs on Virtual Services Platform 4000.

This is a simplified command which automatically creates the MD, MA, MEP and associates it with the B-VLAN and the MIP level with the B-VLAN.

Procedure

1. Log on to Global Configuration mode:
   
   enable
   configure terminal

2. Enable CFM for SPBM VLANs:

   cfm spbm enable

3. Set the maintenance level for MEP and MIP:

   cfm spbm level <0–7> mepid <1–8191>

4. Set the default maintenance level for MEP and MIP:

   default cfm spbm level

5. Configure MEPID for all SPBM VLANs:

   cfm spbm mepid <1–8191>

6. Set the default SPBM MEPID:

   default cfm spbm mepid

7. Disable an existing CFM SPBM:

   no cfm spbm enable

8. Display the CFM MEP configuration:

   show cfm spbm

Example

VSP-4850GTS> enable
VSP-4850GTS# configure terminal
VSP-4850GTS(config)# cfm spbm enable
VSP-4850GTS(config)# cfm spbm level 4 mepid 1
VSP-4850GTS> show cfm spbm

========================================================================

Cfm Spbm
========================================================================

LEVEL  ADMIN            MEP ID            MAC
------------------------------------------------------------------------
 4      enable                1                00:00:00:00:00:00

Variable definitions

Use the data in the following table to use cfm spbm command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables CFM for SPBM VLANs.</td>
</tr>
<tr>
<td>level&lt;0–7&gt;</td>
<td>Sets the maintenance level for MEP and MIP.</td>
</tr>
<tr>
<td>mepid&lt;1–8191&gt;</td>
<td>Specifies the MEP ID for all SPBM VLANs.</td>
</tr>
</tbody>
</table>

Triggering a loopback test (LBM)

Use this procedure to trigger a loopback test.

The LBM packet is often compared to ping. An MEP transmits the loopback message to an intermediate or endpoint within a domain for the purpose of fault verification. This can be used to check the ability of the network to forward different sized frames.

Before you begin

- You must have a MEP that is associated with a B-VLAN.

Procedure

Trigger the loopback test:

loopback WORD<0–22> WORD<0–22> <1–8191> <0x00:00:00:00:00:00:00:00:00:00:00> [burst-count <1–200>] [data-tlv-size <0–400>] [frame-size <64–1500>] [interframe-interval <msecs>] [priority <0–7>] [source-mode <nodal| noVlanMac|smltVirtual>] [testfill-pattern <all-zero|all-zero-crc|pseudo-random-bit-sequence|pseudo-random-bit-sequence-crc>] [time-out <1–10>]

Example

VSP-4850GTS# loopback md1 4001 13 00:14:0D:A2:B3:DF burst-count 10 priority 3 time-out 5

Result of LBM from mep: md1.4002.13 to MAC address: 00:14:0D:A2:B3:DF :
    Sequence number of the first LBM is 10575
    The total number of LBMs sent out is 10
    The number of LBRs received is 10
    The number of LBRs lost is 0
    The percentage of LBMs lost is 0.00%
    The RTT Min is 764 microsecs, Max is 800 microsecs, Average is 783.00 microsecs
    The RTTDV min is 3 microsecs, Max is 23 microsecs, Average is 9.11 microsecs
    The Standard Deviation of RTT is 11.53 microsecs
Variable definitions

Use the data in the following table to use the `loopback` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>WORD&lt;0–22&gt;</code></td>
<td>The first parameter, specifies the MD name.</td>
</tr>
<tr>
<td><code>WORD&lt;0–22&gt;</code></td>
<td>The second parameter, specifies the MA name.</td>
</tr>
<tr>
<td><code>&lt;1–8191&gt;</code></td>
<td>Specifies the MEP ID.</td>
</tr>
<tr>
<td><code>&lt;0x00:0x00:0x00:0x00:0x00:0x00&gt;</code></td>
<td>Specifies the remote MAC address to reach the MEP/MIP.</td>
</tr>
<tr>
<td><code>burst-count &lt;1–200&gt;</code></td>
<td>Specifies the burst-count.</td>
</tr>
<tr>
<td><code>data-tlv-size &lt;0–400&gt;</code></td>
<td>Specifies the data TLV size.</td>
</tr>
<tr>
<td><code>frame-size &lt;64–1500&gt;</code></td>
<td>Specifies the frame-size. The default is 0.</td>
</tr>
<tr>
<td><code>priority &lt;0–7&gt;</code></td>
<td>Specifies the priority. The default is 7.</td>
</tr>
<tr>
<td>`source-mode &lt;nodal</td>
<td>noVlanMac</td>
</tr>
<tr>
<td></td>
<td>• nodal</td>
</tr>
<tr>
<td></td>
<td>• noVlanMac — Use this value with C-VLAN only. When you select this option, even if a VLAN MAC address exists, the system uses the CFM C-MAC as the BMAC-SA.</td>
</tr>
<tr>
<td></td>
<td>• smltVirtual — Use this value with B-VLANs only. The default is nodal.</td>
</tr>
<tr>
<td>`testfill-pattern {all-zero</td>
<td>all-zero-crc</td>
</tr>
<tr>
<td></td>
<td>• all-zero — null signal without cyclic redundancy check</td>
</tr>
<tr>
<td></td>
<td>• all-zero-crc — null signal with cyclic redundancy check with 32-bit polynomial</td>
</tr>
<tr>
<td></td>
<td>• pseudo-random-bit-sequence — pseudo-random-bit-sequence without cyclic redundancy check</td>
</tr>
<tr>
<td></td>
<td>• pseudo-random-bit-sequence-crc — pseudo-random-bit-sequence with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is 1: all-zero.</td>
</tr>
<tr>
<td><code>time-out &lt;1–10&gt;</code></td>
<td>Specifies the time-out interval in seconds. The default is 3.</td>
</tr>
</tbody>
</table>

---

Triggering linktrace (LTM)

Use the following procedure to trigger a linktrace.

The Linktrace Message is often compared to traceroute. An MEP transmits the Linktrace Message packet to a maintenance endpoint with intermediate points responding to indicate the path of the traffic within a domain for the purpose of fault isolation. The packet specifies the target MAC...
address of an MP, which is the SPBM system ID or the virtual SMLT MAC. MPs on the path to the
target address respond with an LTR.

**Before you begin**

- You must have a MEP that is associated with a VLAN.

**Procedure**

Trigger the linktrace:

```
linktrace WORD<0–22> WORD<0–22> <1–8191> <0x00:0x00:0x00:0x00:0x00:0x00>
[detail] [priority <0–7>] [source-mode <nodal|noVlanMac|smltVirtual>]
[ttl-value <1–255>]
```

**Example**

```
VSP-4850GTS# linktrace md1 4001 13 00:bb:00:00:14:00 priority 7
```

Please wait for LTM to complete or press any key to abort

```
Received LTRs:
SeqNum: 10575 MD: md1 MA:4001 MepId: 13 Priority: 7
--------------------------------------------------------------
TTL SRC MAC                    FWDYES    TERMMEP    RELAY        ACTION
--- ------------------ ------  -------- ----------------------
63    00:bb:00:00:10:00         true        false        Fdb
62     00:bb:00:00:14:00      false        true        Hit
```

**Variable definitions**

Use the data in the following table to use the `linktrace` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>WORD&lt;0–22&gt;</code></td>
<td>The first parameter, specifies the MD name.</td>
</tr>
<tr>
<td><code>WORD&lt;0–22&gt;</code></td>
<td>The second parameter, specifies the MA name.</td>
</tr>
<tr>
<td><code>&lt;1–8191&gt;</code></td>
<td>Specifies the MEP ID.</td>
</tr>
<tr>
<td><code>&lt;0x00:0x00:0x00:0x00:0x00&gt;</code></td>
<td>Specifies the target MAC address to reach the MEP.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays linktrace result details.</td>
</tr>
<tr>
<td><code>priority &lt;0–7&gt;</code></td>
<td>Specifies the priority. The default is 7.</td>
</tr>
<tr>
<td>source-mode `&lt;nodal</td>
<td>noVlanMac</td>
</tr>
<tr>
<td></td>
<td>• 1: nodal</td>
</tr>
<tr>
<td></td>
<td>• noVlanMac — Use this value with C-VLAN only. When you select this option, even if a VLAN MAC address exists, the system uses the CFM C-MAC as the BMAC-SA.</td>
</tr>
<tr>
<td></td>
<td>• 2: smltVirtual—Use this value with B-VLANs only. The default is 1: nodal.</td>
</tr>
<tr>
<td><code>ttl-value &lt;1–255&gt;</code></td>
<td>Specifies the Time-to-Live value. The default is 64.</td>
</tr>
</tbody>
</table>
Triggering a Layer 2 ping

Use this procedure to trigger a Layer 2 ping inside an SPBM cloud or network, which acts like native ping. This feature enables CFM to debug Layer 2. It can also help you debug IP shortcuts and the record for the shortcuts’ ARP.

Before you begin

- You must have a MEP that is associated with a VLAN.

Procedure

Trigger a Layer 2 ping:

```
12 ping {vlan <1-4059> routernodename WORD<0–255> | vlan <1-4059> mac 0x00:00:00:00:00:00 | vlan <1-4059>} [burst-count <1–200>] [data-tlv-size <0–400>] [frame-size <64–1500>] [priority <0–7>] [source-mode <nodal|noVlanMac|smltVirtual>] [testfill-pattern <all-zero|all-zero-crc|pseudo-random-bit-sequence|pseudo-random-bit-sequence-crc>] [time-out <1–10>]
```

```
12 ping {ip-address WORD<0–255>} [burst-count <1–200>] [data-tlv-size <0–400>] [frame-size <64–1500>] [priority <0–7>] [source-mode <nodal|noVlanMac|smltVirtual>] [testfill-pattern <all-zero|all-zero-crc|pseudo-random-bit-sequence|pseudo-random-bit-sequence-crc>] [time-out <1–10>] [vrf WORD<0–16>]
```

Example

```
VSP-4850GTS# 12 ping vlan 500 mac 00.14.0d.bf.a3.df
Please wait for l2ping to complete or press any key to abort
---00:14:0d:bf:a3:df L2 PING Statistics---- 0(68) bytes of data
1 packets transmitted, 0 packets received, 100.00% packet loss

VSP-4850GTS# VSP-4850GTS# 12 ping vlan 500 routernodename VSP-MONTI0
Please wait for l2ping to complete or press any key to abort
---00:14:0d:a2:b3:df L2 PING Statistics---- 0(68) bytes of data
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip (us) min/max/ave/stdv = 26895/26895/26895.00/ 0.00

VSP-4850GTS# 12 ping ip-address 10.1.1.1
Please wait for l2ping to complete or press any key to abort

L2 PING Statistics : IP 10.1.1.1, paths found 1, replies 1
=================================================================================================
TX RX PERCENT ROUND TRIP TIME
VLAN NEXT HOP (us) PKTS PKTS LOSS MIN/MAX/AVE
=================================================================================================
500 VSP-SHAMIM (00:1a:8f:08:53:df) 1 0 100.00% 0/0/0.00
```

Variable definitions

Use the data in the following table to configure the L2 ping parameters.
### Triggering a Layer 2 traceroute

Use this procedure to trigger a Layer 2 traceroute, which acts like native traceroute. This feature enables CFM to debug Layer 2 in an SPBM cloud or network. It can determine the path used by IS-
IS to get from one MEP to another, by showing all the hops between. Therefore, it can show where connectivity is lost. It can also work for IP shortcuts.

**Important:**

To trace a route to a MAC address, the MAC address must be in the VLAN FDB table.

- For B-VLANs, you do not have to trigger an **l2ping** to learn the MAC address because IS-IS populates the MAC addresses in the FDB table.

**linktrace** traces the path up to the closest device to that MAC address that supports CFM.

**Before you begin**

- You must have a MEP that is associated with a VLAN.

**Procedure**

Trigger a Layer 2 traceroute:

```
l2 traceroute {<vlan <1-4059> routernodename WORD<0–255> | <vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00>} [priority <0–7>] [source-mode <nodal|noVlanMac|smltVirtual>] [ttl <1–255>]
l2 traceroute {ip-address WORD<0–255>} [priority <0–7>] [source-mode <nodal|noVlanMac|smltVirtual>] [ttl <1–255>] [vrf WORD <0–16>]
```

**Example**

```
VSP-4850GTS# l2 traceroute vlan 500 routernodename VSP-MONTIO

Please wait for l2traceroute to complete or press any key to abort

l2traceroute to VSP-MONTIO  (00:14:0d:a2:b3:df),  vlan 500
0    VSP-PETER4         (00:15:9b:11:33:df)
1    VSP-MONTIO          (00:14:0d:a2:b3:df)

VSP-4850GTS# l2 traceroute ip-address 10.1.1.1

Please wait for l2trace to complete or press any key to abort

L2 Trace  Statistics : IP 10.1.1.1, paths found 1
------------------------------------------------------------------------
VSP-SHAMIM  (00:1a:8f:08:53:df),  vlan 500
0    VSP-PETER4          (00:15:9b:11:33:df)
1    VSP-MONTIO          (00:14:0d:a2:b3:df)
```

**Variable definitions**

Use the data in the following table to use the **l2 traceroute** command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>{vlan &lt;1-4059&gt; routernodename WORD&lt;0–255&gt;}</td>
<td>Specifies the destination for the L2 traceroute:</td>
</tr>
<tr>
<td>(vlan &lt;1-4059&gt; mac &lt;0x00:0x00:0x00:0x00:0x00:0x00})</td>
<td>• &lt;1-4059&gt; Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs</td>
</tr>
</tbody>
</table>
### Triggering a Layer 2 tracetree

Use this procedure to trigger a Layer 2 tracetree. Layer 2 tracetree allows a user to trigger a multicast LTM message by specifying the B-VLAN and I-SID. The command allows the user to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID.

**Note:**

This command is supported on SPBM B-VLANs only, not C-VLANs.

**Before you begin**

- On the source and destination nodes, you must configure a CFM MD, MA, and MEP.
- Enable the MEP.
- Assign a nodal MEP to the B-VLAN.

**Procedure**

Trigger a Layer 2 tracetree:

```
l2 tracetree {<1-4059> <1-16777215> [routernodename WORD<0–255> | <1-4059> <1-16777215>] [mac <0x00:0x00:0x00:0x00:0x00:0x00>] [source-mode <nodal|noVlanMac|smltVirtual>] [priority <0–7>] [ttl-value <1–255>]
```
Example

VSP-4850GTS# l2 tracetree 500 1

Please wait for l2tracetree to complete or press any key to abort

l2tracetree to 53:55:10:00:00:01, vlan 500 i-sid 1 nickname 5.55.10
hops 64
1   VSP-PETER4        00:15:9b:11:33:df -> VSP-MONTI0        00:14:0d:a2:b3:df
2   VSP-MONTI0        00:14:0d:a2:b3:df -> VSP-LEE2          00:15:e8:b8:a3:df

Variable definitions

Use the data in the following table to use the `l2 tracetree` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-4059&gt;</code> <code>&lt;1–16777215&gt;</code> routernodename WORD&lt;0–255&gt;</td>
<td><code>&lt;1-4059&gt;</code></td>
</tr>
<tr>
<td><code>&lt;1-4059&gt;</code> <code>&lt;1–16777215&gt;</code> mac <code>&lt;0x00:0x00:0x00:0x00:0x00:0x00&gt;</code></td>
<td><code>&lt;1–16777215&gt;</code> — Specifies the I-SID.</td>
</tr>
<tr>
<td><code>&lt;1-4059&gt;</code> routernodename WORD&lt;0–255&gt;</td>
<td>WORD&lt;0–255&gt; — Specifies the Router Node Name.</td>
</tr>
<tr>
<td><code>&lt;1-4059&gt;</code> <code>&lt;1–16777215&gt;</code> mac <code>&lt;0x00:0x00:0x00:0x00:0x00:0x00&gt;</code></td>
<td><code>&lt;0x00:0x00:0x00:0x00:0x00:0x00&gt;</code> — Specifies the MAC address.</td>
</tr>
<tr>
<td>ttl-value <code>&lt;1–255&gt;</code></td>
<td>Specifies the TTL value. The default is 64.</td>
</tr>
<tr>
<td>priority <code>&lt;0–7&gt;</code></td>
<td>Specifies the priority value. The default is 7.</td>
</tr>
<tr>
<td>source-mode `&lt;nodal</td>
<td>noVlanMac</td>
</tr>
<tr>
<td>`&lt;nodal</td>
<td>noVlanMac</td>
</tr>
<tr>
<td>`&lt;nodal</td>
<td>noVlanMac</td>
</tr>
<tr>
<td>`&lt;nodal</td>
<td>noVlanMac</td>
</tr>
</tbody>
</table>

Triggering a Layer 2 tracemroute

Use this procedure to debug the IP Multicast over Fabric Connect stream path using `l2 tracemroute` on the VLAN (Layer 2) or the VRF (Layer 3). This procedure queries the SPBM multicast module to determine the B-VLAN, I-SID and nickname for the S and G streams. The nickname and I-SID are used to create a multicast MAC address.

**Note:**

The VLAN option is only valid for a VLAN that has an I-SID configured and IGMP snooping enabled.
Before you begin

- On the source and destination nodes, you must configure an autogenerated or an explicit CFM MD, MA, and MEP.
- Enable the MEP.
- Assign a nodal MEP to the B-VLAN.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Trigger a Layer 2 tracemroute on the VLAN:
   
   ```
   l2 tracemroute source <A.B.C.D> group <A.B.C.D> vlan <1-4059> [priority <0-7>] [ttl-value <1-255>]
   ```

   **Note:**

   For the preceding command, if you do not specify a VLAN, `l2 tracemroute` uses the global default VRF.

   Wait for the l2 tracemroute to complete or press any key to abort.

3. Trigger a Layer 2 tracemroute on the VRF:
   
   ```
   l2 tracemroute source <A.B.C.D> group <A.B.C.D> vrf WORD<1-16> [priority <0-7>] [ttl-value <1-255>]
   ```

   **Note:**

   For the preceding command, if you do not specify a VRF, `l2 tracemroute` uses the global default VRF.

   Wait for the l2 tracemroute to complete or press any key to abort.

Example

The following is a sample output for a Layer 2 tracemroute on a VLAN:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#l2 tracemroute source 192.0.2.81 233.252.0.1 vlan 201
Please wait for l2 tracemroute to complete or press any key to abort.
Source 192.0.2.81
Group: 233.252.0.1
VLAN:201
BMAC: 03:00:03:f4:24:01
B-VLAN: 10
I-SID: 16000001
===============================================
1 PETER4 00:03:00:00:00:00 -> LEE1 00:14:0d:bf:a3:df
2 LEE1 00:14:0d:bf:a3:df -> LEE2 00:15:e8:b8:a3:df
```
The following is a sample output for a Layer 2 tracemroute on a VRF:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#l2 tracemroute source 192.0.2.10 group 233.252.0.1 vrf red

Please wait for l2 tracemroute to complete or press any key to abort.

Source 192.0.2.10
Group: 233.252.0.1
VRF: redID 1
BMAC: 03:00:04:f4:24:01
B-VLAN: 20
I-SID: 16000001
```

```
===============================================================================
1 PETER4 00:03:00:00:00:00 -> LEE1 00:14:0d:bf:a3:df
2 LEE1 00:14:0d:bf:a3:df -> LEE2 00:15:e8:b8:a3:df
```

### Variable definitions

Use the data in the following table to use the `l2 tracemroute` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>source <code>&lt;A.B.C.D&gt;</code></td>
<td>Specifies the source IP address.</td>
</tr>
<tr>
<td>group <code>&lt;A.B.C.D&gt;</code></td>
<td>Specifies the IP address of the multicast group.</td>
</tr>
<tr>
<td>vlan <code>&lt;1–4084&gt;</code></td>
<td>Specifies the VLAN value.</td>
</tr>
<tr>
<td>vrf <code>WORD&lt;1–16&gt;</code></td>
<td>Specifies the VRF name. If you do not specify a VRF name, then the results are shown for the flow in the Global Router (default) context.</td>
</tr>
<tr>
<td>priority <code>&lt;0–7&gt;</code></td>
<td>Specifies the priority value.</td>
</tr>
<tr>
<td>ttl <code>&lt;1–255&gt;</code></td>
<td>Specifies the time-to-live (TTL) for the trace packet, which is how many hops the trace packet takes before it is dropped.</td>
</tr>
</tbody>
</table>

### Job aid

The following table describes the fields in the output for `l2 tracemroute` command for a VLAN.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Specifies the source IP address of the flow where the multicast trace tree originates.</td>
</tr>
<tr>
<td>Group</td>
<td>Specifies the IP address of the multicast group.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Specifies the VLAN.</td>
</tr>
<tr>
<td>BMAC</td>
<td>Specifies the backbone MAC address.</td>
</tr>
<tr>
<td>B-VLAN</td>
<td>Specifies the backbone VLAN.</td>
</tr>
<tr>
<td>I-SID</td>
<td>Specifies the service identifier.</td>
</tr>
</tbody>
</table>
The following table describes the fields in the output for `l2 tracemroute` command for a VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Specifies the source IP address of the flow where the multicast trace tree originates.</td>
</tr>
<tr>
<td>Group</td>
<td>Specifies the IP address of the multicast group.</td>
</tr>
<tr>
<td>VRF</td>
<td>Specifies the VRF.</td>
</tr>
<tr>
<td>BMAC</td>
<td>Specifies the backbone MAC address.</td>
</tr>
<tr>
<td>B-VLAN</td>
<td>Specifies the backbone VLAN.</td>
</tr>
<tr>
<td>I-SID</td>
<td>Specifies the service identifier.</td>
</tr>
</tbody>
</table>

Using trace CFM to diagnose problems

Use the following procedure to display trace information for CFM.

**About this task**

Use trace to observe the status of a software module at a certain time.

For example, if you notice a CPU utilization issue (generally a sustained spike above 90%) perform a trace of the control plane activity.

Use the `trace level 120 <0–4>` command to trace CFM module information, including ACLI, instrumentation, show config, and platform dependent code. The CFM module ID is 120.

Use the `trace cfm level <0–4>` command to trace platform independent code and CFM protocol code.

⚠️ **Caution:**

**Risk of traffic loss**

Using the trace tool inappropriately can cause primary CPU lockup conditions, loss of access to the device, loss of protocols, and service degradation.

**Procedure**

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. Clear the trace:
   ```
   clear trace
   ```
3. Begin the trace operation:
   ```
   trace cfm level <0–4>
   ```
   Wait approximately 30 seconds, and then stop trace.
4. Stop tracing:
   trace shutdown

5. View the trace results:
   show trace cfm

6. Begin the trace operation for the CFM module:
   trace level 120 <0-4>
   Wait approximately 30 seconds, and then stop trace.

7. View trace results:
   trace screen enable

   ! Important:
   If you use trace level 3 (verbose) or trace level 4 (very verbose), Avaya recommends
   you do not use the screen to view commands, due to the volume of information the
   system generates and the effect on the system.

8. Save the trace file to the Compact Flash card for retrieval.
   save trace [file WORD<1-99>]
   If you do not specify a file name, the file name is systrace.txt. By default, the system saves
   the file to the external flash.

9. Search trace results for a specific string value, for example, the word error:
   trace grep [WORD<0-128>]
   If you use this command and do not specify a string value, you clear the results of a previous
   search.

Example
--- Switch:1>enable
Switch:1#configure terminal
Switch:1(config)# clear trace
Switch:1(config)# trace cfm level 3
Switch:1(config)# trace shutdown
Switch:1(config)# show trace cfm
-------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>CFM Tracing Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status : Enabled</td>
</tr>
<tr>
<td>Level  : VERBOSE</td>
</tr>
<tr>
<td>Level  : VERBOS</td>
</tr>
</tbody>
</table>
Switch:1(config)#trace level 120 3
Switch:1(config)# save trace
Switch:1(config)# trace grep error
Switch:1(config)#trace grep 00-1A-4B-8A-FB-6B

Variable definitions
--- Use the data in the following table to use the trace command.
### Variable | Value
--- | ---
| cfm level \[<0-4>\] | Starts the trace by specifying the level.  
|  | • <0–4> specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is verbose, 4 is very verbose.  
| filter | Configures a filter trace for a file or module.  
| flags | Configures trace flags for IS-IS or OSPF.  
| grep \[WORD\]<0-128>\] | Searches trace results for a specific string value, for example, the word error. Performs a comparison of trace messages.  
| level \(<0–234>\)[<0-4>] | Starts the trace by specifying the module ID and level.  
|  | • <0–234> specifies the module ID.  
|  | • <0-4> specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is verbose, 4 is very verbose.  
| route-map | Enables or disables the trace route-map. The values are on and off.  
| screen \{disable|enable\} | Enables the display of trace output to the screen.  
| shutdown | Stops the trace operation.  
| spbm isis level \[<0-4>\] | Starts the trace by specifying the level.  
|  | • <0-4> specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is verbose, 4 is very verbose.  
|  | The default is 1, very terse.  

Use the data in the following table to use the **save trace** command.

### Variable | Value
--- | ---
| file \[WORD\]<1–99> | Specifies the file name in one of the following formats:  
|  | • a.b.c.d:<file>  
|  | • x:x:x:x:x:x:x <file>  
|  | • /intflash/<file>  
|  | • /extflash/<file>  
|  | • /usb/<file>  
|  | • /mnt/intflash/ <file>  
|  | • /mnt/extflash/ <file>  
|  | /mnt/intflash is the internal flash of the CPU.  
|  | /mnt/extflash is the external flash of the CPU.  

Comments on this document? infodev@avaya.com
Using trace SPBM to diagnose problems

Use the following procedure to display trace information for SPBM IS-IS. In the case of IS-IS, this procedure also provides information related to the flags set.

About this task

Use the `trace level 119 <0–4>` command to trace IS-IS module information, including ACLI, instrumentation, show config and platform dependent code. The IS-IS module ID is 119.

Use the `trace level 125 <0–4>` command to trace SPBM module information, including ACLI, instrumentation, show config and platform dependent code. The SPBM module ID is 125.

Use the `trace spbm isis level` command to trace platform independent code, IS-IS protocol, IS-IS hello, IS-IS adjacency, LSP processing, and IS-IS computation.

⚠️ Caution:

Risk of traffic loss

Using the trace tool inappropriately can cause primary CPU lockup conditions, loss of access to the device, loss of protocols, and service degradation.

Procedure

1. Enter Global Configuration mode:
   
   ```
   enable
   configure terminal
   ```

2. Clear the trace:
   
   ```
   clear trace
   ```

3. Begin the trace operation:
   
   ```
   trace spbm isis level <0-4>
   ```
   
   Wait approximately 30 seconds, and then stop trace.

4. Stop tracing:
   
   ```
   trace shutdown
   ```

5. Display the trace information for SPBM IS-IS:
   
   ```
   show trace spbm isis
   ```

6. Begin the trace operation for the SPBM module:
   
   ```
   trace level 125 <0-4>
   ```
   
   Wait approximately 30 seconds, and then stop trace.

7. Begin the trace operation for the IS-IS module:
   
   ```
   trace level 119 <0-4>
   ```
Wait approximately 30 seconds, and then stop trace.

8. View trace results:

```
trace screen enable
```

⚠️ Important:

If you use trace level 3 (verbose) or trace level 4 (very verbose), Avaya recommends you do not use the screen to view commands due to the volume of information the system generates and the effect on the system.

9. Save the trace file to the Compact Flash card for retrieval.

```
save trace [file WORD<1–99>]
```

If you do not specify a file name, the file name is systrace.txt. By default, the system saves the file to the external flash.

10. Search trace results for a specific string value, for example, the word error:

```
trace grep [WORD<0–128>]
```

If you use this command and do not specify a string value, you clear the results of a previous search.

**Example**

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)# clear trace
Switch:1(config)# trace spbm isis level 3
Switch:1(config)# trace shutdown
Switch:1(config)# show trace spbm isis
```

