Traps Reference for Avaya Virtual Services Platform 9000

Release 4.1
NN46250-704
Issue 02.01
October 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on 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: http://support.avaya.com 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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 ANYONE OTHER THAN 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software 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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Downloading Documentation

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

Contact Avaya Support

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

Purpose

The document describes the proprietary and standard traps available for Avaya Virtual Services Platform 9000.

Related resources

Documentation

See *Documentation Reference for Avaya Virtual Services Platform 9000,* NN46250-100 for a list of the documentation for this product.

Training

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

Course code	Course title
4D00010E	Knowledge Access: ACIS - Avaya ERS 8000 and VSP 9000 Implementation
5D00040E	Knowledge Access: ACSS - Avaya VSP 9000 Support

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.

Support

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

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: New in this release

The following sections detail what is new in *Traps Reference for Avaya Virtual Services Platform 9000,* NN46250-704, for Release 4.1.

Features

There are no feature-related changes in the current document in Release 4.1.

Chapter 3: Traps reference

This chapter provides information about traps.

The Virtual Services Platform 9000 generates alarms, traps, and logs.

For more information about specific log messages, see *Logs Reference for Avaya Virtual Services Platform 9000,* NN46250-702.

Proprietary traps

The following tables describe Avaya proprietary traps for Virtual Services Platform 9000. Unless otherwise noted, all of the traps have a status of current.

1.3.6.1.4.1.45.4.8.0.xx series

The following table describes 1.3.6.1.4.1.45.4.8.0.xx series traps.

OID	Notification type	Objects	Description
1.3.6.1.4.1.45.4.8.0.1	slaMonitorAgentExceptionDetected	slaMonitorAgentExceptionDetected	The SLA Mon agent process has terminated unexpectedly. You must reenable SLA Mon to restart the SLA Mon agent.

1.3.6.1.4.1.2272.1.21.0.xx series

The following table describes 1.3.6.1.4.1.2272.1.21.0.xx series traps.

OID	Notification type	Objects	Description
1.3.6.1.4.1.2272.1.21.0.1	rcnCardDown	rcCardIndex rcCardAdminStatus rcCardOperStatus	An rcnCardDown trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the

Table continues…

OID	Notification type	Objects	Description
			rcCardOperStatus object for one of its cards is about to transition into the down state.
1.3.6.1.4.1.2272.1.21.0.2	rcnCardUp	rcCardIndex rcCardAdminStatus rcCardOperStatus	An rcnCardUp trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the up state.
1.3.6.1.4.1.2272.1.21.0.3	rcnErrorNotification	rcErrorLevel rcErrorCode rcErrorText	An rcnErrorNotification trap signifies that the SNMPv2 entity, acting in an agent role, has detected that an error condition has occurred.
1.3.6.1.4.1.2272.1.21.0.4	rcnStpNewRoot	rcStgId	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.
1.3.6.1.4.1.2272.1.21.0.5	rcnStpTopologyChange	rcStgId rcPortIndex	An rcnStpTopologyChange trap signifies that the SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has gone due a topology change event.
1.3.6.1.4.1.2272.1.21.0.6	rcnChasPowerSupplyDown	rcChasPowerSupplyId rcChasPowerSupplyOperStatus	An rcnChasPowerSupplyDown trap signifies

Table continues…

OID	Notification type	Objects	Description
			that the SNMPv2 entity, acting in an agent role, has detected that the rcChasPowerSupply OperStatus object for one of its power supply unit is about to transition into the down state.
1.3.6.1.4.1.2272.1.21.0.7	rcnChasFanDown	rcChasFanId rcChasFanOperStatus	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.
1.3.6.1.4.1.2272.1.21.0.8	rcnLinkOscillation	rcPortIndex	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.
1.3.6.1.4.1.2272.1.21.0.9	rcnMacViolation	rcErrorText rcPortIndex	An rcnMacViolation trap signifies that the SNMPv2 entity, acting in an agent role, has received a PDU with an invalid source MAC address.
1.3.6.1.4.1.2272.1.21.0.10	rcnSonetTrap	rcPortIndex rcPosSonetTrapType rcPosSonetTrapIndication	An rcnSonetTrap trap signifies that the SNMPv2 entity, acting in an agent role, has detected a change of status on a Sonet port.
1.3.6.1.4.1.2272.1.21.0.11	rcn2kCardDown	rc2kCardIndex rc2kCardFrontAdminStatus rc2kCardFrontOperStatus	An rcn2kCardDown trap signifies that the SNMPv2 entity, acting in an agent