```
================================================================================
SPBM ISIS Tracing Info
================================================================================
Status    : Enabled
Level     : VERY_TERSE
Flag Info :
Switch:1(config)#trace level 125 3
Switch:1(config)#trace level 119 3
Switch:1(config)#save trace
Switch:1(config)#trace grep error
Switch:1(config)#trace grep 00-1A-4B-8A-FB-6B
```

**Variable definitions**

Use the data in the following table to use the `trace` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cfm level [&lt;0-4&gt;]</code></td>
<td>Starts the trace by specifying the level.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;0-4&gt;</code> specifies the trace level from 0–4, where 0 is disabled; 1</td>
</tr>
<tr>
<td></td>
<td>is very terse; 2 is terse; 3 is verbose, 4 is very verbose.</td>
</tr>
<tr>
<td><code>filter</code></td>
<td>Configure a filter trace for a file or module.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>flags</td>
<td>Configure trace flags for IS-IS or OSPF.</td>
</tr>
<tr>
<td>grep [WORD&lt;0-128&gt;]</td>
<td>Searches trace results for a specific string value, for example, the word error. Performs a comparison of trace messages.</td>
</tr>
</tbody>
</table>
| level <0–234>[<0–4>] | Starts the trace by specifying the module ID and level. 
  • <0–234> specifies the module ID.  
  • <0–4> specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is verbose, 4 is very verbose. |
| route-map           | Enables or disables the trace route-map. The values are on and off.   |
| screen {disable|enable} | Enables the display of trace output to the screen.                   |
| shutdown            | Stops the trace operation.                                           |
| spbm isis level [<0–4>] | Starts the trace by specifying the level. 
  • <0–4> specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is verbose, 4 is very verbose. 
  The default is 1, very terse. |

Use the data in the following table to use the `save trace` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
</table>
| file WORD<1–99>     | Specifies the file name in one of the following formats: 
  • a.b.c.d:<file> 
  • x:x:x:x:x:x:x <file> 
  • /intflash/<file> 
  • /extflash/<file> 
  • /usb/<file> 
  • /mnt/intflash/ <file> 
  • /mnt/extflash/ <file> 
  /mnt/intflash is the internal flash of the CPU. 
  /mnt/extflash is the external flash of the CPU. |

---

**CFM configuration using EDM**

This section provides procedures to configure Connectivity Fault Management (CFM) using Enterprise Device Manager (EDM).
When you enable CFM in an SPBM network, Avaya recommends that you enable CFM on the Backbone Edge Bridges (BEB) and on all Backbone Core Bridges (BCB). If you do not enable CFM on a particular node, you cannot obtain CFM debug information from that node.

Autogenerated CFM

CFM provides two methods for creating MEPs: autogenerated and explicit. You cannot use both. You must choose one or the other. Use the procedures in this section to configure autogenerated MEPs that eliminate the need to configure an MD, MA, and MEP ID to create a MEP.

Note:

• For SPBM B-VLANs, you can use either autogenerated or explicitly configured CFM MEPs.
• For C-VLANs, you can only use autogenerated CFM MEPs. Only VSP 4000 Series supports configuring autogenerated CFM on a C-VLAN.

Previous explicit CFM configurations of MDs, MAs and MEPs on SPBM B-VLANs continue to function in this release. However, if you want to enable the new autogenerated commands, you must first remove the existing MEP and MIP on the SPBM B-VLAN. The switch only supports one MEP or MIP on the SPBM B-VLAN, either explicitly configured or autogenerated.

For autogenerated CFM configuration information for EDM, see:

• Configuring autogenerated CFM on SPBM B-VLANs on page 184
• Configuring autogenerated CFM on C-VLANs on page 186 (VSP 4000 Series only)

Configuring autogenerated CFM on SPBM B-VLANs

Use this procedure to configure the autogenerated CFM MEP and MIP level for every SPBM B-VLAN on the chassis. This configuration eliminates the need to explicitly configure an MD, MA, and MEP ID and to associate the MEP and MIP level to the SPBM B-VLAN.

To configure autogenerated CFM on C-VLANs for VSP 4000 Series, see Configuring autogenerated CFM on C-VLANs on page 186.

About this task

When you enable this feature, the device creates a global MD (named spbm) for all the SPBM Nodal MEPs. This MD has a default maintenance level of 4, which you can change with the level attribute. All the MEPs that the device creates use the MEP ID configured under the global context, which has a default value of 1. The nodal MEPs are automatically associated with the SPBM B-VLANs configured. The MIP level maps to the global level. When you enable the feature, the device automatically associates the MIP level with the SPBM B-VLANs configured. The feature is disabled by default.

Important:

CFM supports one MEP or MIP for each SPBM B-VLAN only. This means that if you want to use these autogenerated MEPs, you cannot use your existing CFM configuration. You must first
remove the existing MEP or MIP on the SPBM B-VLAN. If you want to continue configuring MEPs manually, skip this procedure.

Procedure
1. From the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click CFM.
3. Click the Global tab.
4. Select enable next to SpbmAdminState.
5. Click Apply.
6. To verify the values assigned to MA, MD, and MEP, perform the following steps:
   a. Click the MD tab.
   b. Select SPBM, and then check the MA and MEP values.

CFM Global field descriptions
Use the data in the following table to configure the global MEP and MIP parameters.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpbmAdminState</td>
<td>Enables or disables autogenerated CFM for B-VLANs. The default is disable.</td>
</tr>
<tr>
<td>SpbmLevel</td>
<td>Specifies the global SPBM CFM maintenance level for the chassis within the range of 0 to 7. The default is 4. Only configure global CFM at one MD level for each VLAN type.</td>
</tr>
<tr>
<td>SpbmMepId</td>
<td>Specifies the global MEP ID within the range of 1 to 8191. Select a unique ID for each switch to ensure that the MEPs are unique across the network. The default is 1.</td>
</tr>
<tr>
<td>CmacAdminState</td>
<td>Enables or disables autogenerate CFM for C-VLANs. The default is disable. This field appears only for VSP 4000 Series.</td>
</tr>
<tr>
<td>CmacLevel</td>
<td>Specifies the global C-MAC CFM maintenance level for the chassis within the range of 0 to 7. The default is 4. Only configure global CFM at one MD level for each VLAN type. This field appears only for VSP 4000 Series.</td>
</tr>
<tr>
<td>CmacMepId</td>
<td>Specifies the global MEP ID within the range of 1 to 8191. Select a unique ID for each switch to ensure that the MEPs are unique across the network. The default is 1.</td>
</tr>
</tbody>
</table>

Table continues...
Configuring autogenerated CFM on C-VLANs

This procedure applies only to VSP 4000 Series.

Use this procedure to configure the autogenerated CFM MEP and MIP level for every C-VLAN on the chassis.

To configure autogenerated CFM on SPBM B-VLANs, see Configuring autogenerated CFM on SPBM B-VLANs on page 184.

**Important:**

CFM supports one MEP or MIP on each C-VLAN. Only autogenerated CFM provides support for configuring MEP and MIPs on C-VLANs. You cannot explicitly configure C-VLANs.

**About this task**

When you enable this feature, you create a global MD (named cmac) for all the customer MAC (C-MAC) MEPs. This MD has a default maintenance level of 4, which you can change with the level attribute. The autogenerated CFM commands also create an MA for each C-VLAN, a MEP for each C-VLAN, and associate the MEP with the corresponding C-VLAN and a MIP with the C-VLAN.

All the MEPs that the device creates use the MEP ID configured under the global context, which has a default value of 1. The device automatically associates the MEPs with the C-VLANs configured. The MIP level maps to the global level. The device automatically associates the MIP level with the C-VLANs configured when you enable the feature.

The feature is disabled by default.

**Procedure**

1. From the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click CFM.
3. Click the Global tab.
4. Select enable next to CmacAdminState.
5. In the fields provided, specify a maintenance level and a MEP ID.
6. Click Apply.

**CFM Global field descriptions**

Use the data in the following table to configure the global MEP and MIP parameters.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpbmAdminState</td>
<td>Enables or disables autogenerated CFM for B-VLANs. The default is disable.</td>
</tr>
<tr>
<td>SpbmLevel</td>
<td>Specifies the global SPBM CFM maintenance level for the chassis within the range of 0 to 7. The default is 4. Only configure global CFM at one MD level for each chassis for each VLAN type.</td>
</tr>
<tr>
<td>SpbmMepId</td>
<td>Specifies the global MEP ID within the range of 1 to 8191. Select a unique ID for each switch to ensure that the MEPs are unique across the network. The default is 1.</td>
</tr>
<tr>
<td>CmacAdminState</td>
<td>Enables or disables autogenerated CFM for C-VLANs. The default is disable. This field appears only for VSP 4000 Series.</td>
</tr>
<tr>
<td>CmacLevel</td>
<td>Specifies the global C-MAC CFM maintenance level for the chassis within the range of 0 to 7. The default is 4. Only configure global CFM at one MD level for each chassis for each VLAN type. This field appears only for VSP 4000 Series.</td>
</tr>
<tr>
<td>CmacMepId</td>
<td>Specifies the global MEP ID within the range of 1 to 8191. Select a unique ID for each switch to ensure that the MEPs are unique across the network. The default is 1. This field appears only for VSP 4000 Series.</td>
</tr>
<tr>
<td>Bmac</td>
<td>Displays the B-MAC address of the node. This field appears only for VSP 4000 Series.</td>
</tr>
<tr>
<td>Cmac</td>
<td>Displays the C-MAC address of the node. This field appears only for VSP 4000 Series.</td>
</tr>
</tbody>
</table>

**Configuring explicit CFM**

For SPBM B-VLANs, CFM provides two methods for creating MEPs: autogenerated and explicit. You cannot use both. Use the procedures in this section to configure MEPs explicitly.

If you want to create autogenerated CFM MEPs that eliminate the need to configure an MD, MA, and MEP ID, see the procedures in [Autogenerated CFM](#) on page 184. For C-VLANs, you can only use the autogenerated method.

**Note:**

The CFM show commands that display MD, MA, and MEP information work for both autogenerated and explicitly-configured CFM MEPs.
Configuring CFM MD

Use this procedure to configure a Connectivity Fault Management (CFM) Maintenance Domain (MD). An MD is the part of a network that is controlled by a single administrator. A single MD can contain several Maintenance Associations (MA).

Procedure

1. From the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click CFM.
3. Click the MD tab.
4. Click Insert.
5. In the fields provided, specify an index value, name, and level for the MD.
6. Click Insert.

MD field descriptions

Use the data in the following table to use the MD tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Specifies a maintenance domain entry index.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the MD name.</td>
</tr>
<tr>
<td>NumOfMa</td>
<td>Indicates the number of MAs that belong to this maintenance domain.</td>
</tr>
<tr>
<td>Level</td>
<td>Specifies the MD maintenance level. The default is 4.</td>
</tr>
<tr>
<td>NumOfMip</td>
<td>Indicates the number of MIPs that belong to this maintenance domain</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the type of domain.</td>
</tr>
</tbody>
</table>

Configuring CFM MA

Use this procedure to configure a CFM Maintenance Association (MA). An MA represents a logical grouping of monitored entities within its Domain. It can therefore represent a set of Maintenance Endpoints (MEPs), each configured with the same Maintenance Association ID (MAID) and MD Level, established to verify the integrity of a single service instance.

Before you begin

• You must configure a CFM MD.

Procedure

1. In the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click CFM.
3. Click the MD tab.
4. Highlight an existing MD, and then click MaintenanceAssociation.
5. In the MA tab, click **Insert**.
6. In the fields provided, specify an index value and name for the MA.
7. Click **Insert**.

### MA field descriptions

Use the data in the following table to use the MA tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainIndex</td>
<td>Specifies the maintenance domain entry index.</td>
</tr>
<tr>
<td>AssociationIndex</td>
<td>Specifies a maintenance association entry index.</td>
</tr>
<tr>
<td>DomainName</td>
<td>Specifies the MD name.</td>
</tr>
<tr>
<td>AssociationName</td>
<td>Specifies the MA name.</td>
</tr>
<tr>
<td>NumOfMep</td>
<td>Indicates the number of MEPs that belong to this maintenance association.</td>
</tr>
</tbody>
</table>

### Configuring CFM MEP

Use this procedure to configure the CFM Maintenance Endpoint (MEP). A MEP represents a managed CFM entity, associated with a specific Domain Service Access Point (DoSAP) of a service instance, which can generate and receive CFM Protocol Data Units (PDU) and track any responses. A MEP is created by MEP ID under the context of an MA.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **CFM**.
3. Click the **MD** tab.
4. Highlight an existing MD, and then click **MaintenanceAssociation**.
5. In the **MA** tab, highlight an existing MA, and then click **MaintenanceEndpoint**.
6. Click **Insert**.
7. In the fields provided, specify the ID and the administrative state of the MEP.
8. Click **Insert**.

### MEP field descriptions

Use the data in the following table to use the MEP tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainIndex</td>
<td>Specifies the MD index.</td>
</tr>
<tr>
<td>AssociationIndex</td>
<td>Specifies the MA index.</td>
</tr>
<tr>
<td>Id</td>
<td>Specifies the MEP ID.</td>
</tr>
<tr>
<td>DomainName</td>
<td>Specifies the MD name.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AssociationName</td>
<td>Specifies the MA name.</td>
</tr>
<tr>
<td>AdminState</td>
<td>Specifies the administrative state of the MEP. The default is disable.</td>
</tr>
<tr>
<td>MepType</td>
<td>Specifies the MEP type:</td>
</tr>
<tr>
<td></td>
<td>• trunk</td>
</tr>
<tr>
<td></td>
<td>• sg</td>
</tr>
<tr>
<td></td>
<td>• endpt</td>
</tr>
<tr>
<td></td>
<td>• vlan</td>
</tr>
<tr>
<td></td>
<td>• port</td>
</tr>
<tr>
<td></td>
<td>• endptClient</td>
</tr>
<tr>
<td></td>
<td>• nodal</td>
</tr>
<tr>
<td></td>
<td>• remotetrunk</td>
</tr>
<tr>
<td></td>
<td>• remotestg</td>
</tr>
<tr>
<td></td>
<td>• remoteendpt</td>
</tr>
<tr>
<td></td>
<td>• remoteVlan</td>
</tr>
<tr>
<td></td>
<td>• remotePort</td>
</tr>
<tr>
<td></td>
<td>• remoteEndptClient</td>
</tr>
<tr>
<td>ServiceDescription</td>
<td>Specifies the service to which this MEP is assigned.</td>
</tr>
</tbody>
</table>

**Configuring CFM nodal MEP**

Use this procedure to configure the CFM nodal Maintenance Endpoint (MEP). The Nodal MEP provides traceability and troubleshooting at the system level for a given B-VLAN. The Nodal B-VLAN MEPs created on the CP and function as if they are connected to the virtual interface of the given B-VLAN. Because of this they are supported for both port and MLT based B-VLANs.

Nodal MPs provide both MEP and Maintenance Intermediate Point (MIP) functionality for SPBM deployments. Nodal MPs are associated with a B-VLAN and are VLAN encapsulated packets. Each node (chassis) has a given MAC address and communicates with other nodes. The SPBM instance MAC address is used as the MAC address of the Nodal MP.

**Before you begin**

- You must configure a CFM MD, MA, and MEP.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > VLAN**.
2. Click **VLANs**.
3. Click the **Advanced** tab.
4. Select a VLAN with a type of spbm-bvlan.
5. Click **Nodal**.
6. In the **NodalMepList** field, specify the nodal MEPs to add to the VLAN.
7. Click **Apply**.

### Nodal MEP/MIP field descriptions

Use the data in the following table to use the **Nodal MEP/MIP** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodalMepList</td>
<td>Specifies the nodal MEPs to add to the VLAN, in the format <code>&lt;mdName.maName.mepId&gt;</code>, for example <code>md10.ma20.30</code>.</td>
</tr>
<tr>
<td>NumOfNodalMep</td>
<td>Indicates the number of nodal MEPs assigned to this VLAN.</td>
</tr>
<tr>
<td>NodalMipLevelList</td>
<td>Specifies a MIP level list.</td>
</tr>
<tr>
<td>NumOfNodalMipLevel</td>
<td>Indicates the number of nodal MIP levels assigned to this VLAN that allows MIP functionality to be enabled on a per level per VLAN basis.</td>
</tr>
</tbody>
</table>

### Configuring Layer 2 ping

Use this procedure to configure a Layer 2 ping inside an SPBM cloud or network. This feature enables CFM to debug Layer 2. It can also help you debug IP shortcuts and the record for the shortcuts' ARP.

**Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software*, NN47227-401. As an alternative, use the ACLI.

### Before you begin

- On the source and destination nodes, you must configure a CFM MD, MA, and MEP, and assign a nodal MEP to the B-VLAN.

### Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. From the **L2Ping** tab, configure the Layer 2 ping properties.
4. To initiate a Layer 2 ping, highlight an entry and click the **Start** button.
5. To update a Layer 2 ping, click the **Refresh** button.
6. To stop the Layer 2 ping, click the **Stop** button.
## L2Ping field descriptions

Use the data in the following table to use the **L2Ping** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VlanId</td>
<td>Identifies the backbone VLAN.</td>
</tr>
<tr>
<td>DestMacAddress</td>
<td>Specifies the target MAC address.</td>
</tr>
<tr>
<td>HostName</td>
<td>Specifies the target host name.</td>
</tr>
<tr>
<td>DestIsHostName</td>
<td>Indicates whether the host name is (true) or is not (false) used for L2Ping transmission.</td>
</tr>
<tr>
<td>Messages</td>
<td>Specifies the number of L2Ping messages to be transmitted. The default is 1.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the status of the transmit loopback service:</td>
</tr>
<tr>
<td></td>
<td>• ready: the service is available.</td>
</tr>
<tr>
<td></td>
<td>• transmit: the service is transmitting, or about to transmit, the L2Ping messages.</td>
</tr>
<tr>
<td></td>
<td>• abort: the service aborted or is about to abort the L2Ping messages.</td>
</tr>
<tr>
<td></td>
<td>This field is also used to avoid concurrency or race condition problems that can occur if two or more management entities try to use the service at the same time.</td>
</tr>
<tr>
<td></td>
<td>The default is ready.</td>
</tr>
<tr>
<td>ResultOk</td>
<td>Indicates the result of the operation:</td>
</tr>
<tr>
<td></td>
<td>• true: the L2Ping Messages will be (or have been) sent.</td>
</tr>
<tr>
<td></td>
<td>• false: the L2Ping Messages will not be sent.</td>
</tr>
<tr>
<td></td>
<td>The default is true.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies a 3–bit value to be used in the VLAN header, if present in the transmitted frame.</td>
</tr>
<tr>
<td></td>
<td>The default is 7.</td>
</tr>
<tr>
<td>TimeoutInt</td>
<td>Specifies the interval to wait for an L2Ping time-out. The default value is 3 seconds.</td>
</tr>
<tr>
<td>TestPattern</td>
<td>Specifies the test pattern to use in the L2Ping PDU:</td>
</tr>
<tr>
<td></td>
<td>• allZero: null signal without cyclic redundancy check</td>
</tr>
<tr>
<td></td>
<td>• allZeroCrc: null signal with cyclic redundancy check with 32-bit polynomial</td>
</tr>
<tr>
<td></td>
<td>• pseudoRandomBitSequence: pseudo-random-bit-sequence without cyclic redundancy check</td>
</tr>
</tbody>
</table>

*Table continues*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>pseudoRandomBitSequenceCrc</td>
<td>• pseudo-random-bit-sequence with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default value is allZero.</td>
</tr>
<tr>
<td>DataSize</td>
<td>Specifies an arbitrary amount of data to be included in the data TLV, if the data size is selected to be sent. The default is 0.</td>
</tr>
<tr>
<td>FrameSize</td>
<td>Specifies the frame size. If the frame size is specified then the data size is internally calculated and the calculated data size is included in the data TLV. The default is 0.</td>
</tr>
<tr>
<td>SourceMode</td>
<td>Specifies the source mode of the transmit loopback service: • nodal • noVlanMac — Use this value with C-VLAN only. When you select this option, even if a VLAN MAC address exists, the system uses the CFM C-MAC as the BMAC-SA. • smltVirtual — Use the smltVirtual option with B-VLANs only. The default is nodal.</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>The transaction identifier/sequence number of the first loopback message (to be) sent. The default is 0.</td>
</tr>
<tr>
<td>Result</td>
<td>Displays the Layer 2 Ping result.</td>
</tr>
</tbody>
</table>

### Initiating a Layer 2 traceroute

Use this procedure to trigger a Layer 2 traceroute. This feature enables CFM to debug Layer 2 in an SPBM cloud or network. It can determine the path used by IS—IS to get from one MEP to another, by showing all the hops between. Therefore, it can show where connectivity is lost. It can also work for IP shortcuts.

**Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software*, NN47227-401. As an alternative, use the ACLI.

If you configure `IsTraceTree` to false then EDM performs Traceroute on the unicast path. If you configure `IsTraceTree` to true then EDM performs TraceTree on the multicast tree.

For more information on configuring tracetree, see *Configuring Layer 2 tracetree* on page 210.
Important:
To trace a route to a MAC address, the MAC address must be in the VLAN FDB table.
For B-VLANs, you do not have to trigger an L2Ping to learn the MAC address because IS-IS populates the MAC addresses in the FDB table.
Linktrace traces the path up to the closest device to that MAC address that supports CFM.

Before you begin
• On the source and destination nodes, you must configure a CFM MD, MA, and MEP, and assign a nodal MEP to the B-VLAN.

Procedure
1. In the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click L2Ping/L2Trace Route.
3. Click the L2 Traceroute/TraceTree tab.
4. To start the traceroute, highlight an entry, and then click the Start button.
5. To update the traceroute, click the Refresh button.
6. To stop the traceroute, click the Stop button.

L2Traceroute field descriptions
Use the data in the following table to use the L2 Traceroute/TraceTree tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VlanId</td>
<td>Specifies a value that uniquely identifies the Backbone VLAN (B-VLAN).</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies a 3–bit value to be used in the VLAN header, if present in the transmitted frame. The default is 7.</td>
</tr>
<tr>
<td>DestMacAddress</td>
<td>Specifies the target MAC address.</td>
</tr>
<tr>
<td>HostName</td>
<td>Specifies the target host name.</td>
</tr>
<tr>
<td>DestIsHostName</td>
<td>Specifies whether the host name is (true) or is not (false) used for the L2Trace transmission.</td>
</tr>
<tr>
<td>Isid</td>
<td>Specifies the Service Instance Identifier (I-SID).</td>
</tr>
<tr>
<td>IsTraceTree</td>
<td>Specifies whether the multicast tree or unicast path is traced:</td>
</tr>
<tr>
<td></td>
<td>• If you configure IsTraceTree to false then EDM performs Traceroute on the unicast path.</td>
</tr>
<tr>
<td></td>
<td>• If you configure IsTraceTree to true then EDM performs TraceTree on the multicast tree.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates the status of the transmit loopback service:</td>
</tr>
<tr>
<td></td>
<td>• ready: the service is available.</td>
</tr>
<tr>
<td></td>
<td>• transmit: the service is transmitting, or about to transmit, the L2Trace messages.</td>
</tr>
<tr>
<td></td>
<td>• abort: the service aborted or is about to abort the L2Trace messages.</td>
</tr>
<tr>
<td></td>
<td>This field is also used to avoid concurrency or race condition problems that can occur if two or more management entities try to use the service at the same time.</td>
</tr>
<tr>
<td></td>
<td>The default is ready.</td>
</tr>
<tr>
<td>ResultOk</td>
<td>Indicates the result of the operation:</td>
</tr>
<tr>
<td></td>
<td>• true: the L2Trace messages will be (or have been) sent.</td>
</tr>
<tr>
<td></td>
<td>• false: the L2Trace messages will not be sent.</td>
</tr>
<tr>
<td></td>
<td>The default is true.</td>
</tr>
<tr>
<td>Ttl</td>
<td>Specifies the number of hops remaining to this L2Trace.</td>
</tr>
<tr>
<td></td>
<td>This value is decremented by 1 by each Bridge that handles the L2Trace. The decremented value is returned in the L2Trace. If 0 on output, the L2Trace is not transmitted to the next hop. The value of the time-to-live (TTL) field in the L2Trace is defined by the originating MEP.</td>
</tr>
<tr>
<td></td>
<td>The default value is 64.</td>
</tr>
<tr>
<td>SourceMode</td>
<td>Specifies the source mode:</td>
</tr>
<tr>
<td></td>
<td>• 1: nodal</td>
</tr>
<tr>
<td></td>
<td>• noVlanMac — Use this value with C-VLAN only. When you select this option, even if a VLAN MAC address exists, the system uses the CFM C-MAC as the BMAC-SA.</td>
</tr>
<tr>
<td></td>
<td>• 2: smitVirtual—Use this value with B-VLANs only.</td>
</tr>
<tr>
<td></td>
<td>The default is 1: nodal.</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>Specifies the transaction identifier/sequence number of the first loopback message (to be) sent. The default is 0.</td>
</tr>
<tr>
<td>Flag</td>
<td>L2Trace result flag that indicates L2Trace status or error code:</td>
</tr>
<tr>
<td></td>
<td>• none (1): No error</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• internalError (2):</td>
<td>L2Trace internal error</td>
</tr>
<tr>
<td>• invalidMac (3):</td>
<td>Invalid MAC address</td>
</tr>
<tr>
<td>• mepDisabled (4):</td>
<td>MEP must be enabled in order to perform L2Trace</td>
</tr>
<tr>
<td>• noL2TraceResponse (5):</td>
<td>No L2Trace response received</td>
</tr>
<tr>
<td>• l2TraceToOwnMepMac (6):</td>
<td>L2Trace to own MEP MAC is not sent</td>
</tr>
<tr>
<td>• l2TraceComplete (7):</td>
<td>L2Trace completed</td>
</tr>
<tr>
<td>• l2TraceLookupFailure (8):</td>
<td>Lookup failure for L2Trace</td>
</tr>
<tr>
<td>• l2TraceLeafNode (9):</td>
<td>On a leaf node in the I-SID tree</td>
</tr>
<tr>
<td>• l2TraceNotInTree (10):</td>
<td>Not in the I-SID tree</td>
</tr>
<tr>
<td>• l2TraceSmltNotPrimary (11):</td>
<td>Requested SMLT source from non-primary node</td>
</tr>
</tbody>
</table>

**Viewing Layer 2 traceroute results**

Use this procedure to view Layer 2 traceroute results. This feature enables CFM to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

⚠️ **Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software*, NN47227-401. As an alternative, use the ACLI.

**About this task**

You can display Layer 2 tracetree results to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID. For more information, see *Viewing Layer 2 tracetree results* on page 213.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. Click the **L2Traceroute/TraceTree** tab.
4. Click the **Refresh** button to update the results.
5. To view the traceroute results, highlight an entry, and then click **Result**.
L2 Traceroute/Tracetree Result field descriptions

Use the data in the following table to use the L2 Traceroute/Tracetree Result tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VlanId</td>
<td>A value that uniquely identifies the Backbone VLAN (B-VLAN).</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>The transaction identifier/sequence number returned by a previous transmit linktrace message command, indicating which L2Trace's response of the L2Trace is going to be returned. The default is 0.</td>
</tr>
<tr>
<td>Hop</td>
<td>The number of hops away from L2Trace initiator.</td>
</tr>
<tr>
<td>ReceiveOrder</td>
<td>An index to distinguish among multiple L2Trace responses with the same Transaction Identifier field value. This value is assigned sequentially from 1, in the order that the Linktrace Initiator received the responses.</td>
</tr>
<tr>
<td>Ttl</td>
<td>Time-to-Live (TTL) field value for a returned L2Trace response.</td>
</tr>
<tr>
<td>SrcMac</td>
<td>MAC address of the MP that responds to the L2Trace request for this L2TraceReply.</td>
</tr>
<tr>
<td>HostName</td>
<td>The host name of the replying node.</td>
</tr>
<tr>
<td>LastSrcMac</td>
<td>The MAC address of the node that forwarded the L2Trace to the responding node.</td>
</tr>
<tr>
<td>LastHostName</td>
<td>The host name of the node that forwarded the L2Trace to the responding node.</td>
</tr>
</tbody>
</table>

Configuring Layer 2 IP ping

Use this procedure to configure Layer 2 IP ping

**Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see Release Notes for VSP Operating System Software, NN47227-401. As an alternative, use the ACLI.

**Before you begin**

- On the source and destination nodes, you must configure a CFM MD, MA, and MEP, and assign a nodal MEP to the B-VLAN.
- If you want to run a Layer 2 IP Ping for a specific VRF, you must use EDM in the specific VRF context first. For more information, see the procedure for selecting and launching a VRF context view in Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series, NN46251-505 or Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series, NN47227-505.
Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. Click the **L2 IP Ping** tab.
4. To add a new entry, click **Insert**, specify the destination IP address and optional parameters, and then click **Insert**.
5. To start the Layer 2 IP ping, highlight an entry, and then click **Start**.
6. To update the Layer 2 IP ping, click the **Refresh** button.
7. To stop the Layer 2 IP ping, click **Stop**.

L2 IP Ping field descriptions

Use the data in the following table to use the **L2 IP Ping** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IpAddrType</td>
<td>Specifies the address type of destination IP Address (only IPv4 is supported).</td>
</tr>
<tr>
<td>IpAddr</td>
<td>Specifies the destination IP Address.</td>
</tr>
<tr>
<td>VrflId</td>
<td>Specifies the VRF ID.</td>
</tr>
<tr>
<td>VrfName</td>
<td>Specifies the name of the virtual router.</td>
</tr>
<tr>
<td>Messages</td>
<td>Specifies the number of L2IpPing messages to be transmitted per MAC/VLAN pair. Range is 1–200. The default is 1.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the status of the transmit loopback service:</td>
</tr>
<tr>
<td></td>
<td>• ready: the service is available.</td>
</tr>
<tr>
<td></td>
<td>• transmit: the service is transmitting, or about to transmit, the L2IpPing messages.</td>
</tr>
<tr>
<td></td>
<td>• abort: the service is aborted or about to abort the L2IpPing messages.</td>
</tr>
<tr>
<td></td>
<td>This field is also used to avoid concurrency or race condition problems that could occur if two or more management entities try to use the service at the same time.</td>
</tr>
<tr>
<td></td>
<td>The default is ready.</td>
</tr>
<tr>
<td>ResultOk</td>
<td>Indicates the result of the operation:</td>
</tr>
<tr>
<td></td>
<td>• true: L2IpPing Messages will be or have been sent.</td>
</tr>
<tr>
<td></td>
<td>• false: L2IpPing Messages will not be sent.</td>
</tr>
<tr>
<td></td>
<td>The default is true.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TimeoutInt</td>
<td>Specifies the interval to wait for an L2IpPing time-out with a range of 1–10 seconds with a default value of 3 seconds.</td>
</tr>
<tr>
<td>TestPattern</td>
<td>Specifies the test pattern to use in the L2IPPing PDU:</td>
</tr>
<tr>
<td></td>
<td>• <code>allZero</code> — null signal without cyclic redundancy check</td>
</tr>
<tr>
<td></td>
<td>• <code>allZeroCrc</code> — null signal with cyclic redundancy check with 32-bit polynomial</td>
</tr>
<tr>
<td></td>
<td>• <code>pseudoRandomBitSequence</code> — pseudo-random-bit-sequence without cyclic redundancy check</td>
</tr>
<tr>
<td></td>
<td>• <code>pseudoRandomBitSequenceCrc</code> — pseudo-random-bit-sequence with cyclic redundancy check with 32-bit polynomial.</td>
</tr>
<tr>
<td></td>
<td>A cyclic redundancy check is a code that detects errors.</td>
</tr>
<tr>
<td></td>
<td>The default value is <code>allZero</code>.</td>
</tr>
<tr>
<td>DataSize</td>
<td>Specifies an arbitrary amount of data to be included in the data TLV, if the data size is selected to be sent. The range is 0–400. The default is 0.</td>
</tr>
<tr>
<td>PathsFound</td>
<td>Specifies the number of paths found to execute the command. The default is 0.</td>
</tr>
</tbody>
</table>

**Viewing Layer 2 IP Ping results**

Use this procedure to view Layer 2 ip ping results.

⚠️ **Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software*, NN47227-401. As an alternative, use the ACLI.

⚠️ **Note:**

After you trigger Layer 2 IP Ping, you must click the Refresh button to update the results.

**Procedure**

1. In the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click L2Ping/L2Trace Route.
3. Click the L2 IP Ping tab.
4. To view the Layer 2 IP ping results, highlight an entry, and then click Result.
L2 IP Ping Result field descriptions

Use the data in the following table to use the L2 IP Ping Result tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IpAddrType</td>
<td>The address type of the destination IP Address.</td>
</tr>
<tr>
<td>IpAddr</td>
<td>Destination IP Address.</td>
</tr>
<tr>
<td>SendOrder</td>
<td>Specifies the order that sessions were sent. It is an index to distinguish among multiple L2Ping sessions. This value is assigned sequentially from 1. It correlates to the number of paths found.</td>
</tr>
<tr>
<td>VrfId</td>
<td>Specifies the VRF ID.</td>
</tr>
<tr>
<td>VlanId</td>
<td>Specifies the VLAN ID found from the Layer 3 lookup and used for transmission.</td>
</tr>
<tr>
<td>DestMacAddress</td>
<td>An indication of the target MAC Address transmitted.</td>
</tr>
<tr>
<td>PortNum</td>
<td>Either the value '0', or the port number of the port used for the l2 IP ping.</td>
</tr>
<tr>
<td>DestHostName</td>
<td>The host name of the responding node.</td>
</tr>
<tr>
<td>Size</td>
<td>The number of bytes of data sent.</td>
</tr>
<tr>
<td>PktsTx</td>
<td>Number of Packets transmitted for this VLAN/MAC.</td>
</tr>
<tr>
<td>PktsRx</td>
<td>Number of Packets received for this VLAN/MAC.</td>
</tr>
<tr>
<td>PercentLossWhole</td>
<td>Percentage of packet loss for this VLAN/MAC.</td>
</tr>
<tr>
<td>PercentLossFract</td>
<td>Percentage of packet loss for this VLAN/MAC.</td>
</tr>
<tr>
<td>MinRoundTrip</td>
<td>Minimum time for round-trip for this VLAN/MAC in us.</td>
</tr>
<tr>
<td>MaxRoundTrip</td>
<td>Maximum time for round-trip for this VLAN/MAC in us.</td>
</tr>
<tr>
<td>RttAvgWhole</td>
<td>Average time for round-trip for this VLAN/MAC in us.</td>
</tr>
<tr>
<td>RttAvgFract</td>
<td>Fractional portion of average time for round-trip.</td>
</tr>
<tr>
<td>Flag</td>
<td>Result flag indicating status or error code:</td>
</tr>
<tr>
<td></td>
<td>• 1 - No error</td>
</tr>
<tr>
<td></td>
<td>• 2 - Internal error</td>
</tr>
<tr>
<td></td>
<td>• 3 - Invalid IP</td>
</tr>
<tr>
<td></td>
<td>• 4 - L2Trace completed</td>
</tr>
<tr>
<td></td>
<td>• 5 - Lookup failure for IP (no VLAN/MAC entries)</td>
</tr>
</tbody>
</table>

Configuring Layer 2 IP traceroute

Use this procedure to configure Layer 2 IP traceroute.
**Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software*, NN47227-401. As an alternative, use the ACLI.

Before you begin

- On the source and destination nodes, you must configure a CFM MD, MA, and MEP, and assign a nodal MEP to the B-VLAN.
- If you want to run a Layer 2 IP Traceroute for a specific VRF, you must use EDM in the specific VRF context first. For more information, see the procedure for selecting and launching a VRF context view in *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 or *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. Click the **L2 IP Traceroute** tab.
4. To add a new entry, click **Insert**, specify the destination IP address and, optionally, the TTL value, and then click **Insert**.
5. To start the Layer 2 IP traceroute, highlight an entry, and then click the **Start** button.
6. To update the L2 IP traceroute, click the **Refresh** button.
7. To stop the Layer 2 IP traceroute, click the **Stop** button.

L2 IP Traceroute field descriptions

Use the data in the following table to use the **L2 IP Traceroute** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IpAddrType</td>
<td>Specifies the address type of destination IP address (only IPv4 is supported).</td>
</tr>
<tr>
<td>IPAddr</td>
<td>Specifies the destination IP Address.</td>
</tr>
<tr>
<td>VrfId</td>
<td>Specifies the VRF ID.</td>
</tr>
<tr>
<td>VrfName</td>
<td>Specifies the name of the virtual router.</td>
</tr>
<tr>
<td>Ttl</td>
<td>Specifies the number of hops remaining to this L2Trace. This value is decremented by 1 by each Bridge that handles the L2Trace. The decremented value is returned in the L2Trace. If 0 on output, the L2Trace is not transmitted to the next hop. The default value is 64.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the status of the transmit loopback service:</td>
</tr>
<tr>
<td></td>
<td>• ready: the service is available.</td>
</tr>
</tbody>
</table>

Table continues…
Viewing Layer 2 IP traceroute results

Use this procedure to view Layer 2 IP traceroute results.

 ApiException

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see Release Notes for VSP Operating System Software, NN47227-401. As an alternative, use the ACLI.

 ApiException

After you trigger Layer 2 IP traceroute, you must click the Refresh button to update the results.

Procedure

1. In the navigation tree, expand the following folders: Configuration > Edit > Diagnostics.
2. Click L2Ping/L2Trace Route.
3. Click the L2 IP Traceroute tab.
4. To view the Layer 2 IP traceroute results, highlight an entry, and then click Result.

L2 IP Traceroute Result field descriptions

Use the data in the following table to use the L2 IP Traceoute Result tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IpAddrType</td>
<td>Specifies the address type of destination IP address.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IpAddr</td>
<td>Specifies the destination IP address.</td>
</tr>
<tr>
<td>SendOrder</td>
<td>Denotes the order that sessions are sent. It is an index to distinguish among multiple L2Trace sessions. It correlates to the number of paths found. This value is assigned sequentially from 1.</td>
</tr>
<tr>
<td>Hop</td>
<td>Specifies the number of L2 hops away from L2Trace initiator.</td>
</tr>
<tr>
<td>ReceiveOrder</td>
<td>Specifies the order that sessions are sent. It is an index to distinguish among multiple L2Trace responses with the same Send Transaction Identifier field value. This value is assigned sequentially from 1, in the order that the Linktrace Initiator received the responses.</td>
</tr>
<tr>
<td>Ttl</td>
<td>Specifies the time-to-live (TTL) field value for a returned L2Trace response.</td>
</tr>
<tr>
<td>VrflId</td>
<td>Specifies the VRF ID.</td>
</tr>
<tr>
<td>VlanId</td>
<td>Specifies the VLAN found from Layer 3 lookup and used for transmission.</td>
</tr>
<tr>
<td>DestMacAddress</td>
<td>Indicates the target MAC address transmitted.</td>
</tr>
<tr>
<td>PortNum</td>
<td>Specifies either the value '0', or the port number of the port used for the l2trace.</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>Specifies the transaction identifier/sequence number used in linktrace message packet. The default is 0.</td>
</tr>
<tr>
<td>SrcMac</td>
<td>Specifies the MAC address of the MP that responded to L2Trace request for this L2traceReply.</td>
</tr>
<tr>
<td>HostName</td>
<td>Specifies the host name of the replying node.</td>
</tr>
<tr>
<td>LastSrcMac</td>
<td>Specifies the MAC address of the node that forwarded the L2Trace to the responding node.</td>
</tr>
<tr>
<td>LastHostName</td>
<td>Specifies the host name of the node that forwarded the L2Trace to the responding node.</td>
</tr>
<tr>
<td>Flag</td>
<td>L2Trace result flag indicating status or error code:</td>
</tr>
<tr>
<td></td>
<td>• none (1): No error</td>
</tr>
<tr>
<td></td>
<td>• internalError (2): L2Trace internal error</td>
</tr>
<tr>
<td></td>
<td>• invalidMac (3): Invalid MAC address</td>
</tr>
<tr>
<td></td>
<td>• mepDisabled (4): MEP must be enabled in order to perform L2Trace</td>
</tr>
<tr>
<td></td>
<td>• noL2TraceResponse (5): No L2Trace response received</td>
</tr>
<tr>
<td></td>
<td>• l2TraceToOwnMepMac (6): L2Trace to own MEP MAC is not sent</td>
</tr>
<tr>
<td></td>
<td>• l2TraceComplete (7): L2Trace completed</td>
</tr>
</tbody>
</table>

*Table continues…*
**Triggering a loopback test**

Use this procedure to trigger a loopback test.

The LBM packet is often compared to ping. An MEP transmits the loopback message to an intermediate or endpoint within a domain for the purpose of fault verification. This can be used to check the ability of the network to forward different sized frames.

**Before you begin**

- On the source and destination nodes, you must configure a CFM MD, MA, and MEP.
- Enable the MEP.
- Assign a nodal MEP to the B-VLAN.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **CFM**.
3. Click the **LBM** tab.
4. Configure the loopback test properties as required.
5. Click **Apply**.
6. To trigger the loopback test, double-click in the **Status** field, select **transmit**.
7. Click **Apply**.
8. To update the loopback test, click the **Refresh** button.

**LBM field descriptions**

Use the data in the following table to use the **LBM** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainIndex</td>
<td>Specifies the MD index value.</td>
</tr>
<tr>
<td>AssociationIndex</td>
<td>Specifies the MA index value.</td>
</tr>
<tr>
<td>Index</td>
<td>Specifies the Maintenance Endpoint index value.</td>
</tr>
<tr>
<td>DomainName</td>
<td>Specifies the MD name.</td>
</tr>
<tr>
<td>AssociationName</td>
<td>Specifies the MA name.</td>
</tr>
<tr>
<td>DestMacAddress</td>
<td>Specifies the remote MAC address to reach the MEP/MIP.</td>
</tr>
</tbody>
</table>

**Table continues…**
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages</td>
<td>Specifies the number of loopback messages to be transmitted. The default is 1.</td>
</tr>
<tr>
<td>VlanPriority</td>
<td>Specifies the priority. The default is 7.</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>Specifies the transaction identifier/sequence number of the first loopback message (to be) sent. The default is 0.</td>
</tr>
<tr>
<td>ResultOk</td>
<td>Indicates the result of the operation:</td>
</tr>
<tr>
<td></td>
<td>• true: The Loopback Messages will be (or have been) sent.</td>
</tr>
<tr>
<td></td>
<td>• false: The Loopback Messages will not be sent.</td>
</tr>
<tr>
<td></td>
<td>The default is true.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the status of the transmit loopback service:</td>
</tr>
<tr>
<td></td>
<td>• ready: The service is available.</td>
</tr>
<tr>
<td></td>
<td>• transmit: The service is transmitting, or about to transmit, the Loopback messages.</td>
</tr>
<tr>
<td></td>
<td>• abort: The service is aborted or about to abort the Loopback messages.</td>
</tr>
<tr>
<td></td>
<td>The default is ready.</td>
</tr>
<tr>
<td>Result</td>
<td>Displays the LBM result.</td>
</tr>
<tr>
<td>TimeoutInt</td>
<td>Specifies the timeout interval in seconds. The default value is 3 seconds.</td>
</tr>
<tr>
<td>InterFrameInt</td>
<td>Specifies the interval between LBM frames with a range of (0..1000) msecs and a default value of 500 msecs. The value of 0 msecs indicates to send the frames as fast as possible. The default is 500.</td>
</tr>
<tr>
<td>TestPattern</td>
<td>Specifies the testfill pattern:</td>
</tr>
<tr>
<td></td>
<td>• allZero — null signal without cyclic redundancy check</td>
</tr>
<tr>
<td></td>
<td>• allZeroCrc — null signal with cyclic redundancy check with 32-bit polynomial</td>
</tr>
<tr>
<td></td>
<td>• pseudoRandomBitSequence — pseudo-random-bit-sequence without cyclic redundancy check</td>
</tr>
<tr>
<td></td>
<td>• pseudoRandomBitSequenceCrc — pseudo-random-bit-sequence with cyclic redundancy check with 32-bit polynomial.</td>
</tr>
<tr>
<td></td>
<td>A cyclic redundancy check is a code that detects errors. The default value is allZero.</td>
</tr>
<tr>
<td>DataSize</td>
<td>Specifies the data type-length-value (TLV) size. The default is 0.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FrameSize</td>
<td>Specifies the frame-size. The default is 0.</td>
</tr>
<tr>
<td>Sourcemode</td>
<td>Specifies the source mode of the transmit loopback service:</td>
</tr>
<tr>
<td></td>
<td>• nodal</td>
</tr>
<tr>
<td></td>
<td>• noVlanMac — Use this value with C-VLAN only. When you select this option, even if a VLAN MAC address exists, the system uses the CFM C-MAC as the BMAC-SA.</td>
</tr>
<tr>
<td></td>
<td>• smltVirtual — Use the smltVirtual option with B-VLANs only.</td>
</tr>
<tr>
<td></td>
<td>The default is nodal.</td>
</tr>
</tbody>
</table>

**Triggering linktrace**

Use the following procedure to trigger a linktrace. The link trace message is often compared to traceroute. An MEP transmits the Linktrace Message packet to a maintenance endpoint with intermediate points responding to indicate the path of the traffic within a domain for the purpose of fault isolation. The packet specifies the target MAC address of an MP, which is the SPBM system ID or the virtual SMLT MAC. MPs on the path to the target address respond with an LTR.

**Before you begin**

- On the source and destination nodes, you must configure a CFM MD, MA, and MEP.
- Enable the MEP.
- Assign a nodal MEP to the B-VLAN.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **CFM**.
3. Click the **LTM** tab.
4. Configure the linktrace test properties as required.
5. Click **Apply**.
6. To trigger the linktrace test, double-click in the Status field, select **transmit**, and then click **Apply**.
   OR
   Highlight an entry, and then click **Start**.
7. To update the linktrace, click the **Refresh** button.
8. To stop the linktrace, click **Stop**.
9. To view the results of the linktrace, click **Result**.
# LTM field descriptions

Use the data in the following table to use the LTM tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainIndex</td>
<td>Specifies the MD index value.</td>
</tr>
<tr>
<td>AssociationIndex</td>
<td>Specifies the MA index value.</td>
</tr>
<tr>
<td>Index</td>
<td>Specifies the MEP index value.</td>
</tr>
<tr>
<td>DomainName</td>
<td>Specifies the MD name.</td>
</tr>
<tr>
<td>AssociationName</td>
<td>Specifies the MA name.</td>
</tr>
<tr>
<td>VlanPriority</td>
<td>Specifies the VLAN priority, a 3–bit value to be used in the VLAN tag, if present in the transmitted frame. The default is 7.</td>
</tr>
<tr>
<td>DestMacAddress</td>
<td>Specifies the remote MAC address to reach the MEP.</td>
</tr>
<tr>
<td>Ttl</td>
<td>Indicates the number of hops remaining to this LTM. This value is decremented by 1 by each bridge that handles the LTM. The decremented value is returned in the LTR. If the value is 0 on output, the LTM is not transmitted to the next hop. The value of the TTL field in the LTM is specified at the originating MEP. The default value is 64.</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>Specifies the transaction identifier/sequence number of the first loopback message (to be) sent. The default is 0.</td>
</tr>
<tr>
<td>ResultOk</td>
<td>Indicates the result of the operation:</td>
</tr>
<tr>
<td></td>
<td>• true: The Loopback Messages will be (or have been) sent.</td>
</tr>
<tr>
<td></td>
<td>• false: The Loopback Messages will not be sent.</td>
</tr>
<tr>
<td></td>
<td>The default is true.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the status of the transmit loopback service:</td>
</tr>
<tr>
<td></td>
<td>• ready: The service is available.</td>
</tr>
<tr>
<td></td>
<td>• transmit: The service is transmitting, or about to transmit, the LTM messages.</td>
</tr>
<tr>
<td></td>
<td>• abort: The service is aborted, or about to abort, the LTM message.</td>
</tr>
<tr>
<td></td>
<td>The default is ready.</td>
</tr>
<tr>
<td>Flag</td>
<td>Displays the LTM result flag indicating LTM status or error code. Each value represents a status or error case:</td>
</tr>
<tr>
<td></td>
<td>• 1 - No error</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 - LTM internal error</td>
<td></td>
</tr>
<tr>
<td>3 - Unknown Remote Maintenance Endpoint</td>
<td></td>
</tr>
<tr>
<td>4 - Invalid Remote Maintenance Endpoint MAC Address</td>
<td></td>
</tr>
<tr>
<td>5 - Unset Remote Maintenance Endpoint MAC address</td>
<td></td>
</tr>
<tr>
<td>6 - MEP must be enabled in order to perform LTM</td>
<td></td>
</tr>
<tr>
<td>7 - No LTR response received</td>
<td></td>
</tr>
<tr>
<td>8 - Linktrace to own MEP MAC is not sent</td>
<td></td>
</tr>
<tr>
<td>9 - Endpoint must be enabled in order to perform LTM</td>
<td></td>
</tr>
<tr>
<td>10 - Pbt-trunk must be enabled in order to perform LTM</td>
<td></td>
</tr>
<tr>
<td>11 - LTM completed</td>
<td></td>
</tr>
<tr>
<td>12 - LTM leaf node</td>
<td></td>
</tr>
</tbody>
</table>

**SourceMode**

Specifies the source mode of the transmit loopback service:

- nodal
- noVlanMac — Use this value with C-VLAN only. When you select this option, even if a VLAN MAC address exists, the system uses the CFM C-MAC as the BMAC-SA.
- smltVirtual — Use the smltVirtual option with B-VLANs only.

The default is nodal.

## Viewing linktrace results

Use this procedure to view linktrace results.

**Note:**

After you trigger linktrace, you must click the **Refresh** button to update the results.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **CFM**.
3. Click the **LTM** tab.
4. Highlight an entry, and then click **Result**.
## Link Trace Replies field descriptions

Use the data in the following table to use the Link Trace Result tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainIndex</td>
<td>Indicates the Maintenance Domain Index.</td>
</tr>
<tr>
<td>AssociationIndex</td>
<td>Indicates the Maintenance Association Index.</td>
</tr>
<tr>
<td>MepId</td>
<td>Indicates the Maintenance EndPoint ID.</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>Indicates the transaction identifier/sequence number returned by a previous transmit linktrace message command, indicating which LTM response is going to be returned. The default is 0.</td>
</tr>
<tr>
<td>Hop</td>
<td>Indicates the number of hops away from the LTM initiator.</td>
</tr>
<tr>
<td>ReceiveOrder</td>
<td>Indicates the index value used to distinguish among multiple LTRs with the same LTR Transaction Identifier field value. This value is assigned sequentially from 1, in the order that the Linktrace Initiator received the LTRs.</td>
</tr>
<tr>
<td>Ttl</td>
<td>Indicates the TTL field value for a returned LTR.</td>
</tr>
<tr>
<td>DomainName</td>
<td>Indicates the Maintenance Domain Name.</td>
</tr>
<tr>
<td>AssociationName</td>
<td>Indicates the Maintenance Association Name.</td>
</tr>
<tr>
<td>Forwarded</td>
<td>Indicates if a LTM was forwarded by the responding MP, as returned in the FwdYes flag of the flags field.</td>
</tr>
<tr>
<td>TerminalMep</td>
<td>Displays a boolean value stating whether the forwarded LTM reached a MEP enclosing its MA, as returned in the Terminal MEP flag of the Flags field.</td>
</tr>
<tr>
<td>LastEgressIdentifier</td>
<td>Displays an octet field holding the Last Egress Identifier returned in the LTR Egress Identifier TLV of the LTR. The Last Egress Identifier identifies the MEP Linktrace Indicator that originated, or the Linktrace Responder that forwarded, the LTM to which this LTR is the response. This is the same value as the Egress Identifier TLV of that LTM.</td>
</tr>
<tr>
<td>NextEgressIdentifier</td>
<td>Displays an octet field holding the Next Egress Identifier returned in the LTR Egress Identifier TLV of the LTR. The Next Egress Identifier identifies the Linktrace Responder that transmitted this LTR, and can forward the LTM to the next hop. This is the same value as the Egress Identifier TLV of the forwarded LTM, if any. If the FwdYes bit of the Flags field is false, the contents of this field are undefined, and the field is ignored by the receiver.</td>
</tr>
<tr>
<td>RelayAction</td>
<td>Indicates the value returned in the RelayAction field.</td>
</tr>
</tbody>
</table>

*Table continues...*
### Configuring Layer 2 tracetree

Use this procedure to configure a Layer 2 Tracetree. This feature enables CFM to debug Layer 2. Layer 2 Tracetree allows a user to trigger a multicast LTM message by specifying the B-VLAN and I-SID. The command allows the user to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID.

**Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software*, NN47227-401. As an alternative, use the ACLI.

If you configure **IsTraceTree** to false then EDM performs Traceroute on the unicast path. If you configure **IsTraceTree** to true then EDM performs TraceTree on the multicast tree.

**Note:**

This command is supported on SPBM B-VLANs only, not C-VLANs.

**Before you begin**

- On the source and destination nodes, you must configure a CFM MD, MA, and MEP.
- Enable the MEP.
- Assign a nodal MEP to the B-VLAN.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **L2Ping/L2Trace Route**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcMac</td>
<td>Displays the MAC address of the MP that responded to the LTM request for this LTR.</td>
</tr>
<tr>
<td>IngressAction</td>
<td>Displays the value returned in the IngressAction Field of the LTM. The value ingNoTlv indicates that no Reply Ingress TLV was returned in the LTM.</td>
</tr>
<tr>
<td>IngressMac</td>
<td>Displays the MAC address returned in the ingress MAC address field. If the rcCfmLtrReplyIngress object contains the value ingNoTlv(5), then the contents of this field are meaningless.</td>
</tr>
<tr>
<td>EgressAction</td>
<td>Displays the value returned in the Egress Action Field of the LTM. The value egrNoTlv(5) indicates that no Reply Egress TLV was returned in the LTM.</td>
</tr>
<tr>
<td>EgressMac</td>
<td>Displays the MAC address returned in the egress MAC address field. If the rcCfmLtrReplyEgress object contains the value egrNoTlv(5), then the contents of this field are meaningless.</td>
</tr>
</tbody>
</table>
3. From the **L2 Traceroute/TraceTree** tab, configure the Layer 2 tracetree properties.

4. In the **IsTraceTree** field double-click and select **true** for EDM to perform Tracetree on the multicast tree.

5. Click **Apply**.

6. Click the **Refresh** button to update the results.

### L2Tracetree field descriptions

Use the data in the following table to use the **L2Tracetree** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VlanId</td>
<td>Identifies the Backbone VLAN.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies a 3–bit value to be used in the VLAN header, if present in the transmitted frame. The default is 7.</td>
</tr>
<tr>
<td>DestMacAddress</td>
<td>Specifies the target MAC address.</td>
</tr>
<tr>
<td>HostName</td>
<td>Specifies the target host name.</td>
</tr>
<tr>
<td>DestIsHostName</td>
<td>Indicates whether the host name is (true) or is not (false) used for L2Tracetree transmission.</td>
</tr>
<tr>
<td>Isid</td>
<td>Specifies the service instance identifier (I-SID).</td>
</tr>
<tr>
<td>IsTraceTree</td>
<td>Specifies whether the multicast tree or unicast path is traced. If you configure <strong>IsTraceTree</strong> to false then EDM performs Traceroute on the unicast path. If you configure <strong>IsTraceTree</strong> to true then EDM performs TraceTree on the multicast tree.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the status of the transmit loopback service:</td>
</tr>
<tr>
<td></td>
<td>• ready: the service is available.</td>
</tr>
<tr>
<td></td>
<td>• transmit: the service is transmitting, or about to transmit, the L2Tracetree messages.</td>
</tr>
<tr>
<td></td>
<td>• abort: the service aborted or is about to abort the L2Tracetree messages.</td>
</tr>
<tr>
<td></td>
<td>This field is also used to avoid concurrency or race condition problems that can occur if two or more management entities try to use the service at the same time.</td>
</tr>
<tr>
<td></td>
<td>The default is ready.</td>
</tr>
<tr>
<td>ResultOk</td>
<td>Indicates the result of the operation:</td>
</tr>
<tr>
<td></td>
<td>• true: the L2Tracetree Messages will be (or have been) sent.</td>
</tr>
<tr>
<td></td>
<td>• false: the L2Tracetree Messages will not be sent</td>
</tr>
<tr>
<td></td>
<td>The default is true.</td>
</tr>
</tbody>
</table>

*Table continues...*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ttl</strong></td>
<td>Specifies the Time-to-Live value. Indicates the number of hops remaining to this L2Tracetree. The tracetree is decremented by one by each bridge that handles the Layer 2 tracetree and the decremented value is returned to the tracetree. If the output is 0, then the L2Tracetree is not transmitted to the next hop. The value of the TTL field in the L2Tracetree is transmitted by the originating MEP is controlled by a managed object. The default is 64.</td>
</tr>
</tbody>
</table>
| **SourceMode** | Specifies the source mode of the transmit loopback service:  
  • nodal  
  • noVlanMac — Use this value with C-VLAN only. When you select this option, even if a VLAN MAC address exists, the system uses the CFM C-MAC as the BMAC-SA.  
  • smltVirtual — Use the smltVirtual option with B-VLANs only.  
  The default is nodal. |
| **SeqNumber** | The transaction identifier/sequence number of the first loopback message (to be) sent. The default is 0. |
| **Flag** | Specifies the L2Tracetree result flag, which indicates the L2Tracetree status or error code. Each sum represents a status or error:  
  • 1 — No error  
  • 2 — L2Tracetree internal error  
  • 3 — Invalid MAC address  
  • 4 — MEP must be enabled in order to perform L2Tracetree  
  • 5 — No L2Tracetree response received  
  • 6 — L2Tracetree to own MEP MAC is not sent  
  • 7 — L2Tracetree completed  
  • 8 — Lookup failure for L2Tracetree  
  • 9 — On a leaf node in the I-SID tree  
  • 10 — Not in the I-SID tree  
  • 11 — Requested SMLT source from nonprimary node |
Viewing Layer 2 tracetree results

Use this procedure to view Layer 2 Tracetree results. The Layer 2 Tracetree command is a proprietary command that allows a user to trigger a multicast LTM message by specifying the B-VLAN and I-SID. This command allows the user to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID.

**Note:**

In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. For more information, see *Release Notes for VSP Operating System Software*, NN47227-401. As an alternative, use the ACLI.

**Procedure**

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. Click the **L2 Traceroute/TraceTree** tab.
4. In the **IsTraceTree** field double-click and select **true** for EDM to perform Tracetree on the multicast tree.
5. Click **Apply**.
6. Click the **Refresh** button to update the results.
7. To view the tracetree results, highlight an entry, and then click **Result**.

**L2 Traceroute/Tracetree Result field descriptions**

Use the data in the following table to use the **L2 Traceroute/Tracetree Result** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VlanId</td>
<td>A value that uniquely identifies the Backbone VLAN (B-VLAN).</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>The transaction identifier/sequence number returned by a previous transmit linktrace message command, that indicates which response of the L2Tracetree is going to be returned. The default is 0.</td>
</tr>
<tr>
<td>Hop</td>
<td>The number of hops away from L2Tracetree initiator.</td>
</tr>
<tr>
<td>ReceiveOrder</td>
<td>An index to distinguish among multiple L2Tracetree responses with the same Transaction Identifier field value. This value is assigned sequentially from 1, in the order that the Linktrace Initiator received the responses.</td>
</tr>
<tr>
<td>Ttl</td>
<td>Time-to-Live (TTL) field value for a returned L2Tracetree response.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcMac</td>
<td>MAC address of the MP that responds to the L2Tracetree request for this L2tractreeReply.</td>
</tr>
<tr>
<td>HostName</td>
<td>The host name of the replying node.</td>
</tr>
<tr>
<td>LastSrcMac</td>
<td>The MAC address of the node that forwarded the L2Tracetree to the responding node.</td>
</tr>
<tr>
<td>LastHostName</td>
<td>The host name of the node that forwarded the L2Tracetree to the responding node.</td>
</tr>
</tbody>
</table>

### Configuring Layer 2 trace multicast route on a VLAN

Use this procedure to configure the Layer 2 tracemroute on the VLAN (Layer 2). This procedure queries the SPBM multicast module to determine the B-VLAN, I-SID, and nickname for the S and G streams. The nickname and I-SID are used to create a multicast MAC address.

**Note:**

- In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) are not supported in EDM. As an alternative, use the command line interface.
- If you want to run a Layer 2 tracemroute on a VRF, make sure you are in the proper VRF context.

### Before you begin

On the source and destination nodes, you must configure a CFM MD, MA, and MEP, and assign a nodal MEP to the B-VLAN.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration > Edit > Diagnostics > L2Ping/L2Trace Route**.
2. Click the **L2MCAST Traceroute** tab.
3. Click **Insert** to insert the L2 MCAST Traceroute.
4. Enter the **SrcIpAddr**.
5. Enter the **GroupIpAddr**.
6. Enter the **ServiceType**. If you want to perform a Layer 2 tracemroute on a VLAN, select **vlan**. If you want to perform a Layer 2 tracemroute on a Layer 3 GRT, select **vrfid**.
   **Note:**
   If you want to perform a Layer 2 tracemroute on a Layer 2 or a Layer 3 VRF, review the following procedure **Configuring Layer 2 tracemroute on a VRF** on page 216.
7. In the **ServiceId**field, enter the VLAN ID.
8. Enter the **Priority**.
9. Enter the **Ttl** value.
10. Click **Insert**.
11. Click **Apply** to save your changes.
12. To start the Layer 2 tracemoute, set the Status to transmit and click **Start**.
13. Update the Layer 2 tracemroute by clicking **Refresh**.
14. To stop the Layer 2 tracemroute, click **Stop**.
15. To see the result, click **Result**.

**L2 MCAST Traceroute field descriptions**

Use the data in the following table to use the L2MCAST Traceroute tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SrcIpAddrType</strong></td>
<td>Specifies the source IP address type as IPv4.</td>
</tr>
<tr>
<td><strong>SrcIpAddr</strong></td>
<td>Specifies the source IP address of the flow where the multicast trace tree originates.</td>
</tr>
<tr>
<td><strong>GroupIpAddrType</strong></td>
<td>Specifies the group IP address type as IPv4.</td>
</tr>
<tr>
<td><strong>GroupIpAddr</strong></td>
<td>Specifies the group IP address.</td>
</tr>
<tr>
<td><strong>ServiceType</strong></td>
<td>Specifies where you configure the Layer 2 tracemroute. This is either VLAN or VRF.</td>
</tr>
<tr>
<td><strong>VRFName</strong></td>
<td>Specifies the VRF name.</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Specifies the priority value. The value is between 0 and 7.</td>
</tr>
<tr>
<td><strong>Ttl</strong></td>
<td>Specifies the returned trace response. The TTL value is between 1 and 255.</td>
</tr>
<tr>
<td><strong>SeqNumber</strong></td>
<td>Specifies the transaction identifier/sequence number of the first message to be sent.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Specifies the status of the transmit loopback service:</td>
</tr>
<tr>
<td></td>
<td>• ready: Specifies the service is available.</td>
</tr>
<tr>
<td></td>
<td>• transmit: Specifies the service is transmitting, or about to transmit the trace messages.</td>
</tr>
<tr>
<td></td>
<td>• abort: Specifies the services is aborted or about to abort the trace messages.</td>
</tr>
<tr>
<td></td>
<td>The column will also be used to avoid concurrency or race condition problems that can occur if two or more management entities try to use the service at the same time.</td>
</tr>
<tr>
<td><strong>ResultOK</strong></td>
<td>Specifies the result of the operation:</td>
</tr>
<tr>
<td></td>
<td>• true: The trace messages will be or have been sent.</td>
</tr>
<tr>
<td></td>
<td>• false: The trace messages will not be sent.</td>
</tr>
</tbody>
</table>

Table continues…
### Configuring Layer 2 tracemroute on a VRF

Use this procedure to configure the Layer 2 tracemroute on the VRF (Layer 3). This procedure queries the SPBM multicast module to determine the B-VLAN, I-SID and nickname for the S and G streams. The nickname and I-SID are used to create a multicast MAC address.

**Note:**
- In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. As an alternative, use the ACLI.
- If you want to run a Layer 2 tracemroute on a VRF, make sure you are in the proper VRF context.

See the following procedure to perform a Layer 3 tracemroute on a VLAN [Configuring Layer 2 tracemroute on a VLAN](#) on page 214.

**Before you begin**

On the source and destination nodes, you must configure a CFM MD, MA, and MEP, and assign a nodal MEP to the B-VLAN.

**Procedure**

1. In the navigation pane, expand the following folders: `Configuration > VRF Context View > Set VRF Context View`
2. Select a VRF and click the `Launch VRF Context View` tab.
3. In the navigation pane, expand the following folders:`Configuration > Edit > Diagnostics > L2Ping/L2Trace Route`
4. Click the `L2MCAST Traceroute` tab.
5. Click `Insert` to insert the L2 MCAST tracemroute.
6. Enter the `SrcIpAddr`.
7. Enter the `GroupIpAddr`.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flag</td>
<td>Specifies the result flag indicating that the L2 trace status or error code. Each value represents a status or error case.</td>
</tr>
<tr>
<td></td>
<td>• 1 — No error</td>
</tr>
<tr>
<td></td>
<td>• 2 — Internal Error</td>
</tr>
<tr>
<td></td>
<td>• 3 — Mep must be enabled to perform the trace</td>
</tr>
<tr>
<td></td>
<td>• 4 — No response received</td>
</tr>
<tr>
<td></td>
<td>• 5 — Trace completed</td>
</tr>
<tr>
<td></td>
<td>• 6 — On a leaf node in the I-SID tree</td>
</tr>
<tr>
<td></td>
<td>• 7 — No data I-SID was found for S, G</td>
</tr>
</tbody>
</table>
8. Enter the **ServiceType**. If you want to perform a Layer 2 tracemroute on a Layer 2 VRF, select **vlan**. If you want to perform a Layer 2 tracemroute on a Layer 3 VRF, select **vrid**.

9. In the **ServiceId**, enter the VLAN ID.

10. Enter the **Priority**.

11. Enter the **Ttl** value.

12. Click **Insert**.

13. Click **Apply** to save your changes.

14. To start the Layer 2 tracemoute, set the **Status** to transmit and click **Start**.

15. Update the Layer 2 tracemroute by clicking **Refresh**.

16. To stop the Layer 2 tracemroute, click **Stop**.

17. To see the result, click **Result**.

**L2 MCAST Traceroute field descriptions**

Use the data in the following table to use the **L2MCAST Traceroute** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcIPAddrType</td>
<td>Specifies the source IP address type as IPv4.</td>
</tr>
<tr>
<td>SrcIPAddr</td>
<td>Specifies the source IP address of the flow where the multicast trace tree originates.</td>
</tr>
<tr>
<td>GroupIPAddrType</td>
<td>Specifies the group IP address type as IPv4.</td>
</tr>
<tr>
<td>GroupIPAddr</td>
<td>Specifies the group IP address.</td>
</tr>
<tr>
<td>ServiceType</td>
<td>Specifies where you configure the Layer 2 tracemroute. This is either VLAN or VRF.</td>
</tr>
<tr>
<td>VRFName</td>
<td>Specifies the VRF name.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the priority value. The value is between 0 and 7.</td>
</tr>
<tr>
<td>Ttl</td>
<td>Specifies the returned trace response. The TTL value is between 1 and 255.</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>Specifies the transaction identifier/sequence number of the first message to be sent.</td>
</tr>
</tbody>
</table>
| Status                | Specifies the status of the transmit loopback service:  
  * ready: Specifies the service is available.  
  * transmit: Specifies the service is transmitting, or about to transmit the trace messages.  
  * abort: Specifies the services is aborted or about to abort the trace messages.  

The column will also be used to avoid concurrency or race condition problems that can occur if two or more management entities try to use the service at the same time.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResultOK</td>
<td>Specifies the result of the operation:</td>
</tr>
<tr>
<td></td>
<td>• true: The trace messages will be or have been sent.</td>
</tr>
<tr>
<td></td>
<td>• false: The trace messages will not be sent.</td>
</tr>
<tr>
<td>Flag</td>
<td>Specifies the result flag indicating that the L2 trace status or error code.</td>
</tr>
<tr>
<td></td>
<td>Each value represents a status or error case.</td>
</tr>
<tr>
<td></td>
<td>• 1 — No error</td>
</tr>
<tr>
<td></td>
<td>• 2 — Internal Error</td>
</tr>
<tr>
<td></td>
<td>• 3 — Mep must be enabled to perform the trace</td>
</tr>
<tr>
<td></td>
<td>• 4 — No response received</td>
</tr>
<tr>
<td></td>
<td>• 5 — Trace completed</td>
</tr>
<tr>
<td></td>
<td>• 6 — On a leaf node in the I-SID tree</td>
</tr>
<tr>
<td></td>
<td>• 7 — No data I-SID was found for S, G</td>
</tr>
</tbody>
</table>

Viewing Layer 2 trace multicast route results

Use this procedure to view Layer 2 tracemroute results.

⚠️ Note:

- In the current release, troubleshooting using ping and traceroute (including Layer 2 ping and Layer 2 traceroute) is not supported on EDM. As an alternative, use the ACLI.
- If you want to run a Layer 2 tracemroute on a VRF, make sure you are in the proper VRF context.

Procedure

1. In the navigation pane, expand the following folders: **Configuration > Edit > Diagnostics > L2Ping/L2Trace Route**
2. Click the **L2 MCAST Traceroute** tab.
3. To view the CFMI2 trace multicast route results, highlight an entry and click **Result**.

L2tracemroute Result field descriptions

Use the data in the following table to use the **L2tracemroute Result** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VlanId</td>
<td>Specifies a value that uniquely identifies the C-VLAN.</td>
</tr>
<tr>
<td>SeqNumber</td>
<td>Specifies the transaction identifier/sequence number returned by a previous transmit linktrace message command. Indicates which l2 tracemroute response is going to be returned.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hop</td>
<td>Specifies the number of hops away from the l2 tracemroute initiator.</td>
</tr>
<tr>
<td>ReceiveOrder</td>
<td>Specifies an index to distinguish among multiple l2 tracemroute responses with the same transaction identifier field value. This value is assigned sequentially from 1, in the order that the linktrace initiator received the responses.</td>
</tr>
<tr>
<td>Ttl</td>
<td>Specifies the TTL value for a returned l2 tracemroute response.</td>
</tr>
<tr>
<td>SrcMac</td>
<td>Specifies the MAC address of the MP that responds to the l2 tracemroute request for this l2 tracemrouteReply.</td>
</tr>
<tr>
<td>HostName</td>
<td>Specifies the host name of the replying node.</td>
</tr>
<tr>
<td>LastSrcMac</td>
<td>Specifies the MAC address of the node that forwarded the l2 tracemroute to the responding node.</td>
</tr>
<tr>
<td>LastHostName</td>
<td>Specifies the host name of the node that forwarded the l2 tracemroute to the responding node.</td>
</tr>
</tbody>
</table>

**CFM configuration example**

This section provides a configuration example for Connectivity Fault Management (CFM).

The following sections show the steps required to configure CFM.

**VSP4000 A**

```
MAINTENANCE-DOMAIN CONFIGURATION

cfm maintenance-domain "spbm" index 1 maintenance-level 6
```

```
MAINTENANCE-ASSOCIATION CONFIGURATION

cfm maintenance-association "spbm" "2" index 1

cfm maintenance-association "spbm" "3" index 2
```

```
MAINTENANCE-ENDPOINT CONFIGUARATION

cfm maintenance-endpoint "spbm" "2" 1 state enable

cfm maintenance-endpoint "spbm" "3" 1 state enable
```

```
VLAN NODAL MEP/MIP CONFIGURATION

vlan nodal-mep 2 spbm 2 1
vlan nodal-mip-level 2 6
vlan nodal-mep 3 spbm 3 1
vlan nodal-mip-level 3 6
```
VSP4000 B

MAINTENANCE-DOMAIN CONFIGURATION

cfm maintenance-domain spbm index 1 maintenance-level 6

MAINTENANCE-ASSOCIATION CONFIGURATION

cfm maintenance-association "spbm" "2" index 1
cfm maintenance-association "spbm" "3" index 2

MAINTENANCE-ENDPOINT CONFIGURATION

cfm maintenance-endpoint "spbm" "2" 2 state enable
cfm maintenance-endpoint "spbm" "3" 2 state enable

VLAN NODAL MEP/MIP CONFIGURATION

vlan nodal-mep 2 spbm 2 2
vlan nodal-mip-level 2 6
vlan nodal-mep 3 spbm 3 2
vlan nodal-mip-level 3 6

CFM sample output

The following sections show sample CFM output.

L2ping can use the system ID or the router name. The example below shows a case where the VLAN and MAC are given.

show isis adjacencies

VSP-4850GTS# show isis adjacencies

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>IP ADDR</th>
<th>L STATE</th>
<th>UPTIME</th>
<th>PRI</th>
<th>HOLDTIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port1/3</td>
<td>44.17.10.33</td>
<td>1 UP</td>
<td>00:37:37</td>
<td>127</td>
<td>19</td>
</tr>
<tr>
<td>Port1/19</td>
<td>44.17.10.36</td>
<td>1 UP</td>
<td>1d 05:09:16</td>
<td>127</td>
<td>21</td>
</tr>
</tbody>
</table>

2 out of 2 interfaces have formed an adjacency

l2 ping

VSP-4850GTS# l2 ping vlan 500 mac 00.14.0d.bf.a3.df

Please wait for l2ping to complete or press any key to abort

L2 PING Statistics---- 0(68) bytes of data
1 packets transmitted, 0 packets received, 100.00% packet loss

l2 ping

VSP-4850GTS# l2 ping vlan 500 routernodename VSP-MONTIO
Please wait for l2ping to complete or press any key to abort

-----00:14:0d:a2:b3:df    L2 PING Statistics-----  0(68) bytes of data
1 packets transmitted, 1 packets received, 0.00% packet loss
  round-trip (us)    min/max/ave/stdv = 26895/26895/26895.00/ 0.00

l2 traceroute

VSP-4850GTS# l2 traceroute vlan 500 routernodename VSP-MONTI0

Please wait for l2traceroute to complete or press any key to abort

l2traceroute to VSP-MONTI0 (00:14:0d:a2:b3:df), vlan 500
0   VSP-PETER4  (00:15:9b:11:33:df)
1   VSP-MONTI0  (00:14:0d:a2:b3:df)

l2 tracetree

VSP-4850GTS# l2 tracetree 500 1

Please wait for l2tracetree to complete or press any key to abort

l2tracetree to 53:55:10:00:00:01, vlan 500 i-sid 1 nickname 5.55.10 hops 64
1   VSP-PETER4  00:15:9b:11:33:df -> VSP-MONTI0  00:14:0d:a2:b3:df
2   VSP-MONTI0  00:14:0d:a2:b3:df -> VSP-LEE2   00:15:e8:b8:a3:df

L2ping and L2traceroute can also be used with an IP address. The following outputs show examples using an IP address.

l2 ping

VSP-4850GTS# l2 ping ip-address 10.1.1.1

Please wait for l2ping to complete or press any key to abort

L2 PING Statistics : IP 10.1.1.1, paths found 1, paths attempted 1
================================================================================
TX    RX    PERCENT  ROUND TRIP TIME
VLAN NEXT HOP                               PKTS  PKTS  LOSS     MIN/MAX/AVE (us)
================================================================================
500  VSP-SHAMIM        (00:1a:8f:08:53:df)  1     0     100.00%  0/0/0.00

l2 traceroute

VSP-4850GTS# l2 traceroute ip-address 10.1.1.1

Please wait for l2trace to complete or press any key to abort

L2 Trace Statistics : IP 10.1.1.1, paths found 1
================================================================================
VSP-SHAMIM (00:1a:8f:08:53:df), vlan 500
0   VSP-PETER4  (00:15:9b:11:33:df)
1   VSP-MONTI0  (00:14:0d:a2:b3:df)

show cfm maintenance-domain

VSP-4850GTS#show cfm maintenance-domain
================================================================================
Maintenance Domain
================================================================================
Domain Name  Domain Index  Level Domain Type
================================================================================

show cfm maintenance-association

VSP-4850GTS#show cfm maintenance-association

Maintenance Association Status

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Assn Name</th>
<th>Domain Idx</th>
<th>Assn Idx</th>
</tr>
</thead>
<tbody>
<tr>
<td>md1</td>
<td>ma1</td>
<td>1</td>
<td>98</td>
</tr>
</tbody>
</table>

Total number of Maintenance Association entries: 1.

Maintenance Association config

Domain Name Assn Name
md1 ma1

Total number of MA entries: 1.

show cfm maintenance-endpoint

VSP-4850GTS#show cfm maintenance-endpoint

Maintenance Endpoint Config

<table>
<thead>
<tr>
<th>DOMAIN NAME</th>
<th>ASSN NAME</th>
<th>MEP ID</th>
<th>ADMIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>md1</td>
<td>ma1</td>
<td>1</td>
<td>enable</td>
</tr>
</tbody>
</table>

Total number of MEP entries: 1.

Maintenance Endpoint Service

<table>
<thead>
<tr>
<th>DOMAIN_NAME</th>
<th>ASSN_NAME</th>
<th>MEP_ID</th>
<th>TYPE</th>
<th>SERVICE_DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>md1</td>
<td>ma1</td>
<td>1</td>
<td>unused</td>
<td></td>
</tr>
</tbody>
</table>

Total number of MEP entries: 1.

show vlan nodal-mep

VSP-4850GTS#show vlan nodal-mep

Vlan Nodal Mep

<table>
<thead>
<tr>
<th>VLAN_ID</th>
<th>DOMAIN_NAME.ASSN_NAME.MEP_ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>md1.ma1.1</td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>
show vlan nodal-mip-level

VSP-4850GTS#show vlan nodal-mip-level

================================================================================
Vlan Nodal Mip Level
================================================================================
VLAN_ID    NODAL_MIP_LEVEL_LIST
--------------------------------------------------------------------------------
1
2
3
4          6
5
6
7
8
9
10
11
12
13
14
This section describes troubleshooting for Layer 4 to 7 applications.

**Troubleshooting SNMP**

**About this task**

Troubleshoot Simple Network Management Protocol (SNMP) if the network management station (NMS) does not receive traps.

Verify the management configurations for the management station. Also verify the management station setup. If the management station can reach a device but not receive traps, verify the trap configurations (that is, the trap destination address and the traps to be sent).

If you enable enhanced secure mode, the VSP switch does not support the default SNMPv1 and default SNMPv2 community strings, and default SNMPv3 user name. The individual in the administrator access level role can configure a non-default value for the community strings, and the VSP switch can continue to support SNMPv1 and SNMPv2. The individual in the administrator access level role can also configure a non-default value for the SNMPv3 user name and the VSP switch can continue to support SNMPv3. If you disable enhanced secure mode, the SNMPv1 and SNMPv2 support for community strings remains the same, and the default SNMPv3 user name remains the same. Enhanced secure mode is disabled by default.

**Procedure**

1. From the NMS, ping the IP address for the switch. If you can ping successfully, the IP address is valid and you may have a problem with the SNMP setup.

   If you cannot ping the switch, you have a problem with either the path or the IP address.

2. Telnet to the switch.

   If you can Telnet, the switch IP address is correct.

3. If Telnet does not work, connect to the console port using a serial line connection and ensure that the IP address configuration is correct.

4. If the management station is on a separate subnet, make sure that the gateway address and subnet mask are correct.

5. Using a management application, perform an SNMP Get request and an SNMP Set request (that is, try to poll the device or change a configuration using management software).
6. If you cannot reach the device using SNMP, access the console port, and then ensure that the SNMP community strings and traps are correct.

7. Use sniffer traces to verify that the switch receives the poll.

8. Use sniffer traces to verify that the NMS receives the response.

9. Verify that the data in the response is the data that was requested.

---

**Troubleshooting DHCP**

**About this task**

Perform this procedure to troubleshoot the following Dynamic Host Configuration Protocol (DHCP) scenarios:

- The client cannot obtain a DHCP address when in the same subnet.
- The client cannot obtain a DHCP address when in a different subnet.

When the DHCP server and client are on the different subnets or VLANs, you must configure the device as a DHCP relay agent. The device must forward DHCP requests to the DHCP server. You must perform extra troubleshooting steps to troubleshoot the DHCP relay agent.

**Procedure**

1. Check the physical connectivity between the DHCP client and server.

2. Verify network connectivity by configuring a static IP address on a client workstation.
   
   If the workstation still cannot reach the network, the problem is not DHCP. Start troubleshooting network connectivity.

3. Attempt to obtain an IP address from the DHCP server by manually forcing the client to send a DHCP request.
   
   If the client obtains an IP address after the PC startup is complete, the issue is not the DHCP server.

4. Obtain an IP address on the same subnet or VLAN as the DHCP server.
   
   If the issue persists, the problem may be with the DHCP server. If DHCP is working on the same subnet or VLAN as the DHCP server, the DHCP issue can be with the DHCP relay agent.

5. Confirm the DHCP relay agent configuration is correct.

6. Obtain sniffer traces where the traffic ingresses and egresses the switch and also on the client side of the network.

7. Check the logs on the switch for errors such as size exceeded or incorrect packet format.
Troubleshooting DHCP Relay

Before you begin
- Configure the server to reply to the client subnet. Check the server configuration file to verify the configuration.
- Configure a route on the server for the client subnet to create a path on which to send replies.

About this task
Perform this procedure to troubleshoot the DHCP relay agent.

Procedure
1. Verify that the interfaces that link the client and server are up, and that the ports are in the forwarding state.
   a. To verify client availability, you can configure a temporary static IP address on the client, and then use the `ping` command.
      
      ```
      ping WORD<0-256>
      ```
   b. To verify the port is in the forwarding state, use the following command for the slot and port number:
      
      ```
      show spanning-tree \[rstp|mstp\] port role [{slot/port[-slot/port] [,...]}]
      ```
      
      If STP detects loops in the configuration, it blocks ports to avoid flooding in the network. In this situation, the port is not in the forwarding state.

2. Ensure that DHCP is enabled on the client interface and that a valid forwarding path exists and is enabled. Ensure the server is reachable.

3. View the statistics counters for the relay.

4. If request or reply counters do not increase, use a sniffer tool to ensure that the client sends the packets, and that the interface module receives the packets.
   You can configure mirroring for the ingress port to verify if the packets reach the module.
   a. If the client sends the packets, check that the packets reach the CPP and search the trace results for the ingress port:
      
      ```
      trace level 9 3
      trace grep WORD<0-128>
      ```
   b. If the packets reach the CPP, check that they reach the DHCP protocol; check for errors or packet drop messages:
      
      ```
      trace level 170 3
      trace grep WORD<0-128>
      ```

5. If Option 82 is enabled, check the statistic counters for dropped packets, and perform a trace for the DHCP protocol:
**Example**

VSP-4850GTS-PWR+:1# ping 47.16.10.31

VSP-4850GTS-PWR+:1:# show spanning-tree mstp port role

<table>
<thead>
<tr>
<th>Port-Index</th>
<th>Port-Role</th>
<th>Port-State</th>
<th>PortSTPStatus</th>
<th>PortOperStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Disabled</td>
<td>Forwarding</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/2</td>
<td>Disabled</td>
<td>Forwarding</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/3</td>
<td>Disabled</td>
<td>Discarding</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/4</td>
<td>Disabled</td>
<td>Discarding</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/5</td>
<td>Disabled</td>
<td>Forwarding</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/6</td>
<td>Disabled</td>
<td>Forwarding</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/7</td>
<td>Disabled</td>
<td>Forwarding</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/8</td>
<td>Disabled</td>
<td>Forwarding</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/9</td>
<td>Disabled</td>
<td>Discarding</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/10</td>
<td>Disabled</td>
<td>Discarding</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/11</td>
<td>Disabled</td>
<td>Discarding</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/12</td>
<td>Designated</td>
<td>Forwarding</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/13</td>
<td>Disabled</td>
<td>Forwarding</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/14</td>
<td>Disabled</td>
<td>Forwarding</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

--More-- (q = quit)

VSP-4850GTS-PWR+:1:# trace level 9 3

VSP-4850GTS-PWR+:1:# trace grep 00-1A-4B-8A-FB-6B

---

**Variable definitions**

Use the data in the following table to use the troubleshooting commands in this procedure.

**Table 38: Variable definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>{slot/port[-slot/port][,...]}</td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (1/1), a range ports (1/2-1/4), or a series of ports (1/2,1/3).</td>
</tr>
<tr>
<td>WORD&lt;0-128&gt;</td>
<td>Specifies the text string to use as the search criterion.</td>
</tr>
<tr>
<td>WORD&lt;0-256&gt;</td>
<td>Specifies the IP address.</td>
</tr>
</tbody>
</table>
Troubleshooting client connection to the DHCP server

About this task
Perform this procedure if the client cannot reach the DHCP server.

Procedure
1. Check that the DHCP relay agent in the network switch is correctly configured.
2. Check that the DHCP server configuration is correct.
3. Check for routing issues.
   The routing in the network may not be configured so that DHCP request and reply packets are propagated. You can use ping and traceroute.
4. Check that the DHCP pools are correctly configured.
5. If the client cannot reach the server because the link is down, enable auto-negotiation on the link.

Troubleshooting IPv6 DHCP Relay

The following sections provide troubleshooting information for IPv6 DHCP Relay.

IPv6 DHCP Relay switch side troubleshooting

With DHCP Relay, the switch only participates in forwarding the requests and replies to and from the client and the DHCP server. The switch always acts as the relay agent, on which you configure the forward path to the server.

To troubleshoot DHCP Relay issues on the switch, use the following procedure.

Procedure
1. Verify that the DHCP server is reachable using ping. If ping is working and the DHCP server is reachable, DHCP should work.
2. Verify that the relay agents and the forward path configured are reachable. Ping the server and the gateway to the server.
3. Check that the relay agent configurations are correct. Also verify that DHCP is enabled on the switch:
   show ipv6 dhcp-relay interface {gigabitEthernet {slot/port[/sub-port][=-slot/port[/sub-port]][,...]}|vlan <1-4059>
4. Verify that IPv6 forwarding is enabled globally:
show ipv6 global

5. Verify that the IPv6 based VLAN where the DHCP relay agent is configured is enabled:
   show ipv6 interface vlan <1-4059>

6. In a scenario with VRRP and SMLT, configure VRRP IP as the DHCP relay agent.

7. When using the VRRP VRID as the relay agent, make sure the VRRP configurations are proper.

8. To verify that relay forward and relay receive are working, enable trace for DHCP with IPv6, and grep trace for relay:
   trace level 66 3
   trace grep relay
   trace screen enable

9. Display the count of DHCP Relay requests and replies to verify the system received requests and replies:
   show ipv6 dhcp-relay counters

---

IPv6 DHCP Relay server side troubleshooting

Use the following procedure to troubleshoot IPv6 DHCP Relay on the server side.

**Procedure**

1. Enable the services on the server side, and then create an IP pool.
   The IP pool must contain the range of addresses that you want to assign to the clients.
   Configure the IP pool with the same network subnet as that of the relay agent.

2. When the configuration is complete, initiate a DHCP request from a client.

3. Check the log file available on the server to verify the reason for packet drop.

4. Capture the packets on the server side using Ethereal.

5. From the server side, use ping to verify that the relay agent address is reachable.
   Ensure that a route to the relay is configured.

6. For more configuration aspects, see the Microsoft webpage for troubleshooting and configuration issues.

**Note:**
You can receive some log messages that indicate the system cannot forward packets.
However, certain situations are not DHCP failures.
Example 1: if you receive the message 0x00108796 (relayMsgSend): cannot find route entry for destination on the console, you must ping the server. If the server is not reachable, the system cannot forward the packet. This is not a DHCP issue.

Example 2: if you receive the message 0x00108705 this indicates a problem at the transmission level. Check the server reachability and ensure that MAC learning is correct before you pursue DHCP issues.

IPv6 DHCP Relay client side troubleshooting

You can collect a client console dump, which can be used to analyze why the received packet cannot be processed and the allocated address cannot be used by the client.

In addition, restarting the client can also fix the issue in some cases.

Make sure the client supports IPv6 requests.

Connect the server directly to the client. If the IP is assigned, then the problem is with the relay.

Enabling trace messages for IPv6 DHCP Relay

Use this procedure to enable trace for IPv6 DHCP Relay and enable IPv6 forwarding trace.

Procedure

1. Enter Privileged EXEC mode:
   
   enable

2. To troubleshoot IPv6 DHCP Relay, you can enable rcip6 trace messages using the following command:

   trace level 66 3

3. You can also enable IPv6 forwarding trace using the following command:

   trace ipv6 forwarding enable <all|debug|error|info|pkt|warn>

Example

Enable rcip6 trace messages and enable IPv6 forwarding trace:

Switch:1>enable
Switch:1#trace level 66 3
Switch:1#trace ipv6 forwarding enable
Troubleshooting IPv6 VRRP

The following sections describe troubleshooting information for IPv6 Virtual Router Redundancy Protocol (VRRP).

VRRP transitions

When a VRRP transition takes place with the backup taking over as the master, look for the following message in the syslog on the new master, as well as the old master. This message provides information to allow you to determine the cause of the transition.

IPv6 Vrrp State Transition Trap(Port/Vlan=200, Type=masterToInitialize, Cause=shutdownReceived, VrId=20,VrIpAddr=fe80:0:0:0:0:0:0:200, Addr=fe80:0:0:0:224:7fff:fe9d:1a03)

In this message, see the Type and Cause fields.

Note:

Although all of the possible causes and types are listed below, not all of the listed causes and types appear in the trap/log message.

The following table describes the VRRP transition types.

Table 39: Transition type

<table>
<thead>
<tr>
<th>Type value</th>
<th>Type definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>None</td>
</tr>
<tr>
<td>2</td>
<td>Master to backup</td>
</tr>
<tr>
<td>3</td>
<td>Backup to master</td>
</tr>
<tr>
<td>4</td>
<td>Initialize to master</td>
</tr>
<tr>
<td>5</td>
<td>Master to initialize</td>
</tr>
<tr>
<td>6</td>
<td>Initialize to backup</td>
</tr>
<tr>
<td>7</td>
<td>Backup to initialize</td>
</tr>
<tr>
<td>8</td>
<td>Backup to backup master</td>
</tr>
<tr>
<td>9</td>
<td>Backup master to backup</td>
</tr>
</tbody>
</table>

The following table describes the VRRP transition causes.

Table 40: Transition cause

<table>
<thead>
<tr>
<th>Cause value</th>
<th>Cause definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>None</td>
</tr>
</tbody>
</table>

Table continues...
<table>
<thead>
<tr>
<th>Cause value</th>
<th>Cause definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Higher priority advertisement received</td>
</tr>
<tr>
<td>3</td>
<td>Shutdown received</td>
</tr>
<tr>
<td>4</td>
<td>VRRP address and physical address match</td>
</tr>
<tr>
<td>5</td>
<td>Master down interval</td>
</tr>
<tr>
<td>6</td>
<td>Preemption</td>
</tr>
<tr>
<td>7</td>
<td>Critical IP goes down</td>
</tr>
<tr>
<td>8</td>
<td>User disabling VRRP</td>
</tr>
<tr>
<td>9</td>
<td>VRRP status synced from primary</td>
</tr>
<tr>
<td>10</td>
<td>IPv6 interface on which VRRP is configured goes down</td>
</tr>
<tr>
<td>11</td>
<td>Lower priority advertisement received</td>
</tr>
<tr>
<td>12</td>
<td>Advertisement received from higher interface IP address with equal priority</td>
</tr>
<tr>
<td>13</td>
<td>Advertisement received from lower interface IP address with equal priority</td>
</tr>
<tr>
<td>14</td>
<td>User enabled VRRP</td>
</tr>
<tr>
<td>15</td>
<td>Transition because of any other cause</td>
</tr>
</tbody>
</table>

---

**Enabling trace messages for IPv6 VRRP troubleshooting**

Use this procedure to enable trace messages for IPv6 VRRP.

When VRRP is enabled on two routing switches, the master-backup relationship forms with one router taking the responsibility of routing. If the master-backup relationship is not formed between the VRRP virtual routers, look for the following trace messages to ensure that the master is sending the advertisements correctly and the backup is processing them.

**Procedure**

1. Enter Privileged EXEC mode:
   ```
   enable
   ```

2. To troubleshoot IPv6 VRRP, you can enable RCIP6 trace messages with the command:
   ```
   trace level 66 3
   ```

3. And to provide additional trace information, you can also enable the following traces:
   ```
   trace ipv6 nd enable
   trace ipv6 base enable all
   trace ipv6 forwarding enable all
   trace ipv6 rtm enable all
   trace ipv6 transport enable all
   ```
4. When VRRP is enabled on two routing switches, the master-backup relationship forms with one router taking the responsibility of routing. If the master-backup relationship is not formed between the VRRP virtual routers, look for the following trace messages to ensure that the master is sending the advertisements correctly and the backup is processing them. On the master router, look for the following RCIP6 trace messages.

- tMainTask RCIP6: rcip6_vrrp.c: 5118: VRF name: GlobalRouter (VRF id 0): ipv6VrrpTic: Am Master for Vrid 200 on IfIndex 2053 Timer 1

If VRRP is enabled on the interface, this timer kicks off every second and shows the state for the VRID.


The preceding trace messages show that the VRRP master is sending the advertisements correctly at the end of advertisement interval for a VRID.

5. On the backup router, look for the following RCIP6 trace messages.

- tMainTask RCIP6: rcip6_vrrp.c: 5236: VRF name: GlobalRouter (VRF id 0): ipv6VrrpTic: Am Backup for VrId 200 on IfIndex 2052 Timer 1
- tMainTask RCIP6: rcip6_vrrp.c: 4854: ipv6VrrpIn: Vrid 200 on IfIndex 2052
- tMainTask RCIP6: rcip6_vrrp.c: 5545: VRF name: GlobalRouter (VRF id 0): rcIpVrrpProcessAdvt: Am backup for Vrid 200 on IfIndex 2052

The preceding trace messages show that the backup router is receiving the advertisements sent by the master and correctly processing them.

---

**Risks associated with enabling trace messages**

When traces are enabled on VRRP master, VrrpTic messages are logged for every second and any other configured traces keep displaying, so there is no guarantee that the backup will receive the advertisement from the master within 3 seconds, so it can transit to master also. There is also the risk of toggling of VRRP states (from backup to master and back again).

Enable the limited traces based on whichever is required.
VRRP with higher priority running as backup

The VRRP router with the higher priority can display as the backup for the following reasons:

- Hold-down timer is running.
- The configured Critical IP is not reachable or does not exist.

If the critical-IP is configured for VRRP master, and the critical interface goes down or is deleted, the master transitions to the backup state. In this case, the log shows the transition cause as 1 like many other cases.

If the holddown timer is configured for VRRP master, the holddown timer delays the preemption, giving the device, which is becoming the master enough time to construct routing tables.

Procedure

1. To determine that the issue is with the critical interface, look for the following trace message.
   
   tMainTask RCIP6: rcip6_vrrp.c: 5152: VRF name: GlobalRouter (VRF id 0): ipv6VrrpTic: Becoming backup for Vrid 200 on IfIndex 2052 because of invalid critical IP

2. If the holddown Timer is configured for VRRP master, the holddown timer delays the preemption, giving the device, which is becoming the master enough time to construct routing tables.
   
   tMainTask RCIP6: rcip6_vrrp.c: Enter in HoldDown processing, Vrid 200 LastRecvd 0 MasterDown 3, Holddown time remaining 970, Holddownstate 2

Downgrading or upgrading from releases that support different key sizes

Use this procedure if you need to downgrade or upgrade from a release that supports different key sizes.

Different releases can support different DSA host key, RSA host key, and DSA user key sizes. If you need to upgrade or downgrade to an earlier release that does not support the same key size, you must delete all of the keys from the .ssh directory and generate new keys for SSH. If you do not do this, key sizes that are no longer supported will no longer function.

For more information about supported software, see Release Notes for VSP Operating System Software, NN47227-401.

You only need to perform this procedure if you have previously generated DSA host, RSA host, or DSA user keys with a release that supports different key sizes.
Procedure

1. Use the following command to disable SSH:
   
   no ssh

2. From the config terminal go to the .ssh directory using the command:
   
   cd /intflash/.ssh

3. After you upgrade or downgrade, delete the following keys from the .ssh directory.

   ssh_dsa.key
   ssh_rsa.key
   moc_sshc_dsa_file
   moc_sshc_rsa_file
   id_dsa_rwa
   id_dsa_rwa.pub
   id_rsa_rwa
   id_rsa_rwa.pub
   moc_sshc_dsa_file_fed
   moc_sshc_rsa_file_fed
   known_hosts
   ssh_ecdsa.key
   dsa_key_<access level like rwa/rw/ro/admin/security/privilege/operator/auditor>,
   example: dsa_key_rwa
   rsa_key_<access level like rwa/rw/ro/admin/security/privilege/operator/auditor>,
   example: rsa_key_rwa

4. Generate a new DSA host key:
   
   ssh dsa-host-key [<1024–1024>]

5. Generate a new SSH DSA user key:
   
   ssh dsa-user-key WORD<1–15> [size <1024–1024>]

6. Generate a new RSA host key:
   
   ssh rsa-host-key [<1024–2048>]

Troubleshooting IPv6 connectivity loss

If the switch experiences loss of IPv6 connectivity, use the following procedure to troubleshoot the issue.

Procedure

1. Enter Global Configuration mode:
   
   enable

   configure terminal

2. Through the command line interface, make sure the required routes are in place and the corresponding neighbor entries are resolved (that is, in REACHABLE, PROBE, DELAY or STALE state).
3. INCOMPLETE neighbor state indicates a problem if the corresponding neighbor is used by some of the IPv6 routes. This applies to neighbor entries with link-local addresses.

Note:
Global addresses are not normally used as next hops. Having a global IPv6 neighbor entry as INCOMPLETE does not usually lead to a connectivity issue.

4. If the corresponding route is not in place then this is a routing issue. If the neighbor is not present or is INCOMPLETE, then further debugging is needed on the network level (that is, the state of other nodes needs to be examined).

5. Disabling and re-enabling IPv6 on the VLAN often recovers connectivity.

6. Display the RSMLT and MLT status:
   ```
   show ip rsmlt
   show mlt
   ```
   Make sure the RSMLT peer MAC is learned and the IST state is ist.

Troubleshooting TACACS+

The switch supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a remote authentication protocol that provides centralized validation of users who attempt to gain access to a router or network access server (NAS). The TACACS+ feature is disabled by default.

The current implementation of TACACS+ does not support:
- Earlier versions of TACACS
- Point-to-Point Protocol (PPP) authentication and accounting
- IPv6 addresses

TACACS+ is part of the Base Software License. For more information about licensing, see Administration for Avaya Virtual Services Platform 4000 Series, NN46251-600.

See the following sections to troubleshoot TACACS+.

Unable to log on using Telnet or rlogin

If you cannot log on using Telnet or rlogin, perform the following steps.

Procedure

1. Check whether the TACACS+ server is available or unreachable.
2. On the TACACS+ server, check whether you configured the privilege level correctly. On successful authorization, the TACACS+ server returns an access level to the switch for the
current user, which determines the user access privileges. The switch supports access levels 1 to 6 and access level 15.

The following table maps user accounts to TACACS+ privilege level.

<table>
<thead>
<tr>
<th>Switch access level</th>
<th>TACACS+ privilege level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>0</td>
<td>If the TACACS+ server returns an access level of 0, the user is denied access. You cannot log into the device if you have an access level of 0.</td>
</tr>
<tr>
<td>READ ONLY</td>
<td>1</td>
<td>Permits you to view only configuration and status information.</td>
</tr>
<tr>
<td>LAYER 1 READ WRITE</td>
<td>2</td>
<td>Permits you to view most of the switch configuration and status information and change physical port settings.</td>
</tr>
<tr>
<td>LAYER 2 READ WRITE</td>
<td>3</td>
<td>Permits you to view and change configuration and status information for Layer 2 (bridging and switching) functions.</td>
</tr>
<tr>
<td>LAYER 3 READ WRITE</td>
<td>4</td>
<td>Permits you to view and change configuration and status information for Layer 2 and Layer 3 (routing) functions.</td>
</tr>
<tr>
<td>READ WRITE</td>
<td>5</td>
<td>Permits you to view and change configuration and status information across the switch. This level does not allow you to change security and password settings.</td>
</tr>
<tr>
<td>READ WRITE ALL</td>
<td>6</td>
<td>Permits you to have all the rights of read-write access and the ability to change security settings, including Avaya command line interface (ACLI) and web-based management user names and passwords, and the SNMP community strings.</td>
</tr>
<tr>
<td>NONE</td>
<td>7 to 14</td>
<td>If the TACACS+ server returns an access level of 7 to 14, the user is denied access. You cannot log into the device if you have an access level of 7 to 14.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Switch access level</th>
<th>TACACS+ privilege level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>READ WRITE ALL</td>
<td>15</td>
<td>Permits you to have all the rights of read-write access and the ability to change security settings, including Avaya command line interface (ACLI) and Web-based management user names and passwords, and the SNMP community strings.</td>
</tr>
</tbody>
</table>

**Note:**
Access level 15 is internally mapped to access level 6, which ensures consistency with other vendor implementations. The switch does not differentiate between an access level of 6 and an access level of 15.

After you enable TACACS+ authorization, the current privilege-level to command mapping on the switch is no longer relevant because the TACACS+ server has complete responsibility for command authorization. TACACS+ authorization provides access to the system based on username, not based on privilege level.

**Note:**
If you want to switch to a privilege level 'X' using `tacacs switch level <1-15>` command, you must create a user "$enabX$" on the TACACS+ server. X is the privilege level that you want to change.

3. On the TACACS+ server, check whether you configured the password and user name correctly.
4. On the TACACS+ server, check whether you configured the switch IP address in the trust list.
5. Check whether you configured the encryption key, connection mode (single connection or per-session connection), and TCP port number the same on the TACACS+ server and switch.
6. If you can log on to the switch, check whether the TACACS+ server configured on the platform has the correct IP address:
   ```bash
   show tacacs
   ```
7. Use the output from the preceding step to verify whether the key field configured on the platform is the same as that on the TACACS+ server.
8. Also use the output from the `show tacacs` command to verify whether you configured the single connection option on the platform, and whether the TACACS+ server supports the single connection.

Example

Check whether the TACACS+ server configured on the platform has the correct IP address:

```sh
Switch:1>enable
Switch:1(config)#show tacacs

Global Status:
  global enable : false
  authentication enabled for : cli
  accounting enabled for : none
  authorization : disabled

User privilege levels set for command authorization : None

Server:

  create :

<table>
<thead>
<tr>
<th>Prio</th>
<th>Status</th>
<th>Key</th>
<th>Port</th>
<th>IP address</th>
<th>Timeout</th>
<th>Single</th>
<th>Source</th>
<th>SourceEnabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>NotConn</td>
<td>******</td>
<td>3</td>
<td>192.0.2.254</td>
<td>30</td>
<td>true</td>
<td>5.5.5.5</td>
<td>true</td>
</tr>
<tr>
<td>Backup</td>
<td>NotConn</td>
<td>******</td>
<td>47</td>
<td>198.51.100.1</td>
<td>10</td>
<td>false</td>
<td>0.0.0.0</td>
<td>false</td>
</tr>
</tbody>
</table>
```

Job aid

The following table describes the fields in the output for the `show tacacs` command.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Status</td>
<td></td>
</tr>
<tr>
<td>global enable</td>
<td>Displays if the TACACS+ feature is enabled globally.</td>
</tr>
<tr>
<td>authentication enabled for</td>
<td>Displays which application is authenticated by TACACS+. The possibilities are CLI, web, or all.</td>
</tr>
<tr>
<td>accounting enabled for</td>
<td>Displays if accounting is enabled. You can only enable accounting for CLI. By default, accounting is not enabled.</td>
</tr>
<tr>
<td>authorization</td>
<td>Displays if authorization is enabled.</td>
</tr>
<tr>
<td>User privilege levels set for command authorization</td>
<td>Displays the privilege levels set for command authorization. When you configure command authorization for a particular level, all commands that you execute are sent to the TACACS+ server for authorization. The device can only execute the commands the TACACS+ server authorizes.</td>
</tr>
<tr>
<td></td>
<td>The user privilege levels are:</td>
</tr>
<tr>
<td></td>
<td>• 0: denied access</td>
</tr>
</tbody>
</table>
### Name | Description
---|---
• 1: read only (ro) access
• 2: Layer 1 read and write (l1) access
• 3: Layer 2 read and write (l2) access
• 4: Layer 3 read and write (l3) access
• 5: read and write (rw) access
• 6: read and write all (rwa) access
• 7-14: denied access
• 15: read and write all (rwa) access

<table>
<thead>
<tr>
<th>Server</th>
<th>Displays the priority of the TACACS+ server. The switch attempts to use the primary server first, and the secondary server second.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays the connection status between the server and the switch – connected or not connected.</td>
</tr>
<tr>
<td>Key</td>
<td>Displays as ***** instead of the actual key. The key is secret and is not visible.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the TCP port used to establish the connection to the server. The default port is 49.</td>
</tr>
<tr>
<td>IP address</td>
<td>Displays the IP address for the primary and secondary TACACS+ servers.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Displays the period of time, in seconds, the switch waits for a response from the TACACS+ daemon before it times out and declares an error. The default is 10 seconds.</td>
</tr>
<tr>
<td>Single</td>
<td>Displays if a single open connection is maintained between the switch and TACACS+ daemon, or if the switch opens and closes the TCP connection to the TACACS+ daemon each time they communicate. The default is false, which means the device does not maintain the single open connection.</td>
</tr>
<tr>
<td>Source</td>
<td>Displays the fixed source IP address, if you configure one, for all outgoing TACACS+ packets.</td>
</tr>
<tr>
<td>SourceEnabled</td>
<td>Displays if the fixed source IP address is enabled for all outgoing TACACS+ packets.</td>
</tr>
</tbody>
</table>

---

**Unable to log on using SSH**

If you cannot log on using Secure Shell (SSH), perform the following steps.
**Procedure**

1. Verify that the network, the switch, and the TACACS+ server is reachable.
2. Verify whether you configured the SSH client correctly.
3. Verify whether you enabled and configured the SSH function correctly on the switch:
   ```
   show ssh global
   ```

**Example**

Verify whether you enabled and configured SSH function correctly on the switch:

```bash
Switch:1>enable
Switch:1#show ssh global
```

<table>
<thead>
<tr>
<th>Total Active Sessions</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>v2only</td>
</tr>
<tr>
<td>port</td>
<td>22</td>
</tr>
<tr>
<td>max-sessions</td>
<td>4</td>
</tr>
<tr>
<td>timeout</td>
<td>60</td>
</tr>
<tr>
<td>action rsa-keygen</td>
<td>rsa-keysize 2048</td>
</tr>
<tr>
<td>action dsa-keygen</td>
<td>dsa-keysize 2048</td>
</tr>
<tr>
<td>rsa-auth</td>
<td>true</td>
</tr>
<tr>
<td>dsa-auth</td>
<td>true</td>
</tr>
<tr>
<td>pass-auth</td>
<td>false</td>
</tr>
<tr>
<td>enable</td>
<td>true</td>
</tr>
</tbody>
</table>

**Job Aid**

The following table describes the fields in the output for the `show ssh global` command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total active sessions</td>
<td>Specifies the number of active SSH sessions underway.</td>
</tr>
<tr>
<td>version</td>
<td>Specifies if SSH is version 1 or version 2. The default is v2. Avaya recommends you configure the version to v2 only.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies the SSH connection port. The default is 22. You cannot configure the following TCP ports as SSH connection ports: 0 to 1024 (except port 22), 1100, 4095, 5000, 5111, 6000, or 999.</td>
</tr>
<tr>
<td>max-sessions</td>
<td>Specifies the maximum number of SSH sessions allowed. The default is 4.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the SSH connection authentication timeout in seconds. The default is 60 seconds.</td>
</tr>
<tr>
<td>action rsa-keygen</td>
<td>Specifies the SSH RSA key size.</td>
</tr>
<tr>
<td>action dsa-keygen</td>
<td>Specifies the SSH DSA key size.</td>
</tr>
<tr>
<td>rsa-auth</td>
<td>Specifies if RSA authentication is enabled or disabled. The default is enabled.</td>
</tr>
<tr>
<td>dsa-auth</td>
<td>Specifies if DSA authentication is enabled or disabled. The default is enabled.</td>
</tr>
</tbody>
</table>

*Table continues...*
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pass-auth</td>
<td>Specifies if password authentication is enabled or disabled. The default is enabled.</td>
</tr>
<tr>
<td>enable</td>
<td>Specifies if SSH secure mode is enabled. False is disabled. Secure is enabled.</td>
</tr>
</tbody>
</table>

---

**Unable to log on by any means (Telnet, rlogin, or SSH)**

If you cannot log on by any means, perform the following steps.

**Procedure**

1. Check whether the TACACS+ server runs properly and try to restart the TACACS+ server.

2. Check whether you enabled both TACACS+ and RADIUS on the switch.

   ```
   show radius
   show tacacs
   ```

   If TACACS+ fails, RADIUS can take over the authentication, authorization, and accounting (AAA) process.

3. Check whether you configured the TACACS+ server to unencrypted mode, as the switch always sends encrypted TACACS+ messages.

4. Check whether you configured the switch properly. In particular, check the IP address and key.

   ```
   show tacacs
   ```

5. Check whether you configured the encryption key, connection mode (single connection or per-session connection), and TCP port number the same on the TACACS+ server and switch.

6. If the server connects directly, check whether the administrative and operation status of the port is up:

   ```
   show interface gigabitethernet {slot/port[/sub-port][-slot/port[/sub-port]]|[,...]}
   ```

7. If the server is connected in a network, check whether the switch has a route configured to the server network:

   ```
   show ip route
   ```

**Example**

Check whether you enabled both TACACS+ and RADIUS on the switch:

```bash
Switch:1>enable
Switch:1(config)#show tacacs

Global Status:
```
global enable : false

authentication enabled for : cli

accounting enabled for : none

authorization : disabled

User privilege levels set for command authorization : None

Server:

create :

Prio  Status  Key     Port  IP address  Timeout Single Source SourceEnabled
Primary NotConn ******  3     192.0.2.254      30   true 5.5.5.5  true
Backup  NotConn ******  47    198.51.100.1      10  false 0.0.0.0 false

Switch:1(config)#show radius

acct-attribute-value : 193
acct-enable : false
acct-include-cli-commands : false
access-priority-attribute : 192
auth-info-attr-value : 91
command-access-attribute : 194
cli-commands-attribute : 195
cli-cmd-count : 40
cli-profile-enable : false
cli-enable : false
igap-passwd-attr : standard
igap-timeout-log-fsize : 512
maxserver : 10
mcast-addr-attr-value : 90
sourceip-flag : false

Check whether the administrative and operation status of the port is up:

Switch:1#show interface gigabitethernet 1/2

================================================================================
<table>
<thead>
<tr>
<th>PORT</th>
<th>INTERFACE</th>
<th>LINK</th>
<th>PORT</th>
<th>PHYSICAL</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUM</td>
<td>INDEX</td>
<td>DESCRIPTION</td>
<td>TRAP</td>
<td>LOCK</td>
<td>MTU</td>
</tr>
</tbody>
</table>
-----------------------------------------------------------------------------------------------
| 1/2  | 257       | 1000BaseTX   | true | false | 1950 | 00:24:7f:a1:70:61 | up   | up    |

================================================================================
<table>
<thead>
<tr>
<th>PORT</th>
<th>OPERATE</th>
<th>OPERATE</th>
<th>OPERATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUM</td>
<td>NAME</td>
<td>DESCRIPTION</td>
<td>STATUS</td>
</tr>
<tr>
<td></td>
<td>AN</td>
<td>T</td>
<td></td>
</tr>
</tbody>
</table>
-----------------------------------------------------------------------------------------------
| 1/2 | 1000BaseTX | up | full | 1000 | Ta |

================================================================================
<table>
<thead>
<tr>
<th>PORT</th>
<th>DIFF-SERV</th>
<th>QoS</th>
<th>MIL</th>
<th>VENDOR</th>
</tr>
</thead>
</table>
Check whether the switch has a route configured to the server network:

```
Switch:1(config)#show ip route
```

---

**IP Route - GlobalRouter**

<table>
<thead>
<tr>
<th>NH</th>
<th>DST</th>
<th>MASK</th>
<th>NEXT</th>
<th>VRF/ISID</th>
<th>COST</th>
<th>FACE</th>
<th>PROT</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>198.51.100.1</td>
<td>255.255.255.255</td>
<td>192.0.2.65</td>
<td>GlobalRouter</td>
<td>1</td>
<td>100</td>
<td>OSPF</td>
<td>0</td>
</tr>
<tr>
<td>125</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>198.51.100.5</td>
<td>255.255.255.255</td>
<td>192.0.2.5</td>
<td>-</td>
<td>1</td>
<td>0</td>
<td>LOC</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>198.51.100.13</td>
<td>255.255.255.255</td>
<td>VSP13</td>
<td>GlobalRouter</td>
<td>10</td>
<td>1000</td>
<td>ISIS</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>198.51.100.200</td>
<td>255.255.255.255</td>
<td>VSP200</td>
<td>GlobalRouter</td>
<td>10</td>
<td>1000</td>
<td>ISIS</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 out of 4 Total Num of Route Entries, 4 Total Num of Dest Networks displayed.

**TYPE Legend:**
- I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route, U=Unresolved Route, N=Not in HW, F=Replaced by FTN, V=IPVPN Route, S=SPBM Route

**PROTOCOL Legend:**
v=Inter-VRF route redistributed

---

**Job aid**

The following table describes the fields in the output for the `show radius` command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acct-attribute-value</td>
<td>Specifies the accounting attribute value.</td>
</tr>
<tr>
<td>acct-enable</td>
<td>Specifies if the accounting attribute is enabled.</td>
</tr>
<tr>
<td>acct-include-cli-commands</td>
<td>Specifies if the accounting attribute includes ACLI commands. The default is false.</td>
</tr>
<tr>
<td>access-priority-attribute</td>
<td>Specifies the value of the access priority attribute. The default is 192.</td>
</tr>
<tr>
<td>auth-info-attr-value</td>
<td>Specifies the value of the authentication information attribute. The default is 91.</td>
</tr>
<tr>
<td>command-access-attribute</td>
<td>Specifies the value of the command access attribute. The default is 194.</td>
</tr>
<tr>
<td>cli-commands-attribute</td>
<td>Specifies the value of the ACLI commands attribute. The default is 195.</td>
</tr>
<tr>
<td>cli-cmd-count</td>
<td>Specifies how many ACLI commands before the system sends a RADIUS accounting interim request. The default is 40.</td>
</tr>
</tbody>
</table>

*Table continues...*
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cli-profile-enable</td>
<td>Specifies if RADIUS ACLI profiling is enabled. ACLI profiling grants or denies access to users being authenticated by way of the RADIUS server. You can add a set of ACLI commands to the configuration on the RADIUS server, and you can specify the command-access mode for these commands. The default is false.</td>
</tr>
<tr>
<td>enable</td>
<td>Specifies if RADIUS authentication is globally enabled on the switch.</td>
</tr>
<tr>
<td>igap-passwd-attr</td>
<td>Specifies the IGMP for user Authentication Protocol (IGAP) password attribute.</td>
</tr>
<tr>
<td>igap-timeout-log-fsize</td>
<td>Specifies the IGMP for user Authentication Protocol (IGAP) timeout log file size.</td>
</tr>
<tr>
<td>maxserver</td>
<td>Specifies the maximum number of servers allowed for the device. The default is 10.</td>
</tr>
<tr>
<td>mcast-addr-attr-value</td>
<td>Specifies the value of the multicast address attribute. The default is 90.</td>
</tr>
<tr>
<td>sourceip-flag</td>
<td>Specifies if the switch can use a configured source IP address. If the outgoing interface on the switch fails, a different source IP address is used, which requires that you make configuration changes to define the new RADIUS client on the RADIUS server. To simplify RADIUS server configuration, you can configure the switch to use a circuitless IP (CLIP) address as the source IP and NAS IP address when transmitting RADIUS packets. By default, the switch uses the IP address of the outgoing interface as the source IP, and the NAS IP address for RADIUS packets that it transmits.</td>
</tr>
</tbody>
</table>

**Administrator unable to obtain accounting information from the TACACS+ server**

If the administrator is unable to obtain accounting information from the TACACS+ server, perform the following steps.

**Procedure**

1. Check whether you enabled accounting on the switch:
   ```
   show tacacs
   ```
2. Check whether you enabled accounting on the TACACS+ server.
Example

Check whether accounting is enabled on the switch:

Switch:1>enable
Switch:1(config)#show tacacs

Global Status:

  global enable : false
  authentication enabled for : cli
  accounting enabled for : none
  authorization : disabled

  User privilege levels set for command authorization : None

Server:

  create :

<table>
<thead>
<tr>
<th>Prio</th>
<th>Status</th>
<th>Key</th>
<th>Port</th>
<th>IP address</th>
<th>Timeout</th>
<th>Single</th>
<th>Source</th>
<th>SourceEnabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>NotConn</td>
<td>*****</td>
<td>3</td>
<td>192.0.2.254</td>
<td>30</td>
<td>true</td>
<td>5.5.5.5</td>
<td>true</td>
</tr>
<tr>
<td>Backup</td>
<td>NotConn</td>
<td>*****</td>
<td>47</td>
<td>198.51.100.1</td>
<td>10</td>
<td>false</td>
<td>0.0.0.0</td>
<td>false</td>
</tr>
</tbody>
</table>

---

Trap server cannot receive trap packets from the switch

If the trap server cannot receive trap packets from the switch, perform the following steps.

Procedure

1. Check whether you configured the trap server correctly on the switch:

   ```
   show snmp-server host
   ```

2. Check whether a firewall exists between the switch and the trap server.

Example

Check whether you configured the trap server correctly on the switch:

Switch:1>enable
Switch:1#show snmp-server host

<table>
<thead>
<tr>
<th>Notify Name</th>
<th>Tag</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inform</td>
<td>informTag</td>
<td>inform</td>
</tr>
<tr>
<td>Trap</td>
<td>trapTag</td>
<td>trap</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Params Name</th>
<th>Profile Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthNoPriv-md5</td>
<td>profile2</td>
</tr>
</tbody>
</table>
Troubleshooting TACACS+ problems

Use the trace level command to check traps and log files to see any TACACS+ failure. If TACACS+ experiences failure conditions, the TACACS+ module sends SNMP traps to notify the user. The TACACS+ module also logs the failure information into the system log file.

About this task

⚠️ Caution:

Using the trace tool inappropriately can cause primary CPU lockup conditions, loss of access to the device, loss of protocols, and service degradation. If you use trace level 3 (verbose) or trace level 4 (very verbose), Avaya recommends that you do not use the screen to view commands due to the volume of information the system generates and the effect on the system.
**Procedure**

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. Configure the trace level for the TACACS+ module:
   ```
   trace level 109 <1–4>
   ```
   The TACACS+ module ID is 109.
3. Stop trace:
   ```
   trace shutdown
   ```
4. View the trace results on screen:
   ```
   trace screen enable
   ```
5. View trace saved to a file:
   ```
   show trace file [tail]
   ```
6. Save the trace file for retrieval:
   ```
   save trace [file WORD<1–99>]
   ```
   If you do not specify a file name, the file name is systrace.txt.

**Variable definitions**

Use the data in the following table to use the `trace` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
</table>
| level [<0–234][<1–4>] | Starts the trace by specifying the module ID and level. `<0-234>` specifies the module ID. Module ID 23 represents the IGMP module. `<0-4>` specifies the trace level:  
  • 0 — Disabled  
  • 1 — Very terse  
  • 2 — Terse  
  • 3 — Verbose  
  • 4 — Very verbose |
| shutdown          | Stops the trace operation.                                          |
| screen {disable|enable} | Enables or disables the display of trace output to the screen.      |

**Important:**

Avaya recommends you avoid using the screen to view commands if you use trace level 3.

*Table continues…*
Variable | Value
--- | ---
(verbose) or trace level 4 (very verbose) due to the volume of information generated and the effect on the system.

Use the data in the following table to use the `show trace` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>file [tail]</td>
<td>Displays the trace results saved to a file.</td>
</tr>
<tr>
<td>level</td>
<td>Displays the current trace level for all modules.</td>
</tr>
<tr>
<td>modid-list</td>
<td>Specifies the module ID list.</td>
</tr>
</tbody>
</table>

---

## Troubleshooting RSMLT

The following sections provide information for troubleshooting IPv4 Split Multi-Link Trunking (RSMLT).

### RSMLT peers not up

If, after a series of reconfigurations, RSMLT peers do not transition to the up state, use the following procedure to troubleshoot the issue. You can observe this issue on dual-stack VLANs after multiple delete and re-adds of IPv4 interfaces.

**Procedure**

1. Display the RSMLT configuration. This command shows whether the peers are up:
   ```
   show ip rsmlt peer
   ```
2. Enter VLAN Interface Configuration mode:
   ```
   enable
   configure terminal
   interface vlan <1-4059>
   ```
3. To recover the peers if they are down, disable and reenable RSMLT on both IST peers:
   ```
   no ip rsmlt
   ip rsmlt
   ```
4. If the problem persists, boot from a saved configuration.
Example

Display the RSMLT configuration:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface vlan 1
Switch:1(config-if)#show ip rsmlt peer
```

```
=====================================================================  
Ip Rsmlt Peer Info - GlobalRouter  
=====================================================================  
VID   IP                MAC                ADMIN   OPER  HDTMR  HUTMR  
---------------------------------------------------------------------  
1     192.0.2.1     00:1f:ca:1e:d3:1e       Enable      Up      60  180  
2     198.51.100.1  00:1b:ca:1d:e3:1d       Enable      Up      60  180  
```

```
VID   HDT REMAIN  HUT REMAIN  SMLT ID  
---------------------------------------------------------------------  
1     60   180     10  
2     60   180     10, 16  
```

```
VID   IPv6            MAC                ADMIN   OPER  HDTMR  HUTMR  
---------------------------------------------------------------------  
```

```
VID   HDT REMAIN  HUT REMAIN  SMLT ID  
---------------------------------------------------------------------  
```

```
Switch:1(config-if)#no ip rsmlt
Switch:1(config-if)#ip rsmlt
```

Enabling trace messages for RSMLT troubleshooting

Use the following procedure to obtain additional RSMLT-related information.

Procedure

If the preceding information does not resolve the issue, you can use the following command to obtain additional RSMLT-related information:

```
trace level 173 4
```

⚠️ Important:

Enabling this trace on a loaded system can slow down the CPU, especially if executed through the console. Use Telnet if possible.
Troubleshooting vIST failure

About this task

When you use Virtual Inter-Switch Trunk (vIST), all critical network traffic runs on this link. If vIST fails, network protocols such as RIP, VRRP, OSPF, and VLACP go down and eventually cause a network outage.

vIST uses an SPBM tunnel to virtually connect two nodes that can be anywhere in the SPBM cloud. Even if the two vIST nodes are directly connected by an MLT link, the vIST VLAN does not have MLT ports as members. Instead, it is configured to be an SPBM C-VLAN.

*Note:*

For more information on vIST and a configuration example, see Configuring Link Aggregation, MLT and SMLT on VSP Operating System Software, NN47227-503.

The vIST tunnel is up as long as there is SPBM connectivity between the IST peers. If there is a vIST failure, check the following procedure for some possible reasons:

Procedure

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. Verify that the vIST VLAN is configured on the vIST switch:
   ```
   show virtual-ist
   ```
3. Verify that an I-SID is associated with the vIST VLAN:
   ```
   show isis spbm i-sid discover
   ```

   **Important:**

   The I-SID associated with the vIST VLAN should be the same on the vIST peer, and this I-SID should not be used anywhere else in the network.

4. Verify that the vIST peers are on the same subnet.
5. If peer ARP is not resolved, enable trace level 14 to see if ARP request/response are being sent/received.
6. If vIST is not up, check the mac fdb table and verify that the peer MAC is synchronized:
   ```
   show vlan mac-address-entry <1-4059>
   ```
7. If the vIST peer MAC is learned, check to see if the peer IP address is reachable.
   a. Use show virtual-ist to obtain the vIST peer IP address.
   b. Ping the peer IP address.
8. If unable to ping the peer IP address, check to see if ARP is resolved.
Upper layer troubleshooting

```
show ip arp vlan <vid>
```
Chapter 21: Unicast routing troubleshooting

Use this section to troubleshoot Layer 3 unicast routing problems.

Using BGP debugging commands

Use global and peer debug commands to display specific debug messages for the global and peer Border Gateway Protocol (BGP) configuration, including the BGP neighbors.

You can use these commands to troubleshoot the BGP configuration.

Procedure

1. Enter BGP Router Configuration mode:
   
   enable
   configure terminal
   router bgp

2. Show specific debug messages for the global BGP configuration:
   
   global-debug mask WORD<1-100>

3. Display specific debug messages for the global BGP neighbors:
   
   neighbor-debug-all mask WORD<1-100>

4. Display specific debug messages for BGP peers or peer groups:
   
   neighbor <nbr_ipaddr|peer-group-name> neighbor-debug-mask WORD<1-100>

5. Display debug messages on the console:
   
   debug-screen <on|off>

Example

Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# router bgp

Display the global debug messages for error and packet:
Switch:1(router-bgp)# global-debug mask error,packet

End (disable) the display of global debug messages:
Switch:1(router-bgp)# global-debug mask none

Display specific debug messages for the global BGP neighbors:
Switch:1(router-bgp)# neighbor-debug-all mask packet,event

Display specific debug messages for BGP peers or peer groups:
Switch:1(router-bgp)# neighbor 45.17.10.23 neighbor-debug-mask event,trace

Display debug messages on the console:
Switch:1(router-bgp)# debug-screen on

---

**Variable definitions**

Use the data in the following table to use the `global-debug mask` and `neighbor-debug-all mask` commands.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD&lt;1-100&gt;</td>
<td>Specifies one or more mask choices that you enter, separated by commas with no space between choices. For example: [&lt;mask&gt;,&lt;mask&gt;,&lt;mask&gt;...]. Options include: none, all, error, packet, event, trace, warning, state, init, filter, update.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `neighbor` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;nbr_ipaddr</td>
<td>peer-group-name&gt;</td>
</tr>
<tr>
<td>WORD&lt;1-100&gt;</td>
<td>Specifies one or more mask choices that you enter, separated by commas with no space between choices. For example: [&lt;mask&gt;,&lt;mask&gt;,&lt;mask&gt;...]. Options include: none, all, error, packet, event, trace, warning, state, init, filter, update.</td>
</tr>
</tbody>
</table>

---

**Job aid**

Use debug command values to control debug messages for global BGP message types, and for message types associated with a specified BGP peer or peer group. The following table identifies mask categories and messages.

---

Comments on this document? infodev@avaya.com
Table 41: Mask categories and messages

<table>
<thead>
<tr>
<th>Mask category</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>None disables the display of all debug messages.</td>
</tr>
<tr>
<td>all</td>
<td>All configures the device to show all categories of debug messages.</td>
</tr>
<tr>
<td>error</td>
<td>Error configures the device to show error debug messages.</td>
</tr>
<tr>
<td>packet</td>
<td>Packet configures the device to show packet debug messages.</td>
</tr>
<tr>
<td>event</td>
<td>Event configures the device to show event debug messages.</td>
</tr>
<tr>
<td>warning</td>
<td>Warning configures the device to show warning debug messages.</td>
</tr>
<tr>
<td>init</td>
<td>Init configures the device to show initialization debug messages.</td>
</tr>
<tr>
<td>filter</td>
<td>Filter configures the device to show filter-related debug messages.</td>
</tr>
<tr>
<td>update</td>
<td>Update configures the device to show update-related debug messages.</td>
</tr>
</tbody>
</table>

Troubleshooting licensed features

About this task
Specific features in the software require a license for operation. Perform this procedure if a licensed feature does not operate.

For more information on licensed features and how to install licenses, see Administration for Avaya Virtual Services Platform 4000 Series, NN46251-600.

Procedure
1. Verify that the license is the correct type.
2. Verify that you installed the license properly.

Example
VSP-4850GTS#show license

```
          License file name  : /intflash/premiersitelicense.xml
        License Type        : PREMIER
         MD5 of Key         : 67d9b8d4 e58172cf 91a3a4c2 5f03c00a
         MD5 of File        : 185f5e5c fea563d0 dda777c 8d54208c
     Generation Time      : 2010/04/12 11:18:08
    Expiration Time      : Base Mac Addr  : 00:24:7f:9f:60:00
         flags             : 0x00000001 SINGLE
        memo               : 
```
Viewing OSPF errors

Before you begin

• You must log on to the Privileged EXEC mode in ACLI.

About this task

Check Open Shortest Path First (OSPF) errors for administrative and troubleshooting purposes.

Procedure

Display information about OSPF errors:

show ip ospf port-error [port {slot/port[-slot/port][,...]}] [vrf WORD<1–16>] [vrfids WORD<0–512>]

Variable definitions

Use the data in the following table to use the show ip ospf port-error command.

Table 42: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>{slot/port[-slot/port][,...]}</td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).</td>
</tr>
<tr>
<td>vrf WORD&lt;1–16&gt;</td>
<td>Specifies a VRF by name.</td>
</tr>
<tr>
<td>vrfids WORD&lt;0–512&gt;</td>
<td>Specifies a range of VRF IDs.</td>
</tr>
</tbody>
</table>

Job aid

The following table explains the fields in the OSPF error command output.

Table 43: OSPF port error field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT NUM</td>
<td>Indicates the port number.</td>
</tr>
<tr>
<td>VERSION MISMATCH</td>
<td>Indicates the number of version mismatches this interface receives.</td>
</tr>
<tr>
<td>AREA MISMATCH</td>
<td>Indicates the number of area mismatches this interface receives.</td>
</tr>
<tr>
<td>AUTHTYPEMISMATCH</td>
<td>Indicates the number of authentication type mismatches this interface receives.</td>
</tr>
</tbody>
</table>

Table continues…

Unicast routing troubleshooting

January 2017

Troubleshooting

Comments on this document? infodev@avaya.com
### Viewing OSPF neighbor state problems

**Before you begin**

- You must log on to the Privileged EXEC mode in ACLI.

**About this task**

View the status of all the OSPF neighbors and their current adjacency state to determine if problems occurred during the device initial startup sequence.

Problems with OSPF occur most often during the initial startup, when the device cannot form adjacencies with other devices, and the state is stuck in the Init or ExStart/Exchange state.

**Procedure**

View the current state of all OSPF neighbors and their current state of adjacency:

```plaintext
show ip ospf neighbor
```

**Example**

```
VSP-4850GTS#show ip ospf neighbor
```

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>NBRROUTERID</th>
<th>NBRIPADDR</th>
<th>PRIO_STATE</th>
<th>RTXQLEN</th>
<th>PERM</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>42.1.1.33</td>
<td>198.95.65.0</td>
<td>42.1.1.34</td>
<td>1</td>
<td>Full</td>
<td>0</td>
<td>Dyn 40</td>
</tr>
</tbody>
</table>

**Job aid**

At initial startup, devices transmit hello packets in an attempt to find other OSPF devices with which to form adjacencies. After the device receives the hello packets, it performs an initialization process, which causes the device to transition through various states before it establishes the adjacency.

The following table describes the various device states during adjacency formation.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTH FAILURES</td>
<td>Indicates the number of authentication failures.</td>
</tr>
<tr>
<td>NET_MASK MISMATCH</td>
<td>Indicates the number of network mask mismatches this interface receives.</td>
</tr>
<tr>
<td>HELLOINT MISMATCH</td>
<td>Indicates the number of hello interval mismatches this interface receives.</td>
</tr>
<tr>
<td>DEADINT MISMATCH</td>
<td>Indicates the number of dead interval mismatches this interface receives.</td>
</tr>
<tr>
<td>OPTION MISMATCH</td>
<td>Indicates the number of options mismatches this interface receives.</td>
</tr>
</tbody>
</table>
Table 44: Device states during OSPF adjacency formation

<table>
<thead>
<tr>
<th>Step</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Down</td>
<td>Indicates that a neighbor was configured manually, but the device did not receive information from the other device. This state can occur only on nonbroadcast multiaccess interfaces.</td>
</tr>
<tr>
<td>2</td>
<td>Attempt</td>
<td>Indicates, on a nonbroadcast multiaccess interface, that the device attempts to send unicast hellos to configured interfaces.</td>
</tr>
<tr>
<td>3</td>
<td>Init</td>
<td>Indicates that the device received a general hello packet (without the router ID) from another device.</td>
</tr>
<tr>
<td>4</td>
<td>2-Way</td>
<td>Indicates that the device received a hello packet directed to it from another device. (The hello contains the router ID.)</td>
</tr>
<tr>
<td>5</td>
<td>ExStart</td>
<td>Indicates the start of the master and backup election process.</td>
</tr>
<tr>
<td>6</td>
<td>Exchange</td>
<td>Indicates the link state database is exchanged.</td>
</tr>
<tr>
<td>7</td>
<td>Loading</td>
<td>Indicates the processing state of the link state database for input into the routing table. The device can request link state advertisements for missing or corrupt routes.</td>
</tr>
<tr>
<td>8</td>
<td>Full</td>
<td>Indicates the normal full adjacency state.</td>
</tr>
</tbody>
</table>

Troubleshooting OSPF Init state problems

Before you begin

- You must log on to the Privileged EXEC mode in ACLI.

About this task

A device can become stuck in the Init state and not form an adjacency. Several possible causes for this type of problem exist:

- access lists implemented on routers
- authentication mismatch or configuration problem

Problems arise if a mismatch exists in authentication keys, or if both sides are not configured for authentication.

Procedure

1. Configure the trace level for the OSPF module to terse:
   
   ```
   trace level 6 2
   ```

2. View the trace information on screen:
   
   ```
   trace screen enable
   ```

3. Verify if the path is not reachable due to access lists implemented on the device.
4. Ensure the multicast address of 224.0.0.5 can traverse the link. If multicast traffic is blocked, you must configure the Avaya Virtual Services Platform 4000 Series for OSPF nonbroadcast multiaccess (NBMA) instead of broadcast.

Example

VSP-4850GTS> enable
VSP-4850GTS# trace level 6 2
VSP-4850GTS# trace screen enable

Troubleshooting OSPF ExStart/Exchange problems

Before you begin

• You must log on to Interface Configuration mode in ACLI.

About this task

Although both devices can recognize each other and move beyond 2-way state, the devices can become stuck in the ExStart/Exchange state. A mismatch in maximum transmission unit (MTU) sizes between the devices usually causes this type of problem. For example, one device can use a high MTU size and the default value on the other device is a smaller value. Depending on the size of the link state database (LSDB), the device with the smaller value cannot process the larger packets and remains in ExStart/Exchange state. This problem is usually encountered during interoperations in networks with other vendor devices.

In Virtual Services Platform 4000, the supported MTU size for OSPF is 1500 bytes by default. Incoming OSPF database description (DD) packets are dropped if their MTU size is greater than 1500 bytes.

If you configure the device to ignore the MTU size, the device does not perform the MTU check on the incoming OSPF DD packet. Virtual Services Platform 4000 automatically checks for OSPF MTU mismatches.

Procedure

1. View the OSPF packets:
   
   trace level 6 2

2. Ensure that the MTU size value for both devices match.

3. Configure the interface to accept OSPF DD packets with a different MTU size:

   ip ospf mtu-ignore enable

Example

VSP-4850GTS> enable
VSP-4850GTS# configure terminal
VSP-4850GTS(config)# interface vlan 100
Unicast routing troubleshooting

VSP-4850GTS(config-if)# trace level 6 2
VSP-4850GTS(config-if)# ip ospf mtu-ignore enable
Chapter 22: Multicast troubleshooting

Use the following information to troubleshoot multicast features and multicast routing.

Multicast feature troubleshooting

Use the information in this section to troubleshoot multicast feature problems.

Troubleshooting IGMP Layer 2 Querier

The following sections provide troubleshooting information for the IGMP Layer 2 Querier feature.

Querier not elected

If a Querier is not elected, use the following procedure to troubleshoot the issue.

Procedure

1. Enter Privileged EXEC mode:
   
   enable

2. As the IGMP Layer 2 Querier is based on IGMP snoop, check whether IGMP snoop is enabled on the VLAN:

   show ip igmp interface vlan

   If IGMP snoop is disabled, the Layer 2 Querier cannot work until IGMP snoop and IGMP Layer 2 Querier are reenabled.

Example

Check whether IGMP snoop is enabled on the VLAN:

Switch:1>enable
Switch:1#show ip igmp interface vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Query</th>
<th>Query Robust</th>
<th>Version</th>
<th>Last Proxy</th>
<th>Snoop</th>
<th>SSM</th>
<th>Fast</th>
<th>Fast</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comments on this document? infodev@avaya.com
### Job aid

The following table describes the fields in the output for the `show ip igmp interface vlan` command.

**Note:**

The following table shows the field descriptions for this command if you use the optional parameter `vlan`. If you do not the output is different.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Identifies the VLAN or port where IGMP is configured.</td>
</tr>
<tr>
<td>QUERY INTVL</td>
<td>Indicates the frequency at which IGMP host query packets transmit on this interface.</td>
</tr>
<tr>
<td>QUERY MAX RESP</td>
<td>Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.</td>
</tr>
<tr>
<td>ROBUST</td>
<td>Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.</td>
</tr>
<tr>
<td>VERSION</td>
<td>Indicates the version of IGMP that runs on this interface. This object configures a router capable of</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.</td>
</tr>
<tr>
<td>LAST MEMB QUERY</td>
<td>Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.</td>
</tr>
<tr>
<td>PROXY SNOOP ENABLE</td>
<td>Indicates if proxy snoop is enabled on the interface.</td>
</tr>
<tr>
<td>SNOOP ENABLE</td>
<td>Indicates if snoop is enabled on the interface.</td>
</tr>
<tr>
<td>SSM SNOOP ENABLE</td>
<td>Indicates if SSM snoop is enabled on the interface.</td>
</tr>
<tr>
<td>FAST LEAVE ENABLE</td>
<td>Indicates if fast leave mode is enabled on the interface.</td>
</tr>
<tr>
<td>FAST LEAVE PORTS (VLAN parameter only)</td>
<td>Indicates the set of ports that are enabled for fast leave.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.</td>
</tr>
<tr>
<td>SNOOP QUERIER ENABLE</td>
<td>Specifies whether the snoop querier is enabled.</td>
</tr>
<tr>
<td>SNOOP QUERIER ADDRESS</td>
<td>Specifies the pseudo address of the IGMP snoop querier.</td>
</tr>
<tr>
<td>DYNAMIC DOWNGRADE VERSION</td>
<td>Indicates if the dynamic downgrade feature is enabled.</td>
</tr>
<tr>
<td>COMPATIBILITY MODE</td>
<td>Indicates whether compatibility mode is enabled.</td>
</tr>
<tr>
<td>EXPLICIT HOST TRACKING</td>
<td>Specifies whether the IGMP protocol version 3 is enabled to track hosts for each channel or groups.</td>
</tr>
</tbody>
</table>

### Enabling trace messages for IGMP Layer 2 querier troubleshooting

If the preceding information does not address your issue, you can also use the following trace command to view additional information related to Layer 2 querier.

⚠️ **Caution:**

Using the trace tool inappropriately can cause primary CPU lockup conditions, loss of access to the device, loss of protocols, and service degradation. If you use trace level 3 (verbose) or trace level 4 (very verbose), do not use the screen to view commands due to the volume of information the system generates and the effect on the system.
Procedure

1. Enter Privileged EXEC mode:
   `enable`

2. Use the following trace command to begin the trace operation for additional information related to Layer 2 querier:
   `trace level 23 <1-4>`

3. Stop tracing:
   `trace shutdown`

4. View the trace results:
   `trace screen enable`

5. View trace saved to a file:
   `show trace file [tail]`

Variable definitions

Use the data in the following table to use the `trace` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
</table>
| `level [<0–234]>[<1–4>]` | Starts the trace by specifying the module ID and level. `<0-234>` specifies the module ID. Module ID 23 represents the IGMP module. `<0-4>` specifies the trace level:  
  • 0 — Disabled  
  • 1 — Very terse  
  • 2 — Terse  
  • 3 — Verbose  
  • 4 — Very verbose |
| `shutdown`        | Stops the trace operation.                                           |
| `screen {disable|enable}` | Enables or disables the display of trace output to the screen. |

⚠️ Important:  
Avoid using the screen to view commands if you use trace level 3 (verbose) or trace level 4 (very verbose) due to the volume of information generated and the effect on the system.

Use the data in the following table to use the `show trace` command.
### Troubleshooting IGMPv3 backwards compatibility

If you configure the switch to operate in v2-v3 compatibility mode, the switch supports all IGMPv2 and v3 messages. The switch parses the group address of the messages. If the group address is out of SSM range and it is a v3 message, the switch drops the message. If it is a v2 message, IGMP snoop processes handle the message.

To troubleshoot issues with the IGMPv3 backwards compatibility feature, perform the following procedure.

**Procedure**

1. Enter Privileged EXEC mode:
   ```
   enable
   ```

2. Verify that the SSM static channel is configured for the v1/v2 joins received. Display the configured SSM static channels:
   ```
   show ip igmp ssm-map
   ```

3. Verify that the SSM group range is configured for the v1/v2 joins received. Display the configured SSM group range:
   ```
   show ip igmp ssm
   ```

**Example**

Display the configured SSM static channels and display the configured SSM group range:

```
Switch:>enable
Switch:1#show ip igmp ssm-map

================================================================================
Igmp Ssm Channel
================================================================================
GROUP           SOURCE          MODE       ACTIVE     STATUS
--------------------------------------------------------------------------------
233.252.0.1       192.0.2.200 dynamic    false      enabled
233.252.0.2       192.0.2.200 dynamic    false      enabled
233.252.0.3       192.0.2.200 dynamic    false      enabled
233.252.0.4       192.0.2.200 dynamic    false      enabled
233.252.0.5       192.0.2.200 dynamic    false      enabled
233.252.0.6       192.0.2.200 dynamic    false      enabled
233.252.0.7       192.0.2.200 dynamic    false      enabled
233.252.0.8       192.0.2.200 dynamic    false      enabled
233.252.0.9       192.0.2.200 dynamic    false      enabled
233.252.0.10      192.0.2.200 dynamic    false      enabled
10 out of 10 entries displayed
```
Switch:1(config)#show ip igmp ssm

================================================================================
Igmp Ssm Global - GlobalRouter
================================================================================
DYNAMIC LEARNING      SSM GROUP RANGE
--------------------------------------------------------------------------------
enable                   233.252.0.0/255.0.0.0

Job aid

The following table shows the field descriptions for the `show ip igmp ssm-map` command.

Table 45: show ip igmp ssm-map command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP</td>
<td>Indicates the IP multicast group address that uses the default range of 232/8.</td>
</tr>
<tr>
<td>SOURCE</td>
<td>Indicates the IP address of the source that sends traffic to the group source.</td>
</tr>
<tr>
<td>MODE</td>
<td>Indicates that the entry is a statically configured entry (static) or a dynamically learned entry from IGMPv3 (dynamic).</td>
</tr>
<tr>
<td>ACTIVE</td>
<td>Indicates the activity on the corresponding source and group. If the source is active and traffic is flowing to the switch, this status is active; otherwise, it is nonactive.</td>
</tr>
<tr>
<td>STATUS</td>
<td>Indicates the administrative state and whether to use the entry. If the status is enabled (default), the entry is used. If the status is disabled, the entry is not used but is saved for future use.</td>
</tr>
</tbody>
</table>

The following table shows the field descriptions for the `show ip igmp ssm` command.

Table 46: show ip igmp ssm command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DYNAMIC LEARNING</td>
<td>Indicates whether dynamic learning is enabled at a global level.</td>
</tr>
<tr>
<td>SSM GROUP RANGE</td>
<td>Indicates the IP address range for the SSM group.</td>
</tr>
</tbody>
</table>
Chapter 23: Multicast routing
troubleshooting using ACLI

Use the information in this section to help you troubleshoot multicast routing problems.

Viewing IGMP interface information

Perform this procedure to view the IGMP interface table.

About this task

If an interface does not use an IP address, it does not appear in the IGMP table. One exception is an IGMP snooping interface, which does not require an interface IP address.

If an interface uses an IP address, but neither IGMP snoop or PIM is enabled, the interface appears as inactive in the Status field.

Procedure

1. Enter Privileged EXEC mode:
   
   `enable`

2. View IGMP interfaces:
   
   `show ip igmp interface [gigabitethernet {slot/port[/sub-port][-slot/port[/sub-port]]|,...||vlan <1-4059>| [vrf WORD<1-16>][vrfids WORD<0-512>]]`

Example

View IGMP interfaces:

```
Switch:1#show ip igmp interface
================================================================================
Igmp Interface - GlobalRouter
================================================================================
QUERY OPER QUERY WRONG
LASTMEM
INTVL STATUS VERS. VERS QUERIER MAXRSPT QUERY JOINS ROBUST QUERY
MODE
--------------------------------------------------------------------------------
V300 125 active 3 21.0.0.12 100 0 674 2 10
```
Variable definitions

Use the data in the following table to use the `show ip igmp interface` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>gigabitethernet {slot/port[/sub-port][slot/port[/sub-port][,...]}</td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. If you do not specify a slot and port, the command output includes all IGMP interfaces.</td>
</tr>
<tr>
<td>vlan &lt;1-4059&gt;</td>
<td>Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. If you do not specify a VLAN ID, the command output includes all IGMP interfaces.</td>
</tr>
<tr>
<td>vrf WORD &lt;1–16&gt;</td>
<td>Optionally, identifies the VRF name. If you do not specify a VRF name, the results display information for the Global Router. If you specify a VRF name, the results display information only for the VRF you specify.</td>
</tr>
<tr>
<td>vrfids WORD &lt;0–512&gt;</td>
<td>Optionally, identifies the VRF ID. If you do not specify a range of VRF IDs, the results display information for the Global Router. If you specify a VRF ID or range of VRF IDs, the results display information only for the VRF you specify.</td>
</tr>
</tbody>
</table>

Job aid

The following table shows the field descriptions for the command output if you do not use the optional parameters.
Table 47: show ip igmp interface command output without parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IF</td>
<td>Indicates the interface where IGMP is configured.</td>
</tr>
<tr>
<td>QUERY INTVL</td>
<td>Indicates the frequency at which IGMP host query packets transmit on this interface.</td>
</tr>
<tr>
<td>STATUS</td>
<td>Indicates the activation of a row, which activates IGMP on the interface. The destruction of a row disables IGMP on the interface.</td>
</tr>
<tr>
<td>VERS</td>
<td>Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.</td>
</tr>
<tr>
<td>OPER VERS</td>
<td>Indicates the operational version of IGMP.</td>
</tr>
<tr>
<td>QUERIER</td>
<td>Indicates the address of the IGMP querier on the IP subnet to which this interface attaches.</td>
</tr>
<tr>
<td>QUERY MAXRSPT</td>
<td>Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.</td>
</tr>
<tr>
<td>WRONG QUERY</td>
<td>Indicates the number of queries received whose IGMP version does not match the interface version. You must configure all routers on a LAN to run the same version of IGMP. If queries are received with the wrong version, a configuration error occurs.</td>
</tr>
<tr>
<td>JOINS</td>
<td>Indicates the number of times this interface added a group membership.</td>
</tr>
<tr>
<td>ROBUST</td>
<td>Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.</td>
</tr>
<tr>
<td>LASTMEM QUERY</td>
<td>Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.</td>
</tr>
</tbody>
</table>

The following table shows the field descriptions for the command output if you use the interface parameters.
Table 48: show ip igmp interface command output with interface parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID or PORT NUM</td>
<td>Identifies the VLAN or port where IGMP is configured.</td>
</tr>
<tr>
<td>QUERY INTVL</td>
<td>Indicates the frequency at which IGMP host query packets transmit on this interface.</td>
</tr>
<tr>
<td>QUERY MAX RESP</td>
<td>Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.</td>
</tr>
<tr>
<td>ROBUST</td>
<td>Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.</td>
</tr>
<tr>
<td>VERSION</td>
<td>Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.</td>
</tr>
<tr>
<td>LAST MEMB QUERY</td>
<td>Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.</td>
</tr>
<tr>
<td>PROXY SNOOP ENABLE</td>
<td>Indicates if proxy snoop is enabled on the interface.</td>
</tr>
<tr>
<td>SNOOP ENABLE</td>
<td>Indicates if snoop is enabled on the interface.</td>
</tr>
<tr>
<td>SSM SNOOP ENABLE</td>
<td>Indicates if SSM snoop is enabled on the interface.</td>
</tr>
<tr>
<td>FAST LEAVE ENABLE</td>
<td>Indicates if fast leave mode is enabled on the interface.</td>
</tr>
<tr>
<td>FAST LEAVE PORTS (VLAN parameter only)</td>
<td>Indicates the set of ports that are enabled for fast leave.</td>
</tr>
<tr>
<td>DYNAMIC DOWNGRADE VERSION</td>
<td>Indicates if the dynamic downgrade feature is enabled.</td>
</tr>
<tr>
<td>COMPATIBILITY MODE</td>
<td>Indicates if compatibility mode is enabled.</td>
</tr>
<tr>
<td>EXPLICIT HOST TRACKING</td>
<td>Indicates if explicit host tracking is enabled for IGMPv3. Explicit host tracking enables the IGMP to track all source and group members.</td>
</tr>
</tbody>
</table>

Viewing multicast group trace information for IGMP snoop
About this task
Multicast group trace tracks the data flow path of the multicast streams.

Procedure
1. Enter Privileged EXEC mode:
   ```enable```
2. Display the multicast group trace for an IGMP snoop-enabled interface:
   ```show ip igmp snoop-trace [source {A.B.C.D}] [group {A.B.C.D}]```

Example
Display the multicast group trace for an IGMP snoop-enabled interface:
```
Switch:1>enable
Switch:1#show ip igmp snoop-trace

================================================================================
Snoop Trace - GlobalRouter
================================================================================
GROUP ADDRESS | SOURCE ADDRESS | IN VLAN | IN PORT | OUT VLAN | OUT PORT | TYPE
---------------|---------------|---------|---------|----------|----------|------
232.10.12.17  | 200.0.15.53   | 1015    | 1/3     | 1015     | 1/35-1/40| ACCESS
232.10.12.20  | 200.0.15.53   | 1015    | 1/3     | 1015     | 1/35-1/40| ACCESS
232.10.12.19  | 200.0.15.53   | 1015    | 1/3     | 1015     | 1/35-1/40| ACCESS
232.10.12.18  | 200.0.15.53   | 1015    | 1/3     | 1015     | 1/35-1/40| ACCESS
```

Variable definitions
Use the data in the following table to use the `show ip igmp snoop-trace` command.

Table 49: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>group {A.B.C.D}</td>
<td>Specifies the group IP address in the format a.b.c.d.</td>
</tr>
<tr>
<td>source {A.B.C.D}</td>
<td>Specifies the source IP address in the format a.b.c.d.</td>
</tr>
</tbody>
</table>

Job aid
The following table shows the field descriptions for the `show ip igmp snoop-trace` command.

Table 50: show ip igmp snoop-trace field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP ADDRESS</td>
<td>Indicates the IP multicast group address for which this entry contains information.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE ADDRESS</td>
<td>Indicates the source of the multicast traffic.</td>
</tr>
<tr>
<td>IN VLAN</td>
<td>Indicates the incoming VLAN ID.</td>
</tr>
<tr>
<td>IN PORT</td>
<td>Indicates the incoming port number.</td>
</tr>
<tr>
<td>OUT VLAN</td>
<td>Indicates the outgoing VLAN ID.</td>
</tr>
<tr>
<td>OUT PORT</td>
<td>Indicates the outgoing port number.</td>
</tr>
<tr>
<td>TYPE</td>
<td>Indicates where the stream is learned. ACCESS indicates the stream is learned locally.</td>
</tr>
</tbody>
</table>

**Viewing IGMP group information**

View information about IGMP groups to see the current group operation on the switch.

**Procedure**

1. Enter Privileged EXEC mode:
   ```
   enable
   ```

2. View IGMP group information:
   ```
   show ip igmp group group <A.B.C.D> detail [port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}][vlan <1-4059>][vrf WORD <1-16>][vrfids WORD <0-512>]
   ```
   ```
   show ip igmp group group <A.B.C.D> tracked-members [member-subnet <A.B.C.D./X>][port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}][source-subnet <A.B.C.D/X>][vlan <1-4059>][vrf WORD <1-16>][vrfids WORD <0-512>]
   ```

**Example**

View IGMP group information:

```
Switch:1>enable
Switch:1#show ip igmp group group 232.0.0.0
================================================================================
Igmp Group - GlobalRouter
================================================================================
GRPADDR    INPORT          MEMBER          EXPIRATION TYPE
--------------------------------------------------------------------------------
232.0.0.0   V1015-1/2     200.0.15.53     258        Dynamic
1 out of 271 group Receivers displayed
Total number of unique groups 271
```
# Variable definitions

Use the data in the following table to use the `show ip igmp group` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Displays the number of entries in the IGMP group.</td>
</tr>
<tr>
<td>group &lt;A.B.C.D&gt;</td>
<td>Specifies the address of the IGMP group.</td>
</tr>
<tr>
<td>member-subnet {default</td>
<td>&lt;A.B.C.D&gt;}</td>
</tr>
<tr>
<td>vrf WORD&lt;1–16&gt;</td>
<td>Specifies the VRF name.</td>
</tr>
<tr>
<td>vrfids WORD&lt;0–512&gt;</td>
<td>Specifies the VRF ID.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `show ip igmp group group <A.B.C.D> tracked-members` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>member-subnet {default</td>
<td>&lt;A.B.C.D&gt;}</td>
</tr>
<tr>
<td>port {slot/port[/sub-port][{-slot/port[/sub-port][{-...}}]}</td>
<td>Specifies the port list.</td>
</tr>
<tr>
<td>source-subnet &lt;A.B.C.D/X&gt;</td>
<td>Specifies the source IP address and the subnet mask.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `show ip igmp group group` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail [port {slot/port[/sub-port][{-slot/port[/sub-port][{-...}}]}</td>
<td>vlan &lt;1-4059&gt;</td>
</tr>
<tr>
<td></td>
<td>— Specifies the port list.</td>
</tr>
<tr>
<td></td>
<td>— Specifies the VLAN.</td>
</tr>
<tr>
<td></td>
<td>— Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.</td>
</tr>
<tr>
<td></td>
<td>— Specifies the VRF name.</td>
</tr>
<tr>
<td></td>
<td>— Specifies the VRF ID.</td>
</tr>
<tr>
<td>tracked-members</td>
<td>Use the tracked-members parameter to view all the tracked members for a specific group.</td>
</tr>
<tr>
<td>vrf WORD&lt;1–16&gt;</td>
<td>Specifies the VRF name.</td>
</tr>
<tr>
<td>vrfids WORD&lt;0–512&gt;</td>
<td>Specifies the VRF ID.</td>
</tr>
</tbody>
</table>
### Variable

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan &lt;1-4059&gt;</td>
<td>Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.</td>
</tr>
<tr>
<td>vrf WORD&lt;1–16&gt;</td>
<td>Specifies the VRF name.</td>
</tr>
<tr>
<td>vrfids WORD&lt;0–512&gt;</td>
<td>Specifies the VRF ID.</td>
</tr>
</tbody>
</table>

### Job aid

The following table shows the field descriptions for the show ip igmp group group command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRPADDR</td>
<td>Shows the multicast group address (Class D). A group address can be the same for many incoming ports.</td>
</tr>
<tr>
<td>INPORT</td>
<td>Shows the port that receives the group membership report.</td>
</tr>
<tr>
<td>MEMBER</td>
<td>Shows the IP address of the host that issues the membership report to this group.</td>
</tr>
<tr>
<td>EXPIRATION</td>
<td>Shows the time left before the group report expires on this port. This variable is updated after the port receives a group report.</td>
</tr>
<tr>
<td>TYPE</td>
<td>Indicates the group type.</td>
</tr>
</tbody>
</table>

### Showing the hardware resource usage

**About this task**

The switch can query the number of ingress and egress IP multicast streams traversing the switch. After you configure the thresholds for ingress and egress records, if the record-usage goes beyond the threshold, the device notifies you by way of a trap on the console, logged message, or both.

If you do not configure the thresholds, the switch displays only the ingress and egress records currently in use.

**Procedure**

1. Log on to the switch to enter User EXEC mode.
2. Show the hardware resource usage:
show ip mroute hw-resource-usage

**Example**

Show the hardware resource usage:

```
Switch:1>show ip mroute hw-resource-usage
================================================================================
Multicast Hardware Resource Usage
================================================================================
EGRESS      INGRESS     EGRESS      INGRESS     LOG MSG   SEND TRAP  SEND TRAP
REC IN-USE  REC IN-USE  THRESHOLD   THRESHOLD   ONLY      ONLY       AND LOG
--------------------------------------------------------------------------------
0           0           0           0           false     false      false
```

**Job aid**

The following table shows the field descriptions for the `show ip mroute hw-resource-usage` command.

**Table 52: show ip mroute hw-resource-usage field descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EGRESS REC IN-USE</td>
<td>Indicates the number of egress records (peps) traversing the switch that are in use.</td>
</tr>
<tr>
<td>INGRESS REC IN-USE</td>
<td>Indicates the number of source and group records traversing the switch that are in use.</td>
</tr>
<tr>
<td>EGRESS THRESHOLD</td>
<td>Indicates the egress records threshold.</td>
</tr>
<tr>
<td>INGRESS THRESHOLD</td>
<td>Indicates the source and group records threshold.</td>
</tr>
<tr>
<td>LOG MSG ONLY</td>
<td>Indicates the status of logging messages only.</td>
</tr>
<tr>
<td>SEND TRAP ONLY</td>
<td>Indicates the status of sending traps only.</td>
</tr>
<tr>
<td>SEND TRAP AND LOG</td>
<td>Indicates the status of both sending traps and logging messages.</td>
</tr>
</tbody>
</table>

**Using PIM debugging commands**

**About this task**

Use Protocol Independent Multicast (PIM) traces to aid in PIM troubleshooting.

**Procedure**

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. Start debug trace message output:
   debug ip pim pimdbgtrace
3. Stop debug trace message output:
   no debug ip pim pimdbgtrace
   default debug ip pim pimdbgtrace
4. Configure the system to display trace messages forwarded by the device:
   debug ip pim send-dbg-trace
5. Stop the system from displaying trace messages forwarded by the device:
   no debug ip pim send-dbg-trace
   default debug ip pim send-dbg-trace
6. Configure the system to display trace messages received by the device:
   debug ip pim rcv-dbg-trace
7. Stop the system from displaying trace messages received by the device:
   no debug ip pim rcv-dbg-trace
   default debug ip pim rcv-dbg-trace
8. Configure the system to display hello messages forwarded or received by the device:
   debug ip pim hello
9. Stop the system from displaying hello messages forwarded or received by the device:
   no debug ip pim hello
   default debug ip pim hello
10. Configure the system to display and log debug trace messages:
    debug ip pim pimdbglog
11. Stop the system from displaying and logging debug trace messages:
    no debug ip pim pimdbglog
    default debug ip pim pimdbglog
12. Configure the system to display register messages forwarded or received by the device:
    debug ip pim register
13. Stop the system from displaying register messages forwarded or received by the device:
    no debug ip pim register
    default debug ip pim register
14. Configure the system to display debug trace messages after an enabled message type, for example, hello or register, is received from a specific sender IP address:
debug ip pim source {A.B.C.D}

Variable definitions

Use the data in the following table to use the `debug ip pim` command.

Table 53: Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>assert</td>
<td>Displays the assert debug traces. The default is false (disabled).</td>
</tr>
<tr>
<td>bootstrap</td>
<td>Displays bootstrap debug traces. The default is false (disabled).</td>
</tr>
<tr>
<td>group {A.B.C.D}</td>
<td>Displays debug traces from a specific group IP address. The default is 0.0.0.0 (disabled).</td>
</tr>
<tr>
<td>hello</td>
<td>Displays hello debug traces. The default is false (disabled).</td>
</tr>
<tr>
<td>joinprune</td>
<td>Displays join and prune debug traces. The default is false (disabled).</td>
</tr>
<tr>
<td>pimdbglog</td>
<td>Logs debug traces. The default is false (disabled).</td>
</tr>
<tr>
<td>pimdbgtrace</td>
<td>Displays PIM debug traces. The default is false (disabled).</td>
</tr>
<tr>
<td>rcv-dbg-trace</td>
<td>Displays trace messages received by the switch. The default is false (disabled).</td>
</tr>
<tr>
<td>register</td>
<td>If enabled, the system displays register debug traces. The default is false (disabled).</td>
</tr>
<tr>
<td>regstop</td>
<td>Displays register stop debug traces. The default is false (disabled).</td>
</tr>
<tr>
<td>rp-adv</td>
<td>Displays RP advertisement debug traces. The default is false (disabled).</td>
</tr>
<tr>
<td>send-dbg-trace</td>
<td>Displays trace messages forwarded by the switch. The default is false (disabled).</td>
</tr>
<tr>
<td>source {A.B.C.D}</td>
<td>Displays debug traces from a specific source IP address. The default is 0.0.0.0 (disabled).</td>
</tr>
</tbody>
</table>

Determining the protocol configured on the added VLAN

Use this procedure to determine the protocol configured on the added VLAN.

The protocol configured on the added VLAN can be one of the following values:

- snoop
- snoop-spb
- route-spb
- pim
**Procedure**

1. Enter Privileged EXEC mode:
   ```
   enable
   ```

2. Determine the protocol configured on the added VLAN:
   ```
   show ip igmp interface [gigabitethernet {slot/port[/sub-port][-slot/port[/sub-port]],[,...]}][vlan <1-4059>][vrf WORD<1-16>] [vrfids WORD<0-512>]
   ```

   The protocol displays under the Mode column of the command output.

**Example**

Determine the protocol configured on the added VLAN:

Switch:1enable
Switch:1#show ip igmp interface

```
================================================================================
IGMP Interface - GlobalRouter
================================================================================
QUERY OPER  QUERY WRONG  LASTMEM IF  INTVL STATUS  VERS  VERS QUERIER MAXRSPT QUERY ROBUST QUERY MODE
--------------------------------------------------------------------------------
V300  activ  3     3   21.0.0.12    100     0     116     2      10    pim
```

1 out of 1 entries displayed

**Variable definitions**

Use the information in the following table to use the `show ip igmp interface` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>gigabitethernet{slot/port[/sub-port][-slot/port[/sub-port]],[,...]}</td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.</td>
</tr>
<tr>
<td>vlan&lt;1-4059&gt;</td>
<td>Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.</td>
</tr>
<tr>
<td>vrfWORD&lt;1–16&gt;</td>
<td>Specifies the VRF instance by the VRF name.</td>
</tr>
<tr>
<td>vrfidsWORD&lt;0–512&gt;</td>
<td>Specifies the VRF ID for which to display statistics.</td>
</tr>
</tbody>
</table>
The following table shows the field descriptions for the `show ip igmp interface` command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IF</td>
<td>Indicates the interfaces where IGMP is configured.</td>
</tr>
<tr>
<td>QUERY INTVL</td>
<td>Indicates the frequency at which the interface transmits IGMP host query packets.</td>
</tr>
<tr>
<td>STATUS</td>
<td>Indicates the activation of a row that enables IGMP on the interface. The destruction of a row disables IGMP on the interface.</td>
</tr>
<tr>
<td>VERS</td>
<td>Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.</td>
</tr>
<tr>
<td>OPER VERS</td>
<td>Indicates the operational version of IGMP.</td>
</tr>
<tr>
<td>QUERIER</td>
<td>Indicates the address of the IGMP querier on the IP subnet to which this interface is attached.</td>
</tr>
<tr>
<td>QUERY MAXRSPT</td>
<td>Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.</td>
</tr>
<tr>
<td>WRONG QUERY</td>
<td>Indicates the number of queries received whose IGMP version does not match the IGMP Interface version. You must configure all routers on a LAN to run the same version of IGMP. Therefore, if the interface receives queries with the wrong version, a configuration error occurs.</td>
</tr>
<tr>
<td>JOINS</td>
<td>Indicates the number of times IGMP added a group membership on this interface.</td>
</tr>
<tr>
<td>ROBUST</td>
<td>Indicates the robustness variable, which you configure for the expected packet loss on a subnet. If packet loss is expected on a subnet, increase the robustness variable.</td>
</tr>
<tr>
<td>LAST MEM QUERY</td>
<td>Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This does not apply if igmpInterface version is 1.</td>
</tr>
<tr>
<td>MODE</td>
<td>Indicates the protocol configured on the VLAN added.</td>
</tr>
<tr>
<td></td>
<td>• snoop — Indicates IGMP snooping is enabled on a VLAN.</td>
</tr>
<tr>
<td></td>
<td>• snoop-spb — Indicates IGMP is enabled on a VLAN with an associated I-SID (IP Multicast over Fabric Connect for a Layer 2 VSN.)</td>
</tr>
</tbody>
</table>
The following table shows the field descriptions for the `show ip igmp interface` command output if you use the optional parameters to specify a port, VLAN, or VRF.

### Table 54: `show ip igmp interface` command with optional parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID or PORT NUM</td>
<td>Identifies the VLAN or port where IGMP is configured.</td>
</tr>
<tr>
<td>QUERY INTVL</td>
<td>Indicates the frequency at which IGMP host query packets transmit on this interface.</td>
</tr>
<tr>
<td>QUERY MAX RESP</td>
<td>Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.</td>
</tr>
<tr>
<td>ROBUST</td>
<td>Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.</td>
</tr>
<tr>
<td>VERSION</td>
<td>Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.</td>
</tr>
<tr>
<td>LAST MEMB QUERY</td>
<td>Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.</td>
</tr>
<tr>
<td>PROXY SNOOP ENABLE</td>
<td>Indicates if proxy snoop is enabled on the interface.</td>
</tr>
<tr>
<td>SNOOP ENABLE</td>
<td>Indicates if snoop is enabled on the interface.</td>
</tr>
<tr>
<td>SSM SNOOP ENABLE</td>
<td>Indicates if SSM snoop is enabled on the interface.</td>
</tr>
<tr>
<td>FAST LEAVE ENABLE</td>
<td>Indicates if fast leave mode is enabled on the interface.</td>
</tr>
<tr>
<td>FAST LEAVE PORTS (VLAN parameter only)</td>
<td>Indicates the set of ports that are enabled for fast leave.</td>
</tr>
<tr>
<td>VLAN ID or PORT NUM</td>
<td>Identifies the VLAN or port where IGMP is configured.</td>
</tr>
<tr>
<td>SNOOP QUERIER ENABLE (VLAN parameter only)</td>
<td>Indicates if the IGMP Layer 2 Querier feature is enabled.</td>
</tr>
<tr>
<td>SNOOP QUERIER ADDRESS (VLAN parameter only)</td>
<td>Indicates the IP address of the IGMP Layer 2 Querier.</td>
</tr>
<tr>
<td>DYNAMIC DOWNGRADE VERSION</td>
<td>Indicates if the dynamic downgrade feature is enabled.</td>
</tr>
<tr>
<td>COMPATIBILITY MODE</td>
<td>Indicates if compatibility mode is enabled.</td>
</tr>
</tbody>
</table>

*Table continues…*
Determining the data stream learned with IP Multicast over Fabric Connect on the VLAN

Use this procedure to determine the data stream learned when IP Multicast over Fabric Connect is configured on the VLAN.

**About this task**

The following section shows sample output for the `show ip mroute route` command.

In this table, every stream uses one (*,G) entry and x (S,G) entries, depending on how many servers forward traffic to the same group.

The 0.0.0.0 mask is always tied to a (*,G) entry.

If you do not specify a VRF name or range of VRF IDs, the results display information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results display information only for the VRFs you specify.

**Procedure**

1. Log on to the switch to enter User EXEC mode.
2. Determine the data stream learned:
   ```
   show ip mroute route [vrf WORD <0–32>] [vrfids <0–255>]
   ```

**Example**

Determine the data stream learned:

```
Switch:1#show ip mroute route
================================================================================
Mroute Route
================================================================================
GROUP       SOURCE          SRCMASK         UPSTREAM_NBR    IF     EXPIR  PROT
--------------------------------------------------------------------------------
233.252.0.119   0.0.0.0         0.0.0.0            203.0.113.207   v504     210   pimsm
233.252.0.119   192.0.2.165     255.255.255.0   203.0.113.207   v504   210   pimsm
233.252.0.119   198.51.100.165  255.255.255.0   198.51.100.204  v155   210   pimsm
233.252.0.119   198.51.100.166  255.255.255.0   198.51.100.204  v155   210   pimsm
233.252.0.113   0.0.0.0         0.0.0.0         203.0.113.208   v504   210   pimsm
233.252.0.113   198.51.100.165  255.255.255.0   203.0.113.208   v504   210   pimsm
```

**Variable definitions**

Use the data in the following table to use the `show ip mroute route` command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXPLICIT HOST TRACKING</td>
<td>Indicates if explicit host tracking is enabled to track all the source and group members.</td>
</tr>
</tbody>
</table>
Job aid

The following table shows the field descriptions for the `show ip mroute route` command.

**Table 55: Job aid: show ip mroute route command output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP</td>
<td>Indicates the IP multicast group for which this entry specifies a next hop on an outgoing interface.</td>
</tr>
<tr>
<td>SOURCE</td>
<td>Indicates the network address that, when combined with the corresponding value of <code>ipMRRouteNextHopSourceMask</code>, identifies the sources for which this entry specifies a next hop on an outgoing interface.</td>
</tr>
<tr>
<td>SRCMASK</td>
<td>Indicates the network mask, when combined with the corresponding value of <code>ipMRRouteNextHopSource</code>, identifies the sources for which this entry specifies a next hop on an outgoing interface.</td>
</tr>
<tr>
<td>UPSTREAM_NBR</td>
<td>Indicates the address of the upstream neighbor from which IP datagrams from these sources to this multicast address are received, or 0.0.0.0 if the upstream neighbor is known.</td>
</tr>
<tr>
<td>IF</td>
<td>Indicates the value of <code>ifIndex</code> for the interface on which IP datagrams sent by these sources to this multicast address are received. A value of 0 indicates that datagrams are not subject to an incoming interface check, but can be accepted on multiple interfaces (for example, in CBT).</td>
</tr>
<tr>
<td>EXPIR</td>
<td>Indicates the minimum amount of time remaining before this entry ages out. The value 0 indicates that the entry is not subject to aging.</td>
</tr>
<tr>
<td>PROT</td>
<td>Indicates the outgoing mechanism through which the switch learns this route. For IP Multicast over Fabric Connect, this value is <code>sb-access</code> or <code>spb-network</code>. <code>Sbp-access</code> indicates the datastream learned was from the UNI ports. <code>Sbp-network</code> indicates that the datastream learned was from the SPBM cloud.</td>
</tr>
</tbody>
</table>
Displaying the SPBM multicast database

You can determine the database used by the SPBM multicast module by using the following procedure.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Show the SPBM multicast database:

```
show isis spbm ip-multicast-route [all][detail][group {A.B.C.D}]
[vlan <2–4059>][vrf WORD<0–16>][vsn-isid <1–16777215>]
```

Example

Show the SPBM multicast database:

```
Switch(config)#show isis spbm ip-multicast-route
```

<table>
<thead>
<tr>
<th>Source</th>
<th>Group</th>
<th>Data ISID</th>
<th>BVLAN</th>
<th>Source-BEB</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.2.0.1</td>
<td>233.252.0.246</td>
<td>16000001</td>
<td>101</td>
<td>EVP</td>
</tr>
</tbody>
</table>

Total Number of SPBM IP MULTICAST ROUTE Entries: 1

Variable definitions

Use the data in the following table to use the `show isis spbm ip-multicast-route` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all IP Multicast over Fabric Connect route information.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed IP Multicast over Fabric Connect route information.</td>
</tr>
<tr>
<td>group {A.B.C.D} source {A.B.C.D}</td>
<td>Displays information on the group IP address for the IP Multicast over Fabric Connect route. If you select source it will also display the source IP address.</td>
</tr>
<tr>
<td>vlan &lt;2–4059&gt;</td>
<td>Displays IP Multicast over Fabric Connect route information by VLAN.</td>
</tr>
<tr>
<td>vrf WORD&lt;0–16&gt;</td>
<td>Displays IP Multicast over Fabric Connect route information by VRF.</td>
</tr>
<tr>
<td>vsn-isid &lt;1–16777215&gt;</td>
<td>Displays IP Multicast over Fabric Connect route information by I-SID.</td>
</tr>
</tbody>
</table>
Job aid

The following table describes fields for the `show isis spbm ip-multicast-route` command.

Table 56: `show isis spbm ip-multicast-route` command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Specifies the IP address of the Global Routing Table.</td>
</tr>
<tr>
<td>Group</td>
<td>Specifies the IP multicast group for which this entry specifies a next hop on an outgoing interface.</td>
</tr>
<tr>
<td>Data ISID</td>
<td>Specifies the VRF ID for the multicast route.</td>
</tr>
<tr>
<td>BVLAN</td>
<td>Specifies the Backbone VLAN (B-VLAN).</td>
</tr>
<tr>
<td>Source-BEB</td>
<td>Specifies the source Backbone Edge Bridge (BEB).</td>
</tr>
<tr>
<td>Total number of SPBM IP MULTICAST Route entries</td>
<td>Specifies the number of SPBM IP multicast route entries.</td>
</tr>
</tbody>
</table>

Troubleshooting IP Multicast over Fabric Connect for Layer 2 VSNs

If traffic is not moving properly, use the following procedure to determine the issue.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```

2. Ensure that all switch nodes in the network operate with the current release:
   ```
   show software
   ```

3. If any ERS 8800 nodes exist in the network, ensure you upgrade them to the current release:
   ```
   show software
   ```

4. Ensure that you create and enable SPBM infrastructure globally.
   a. Ensure that SPBM is enabled globally:
      ```
      show spbm
      ```
   b. Ensure that IS-IS is enabled globally:
      ```
      show isis
      ```
   c. Ensure an SPBM instance exists and at least one Backbone VLAN exists (B-VID). Also ensure multicast is enabled:
      ```
      show isis spbm
      ```
For more information about infrastructure and services configuration, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.

5. Ensure that you enable the CFM configuration.
   a. Ensure a CFM maintenance-association exists:
      
      ```
      show cfm maintenance-association
      ```
   b. Ensure a CFM maintenance-domain exists:
      
      ```
      show cfm maintenance-domain
      ```
   c. Ensure a maintenance-endpoint exists in the MEP ID column and is enabled in the ADMIN column:
      
      ```
      show cfm maintenance-endpoint
      ```

6. Ensure a Customer VLAN (C-VLAN) exists and ensure you add UNI ports to the C-VLAN.
   a. Display C-VLAN information:
      
      ```
      show vlan i-sid
      ```
   b. Display ports for the C-VLAN:
      
      ```
      show vlan members port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
      ```
   c. Display NNI and UNI receivers:
      
      ```
      show isis spbm ip-multicast-route detail
      ```

7. Ensure that you assign the same I-SID to the C-VLAN on all of the BEBs where you configure the C-VLAN:
   
   ```
   show vlan i-sid
   ```

8. Ensure that you enable IP Multicast over Fabric Connect globally:
   
   ```
   show isis spbm
   ```

9. Ensure the you enable IGMP Snooping on the C-VLAN on all of the Backbone Edge Bridges (BEBs). Ensure the protocol configured on the VLAN added is snoop-spb in the MODE column, which indicates IGMP is enabled on a VLAN with an associated I-SID (IP Multicast over Fabric Connect for a Layer 2 VSN):
   
   ```
   show ip igmp interface
   ```

10. Ensure that you enable IGMP Snooping on access Layer 2 switches to prevent flooding of multicast traffic to non-receiver ports:
    
    ```
    show ip igmp snoop-trace
    show ip igmp interface
    ```

11. Ensure that the IGMP version used by the multicast hosts and the Layer 2 switches outside the SPBM network is the same as the IGMP version configured on the C-VLAN:
    
    ```
    show ip igmp interface
    ```
Troubleshooting IP Multicast over Fabric Connect for Layer 3 VSNs

If traffic is not moving properly, use the following procedure to determine the issue.

Procedure

1. Ensure that all switch nodes in the network operate with the current release:
   ```
   show software
   ```

2. If ERS 8800 nodes exist in the network, ensure you upgrade them to the current release:
   ```
   show software
   ```

3. Ensure that you create and enable SPBM infrastructure globally.
   a. Ensure that SPBM is enabled globally:
      ```
      show spbm
      ```
   b. Ensure that IS-IS is enabled globally:
      ```
      show isis
      ```
   c. Ensure an SPBM instance exists and at least one Backbone VLAN exists (B-VID). Also ensure multicast is enabled:
      ```
      show isis spbm
      ```

For more information on infrastructure and services configuration, see Configuring Avaya Fabric Connect on VSP Operating System Software, NN47227-510.

4. Ensure that you enable the CFM configuration.
   a. Ensure a CFM maintenance-association exists:
      ```
      show cfm maintenance-association
      ```
   b. Ensure a CFM maintenance-domain exists:
      ```
      show cfm maintenance-domain
      ```
   c. Ensure a maintenance-endpoint exists in the MEP ID column and is enabled in the ADMIN column:
      ```
      show cfm maintenance-endpoint
      ```

5. Ensure the following on all the Backbone Edge Bridges (BEBs) where the Layer 3 VSN is present.
   a. Ensure that you enable IP multicast globally:
      ```
      show isis spbm
      ```
   b. Ensure that you create an IPVPN for the VRF:
      ```
      show ip ipvpn [vrf WORD<1-16>][vrfids WORD<0-512>]
      ```
   c. Ensure that you assign an I-SID to the VRF:
show isis spbm ip-multicast-route all
d. Ensure that you enable the MVPN:
    show ip vrf mvpn

6. On the VLANs that need Layer 3 VSN IP Multicast over Fabric Connect routing, create an IP
interface on the VLAN if one does not exist. The address should be on the same subnet as
the IGMP hosts connected to the VLAN. Also, ensure that you enable IP Multicast over
Fabric Connect.

7. Enter VLAN Interface Configuration mode:
    enable
    configure terminal
    interface vlan <1–4059>

8. Create an IP interface on the VLAN and enable IP Multicast over Fabric Connect:
    ip address <A.B.C.D>
    ip spb-multicast enable

9. Ensure that you enable IGMP Snooping on access Layer 2 switches to prevent flooding of
multicast traffic to non-receiver ports:
    show ip igmp snoop-trace
    show ip igmp interface

10. Ensure that the IGMP version used by the multicast hosts and the Layer 2 switches outside
the SPBM network is the same as the IGMP version configured on the C-VLAN:
    show ip igmp interface

---

**Troubleshooting IP Multicast over Fabric Connect for IP Shortcuts**

If traffic is not moving properly, use the following procedure to determine the issue.

**Procedure**

1. Ensure that all switch nodes in the network operate with the current release:
   show software

2. Ensure that all ERS 8800 nodes in the network have the current release:
   show software

3. Ensure that you create and enable SPBM infrastructure globally.
   a. Ensure that SPBM is enabled globally:
show spbm

b. Ensure that IS-IS is enabled globally:
   show isis

c. Ensure an SPBM instance exists and at least one Backbone VLAN exists (B-VID). Also ensure multicast is enabled:
   show isis spbm

For more information on infrastructure and services configuration, see Configuring Avaya Fabric Connect on VSP Operating System Software, NN47227-510.

4. Ensure that you enable the CFM configuration.
   a. Ensure a CFM maintenance-association exists:
      show cfm maintenance-association
   b. Ensure a CFM maintenance-domain exists:
      show cfm maintenance-domain
   c. Ensure a maintenance-endpoint exists in the MEP ID column and is enabled in the ADMIN column:
      show cfm maintenance-endpoint

5. Ensure the following on all BEBs where you want IP Multicast over Fabric Connect. Ensure that you enable IP Multicast over Fabric Connect globally:
   show isis spbm

6. On the VLANs that need Layer 3 VSN IP Multicast over Fabric Connect routing, create an IP interface on the VLAN if one does not exist. The address should be on the same subnet as the IGMP hosts connected to the VLAN. Also, ensure that you enable IP Multicast over Fabric Connect. Create an IP interface on the VLAN and enable IP Multicast over Fabric Connect.

7. Enter VLAN Interface Configuration mode:
   enable
   configure terminal
   interface vlan <1-4059>

8. Create an IP interface on the VLAN and enable IP Multicast over Fabric Connect:
   ip address <A.B.C.D>
   ip spb-multicast enable

9. Ensure that you enable IGMP Snooping on access Layer 2 switches to prevent flooding of multicast traffic to non-receiver ports:
   show ip igmp snoop-trace
   show ip igmp interface
10. Ensure that the IGMP version used by the multicast hosts and the Layer 2 switches outside the SPBM network is the same as the IGMP version configured on the C-VLAN:

```
show ip igmp interface
```

---

**Defining the IS-IS trace flag for IP multicast**

Define the IS-IS trace flag for IP multicast.

**Procedure**

1. Log on to the switch to enter User EXEC mode.
2. Define the IS-IS trace flag for IP multicast:

```
trace flags isis [set ip-multicast] [remove ip-multicast]
```
Chapter 24: Multicast routing troubleshooting using EDM

Use the information in this section to help you troubleshoot multicast routing problems using Enterprise Device Manager (EDM).

Viewing IGMP interface information

Use the Interface tab to view the IGMP interface table. You can use this procedure to determine the protocol configured on the added VLAN.

The protocol configured on the added VLAN can be one of the following values:

- snoop
- pim

About this task

If an interface does not use an IP address, it does not appear in the IGMP table. If an interface uses an IP address, but neither IGMP snoop or PIM is enabled, the interface appears as inactive in the Status field.

Procedure

1. In the navigation pane, expand the following folders: Configuration > IP.
2. Click IGMP.
3. Click the Interface tab.

Interface field descriptions

Use the data in the following table to use the Interface tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIndex</td>
<td>Shows the interface where IGMP is enabled.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>QueryInterval</td>
<td>Configures the frequency (in seconds) at which the IGMP host query packets transmit on the interface. The range is from 1–65535 and the default is 125.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the IGMP row status. If an interface uses an IP address and PIM-SM is enabled, the status is active. Otherwise, it is notInService.</td>
</tr>
<tr>
<td>Version</td>
<td>Configures the version of IGMP (1, 2, or 3) that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is version 2.</td>
</tr>
<tr>
<td>OperVersion</td>
<td>Shows the version of IGMP that currently runs on this interface.</td>
</tr>
<tr>
<td>Querier</td>
<td>Shows the address of the IGMP querier on the IP subnet to which this interface attaches.</td>
</tr>
<tr>
<td>QueryMaxResponseTime</td>
<td>Configures the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. You cannot configure this value for IGMPv1. Smaller values allow a router to prune groups faster. The range is from 0–255, and the default is 100 tenths of a second (equal to 10 seconds.)</td>
</tr>
<tr>
<td>Important:</td>
<td>You must configure this value lower than the QueryInterval.</td>
</tr>
<tr>
<td>WrongVersionQueries</td>
<td>Shows the number of queries received with an IGMP version that does not match the interface. You must configure all routers on a LAN to run the same version of IGMP. If the interface receives queries with the wrong version, this value indicates a version mismatch.</td>
</tr>
<tr>
<td>Joins</td>
<td>Shows the number of times this interface added a group membership, which is the same as the number of times an entry for this interface is added to the cache table. This number gives an indication of the amount of IGMP activity over time.</td>
</tr>
<tr>
<td>Robustness</td>
<td>Tunes for the expected packet loss of a network. This value is equal to the number of expected query packet losses for each serial query interval, plus 1. If you expect a network to lose query packets, increase the robustness value. The range is from 2–255 and the default is 2. The default value of 2 means that the switch drops one query for each query interval without the querier aging out.</td>
</tr>
<tr>
<td>LastMembQueryIntvl</td>
<td>Configures the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages. This value is also the time between group-specific query messages. You cannot configure this value for IGMPv1. Decrease the value to reduce the time to detect the loss of the last member of a group. The range is from 0–255 and the default is 10 tenths of second. Avaya recommends that you configure this value lower than the QueryInterval.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OtherQuerierPresent Timeout</td>
<td>Shows the length of time that must pass before a multicast router determines that no other querier exists. If the local router is the querier, the value is 0.</td>
</tr>
<tr>
<td>FlushAction</td>
<td>Configures the flush action to one of the following:</td>
</tr>
<tr>
<td></td>
<td>- none</td>
</tr>
<tr>
<td></td>
<td>- flushGrpMem</td>
</tr>
<tr>
<td></td>
<td>- flushMrouter</td>
</tr>
<tr>
<td></td>
<td>- flushSender</td>
</tr>
<tr>
<td>RouterAlertEnable</td>
<td>Instructs the router to ignore IGMP packets that do not contain the router alert IP option. If you disable this variable (default configuration), the router processes IGMP packets regardless of the status of the router alert IP option.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>To maximize network performance, configure this parameter according to the version of IGMP currently in use.</td>
</tr>
<tr>
<td></td>
<td>- IGMPv1—Disable</td>
</tr>
<tr>
<td></td>
<td>- IGMPv2—Enable</td>
</tr>
<tr>
<td></td>
<td>- IGMPv3—Enable</td>
</tr>
<tr>
<td>SsmSnoopEnable</td>
<td>Enables SSM snoop.</td>
</tr>
<tr>
<td>SnoopQuerierEnable</td>
<td>Enables IGMP Layer 2 Querier.</td>
</tr>
<tr>
<td>SnoopQuerierAddr</td>
<td>Enables the IGMP Layer 2 Querier address.</td>
</tr>
<tr>
<td>ExplicitHostTrackingEnable</td>
<td>Enables or disables IGMPv3 to track hosts for each channel or group. The default is disabled. You must select this field if you want to use fast leave for IGMPv3.</td>
</tr>
<tr>
<td>McastMode</td>
<td>Indicates the protocol configured on the VLAN.</td>
</tr>
<tr>
<td></td>
<td>- snoop — Indicates IGMP snooping is enabled on a VLAN.</td>
</tr>
<tr>
<td></td>
<td>- pim — Indicates PIM is enabled.</td>
</tr>
</tbody>
</table>

### Viewing IGMP snoop trace information

**About this task**

View the multicast group trace to track the data flow path of multicast streams.
Procedure

1. In the navigation pane, expand the following folders: **Configuration > IP**.
2. Click **IGMP**.
3. Click the **Snoop Trace** tab.

---

### Snoop Trace field descriptions

Use the data in the following table to use the **Snoop Trace** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GrpAddr</td>
<td>Displays the IP multicast address of the group traversing the router.</td>
</tr>
<tr>
<td>SrcAddr</td>
<td>Displays the IP source address of the multicast group.</td>
</tr>
<tr>
<td>OutVlan</td>
<td>Displays the egress VLAN ID for the multicast group.</td>
</tr>
<tr>
<td>InPort</td>
<td>Displays the ingress port for the multicast group.</td>
</tr>
<tr>
<td>InVlan</td>
<td>Displays the ingress VLAN ID for the multicast group.</td>
</tr>
<tr>
<td>OutPort</td>
<td>Displays the egress port of the multicast group.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the port type on which the snoop entry is learned.</td>
</tr>
</tbody>
</table>

---

### Viewing IGMP group information

View information about IGMP groups to see the current group operation on the switch.

**About this task**

**Note:**

The following procedure displays the dynamically learned IGMP groups. **IP > IGMP > Static** displays statically configured IGMP groups. This is in contrast to the ACLI command `show ip igmp group`, which displays both dynamically learned and statically configured IGMP groups, and the ACLI command `show ip igmp static`, which displays only the statically configured groups.

You can view IGMP information on a VRF instance the same way you view the Global Router except that you must first launch the appropriate VRF context.

**Procedure**

1. In the navigation pane, expand the following folders: **Configuration > IP**.
2. Click **IGMP**.
3. Click the **Groups** tab.

---

**Groups field descriptions**

Use the data in the following table to use the **Groups** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IpAddress</td>
<td>Shows the multicast group address (Class D). A group address can be the same for many incoming ports.</td>
</tr>
<tr>
<td>Members</td>
<td>Shows the IP address of the host that issues the membership report to this group.</td>
</tr>
<tr>
<td>InPort</td>
<td>Shows the port that receives the group membership report.</td>
</tr>
<tr>
<td>IfIndex</td>
<td>Shows a unique value that identifies a physical interface or a logical interface (VLAN) that receives the membership report.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Shows the time left before the group report expires on this port. This variable is updated after the port receives a group report.</td>
</tr>
</tbody>
</table>

---

**Viewing multicast group sources**

With the Sources tab, you can view all the sources on the subnet that send to the particular group selected in the Mroute-HW table.

**Procedure**

1. In the navigation tree, expand the following folders: **IP > Multicast**.
2. Click the **Mroute-HW** tab.
3. Click any row in the table.
4. Click **Sources**.

---

**Sources field descriptions**

Use the information in the following table to help you understand the **Source** tab fields.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SourceAddress</td>
<td>The IP addresses of the sources on this particular subnet sending traffic to the multicast group for the selected entry in the Mroute-HW table.</td>
</tr>
<tr>
<td>IngressPort</td>
<td>The corresponding ingress port in the multicast stream selected from the Mroute-HW table.</td>
</tr>
</tbody>
</table>
Viewing multicast routes by egress VLAN

With the Egress VLANs tab, you can view the egress VLANs for the streams corresponding to the selected entry in the Mroute-Hw table.

Procedure

1. In the navigation tree, expand the following folders: IP > Multicast.
2. Click the Mroute-HW tab.
3. Click any row in the table.
4. Click EgressVlans.

EgressVlans field descriptions

Use the information in the following table to help you use the EgressVlans tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EgressVlan</td>
<td>All the egress VLANs for the particular multicast stream selected from the Mroute-HW table.</td>
</tr>
<tr>
<td>EgressVlanPorts</td>
<td>The corresponding ports for the particular multicast stream selected from the Mroute-HW table.</td>
</tr>
</tbody>
</table>

Enabling multicast routing process statistics

Enable the collection of multicast routing process statistics. The statistics display based on VRF and multicast group classification. These statistics are not related to the interface (port) statistics. (To display the collected statistics, you must use ACLI.)

Procedure

1. In the navigation tree, expand the following folders: Configuration > IP.
2. Click Multicast.
3. Click the Globals tab.
4. Select the MrouteStatsEnabled check box, and then click Apply.
Determining the data stream learned when IP Multicast over Fabric Connect is configured on the VLAN

Use the following procedure to determine the data stream learned when IP multicast is configured on the VLAN.

Procedure

1. In the navigation pane, expand the following folders: Configuration > IP > Multicast.
2. Click the Routes tab.

Multicast field descriptions

Use the information in the following table to help you use the Multicast tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Indicates the IP multicast group for which this entry specifies a next hop on an outgoing interface.</td>
</tr>
<tr>
<td>Source</td>
<td>Indicates the network address that, when combined with the corresponding value of ipMRouteNextHopSourceMask, identifies the sources for which this entry specifies a next hop on an outgoing interface.</td>
</tr>
<tr>
<td>SourceMask</td>
<td>Indicates the network mask, when combined with the corresponding value of ipMRouteNextHopSource, identifies the sources for which this entry specifies a next hop on an outgoing interface.</td>
</tr>
<tr>
<td>UpstreamNeighbor</td>
<td>Indicates the address of the upstream neighbor from which IP datagrams from these sources to this multicast address are received, or 0.0.0.0 if the upstream neighbor is known.</td>
</tr>
<tr>
<td>Interface</td>
<td>Indicates the value of ifIndex for the interface on which IP datagrams sent by these sources to this multicast address are received. A value of 0 indicates that datagrams are not subject to an incoming interface check, but can be accepted on multiple interfaces (for example, in CBT).</td>
</tr>
<tr>
<td>ExpiryTime</td>
<td>Indicates the minimum amount of time remaining before this entry ages out. The value 0 indicates that the entry is not subject to aging.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Indicates the outgoing mechanism through which the switch learns this route. For IP Multicast over Fabric Connect, this value is spb-access or spb-network. Spb-access indicates the datastream learned was from the UNI ports. Spb-network indicates that the datastream learned was from the SPBM cloud.</td>
</tr>
</tbody>
</table>
Showing the SPBM multicast database

Determine the database used by the SPBM multicast module.

Procedure

1. In the navigation pane, expand the following folders: Configuration > ISIS > SPBM.
2. Click the IpMcastRoutes tab.

IpMcastRoutes field descriptions

Use the information in the following table to use the IpMcastRoutes tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VsnIsid</td>
<td>Specifies the VSN I-SID.</td>
</tr>
<tr>
<td>Group</td>
<td>Specifies the group IP address for the IP multicast route.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the IP address where the IP multicast route originated from.</td>
</tr>
<tr>
<td>SourceBeb</td>
<td>Specifies the Source Backbone Edge Bridge (BEB) for the IP multicast route.</td>
</tr>
<tr>
<td>VlanId</td>
<td>Specifies the VLAN ID.</td>
</tr>
<tr>
<td>VrfName</td>
<td>Specifies the VRF name.</td>
</tr>
<tr>
<td>DataIsid</td>
<td>Specifies the VRF ID for the multicast route.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type for the IP multicast route.</td>
</tr>
<tr>
<td>Bvlan</td>
<td>Specifies the Backbone VLAN (B-VLAN).</td>
</tr>
<tr>
<td>NniInterfaces</td>
<td>Specifies the Network-to-Network Interface ports.</td>
</tr>
</tbody>
</table>
Chapter 25: Transparent Port UNI feature troubleshooting using ACLI

Use the information in this section to help you troubleshoot Transparent Port UNI feature problems.

Viewing all configured I-SIDs

Perform this procedure to view all the configured I-SIDs including their types, ports, and MLTs.

**About this task**

View all configured I-SIDs (both CVLAN and T-UNI). View also the I-SID types and the ports or MLTs that are assigned to each I-SID.

**Procedure**

1. Enter Privileged EXEC mode:
   ```bash
enable
   ```
2. View all configured I-SIDs. This command displays both CVLAN and T-UNI based I-SIDs.
   ```bash
   show i-sid
   ```
3. View all T-UNI (Elan-Transparent) I-SIDs.
   ```bash
   show i-sid [elan-transparent]
   ```
4. View information for a particular T-UNI I-SID.
   ```bash
   show i-sid [<1-16777215>]
   ```
5. View all IS-IS SPBM I-SID information by I-SID ID:
   ```bash
   show isis spbm i-sid {all|config|discover} [vlan <2-4094>] [id <1-16777215>] [nick-name <xx.xx>]
   ```

**Example**

View all configured I-SIDs.

```
Switch:1(config)#show i-sid
========================================================================
Isid Info
========================================================================
ISID  ISID                        PORT               MLT
```
Viewing all configured I-SIDs

<table>
<thead>
<tr>
<th>ID</th>
<th>TYPE</th>
<th>VLANID</th>
<th>INTERFACES</th>
<th>INTERFACES</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>ELAN_TR</td>
<td>N/A</td>
<td>1/2</td>
<td>6</td>
</tr>
<tr>
<td>12</td>
<td>CVLAN</td>
<td>11</td>
<td>1/7</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>ELAN_TR</td>
<td>4450</td>
<td>1/17</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>ELAN_TR</td>
<td>7254</td>
<td>1/12</td>
<td></td>
</tr>
</tbody>
</table>

All 4 out of 4 Total Num of i-sids displayed

Switch:1(config)#

View T-UNI (ELAN Transparent) I-SIDs.

Switch:1(config)#show isid elan-transparent

<table>
<thead>
<tr>
<th>ISID</th>
<th>ISID</th>
<th>PORT</th>
<th>MLT</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>ELAN_TR</td>
<td>N/A</td>
<td>1/12</td>
</tr>
<tr>
<td>6</td>
<td>ELAN_TR</td>
<td>N/A</td>
<td>1/2</td>
</tr>
</tbody>
</table>

All 2 out of 2 Total Num of elan-tp i-sids displayed

View MLT or port information for a particular T-UNI I-SID.

Switch:1(config)#show isid 6

View all IS-IS SPBM I-SID information:

Switch:1#show isis spbm isid all

<table>
<thead>
<tr>
<th>ISID</th>
<th>SOURCE NAME</th>
<th>VLAN</th>
<th>SYSID</th>
<th>TYPE</th>
<th>HOST_NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>1.11.16</td>
<td>20</td>
<td>0014.c7e1.33df</td>
<td>config</td>
<td>Switch1</td>
</tr>
<tr>
<td>6</td>
<td>1.11.20</td>
<td>10</td>
<td>0014.c723.67df</td>
<td>discover</td>
<td>Switch2</td>
</tr>
</tbody>
</table>

Total number of SPBM ISID entries configured: 1

Total number of SPBM ISID entries discovered: 1

Total number of SPBM ISID entries: 2

View all IS-IS SPBM I-SID information by I-SID ID:

Switch:1#show isis spbm isid all id 300

<table>
<thead>
<tr>
<th>ISID</th>
<th>SOURCE NAME</th>
<th>VLAN</th>
<th>SYSID</th>
<th>TYPE</th>
<th>HOST_NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td>7.15.16</td>
<td>20</td>
<td>a425.1b51.9484</td>
<td>config</td>
<td>Switch1</td>
</tr>
</tbody>
</table>
Variable definitions

Use the data in the following table to use the `show i-sid` command.

**Note:**

When SPB is enabled, I-SID IDs 16777216 and greater are reserved for dynamic data I-SIDs, used to carry Multicast traffic over SPB.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
</table>
| `<1–16777215>` | Specifies the service interface identifier (ISID). The ISID range is `<1–16777215>`.
| `elan-transparent` | Displays only all the Elan-Transparent (T-UNI based) ISIDs.
| `spbm i-sid {all|config|discover}` | • all: displays all I-SID entries  
• config: displays configured I-SID entries  
• discover: displays discovered I-SID entries  
| `vlan <1–4094>` | Displays I-SID information for the specified SPBM VLAN.
| `id <1–16777215>` | Displays I-SID information for the specified I-SID.
| `nick-name <x.xx.xx>` | Displays I-SID information for the specified nickname.

Job aid

The following table describes the fields in the output for the `show i-sid` command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISID ID</td>
<td>Specifies the service interface identifier (I-SID)</td>
</tr>
<tr>
<td>ISID TYPE</td>
<td>Specifies the type of I-SID</td>
</tr>
</tbody>
</table>

Table continues…
The following describes the fields in the output for the `show isis spbm i-sid` command.

Table 59: `show isis spbm i-sid`

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISID</td>
<td>Indicates the IS-IS SPBM I-SID identifier.</td>
</tr>
<tr>
<td>SOURCE NAME</td>
<td>Indicates the nickname of the node where this I-SID was configured or discovered.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Indicates the B-VLAN where this I-SID was configured or discovered.</td>
</tr>
<tr>
<td>SYSID</td>
<td>Indicates the system identifier.</td>
</tr>
<tr>
<td>TYPE</td>
<td>Indicates the SPBM I-SID type as either configured or discovered.</td>
</tr>
<tr>
<td>HOST_NAME</td>
<td>Indicates the host name of the multicast FIB entry.</td>
</tr>
</tbody>
</table>

---

Viewing C-MACs learned on T-UNI ports for an ISID

Perform this procedure to view the I-SID bridge forwarding database.

**About this task**

The `show i-sid mac-address-entry` command displays the C-MACs learned on T-UNI I-SIDs. It also displays the C-MACs learned on T-UNI I-SIDs for a specific I-SID, MAC address, port or port list or remote MAC address.

**Procedure**

1. Log on to the switch to enter User EXEC mode.
2. View C-MACs learned on the T-UNI I-SIDs:

   ```
   show i-sid mac-address-entry [<1-16777215>] [mac <0x00:0x00:0x00:0x00:0x00:0x00>][port {slot/port[/sub-port] [-slot/port[/sub-port]] [,..]}][remote]
   ```
Example

View C-MACs learned on all T-UNI I-SIDs.

Switch:1#show i-sid mac-address-entry

I-SID Fdb Table

<table>
<thead>
<tr>
<th>I-SID</th>
<th>STATUS</th>
<th>MAC-ADDRESS</th>
<th>INTERFACE</th>
<th>TYPE</th>
<th>DEST-MAC</th>
<th>BVLAN</th>
<th>DEST-SYSNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>learned</td>
<td>cc:f9:54:ae:28:81</td>
<td>Port-1/16</td>
<td>LOCAL</td>
<td>00:00:00:00:00:00</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>learned</td>
<td>cc:f9:54:ae:2c:18</td>
<td>mlt-6</td>
<td>LOCAL</td>
<td>00:00:00:00:00:00</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>252</td>
<td>learned</td>
<td>cc:f9:54:ae:38:64</td>
<td>Port-1/15</td>
<td>REMOTE</td>
<td>00:13:0a:0c:d3:e0</td>
<td>128</td>
<td>DIST-1B</td>
</tr>
</tbody>
</table>

All 3 out of 3 Total Num of i-sid FDB Entries displayed

View C-MACs learned on a specific T-UNI I-SID.

Switch:1#show i-sid mac-address-entry 100

I-SID Fdb Table

<table>
<thead>
<tr>
<th>I-SID</th>
<th>STATUS</th>
<th>MAC-ADDRESS</th>
<th>INTERFACE</th>
<th>TYPE</th>
<th>DEST-MAC</th>
<th>BVLAN</th>
<th>DEST-SYSNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>learned</td>
<td>cc:f9:54:ae:28:81</td>
<td>Port-1/16</td>
<td>LOCAL</td>
<td>00:00:00:00:00:00</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

All 1 out of 1 Total Num of i-sid FDB Entries displayed

Switch:1#show i-sid mac-address-entry 252

I-SID Fdb Table

<table>
<thead>
<tr>
<th>I-SID</th>
<th>STATUS</th>
<th>MAC-ADDRESS</th>
<th>INTERFACE</th>
<th>TYPE</th>
<th>DEST-MAC</th>
<th>BVLAN</th>
<th>DEST-SYSNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>252</td>
<td>learned</td>
<td>cc:f9:54:ae:38:64</td>
<td>Port-1/15</td>
<td>REMOTE</td>
<td>00:13:0a:0c:d3:e0</td>
<td>128</td>
<td>DIST-1B</td>
</tr>
</tbody>
</table>

All 1 out of 1 Total Num of i-sid FDB Entries displayed

View C-MACs learned on a T-UNI I-SID for a specific MAC address.

Switch:1#show i-sid mac-address-entry mac cc:f9:54:ae:38:64

I-SID Fdb Table

<table>
<thead>
<tr>
<th>I-SID</th>
<th>STATUS</th>
<th>MAC-ADDRESS</th>
<th>INTERFACE</th>
<th>TYPE</th>
<th>DEST-MAC</th>
<th>BVLAN</th>
<th>DEST-SYSNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>252</td>
<td>learned</td>
<td>cc:f9:54:ae:38:64</td>
<td>Port-1/15</td>
<td>REMOTE</td>
<td>00:13:0a:0c:d3:e0</td>
<td>128</td>
<td>DIST-1B</td>
</tr>
</tbody>
</table>

All 1 out of 1 Total Num of i-sid FDB Entries displayed

View C-MACs learned on aT-UNI I-SID for a specific port.

Switch:1#show i-sid mac-address-entry port 1/15

I-SID Fdb Table

<table>
<thead>
<tr>
<th>I-SID</th>
<th>STATUS</th>
<th>MAC-ADDRESS</th>
<th>INTERFACE</th>
<th>TYPE</th>
<th>DEST-MAC</th>
<th>BVLAN</th>
<th>DEST-SYSNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>252</td>
<td>learned</td>
<td>cc:f9:54:ae:38:64</td>
<td>Port-1/15</td>
<td>REMOTE</td>
<td>00:13:0a:0c:d3:e0</td>
<td>128</td>
<td>DIST-1B</td>
</tr>
</tbody>
</table>

All 1 out of 1 Total Num of i-sid FDB Entries displayed
View C-MACs learned on a T-UNI I-SID as a remote MAC address.

Switch:1#show i-sid mac-address-entry remote

<table>
<thead>
<tr>
<th>I-SID Fdb Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-SID STATUS</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>252</td>
</tr>
</tbody>
</table>

All 1 out of 1 Total Num of i-sid FDB Entries displayed

Variable definitions

Use the data in the following table to use the `show i-sid mac-address-entry` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-16777215&gt;</code></td>
<td>Displays the MAC address learned on the service interface identifier (I-SID).</td>
</tr>
<tr>
<td><code>mac &lt;0x00:0x00:0x00:0x00:0x00&gt;</code></td>
<td>Displays the I-SID FDB details for the specified MAC address.</td>
</tr>
<tr>
<td><code>port {slot/port[/sub-port] [-slot/port[/sub-port]] [...]}</code></td>
<td>Displays the MAC address learned on the specified port or port list.</td>
</tr>
<tr>
<td><code>remote</code></td>
<td>Displays the remote MAC address learned on the I-SID.</td>
</tr>
</tbody>
</table>

Job aid

The following table describes the fields in the output for the `show i-sid mac-address-entry` command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-SID</td>
<td>Specifies the service interface identifier (I-SID).</td>
</tr>
<tr>
<td>STATUS</td>
<td>Specifies the learning status of the associated MAC.</td>
</tr>
<tr>
<td>MAC-ADDRESS</td>
<td>Specifies the MAC address of the port assigned to the specific I-SID or MAC learned on the specific I-SID.</td>
</tr>
<tr>
<td>INTERFACE</td>
<td>Specifies the port or MLT on which the MAC is learned for the specific I-SID.</td>
</tr>
<tr>
<td>TYPE</td>
<td>Specifies whether the MAC is a Local or IST PEER or a Remote MAC.</td>
</tr>
</tbody>
</table>
### Viewing I-SID maximum MAC-limit

Perform this procedure to view the maximum MAC learning limit information for an I-SID.

⚠️ **Important:**

The command `show i-sid limit-fdb-learning` is supported only on the Avaya Virtual Services Platform 4000 Series.

**About this task**

The total MAC learning limit per switch is 32000. MAC learning on I-SID stops when the maximum limit is reached.

**Procedure**

View the maximum MAC learning limit configured for an I-SID:

```
show i-sid limit-fdb-learning <1-16777215>
```

**Example**

**View maximum MAC learning limit for all I-SIDs.**

```
Switch:1#show i-sid limit-fdb-learning

====================================================================================================
<table>
<thead>
<tr>
<th>Isid</th>
<th>MAC-Limit</th>
<th>MAXMAC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>STATUS</td>
<td>COUNT</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>10</td>
<td>disabled</td>
<td>32000</td>
</tr>
<tr>
<td>11</td>
<td>disabled</td>
<td>32000</td>
</tr>
<tr>
<td>12</td>
<td>disabled</td>
<td>32000</td>
</tr>
<tr>
<td>15</td>
<td>disabled</td>
<td>32000</td>
</tr>
<tr>
<td>101</td>
<td>disabled</td>
<td>32000</td>
</tr>
</tbody>
</table>

All 5 out of 5 Total Num of i-sid Info displayed
```

**View maximum MAC learning limit for a specific I-SID.**

```
Switch:1#show i-sid limit-fdb-learning 10

====================================================================================================
<table>
<thead>
<tr>
<th>Isid</th>
<th>MAC-Limit</th>
<th>MAXMAC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>STATUS</td>
<td>COUNT</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>10</td>
<td>disabled</td>
<td>32000</td>
</tr>
</tbody>
</table>
```

Comments on this document? infodev@avaya.com
Variable definitions

Use the data in the following table to use the `show i-sid limit-fdb-learning` command.

⚠️ **Important:**

The command `show i-sid limit-fdb-learning` is supported only on the Avaya Virtual Services Platform 4000 Series.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>limit-fdb-learning</td>
<td>Displays the I-SID-based maximum MAC limit information.</td>
</tr>
<tr>
<td>&lt;1–6777215&gt;</td>
<td>Displays the service interface identifier (ISID). The ISID range is 1 to 16777215.</td>
</tr>
</tbody>
</table>

Job aid

The following table describes the fields in the output of the `show i-sid limit-fdb-learning` command.

⚠️ **Important:**

The command `show i-sid limit-fdb-learning` is supported only on the Avaya Virtual Services Platform 4000 Series.

Table 61: `show i-sid limit-fdb-learning`

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISID ID</td>
<td>Specifies the service interface identifier (ISID)</td>
</tr>
<tr>
<td>MAC-LIMIT STATUS</td>
<td>Specifies whether the MAC learning limit is enabled or disabled</td>
</tr>
<tr>
<td>MAXMAC COUNT</td>
<td>Specifies the MAC learning limit</td>
</tr>
</tbody>
</table>
Chapter 26: Troubleshooting MACsec

Use the information in this section to troubleshoot problems with the MACsec feature.

**Note:**

MACsec is supported only on the 4450GSX-PWR+ model of the VSP 4000. It is not supported on the VSP 4000 4850GTS Series models.

The switch also supports viewing MACsec performance statistics. For more information on the supported statistics and procedures to view them, see *Performance Management of Avaya Virtual Services Platform 4000 Series*, NN46251-701.

---

**Viewing the MACsec connectivity association details**

Perform this procedure to view the MACsec connectivity association (CA) details.

**Procedure**

1. Enter Privileged EXEC mode:
   
   ```
   enable
   ```

2. View the MACsec connectivity association (CA) details:

   ```
   show macsec connectivity-association WORD<5–15>
   ```

   **Note:**

   This command displays the MACsec connectivity association (CA) details, including the MD5 hashed value of the CA key.

---

**Example**

View the MACsec connectivity association details:

```
Switch:1>enable
Switch:1#show macsec connectivity-association ca333
```

```
========================================================================
MACSEC Connectivity Associations Info
========================================================================
<table>
<thead>
<tr>
<th>Connectivity Association Name</th>
<th>Connectivity Association Key Hash</th>
<th>Port Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca333</td>
<td>1304a8fcc51296e7229683ff6882424a</td>
<td>1/49</td>
</tr>
</tbody>
</table>
```

---

Comments on this document? infodev@avaya.com
Viewing MACsec status

Perform this procedure to view MACsec status.

About this task

This command displays the status for the following:

- MACsec status
- MACsec encryption status
- The associated Connectivity Association (CA) name

Note:

If you do not specify a port number, the information on all MACsec capable interfaces is displayed.

Procedure

1. Enter Privileged EXEC mode:
   
   enable

2. View the MACsec status:
   
   show macsec status {slot/port[/sub-port][-slot/port[/sub-port]] [,...]}

Example

View the MACsec status:

Note:

The current release does not support replay protect.

Switch:1>enable
Switch:1#show macsec status

===========================================================================
MACSEC Port Status
===========================================================================
<table>
<thead>
<tr>
<th>PortId</th>
<th>MACSEC</th>
<th>Encryption</th>
<th>Replay</th>
<th>Replay W'dow</th>
<th>Encryption Offset</th>
<th>CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/49</td>
<td>enabled</td>
<td>enabled</td>
<td>disabled</td>
<td>--</td>
<td>ipv4Offset(30)</td>
<td>ca333</td>
</tr>
<tr>
<td>1/50</td>
<td>disabled</td>
<td>disabled</td>
<td>disabled</td>
<td>--</td>
<td>none</td>
<td>Nil</td>
</tr>
</tbody>
</table>

Switch:1#show macsec status 1/49

===========================================================================
MACSEC Port Status
===========================================================================
<table>
<thead>
<tr>
<th>PortId</th>
<th>MACSEC</th>
<th>Encryption</th>
<th>Replay</th>
<th>Replay W'dow</th>
<th>Encryption Offset</th>
<th>CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/49</td>
<td>enabled</td>
<td>enabled</td>
<td>disabled</td>
<td>--</td>
<td>ipv4Offset(30)</td>
<td>ca333</td>
</tr>
</tbody>
</table>
Chapter 27: Troubleshooting MACsec using EDM

Use the information in this section to troubleshoot problems with the MACsec feature using Enterprise Device Manager (EDM) interface.

⚠️ Note:

MACsec is supported only on the 4450GSX-PWR+ model of the VSP 4000. It is not supported on the VSP 4000 4850GTS Series models.

Viewing MACsec connectivity association details

Perform this procedure to view the MACsec connectivity association (CA) details.

Procedure

1. In the Device Physical View, click on the chassis.
2. In the navigation pane, expand the following folders: Configuration > Edit.
3. Click Chassis.
4. In the Chassis window, click the MAC Security tab.
Chapter 28: Troubleshooting Fabric Attach

The following sections help you troubleshoot problems with Fabric Attach (FA) using either the Avaya Command Line Interface (ACLI) or the Enterprise Device Manager (EDM).

Troubleshooting workflow

Troubleshoot FA in the following sequence:

• Verify FA configuration:
  As a first step, for proper operation, verify that FA is enabled properly at both the global and interface levels. Use the procedures in this section to verify FA configuration.

• Verify LLDP port-level transmission and reception:
  LLDP operates at the interface level. Enabling FA at the port level automatically enables LLDP transmission and reception at the port level. Similarly, enabling FA at the MLT level automatically enables LLDP transmission and reception for all ports in that MLT. Use the procedures in this section to verify LLDP interface (port or MLT) statistics.

• Verify FA discovery, I-SID-to-VLAN mapping assignments and Switched UNI I-SID creation:
  After you verify LLDP transmission, verify that FA element discovery completed successfully. After a successful FA discovery, FA clients can send I-SID-to-VLAN mapping assignments to the FA Server on an FA-enabled port or MLT. The FA server accepts or rejects these mapping assignments. A prerequisite to successful mapping assignments is that IS-IS and SPBM are properly configured on the FA server. Successful FA mappings result in the creation of ELAN I-SIDs with end-points of type Switched UNI on the FA Server switch.

Troubleshooting Fabric Attach using the ACLI

Verify configuration of Fabric Attach

Viewing Fabric Attach configuration

To operate properly, Fabric Attach (FA) must be configured properly at both the global and interface level on the switch. Use this procedure to verify FA configuration.
Procedure

1. Enter Privileged EXEC mode:
   
enable

2. To verify that FA is enabled globally, enter one of the following commands:
   
   • show fa
   • show fa agent

3. To view all FA interfaces (ports and MLTs), enter:
   
   show fa interface

4. To view FA interface configuration on ports, use one of the following commands:
   
   • To view FA configuration on all ports, enter:
     
     show fa interface port
   
   • To view FA configuration on a specific port, enter:
     
     show fa interface port [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]

5. To view FA interface configuration on MLTs, use one of the following commands:
   
   • To view FA configuration on all MLTs, enter:
     
     show fa interface mlt
   
   • To view FA configuration on a specific MLT, enter:
     
     show fa interface mlt [<1-512>]
   
   • To view FA interface configuration based on the authentication status, enter:
     
     show fa interface [enabled-auth] [disabled-auth]

Example

Verify that FA is configured globally.

Switch:1#show fa

===================================================================
Fabric Attach Configuration
===================================================================
 FA Service : enabled
 FA Element Type : server
 FA Assignment Timeout : 240
 FA Discovery Timeout : 240
 FA Provision Mode : spbm

Verify FA configuration at the interface (port or MLT) level, on all interfaces.

In the following example output, note that:

• FA is enabled on interfaces 2/10, 4/11 and Mlt2.
• Both FA and message authentication are disabled on port 4/6.
• Both FA and message authentication are enabled on port 4/11.

Switch:1#show fa interface

```
====================================================================
Fabric Attach Interfaces  
====================================================================
INTERFACE    SERVER   MGMT  MGMT  MSG AUTH  MSG AUTH
STATUS   ISID  CVID STATUS  KEY
-------------------------------------------------------------
Port2/10     enabled  0  0  disabled ****
Port4/6      disabled 0  0  disabled ****
Port4/11     enabled  0  0  enabled ****
Mlt2         enabled  0  0  disabled ****
-------------------------------------------------------------
4 out of 4 Total Num of fabric attach interfaces displayed
```

Verify FA configuration on a specific port, for example, on port 2/10.

Switch:1#show fa interface port 2/10

```
====================================================================
Fabric Attach Interfaces  
====================================================================
INTERFACE    SERVER   MGMT  MGMT  MSG AUTH  MSG AUTH
STATUS   ISID  CVID STATUS  KEY
-------------------------------------------------------------
Port2/10     enabled  0  0  disabled ****
-------------------------------------------------------------
1 out of 1 Total Num of fabric attach interfaces displayed
```

Verify FA configuration on an MLT, for example, on Mlt2.

Switch:1#show fa interface mlt 2

```
====================================================================
Fabric Attach Interfaces  
====================================================================
INTERFACE    SERVER   MGMT  MGMT  MSG AUTH  MSG AUTH
STATUS   ISID  CVID STATUS  KEY
-------------------------------------------------------------
Mlt2         enabled  0  0  disabled ****
-------------------------------------------------------------
1 out of 1 Total Num of fabric attach interfaces displayed
```

View the FA interfaces that have authentication enabled:

Switch:1#show fa interface enabled-auth

```
====================================================================
Fabric Attach Interfaces  
====================================================================
INTERFACE    SERVER   MGMT  MGMT  MSG AUTH  MSG AUTH
STATUS   ISID  CVID STATUS  KEY
-------------------------------------------------------------
Port4/11     enabled  0  0  enabled ****
```

January 2017
View the FA interfaces that have authentication disabled:

Switch:1#show fa interface disabled-auth

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>SERVER</th>
<th>MGMT</th>
<th>MGMT</th>
<th>MSG AUTH</th>
<th>MSG AUTH</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>STATUS</td>
<td>ISID</td>
<td>CVID</td>
<td>STATUS</td>
<td>KEY</td>
</tr>
<tr>
<td>Port2/10</td>
<td>enabled</td>
<td>0</td>
<td>0</td>
<td>disabled</td>
<td>****</td>
</tr>
<tr>
<td>Port4/6</td>
<td>disabled</td>
<td>0</td>
<td>0</td>
<td>disabled</td>
<td>****</td>
</tr>
<tr>
<td>Mlt2</td>
<td>enabled</td>
<td>0</td>
<td>0</td>
<td>disabled</td>
<td>****</td>
</tr>
</tbody>
</table>

Related links

Troubleshooting Fabric Attach on page 309

Verify LLDP port-level transmission and reception

Viewing port-based LLDP statistics

Use this procedure to verify port-based LLDP statistics.

About this task

LLDP operates at the interface level. Enabling FA on a port automatically enables LLDP transmission and reception on the port. It also enables traffic tagging and disables spanning tree on that port.

Enabling FA on an MLT enables LLDP transmission and reception on all ports in the MLT.

*Note:

When FA is enabled on ports in an MLT or LACP MLT, tagging is enabled and spanning tree is disabled on those ports.

When a port is removed from an MLT, LLDP transmission on that port stops and spanning tree is enabled. Any I-SID-to-VLAN mappings on that port are removed, if not already learned on any other port in the MLT. This also causes the Switched UNI I-SID to be deleted from the MLT. If however, the mappings are learned on another port on the MLT, then the Switched UNI I-SID continues to exist for that MLT.

Procedure

1. Enter Privileged EXEC mode:
   
   enable

2. Verify LLDP statistics:
   
   show lldp stats
3. Verify successful LLDP transmission on a port:
   
   ```
   show lldp tx-stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
   ```

4. Verify that the port is receiving LLDP PDUs successfully:
   
   ```
   show lldp rx-stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
   ```

5. (Optional) To clear LLDP statistics, enter one of the following commands:
   
   - Clear LLDP global statistics using `clear lldp stats summary`
   - Clear LLDP statistics on ports using `clear lldp stats {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

**Example**

Verify LLDP transmission statistics on a port:

Switch:1>en
Switch:1#show lldp tx-stats port 1/2

```
================================================================
LLDP Tx-Stats
================================================================
PORT NUM    FRAMES
----------------------------------------------
1/2          100
```

Verify that the port is receiving LLDP PDUs,

Switch:1#show lldp rx-stats port 1/2

```
================================================================================
LLDP Rx-Stats
================================================================================
Port     Frames   Frames      Frames   TLVs        TLVs           AgeOuts
Num      Discarded Errors   Total    Discarded   Unsupported   (Non FA)   (Non FA)
--------------------------------------------------------------------------------
1/2       0           0        46       0           0              0
```

**Related links**

- [Troubleshooting Fabric Attach](#) on page 309
- [Variable definitions](#) on page 313

**Variable definitions**

Use the data in the following table to use the `show lldp tx-stats` and the `show lldp rx-stats` commands.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>{slot/port[/sub-port][-slot/port[/sub-port]][,...]}</td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of</td>
</tr>
</tbody>
</table>
### Verify FA discovery and I-SID-to-VLAN mapping assignments

#### Displaying learned LLDP neighbors

Use this procedure to verify details of the LLDP neighbors learned.

**Procedure**

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. Verify details of LLDP neighbors learned:
   ```
   show lldp neighbor
   ```
3. Verify details of LLDP neighbors learned on a specific port:
   ```
   show lldp neighbor port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
   ```

**Example**

The following example shows how two switches—an FA Server and an FA Proxy discover each other as LLDP neighbors. Switch A, which is the FA Server is an Avaya VSP 7200 Series switch (model 7254XSQ) and switch B which is the proxy device is an Avaya ERS 4826GTS switch. The following examples shows neighbor discovery on non-channelized and channelized ports (if your platform supports channelization).

On the non-channelized port 1/1 on the VSP 7200 Series switch (FA Server), verify neighbor discovery of the proxy switch.

SwitchA:1>en
SwitchA:1#show lldp neighbor

```
==========================================================================================
<table>
<thead>
<tr>
<th>LLDP Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port: 1/1       Index    : 1                  Time: 1 day(s), 04:03:52</td>
</tr>
<tr>
<td>ChassisId: MAC Address        70:30:18:5a:05:00</td>
</tr>
<tr>
<td>PortId : MAC Address        70:30:18:5a:05:07</td>
</tr>
<tr>
<td>SysName :</td>
</tr>
<tr>
<td>SysCap : Br / Br</td>
</tr>
<tr>
<td>PortDescr: Port 7</td>
</tr>
<tr>
<td>SysDescr : Ethernet Routing Switch 4826GTS HW:10 FW:5.8.0.1 SW:v5.9.2.027</td>
</tr>
</tbody>
</table>
```

---

(Related links)

Viewing port-based LLDP statistics on page 312
On the proxy switch, verify discovery of the FA Server (VSP 7200 Series) switch.

SwitchB:1>en
SwitchB:1#show lldp neighbor

```
Port: 7     Index: 71                 Time: 12 days, 21:40:30
ChassisId: MAC address        a4:25:1b:52:70:00
PortId:    MAC address        a4:25:1b:52:70:04
SysName:   BEB1-7254XSQ
SysCap:    rB / rB            (Supported/Enabled)
PortDesc:  Avaya Virtual Services Platform 7254XSQ - Gbic1000BaseT Port 1/1
SysDescr:  VSP-7254XSQ (5.0.0.0_GA)
```

Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 1

On the channelized port 1/1/1 on the VSP 7200 Series switch (FA Server), verify discovery of the proxy switch.

SwitchA:1>en
SwitchA:1#show lldp neighbor

```
Port: 1/1/1     Index    : 1                  Time: 1 day(s), 04:03:52
ChassisId: MAC Address        70:30:18:5a:05:00
PortId   : MAC Address        70:30:18:5a:05:07
SysName  : 
SysCap   : Br / Br
PortDescr: Port 7
SysDescr : Ethernet Routing Switch 4826GTS HW:10 FW:5.8.0.1  SW:v5.9.2.027
```

Verify neighbor discovery on the proxy switch.

SwitchB:1>en
SwitchB:1#show lldp neighbor

```
Port: 7     Index: 71                 Time: 12 days, 21:40:30
ChassisId: MAC address        a4:25:1b:52:70:00
PortId:    MAC address        a4:25:1b:52:70:04
```
SysName: BEB1-7254XSQ
SysCap: rB / rB (Supported/Enabled)
PortDesc: Avaya Virtual Services Platform 7254XSQ - 40GbCR4-Channel Port 1/1/1
SysDescr: VSP-7254XSQ (5.0.0.0_GA)

---

Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router; T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 1

Related links
Troubleshooting Fabric Attach on page 309
Variable definitions on page 316

Variable definitions
Use the data in the following table to use the `show lldp neighbor` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port {slot/port[/sub-port][slot/port[/sub-port]][,...]}</code></td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. Displays LLDP neighbor information on the specified port.</td>
</tr>
</tbody>
</table>

Related links
Displaying learned LLDP neighbors on page 314

Viewing Fabric Attach discovered elements
Use this procedure to view Fabric Attach discovered elements.

About this task
When FA is enabled on an FA Server switch, LLDP PDUs are exchanged between the FA Server and FA Clients or FA Proxies. Standard LLDPs allow neighbors to be learned. With the help of organizational-specific element discovery TLVs, the client or proxy recognizes that it has attached to the FA Server. Only after the discovery handshake is complete, an FA Client or FA Proxy can transmit I-SID-to-VLAN assignments to join the SPB Fabric network through the FA Server.

Procedure
1. Enter Privileged EXEC mode:
   
   `enable`

2. Display FA discovered elements:

   `show fa elements`

3. Display FA discovered elements on a specific port:
show fa elements [{slot/port[/sub-port]} {-slot/port[/sub-port]} [,...]]

Example

The following example displays the sample output for the `show fa elements` command.

Switch:1#show fa elements

```
--------------------------------------------------------------------------------
| Fabric Attach Discovery Elements                                         |
--------------------------------------------------------------------------------
| PORT | TYPE | VLAN | STATE | SYSTEM-ID | ELEM | ASGN | AUTH | AUTH |
--------------------------------------------------------------------------------
| 1/5  | proxy| 710   | T/S   | 50:61:84:ee:8c:00:20:00:00:01 | AP   | AP   |
| 1/6  | proxy| 710   | T/S   | 50:61:84:ee:8c:00:20:00:00:01 | AP   | AP   |
--------------------------------------------------------------------------------
```

```
Fabric Attach Authentication Detail

```
```
<table>
<thead>
<tr>
<th>PORT</th>
<th>AUTH STATUS</th>
<th>ELEM</th>
<th>OPER</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/5</td>
<td>successAuth</td>
<td>AP</td>
<td>AP</td>
</tr>
<tr>
<td>1/6</td>
<td>successAuth</td>
<td>AP</td>
<td>AP</td>
</tr>
</tbody>
</table>
```

State Legend: (Tagging/AutoConfig)
T= Tagged, U= Untagged, D= Disabled, S= Spbm, V= Vlan, I= Invalid

Auth Legend:
AP= Authentication Pass, AP= Authentication Fail,
NA= Not Authenticated, N= None

2 out of 2 Total Num of fabric attach discovery elements displayed

Related links

- [Troubleshooting Fabric Attach](#)

Viewing Fabric Attach statistics

If FA discovery fails, use this procedure to display FA statistics to determine if FA discovery TLVs were processed. You can also view the FA assignment statistics to determine the number of FA assignments that were accepted or rejected by the FA Server.

You can view the statistics at either the global level or at the port (interface) level.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```

2. View global level FA statistics:
   ```
   show fa statistics [summary]
   ```
3. View FA statistics at the slot/port level:

   ```
   show fa statistics [{slot/port[/sub-port] [-slot/port[/sub-port]] ,...}]
   ```

   **Note:**

   If a slot is removed from the switch chassis, the FA statistics are not displayed on the slot ports. When the slot is inserted back again, the statistics counters are reset.

4. (Optional) Clear FA statistics:

   ```
   clear fa statistics [summary] [{slot/port[/sub-port] [-slot/port[/sub-port]] ,...}] 
   ```

**Examples**

Viewing FA discovery and assignment statistics:

Switch:1>en
Switch:1#show fa statistics

```
== Fabric Attach STATISTICS ========
Port  DiscElem DiscElem DiscElem DiscAuth
     Received Expired Deleted Failed
1/1   3057      0      1      0
1/2   2000      0      1      0
```

```
== Fabric Attach ASSIGNMENTS STATISTICS ========
Port  Asgn Asgn Asgn Asgn Asgn AsgnAuth
     Received Accepted Rejected Expired Deleted Failed
1/1   3149     3      1      3      0      0
1/2   1500     0      1      2      0      0
```

View a summary of the FA discovery and assignment statistics:

Switch:1#show fa statistics summary

```
== Fabric Attach STATISTICS SUMMARY ========
Port  DiscElem DiscElem DiscElem DiscAuth
     Received Expired Deleted Failed
1/1   3057      0      1      0
1/2   2000      0      1      0
```

```
== Fabric Attach ASSIGNMENTS STATISTICS SUMMARY ========
Port  Asgn Asgn Asgn Asgn Asgn AsgnAuth
     Received Accepted Rejected Expired Deleted Failed
1/1   3149     3      1      3      0      0
1/2   1500     0      1      2      0      0
```
Viewing FA statistics on a specific port (port 1/1):

Switch:1>en
Switch:1#show fa statistics 1/1

Fabric Attach STATISTICS

<table>
<thead>
<tr>
<th>Port</th>
<th>DiscElem</th>
<th>DiscElem</th>
<th>DiscElem</th>
<th>DiscAuth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>3057</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Fabric Attach ASSIGNMENTS STATISTICS

<table>
<thead>
<tr>
<th>Port</th>
<th>Asgn</th>
<th>Asgn</th>
<th>Asgn</th>
<th>Asgn</th>
<th>Asgn</th>
<th>Asgn</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>3149</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Optionally, clear FA statistics and verify that the statistics are cleared.

Switch:1#clear fa statistics
Switch:1#show fa statistics

<table>
<thead>
<tr>
<th>Port</th>
<th>DiscElem</th>
<th>DiscElem</th>
<th>DiscElem</th>
<th>DiscAuth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Asgn</th>
<th>Asgn</th>
<th>Asgn</th>
<th>Asgn</th>
<th>Asgn</th>
<th>Asgn</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Related links

Troubleshooting Fabric Attach on page 309
Variable definitions on page 319

Variable definitions

Use the data in the following table to use the show fa statistics command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Displays global level fabric attach statistics</td>
</tr>
<tr>
<td>{slot/port[/sub-port][-slot/port[/sub-port]][...]}</td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your</td>
</tr>
</tbody>
</table>

Table continues…
platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Displays Fabric Attach statistics on ports.

Use the data in the following table to use the **clear fa statistics** command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Clears global level fabric attach statistics</td>
</tr>
<tr>
<td>{slot/port[/sub-port][{-slot/port[/sub-port]}[...]}</td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. Clears Fabric Attach statistics on ports.</td>
</tr>
</tbody>
</table>

**Related links**

- [Viewing Fabric Attach statistics](#) on page 317

**Viewing Fabric Attach I-SID-to-VLAN assignments**

Use this procedure to display the I-SID-to-VLAN assignments advertised by an FA Client or an FA Proxy, to be supported on the FA Server. These assignments can be accepted or rejected by the FA Server. An assignment that is successfully accepted by the FA Server results in the creation of a Switched UNI I-SID on the interface.

**Before you begin**

Verify that IS-IS and SPBM are properly configured on the FA Server switch.

- Verify SPBM configuration using the command `show running-config module spbm`.
- Verify IS-IS configuration using one of the following commands:
  - `show isis`
  - `show isis interface`
  - `show isis adjacency`
  - `show isis lsdb`

**Procedure**

1. Enter Privileged EXEC mode:
   ```bash
enable
   ```
2. Display FA I-SID-to-VLAN assignments:
   ```bash
   show fa assignment
   ```
3. Display FA I-SID-to-VLAN assignments on specific ports:
show fa assignment [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}]

**Example**

The following example displays a sample output for the `show fa assignment` command.

**Note:**

The state of I-SID-to-VLAN assignments on a client or proxy device is pending until it is changed by the FA Server to active or reject.

Switch:>en
Switch:1#show fa assignment
=======================================================================
<table>
<thead>
<tr>
<th>Interface</th>
<th>I-SID</th>
<th>Vlan</th>
<th>State</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>2</td>
<td>2</td>
<td>active</td>
<td>proxy</td>
</tr>
<tr>
<td>1/2</td>
<td>3</td>
<td>3</td>
<td>active</td>
<td>proxy</td>
</tr>
<tr>
<td>1/2</td>
<td>4</td>
<td>4</td>
<td>active</td>
<td>proxy</td>
</tr>
<tr>
<td>1/3</td>
<td>5</td>
<td>5</td>
<td>reject</td>
<td>proxy</td>
</tr>
</tbody>
</table>
-----------------------------------------------------------------------
4 out of 4 Total Num of fabric attach assignment mappings displayed

**Related links**

Troubleshooting Fabric Attach on page 309
Variable definitions on page 321

**Variable definitions**

Use the data in the following table to use the `show fa assignment` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{slot/port[/sub-port][-slot/port[/sub-port]][,...]}</code></td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.</td>
</tr>
</tbody>
</table>

**Related links**

Viewing Fabric Attach I-SID-to-VLAN assignments on page 320

**Displaying Switched UNI (ELAN) I-SID information**

Use this procedure to display information on FA-created Switched UNI (ELAN) I-SIDs.

**Procedure**

1. Enter Privileged EXEC mode:
enable

2. Display all Switched UNI (ELAN) I-SIDs:
   
   show i-sid elan

3. Display ELAN I-SID information on an MLT:
   
   show mlt i-sid [<1–512>]

   **Note:**

   Viewing ELAN I-SID information on an MLT is useful to understand the origin of the I-SID when multiple client or proxy devices connecting to the FA Server using SMLT MLT advertise the same I-SID-to-VLAN mappings. In the event of a link failure on an MLT, the origin of the I-SID helps determine on which MLT, and thereby from which proxy or client device, the mappings were successfully learnt.

4. Display ELAN I-SID information on ports:
   
   show interfaces gigabitEthernet i-sid [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]]}

**Example**

Display information on all Switched UNI (ELAN) I-SIDs.

The following sample output displays, for example, the I-SID information on one of the peer switches of the FA Server, in a dual-homed SMLT configuration.

```
Switch:1>en
Switch:1#show i-sid elan

==========================================================================================
<table>
<thead>
<tr>
<th>ISID</th>
<th>ISID TYPE</th>
<th>VLANID</th>
<th>PORT</th>
<th>MLT</th>
<th>ORIGIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>ELAN</td>
<td>N/A</td>
<td>c2002:1/10</td>
<td>-</td>
<td>DISC_LOCAL</td>
</tr>
<tr>
<td>4000</td>
<td>ELAN</td>
<td>N/A</td>
<td>-</td>
<td>c4000:1</td>
<td>DISC_BOTH</td>
</tr>
<tr>
<td>4001</td>
<td>ELAN</td>
<td>N/A</td>
<td>-</td>
<td>c4001:1</td>
<td>DISC_LOCAL</td>
</tr>
<tr>
<td>4030</td>
<td>ELAN</td>
<td>N/A</td>
<td>-</td>
<td>c4030:1</td>
<td>DISC_BOTH</td>
</tr>
<tr>
<td>4051</td>
<td>ELAN</td>
<td>N/A</td>
<td>-</td>
<td>c4051:1</td>
<td>DISC_BOTH</td>
</tr>
<tr>
<td>10200</td>
<td>ELAN</td>
<td>N/A</td>
<td>-</td>
<td>c200:1</td>
<td>DISC_REMOTE</td>
</tr>
</tbody>
</table>
```

c: customer vid  u: untagged-traffic

All 6 out of 6 Total Num of Elan i-sids displayed

**Note:**

The I-SID TYPE field displays once for each I-SID. The I-SID TYPE of an I-SID that is either learned through FA mapping assignments or configured as an FA management I-SID, is always ELAN. If a platform VLAN has the same I-SID value as that of the I-SID in an FA mapping assignment or in an FA management I-SID configuration, then the platform VLAN is associated with the I-SID endpoint and appears in the VLANID column.
Note:

- The ORIGIN field displays once for each I-SID. It indicates the origin of the I-SID and not the origin of the I-SID endpoint. To view the origin of the I-SID endpoints, execute either the `show mlt i-sid` or the `show interfaces gigabitEthernet i-sid` command.

- The origin of I-SID 4000 displays as DISC_BOTH, because it is discovered on both vIST peers.

- The origin of I-SID 4001 displays as DISC_LOCAL because it is first discovered on the local FA Server switch.

- The origin of I-SID 10200 displays as DISC_REMOTE because it is first discovered on the peer switch and then synchronized with the local switch.

- If the origin of an I-SID is DISC_LOCAL, DISC_REMOTE, DISC_BOTH or MANAGEMENT, it changes to CONFIG, after you manually configure an endpoint on the I-SID.

Display MLT I-SID information for MLT 1.

In this sample output, the ORIGIN field indicates the origin of the I-SID endpoint.

```
Switch:1#show mlt i-sid 1
================================================================================
MLT Isid Info
================================================================================
ISID               ISID
MLTID IFINDEX ID   VLANID C-VID  TYPE     ORIGIN           BPDU
--------------------------------------------------------------------------------
1     6144    4000     N/A    4000   ELAN     DISC_BOTH
1     6144    4001     N/A    4001   ELAN     DISC_LOCAL
1     6144    4030     N/A    4030   ELAN     DISC_BOTH
1     6144    4051     N/A    4051   ELAN     DISC_BOTH
1     6144    10200    N/A    200    ELAN     DISC_REMOTE
--------------------------------------------------------------------------------
5 out of 6 Total Num of i-sid endpoints displayed
```

Display I-SID information on the port 1/10:

In this sample output, the ORIGIN field indicates the origin of the I-SID endpoint.

```
Switch:1#show interfaces gigabitEthernet i-sid 1/10
================================================================================
PORT Isid Info
================================================================================
ISID               ISID
PORTNUM IFINDEX ID VLANID C-VID  TYPE     ORIGIN           BPDU
--------------------------------------------------------------------------------
1/10    201     2002     N/A    601    ELAN     DISC_LOCAL
--------------------------------------------------------------------------------
1 out of 6 Total Num of i-sid endpoints displayed
```

Related links

[Troubleshooting Fabric Attach](#) on page 309
Variable definitions on page 324

Variable definitions

Use the data in the following table to use the `show i-sid` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>elan</td>
<td>Displays all ELAN I-SIDs.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `show mlt i-sid` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1–512&gt;</td>
<td>The valid range for MLT ID.</td>
</tr>
</tbody>
</table>

Use the data in the following table to use the `show interfaces gigabitEthernet i-sid` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>{slot/port/[sub-port] [-slot/port/[sub-port]] [...]}</td>
<td>Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.</td>
</tr>
</tbody>
</table>

Related links

- [Displaying Switched UNI (ELAN) I-SID information](#) on page 321

Troubleshooting Fabric Attach using the EDM

Verify configuration of Fabric Attach

Configuring Fabric Attach globally

Use this procedure to configure FA globally or view existing FA global configuration.

**Procedure**

1. In the navigation pane, navigate to Configuration > Edit > Fabric Attach.
2. In the content pane, click the Globals tab.
3. To enable or disable the Fabric Attach service, click enabled or disabled in the Service field.
**Caution:**
Disabling FA flushes all FA element discovery and mappings.

4. View the element type in the **ElementType** field.

**Note:**
The only supported element type is **faServer** (FA Server).

5. To specify the assignment time-out, enter a time-out value in seconds in the **AsgnTimeout** field.

6. View the provision mode in the **ProvisionMode** field.

**Note:**
The supported provision mode is **spbm**.

7. To specify the discovery time-out, enter a time-out value in seconds in the **DiscTimeout** field.

8. To clear the error counters, select the check boxes **ClearErrorCounters** and/or **ClearGlobalErrorCounters**.

9. Click **Apply**.

**Fabric Attach Globals field descriptions**
Use the data in the following table to use the **Fabric Attach Globals** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Enables or disables Fabric Attach service globally.</td>
</tr>
<tr>
<td></td>
<td>The default is enable.</td>
</tr>
<tr>
<td>ElementType</td>
<td>Specifies the Fabric Attach element type.</td>
</tr>
<tr>
<td></td>
<td>The supported element type is Fabric Attach Server.</td>
</tr>
<tr>
<td>AsgnTimeout</td>
<td>Specifies the Fabric Attach assignment time-out in seconds.</td>
</tr>
<tr>
<td></td>
<td>The range is 45 to 480 seconds. The default is 240 seconds.</td>
</tr>
<tr>
<td>ProvisionMode</td>
<td>Specifies the Fabric Attach provision mode.</td>
</tr>
<tr>
<td></td>
<td>The supported provision mode is SPB.</td>
</tr>
<tr>
<td>DiscTimeout</td>
<td>Specifies the Fabric Attach discovery time-out in seconds.</td>
</tr>
<tr>
<td></td>
<td>The range is 45 to 480 seconds. The default is 240 seconds.</td>
</tr>
</tbody>
</table>

**Configuring Fabric Attach interface-level settings**
Use this procedure to configure FA interface-level settings or view existing interface-level settings.

You can enable Fabric Attach on a port, static MLT or an LACP MLT. Enabling FA on a port not only enables tagging but also disables spanning tree on that port. Enabling FA on an MLT enables FA on all ports of the MLT. When FA is enabled on ports in an MLT or LACP MLT, tagging is enabled and spanning tree is disabled on all those ports.
Before you begin

Ensure that FA is enabled globally on the switch.

About this task

Enabling FA on a port or MLT is necessary for element discovery. On the FA Server, FA is enabled globally by default. However, you must explicitly enable FA on a desired port or MLT interface, following which the FA Server can begin transmitting LLDP PDUs that contain the element discovery TLVs. This information is received by FA Client and FA Proxy devices which in turn also transmit their FA capabilities and settings. After the element handshake completes, the FA Server receives I-SID-to-VLAN assignment mappings from the connected client or proxy devices, on that port or MLT.

Procedure

1. In the navigation pane, expand the Configuration > Edit > Fabric Attach folders.
2. Click the Ports tab.
   The FA interface-level settings are displayed.
3. To modify existing settings, double-click on the fields on this window. After making the required changes, click Apply to save your changes.
4. To configure FA on a new port or MLT interface:
   a. Click Insert.
      The Insert Ports dialog box appears.
   b. To configure FA on a port, enter a port number in the format slot/port[/sub-port], or click Port to select from a list of available ports.
   c. To configure FA on an MLT, enter an MLT ID or click Mlt to select from a list of configured MLTs.
      ✭ Note: 
      FA is successfully enabled on the MLT, only if all ports of the MLT have FA successfully enabled. Enabling FA enables LLDP on all ports. Tagging is enabled and spanning tree is disabled.
   d. Click Insert to save your changes.
5. To remove (delete) FA on a port or MLT:
   a. In the content pane, select a port or MLT from the list.
   b. Click Delete.
      ✠ Caution: 
      Removing FA on an interface flushes all FA element discovery and I-SID-to-VLAN mappings associated with that interface.

Fabric Attach Ports field descriptions

Use the data in the following table to use the Ports tab.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IfIndex</td>
<td>Specifies the interface (port or MLT) on which Fabric Attach is configured.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies the current state of the Fabric Attach port. It is either enabled or disabled. This field indicates whether LLDP PDUs (that include FA TLVs) are generated on the port (enabled) or not (disabled).</td>
</tr>
<tr>
<td>MsgAuthStatus</td>
<td>Specifies the Fabric Attach message authentication status on the port. It is either enabled or disabled.</td>
</tr>
<tr>
<td>MsgAuthKey</td>
<td>Specifies the Fabric Attach message authentication key for the associated port. The maximum length of this key is 32 characters.</td>
</tr>
<tr>
<td>MgmtIsid</td>
<td>Specifies the Fabric Attach management I-SID for the associated port. The range is 0 to 16777215. A zero value indicates that the management I-SID is not specified for the interface.</td>
</tr>
<tr>
<td>MgmtCvid</td>
<td>Specifies the Fabric Attach management customer VLAN ID (C-VID) for the interface. A zero value indicates that no C-VID is specified for the interface. A value of 4096 indicates the port is untagged.</td>
</tr>
</tbody>
</table>

---

**Verify port-level transmission and reception**

**Viewing LLDP Reception statistics**

Use this procedure to view the LLDP reception statistics. You can also view these statistics graphically.

**About this task**

LLDP operates at the port interface level. Enabling FA on a port automatically enables LLDP transmission and reception on that port. It also enables traffic tagging and disables spanning tree on that port.

Enabling FA on an MLT enables LLDP transmission and reception on all ports in that MLT.

**Note:**

When a port is removed from an MLT, LLDP transmission on that port stops and spanning tree is enabled. Any I-SID-to-VLAN mappings on that port are removed, if not already learned on any other port in the MLT. This also causes the Switched UNI I-SID to be deleted from the MLT. If however, the mappings are learned on another port on the MLT, then the Switched UNI I-SID continues to exist for that MLT.

For ports in an LACP MLT, when FA is enabled, tagging is enabled on all ports in the LACP MLT. The consistency check for FA is based on key membership. If all ports with the same key do not support FA, FA is not successfully enabled on those ports.
Note:
If a slot is removed from the switch chassis, the statistics are not displayed on the slot ports. When the slot is inserted back again, the statistics counters are reset.

Procedure
1. In the navigation pane, navigate to Configuration > Edit > Diagnostics > 802_1ab.LLDP.
2. In the content pane, click the RX Stats tab.
3. To view the reception statistics graphically for a port:
   a. Select a row and click Graph.
      The RX Stats-Graph,<port-number> tab displays.
      You can view a graphical representation of the following data:
      • FramesDiscardedTotal — Total number of LLDP received frames that were discarded.
      • FramesErrors — Total number of erroneous LLDP frames received.
      • FramesTotal — Total number of frames received.
      • TLVsDiscardedTotal — Total number of received TLVs that were discarded.
      • TLVsUnrecognizedTotal — Total number of unrecognized TLVs received.
   b. Select one of the above parameters and click the appropriate icon on the top left-hand-side corner of the menu bar to draw a line chart, area chart, bar chart or a pie chart.
   c. Click Clear Counters to clear the existing counters, and fix a reference point in time to restart the counters.
   d. Click Export, to export the statistical data to a file.
   e. To fix a poll interval, select an appropriate value from the Poll Interval drop-down list.

LLDP Reception statistics field descriptions
Use the data in the following table to view the reception statistics.

Field descriptions for the RX Stats tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortNum</td>
<td>Specifies the port number.</td>
</tr>
<tr>
<td>FramesDiscardedTotal</td>
<td>Specifies the number of LLDP frames received on the port, but discarded.</td>
</tr>
<tr>
<td>FramesErrors</td>
<td>Specifies the number of invalid LLDP frames received on the port.</td>
</tr>
<tr>
<td>FramesTotal</td>
<td>Specifies the total number of LLDP frames received on the port.</td>
</tr>
<tr>
<td>TLVsDiscardedTotal</td>
<td>Specifies the number of LLDP TLVs discarded on the port.</td>
</tr>
<tr>
<td>TLVsUnrecognizedTotal</td>
<td>Specifies the number of LLDP TLVs on the port, that are unrecognized.</td>
</tr>
<tr>
<td>AgeoutsTotal</td>
<td>Specifies the number of LLDP age-outs that occur on a specific port.</td>
</tr>
</tbody>
</table>

Field descriptions for the RX Stats-Graph, <port-number> tab.
### Viewing LLDP transmission statistics

Use this procedure to view the LLDP transmission statistics. You can also view the statistics graphically.

**About this task**

LLDP operates at the port interface level. Enabling FA on a port automatically enables LLDP transmission and reception on that port. It also enables traffic tagging and disables spanning tree on that port.

Enabling FA on an MLT enables LLDP transmission and reception on all ports in that MLT.

**Note:**

When a port is removed from an MLT, LLDP transmission on that port stops and spanning tree is enabled. Any I-SID-to-VLAN mappings on that port are removed, if not already learned on any other port in the MLT. This also causes the Switched UNI I-SID to be deleted from the MLT. If however, the mappings are learned on another port on the MLT, then the Switched UNI I-SID continues to exist for that MLT.

For ports in an LACP MLT, when FA is enabled, tagging is enabled on all ports in the LACP MLT. The consistency check for FA is based on key membership. If all ports with the same key do not support FA, FA is not successfully enabled on those ports.

**Note:**

If a slot is removed from the switch chassis, the statistics are not displayed on the slot ports. When the slot is inserted back again, the statistics counters are reset.

**Procedure**

1. In the navigation pane, navigate to **Configuration > Edit > Diagnostics > 802_1ab.LLDP**.
2. In the content pane, click the **TX Stats** tab.
   
   The transmission statistics are displayed.
3. To view the transmission statistics graphically for a port:
   
   a. In the content pane (on the right-hand-side), select a row and click the **Graph** button.
   
   The **TX Stats-Graph,<port-number>** tab displays.
You can view a graphical representation of the LLDP frames transmitted \((\text{FramesTotal})\), for the following parameters:

- AbsoluteValue
- Cumulative
- Average/sec
- Minimum/sec
- Maximum/sec
- LastVal/sec

b. To view the graph, select one of the above parameters and click the appropriate icon on the top left-hand-side of the menu bar to draw a line chart, area chart, bar chart or a pie chart.

c. Click **Clear Counters** to clear the existing counters, and fix a reference point in time to restart the counters.

d. Click **Export**, to export the statistical data to a file.

e. To fix a poll interval, select an appropriate value from the **Poll Interval** drop-down list.

### LLDP Transmission statistics field descriptions

Use the data in the following table to view the transmission statistics.

#### Field descriptions for the **TX Stats** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortNum</td>
<td>Specifies the port number.</td>
</tr>
<tr>
<td>FramesTotal</td>
<td>Specifies the total number of LLDP frames transmitted.</td>
</tr>
</tbody>
</table>

#### Field descriptions for the **TX Stats-Graph, <port-number>** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AbsoluteValue</td>
<td>Specifies the absolute number of LLDP frames at a given point in time.</td>
</tr>
<tr>
<td>Cumulative</td>
<td>Specifies the cumulative rate of change of LLDP frames transmitted.</td>
</tr>
<tr>
<td>Average/sec</td>
<td>Specifies the average rate of change of LLDP frames transmitted.</td>
</tr>
<tr>
<td>Minimum/sec</td>
<td>Specifies the minimum rate of change of LLDP frames transmitted.</td>
</tr>
<tr>
<td>Maximum/sec</td>
<td>Specifies the maximum rate of change of LLDP frames transmitted.</td>
</tr>
<tr>
<td>LastVal/sec</td>
<td>Specifies the rate of change of LLDP frames transmitted in the last second.</td>
</tr>
</tbody>
</table>

### Viewing global FA statistics graphically

Use this procedure to view the global FA statistics graphically.

#### Procedure

1. In the navigation pane, navigate to **Graph > Chassis.**
2. Click the **Fabric Attach** tab.
The global FA statistics are displayed.

3. To view a graphical representation of the statistics, select a row and click the appropriate icon on the top left-hand-side of the menu bar to draw a line chart, area chart, bar chart or a pie chart.

4. Click **Clear Counters** to clear the existing counters, and fix a reference point in time to restart the counters.

5. Click **Export**, to export the statistical data to a file.

6. To fix a poll interval, select an appropriate value from the **Poll Interval** drop-down list.

**Fabric Attach field descriptions**

Use the data in the following table to use the **Fabric Attach** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiscElemReceived</td>
<td>Specifies the number of discovery elements received globally.</td>
</tr>
<tr>
<td>AsgnReceived</td>
<td>Specifies the number of remote I-SID-to-VLAN assignments received globally.</td>
</tr>
<tr>
<td>AsgnAccepted</td>
<td>Specifies the number of remote I-SID-to-VLAN assignments accepted globally.</td>
</tr>
<tr>
<td>AsgnRejected</td>
<td>Specifies the number of remote I-SID-to-VLAN assignments rejected globally.</td>
</tr>
<tr>
<td>AsgnExpired</td>
<td>Specifies the number of remote I-SID-to-VLAN assignments that expired globally.</td>
</tr>
<tr>
<td>DiscAuthFailed</td>
<td>Specifies the number of discovery authentications that failed globally.</td>
</tr>
<tr>
<td>DiscElemExpired</td>
<td>Specifies the number of discovery elements that expired globally.</td>
</tr>
<tr>
<td>DiscElemDeleted</td>
<td>Specifies the number of discovery elements that were deleted globally.</td>
</tr>
<tr>
<td>AsgnDeleted</td>
<td>Specifies the number of remote assignments that were deleted globally.</td>
</tr>
<tr>
<td>AsgnAuthFailed</td>
<td>Specifies the number of assignment authentications that failed globally.</td>
</tr>
</tbody>
</table>

**Viewing FA port statistics graphically**

Use this procedure to view the FA port statistics graphically.

**Before you begin**

Ensure that a switch port is selected in the **Device Physical View** tab.

**Procedure**

1. In the navigation pane, navigate to **Graph > Port**.

2. Click the **Fabric Attach** tab.

   The FA port statistics are displayed.

3. To view a graphical representation of the port statistics, select a row and click the appropriate icon on the top left-hand-side of the menu bar to draw a line chart, area chart, bar chart or a pie chart.

Comments on this document? infodev@avaya.com
4. Click **Clear Counters** to clear the existing counters, and fix a reference point in time to restart the counters.

5. Click **Export**, to export the statistical data to a file.

6. To fix a poll interval, select an appropriate value from the **Poll Interval** drop-down list.

**Fabric Attach field descriptions**

Use the data in the following table to use the **Fabric Attach** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiscElemReceived</td>
<td>Specifies the number of discovery elements received on a given port.</td>
</tr>
<tr>
<td>AsgnReceived</td>
<td>Specifies the number of remote I-SID-to-VLAN assignments received on a given port.</td>
</tr>
<tr>
<td>AsgnAccepted</td>
<td>Specifies the number of remote I-SID-to-VLAN assignments accepted on a given port.</td>
</tr>
<tr>
<td>AsgnRejected</td>
<td>Specifies the number of remote I-SID-to-VLAN assignments rejected on a given port.</td>
</tr>
<tr>
<td>AsgnExpired</td>
<td>Specifies the number of remote I-SID-to-VLAN assignments that expired on a given port.</td>
</tr>
<tr>
<td>DiscAuthFailed</td>
<td>Specifies the number of authentications that failed on a given port.</td>
</tr>
<tr>
<td>DiscElemExpired</td>
<td>Specifies the number of discovery elements that expired on a given port.</td>
</tr>
<tr>
<td>DiscElemDeleted</td>
<td>Specifies the number of discovery elements that were deleted on a given port.</td>
</tr>
<tr>
<td>AsgnDeleted</td>
<td>Specifies the number of remote assignments that were deleted on a given port.</td>
</tr>
<tr>
<td>AsgnAuthFailed</td>
<td>Specifies the number of assignment authentications that failed on a given port.</td>
</tr>
</tbody>
</table>

**Verify FA discovery and I-SID-to-VLAN mapping assignments**

**Configuring LLDP neighbor information**

Use this procedure to configure LLDP neighbor information.

**Procedure**

1. In the navigation pane, navigate to **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP**.
2. In the content pane, click the **Neighbor** tab.
3. After you finish the configuration changes, click **Apply** to save changes.

**LLDP neighbor field descriptions**

Use the data in the following table to use the **Neighbor** tab.
**Configuring Fabric Attach I-SID-to-VLAN assignments**

Use this procedure to view or configure FA I-SID-to-VLAN assignment information.

**Procedure**

1. In the navigation pane, navigate to **Configuration > Edit > Fabric Attach**.
2. In the content pane, click the **Assignment** tab.
3. If you make configuration changes, click **Apply** to save changes.

**Fabric Attach I-SID-to-VLAN assignments field descriptions**

Use the data in the following table to use the **Assignments** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IfIndex</td>
<td>Specifies the interface identifier of the I-SID-to-VLAN assignment.</td>
</tr>
<tr>
<td>Isid</td>
<td>Specifies the I-SID value of the I-SID-to-VLAN assignment.</td>
</tr>
<tr>
<td>Vlan</td>
<td>Specifies the VLAN ID component of the I-SID-to-VLAN assignment.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies the current state of the I-SID-to-VLAN assignment.</td>
</tr>
<tr>
<td></td>
<td>It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Rejected</td>
</tr>
<tr>
<td>Origin</td>
<td>Specifies the origin information of the I-SID-to-VLAN assignment.</td>
</tr>
</tbody>
</table>
Fabric Attach troubleshooting example

Troubleshooting FA Server rejection of I-SID-to-VLAN assignments using trace

Consider an FA solution where the FA Server receives I-SID-to-VLAN assignment requests from a proxy device and some of these assignment requests are rejected by the FA Server. Use this procedure to help you troubleshoot the cause of the rejection.

**Note:**

When the FA Server rejects an I-SID-to-VLAN assignment request, the error message in the log file lists a generic reason for the failure, such as rejected due to application error (status 9). To troubleshoot further, you must use trace.

This procedure also demonstrates how you can configure trace for enhanced troubleshooting.

**Procedure**

**Begin troubleshooting on the FA Server**

1. Enter Privileged EXEC mode:
   ```enable```
2. Verify that router IS-IS is enabled. This is required for proper FA operation.
   ```show isis```
   **Note:**
   
   I-SID-to-VLAN assignments are *always* rejected if router IS-IS is disabled.
3. Verify that FA is enabled on the interface on which I-SID-to-VLAN assignments are expected.
   ```show fa interface [disabled-auth] [enabled-auth] [mlt <1-512>] [port slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]```  
4. Verify the discovery and authentication status of the proxy device, on the interface.
   ```show fa elements [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]```  
5. Determine the I-SID-to-VLAN assignments received on the interface and which ones are rejected.
   ```show fa assignment [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]```  
6. View the log file to determine the cause of the assignment rejection.
   ```show log file module fa```
**Note:**
When the FA Server rejects an I-SID-to-VLAN assignment request, only a generic reason for the rejection is logged.

**Enhanced troubleshooting using trace**

7. Configure trace:
   a. Enable keyword search in the trace output:
      
      \[\text{trace grep \text{WORD}<0-128>}\]
   b. Set the trace level for FA:
      \[\text{trace level <0-226>} \text{sub-system}\]
      
      **Note:**
      FA uses the trace level 221.
   c. Turn on trace:
      \[\text{trace screen [enable] | [disable]}\]

**Example:**
The following example \textit{simulates} a configuration error on the FA Server as a result of which the FA Server rejects I-SID-to-VLAN assignments from the proxy device. When the FA Server rejects an I-SID-to-VLAN assignment, the error message listed in the log file is a generic reason for the rejection, as demonstrated in this example. To troubleshoot further, set up trace.

On the FA Server, assume that the interface MLT 1 consists of ports 1/5 and 1/6. Assume that a proxy device sends I-SID-to-VLAN assignment mapping requests with I-SID 9005 and CVID 400, on this interface.

**Simulate a configuration error on the FA Server:**

Configure a management I-SID with a C-VID value that is different from that of the C-VID in the I-SID-to-VLAN assignment request from the proxy. So, for example, configure a management I-SID with C-VID 999, which is different from the C-VID advertised by the proxy, which is 400. This causes rejection of I-SID-to-VLAN assignment requests on the interface.

Switch:1>en
Switch:1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch:1(config)#interface mlt 1
Switch:1(config-mlt)#no fa enable
Switch:1(config-mlt)#fa management i-sid 9005 c-vid 999
Switch:1(config-mlt)#fa enable
Switch:1(config-mlt)#exit
Switch:1(config)#exit

At this stage, the FA Server rejects I-SID-to-VLAN assignments as shown below.

```
Switch:1#show fa assignment
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>I-SID</th>
<th>Vlan</th>
<th>State</th>
<th>Origin</th>
</tr>
</thead>
</table>

Comments on this document? infodev@avaya.com
Begin troubleshooting on the FA Server:

Verify that IS-IS is enabled.

Switch:1>en
Switch:1#show isis

-----------------------------------------------------------------------
ISIS General Info
-----------------------------------------------------------------------
AdminState : enabled
RouterType : Level 1
System ID : 8404.bcb1.0043
Max LSP Gen Interval : 900
Metric : wide
Overload-on-startup : 20
Overload : false
Csnp Interval : 10
PSNP Interval : 2
Rxmt LSP Interval : 5
spf-delay : 100
Router Name : FAServer
ip source-address : 43.43.43.43
ipv6 source-address : 1:43:0:0:0:0:0:43
ip tunnel source-address : 12.43.43.43
Tunnel vrf : 12
Num of Interfaces : 4
Num of Area Addresses : 1
Switch:1#

Verify that FA is enabled on the interface MLT 1, on which the I-SID-to-VLAN assignments are expected. View the SERVER STATUS field.

Switch:1#show fa interface mlt 1

-----------------------------------------------------------------------
Fabric Attach Interfaces
-----------------------------------------------------------------------
INTERFACE SERVER MGMT MGMT MSG AUTH MSG AUTH
STATUS ISID CVID STATUS KEY
-----------------------------------------------------------------------
Mlt1 enabled 0 0 enabled ****
-----------------------------------------------------------------------
1 out of 1 Total Num of fabric attach interfaces displayed
-----------------------------------------------------------------------

Verify the discovery and authentication status of the proxy device on the interface. Note that the proxy is successfully discovered and authenticated on ports 1/5 and 1/6 of MLT 1.

Switch:1#show fa elements

Fabric Attach Discovery Elements
Fabric Attach troubleshooting example

View the log file to determine the cause of the rejection. The log file displays the generic error rejected due to application error (status 9) as follows:

Switch:1#show log file module fa
...
CP1 [12/04/15 00:45:51.185:UTC] 0x00374583 00000000 GlobalRouter FA INFO Fabric Attach Element Discovered on interface 1/5 Element type proxy (3) Id 50:61:84:ee:8c:00:20:00:00:01 CP1 [12/04/15 00:45:51.187:UTC] 0x0037458f 00000000 GlobalRouter FA INFO Fabric Attach Assignment rejected: interface 1/5 i-sid 9005 cvid 400 rejected due to application error (status 9)
...
...

To troubleshoot further, use trace.

Switch:1#trace grep fa  
Switch:1#trace level 221 3  
Switch:1#trace screen enable  
Screen tracing is on

View the trace output. The trace output displays that the error was caused because the FA interface (MLT 1) was configured with a different C-VID for I-SID 9005.

Switch:1#0:07:57.801252 1 fa.c :858 [lcy-ve][12898-13062]cbcp-main.x:faUpdateSwitchedUni :FA: faUpdateSwitchedUni port 196 isid 9005 cvid 400
0:07:57.801283 1 fa_swuni.c :2900[lcy-ve][12898-13062]cbcp-main.x:faUpdateSwitchedUniCheck :FA: Call faUpdateSwitchedUniCheckSmlt for mlt 1
0:07:57.801644 1 fa_swuni.c :2421[lcy-ve][12898-13062]cbcp-main.x:faUpdateSwitchedUniCheckEndpointParms:FA: Failed rcIsidElanEndPointTblConsistencyCheckCommon for IfIndex 6144 Isid 9005 Cvid 400 error Switched UNI/Fabric Attach MLT cannot be configured for different c-vid for same I-SID
0:07:57.802074 1 fa.c :858 [lcy-ve][12898-13062]cbcp-

Comments on this document? infodev@avaya.com
Troubleshooting Fabric Attach

Related links

Troubleshooting Fabric Attach on page 309