Table continues…

OID	Notification type	Objects	Description
			role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the down state.
1.3.6.1.4.1.2272.1.21.0.12	rcn2kCardUp	rc2kCardIndex rc2kCardFrontAdminStatus rc2kCardFrontOperStatus	An rcn2kCardUp trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the up state.
1.3.6.1.4.1.2272.1.21.0.13	rcn2kTemperature	rc2kChassisTemperature	An rcn2kTemperature trap signifies that the SNMPv2 entity, acting in an agent role, has detected the chassis is overheating.
1.3.6.1.4.1.2272.1.21.0.14	rcnChasPowerSupplyUp	rcChasPowerSupplyId rcChasPowerSupplyOperStatus	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.
1.3.6.1.4.1.2272.1.21.0.15	rcn2kAtmPvcLinkStateChange	rc2kAtmPvcIfIndex rc2kAtmPvcVpi rc2kAtmPvcVci rc2kAtmPvcOamVcStatus	An rc2kAtmPvcLinkStateChange trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the rc2kAtmPvcOamVcStatus object for one of

Table continues…

OID	Notification type	Objects	Description
			PVC is about to transition into a different state, either from up to down or from down to up.
1.3.6.1.4.1.2272.1.21.0.16	rcnStpTCN	rcStgId rcPortIndex rcStgBridgeAddress	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.
1.3.6.1.4.1.2272.1.21.0.17	rcnSmltIstLinkUp	—	An rcnSmltIstLinkUp trap signifies that the split MLT link is from down to up.
1.3.6.1.4.1.2272.1.21.0.18	rcnSmltIstLinkDown	—	An rcnSmltIstLinkDown trap signifies that the split MLT link is from up to down.
1.3.6.1.4.1.2272.1.21.0.19	rcnSmltLinkUp	rcMltSmltId	An rcnSmltLinkUp trap signifies that the split SMLT link is up.
1.3.6.1.4.1.2272.1.21.0.20	rcnSmltLinkDown	rcMltSmltId	An rcnSmltLinkDown trap signifies that the split SMLT link is down.
1.3.6.1.4.1.2272.1.21.0.21	rcnChasFanUp	rcChasFanId rcChasFanOperStatus	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.
1.3.6.1.4.1.2272.1.21.0.22	rcnPasswordChange	rcCliPasswordChange rcCliPassChangeResult	An rcnPasswordChange trap signifies that the SNMPv2 entity, acting in an agent

Table continues…

OID	Notification type	Objects	Description
			role, has detected that the one of the ACLI passwords is changed.
1.3.6.1.4.1.2272.1.21.0.23	rcnEmError	rc2kCardIndex rcChasEmModeError	An rcnEmError trap signifies that the SNMPv2 entity, acting in an agent role, has detected Em error.
1.3.6.1.4.1.2272.1.21.0.25	rcnPcmciaCardRemoved	—	An rcnPcmciaRemoved trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the PCMCIA card is being removed.
1.3.6.1.4.1.2272.1.21.0.26	rcnSmartCpldTimerFired	rc2kCardIndex	An rcnSmartCpldTimerFired trap signifies that the CP ID timer fired.
1.3.6.1.4.1.2272.1.21.0.27	rcnCardCpldNotUpDate	rc2kCardIndex	An rcnCardCpldNotUpDate trap signifies that the CP ID is not up to date.
1.3.6.1.4.1.2272.1.21.0.28	rcnIgapLogFileFull	—	An rcnIgapLogFileFull trap signifies that the IGAP accounting time-out Log File has reached the maximum.
1.3.6.1.4.1.2272.1.21.0.29	rcnCpLimitShutDown	rcPortIndex ifAdminStatus ifOperStatus rcPortCpLimitShutDown	An rcnCpLimitShutDown trap signifies that the cp limit for the port is shutting down.
1.3.6.1.4.1.2272.1.21.0.30	rcnSshServerEnabled	rcSshGlobalPort	An rcnSshServerEnabled trap signifies that the SSH server is enabled.
1.3.6.1.4.1.2272.1.21.0.31	rcnSshServerDisabled	rcSshGlobalPort	An rcnSshServerDisable

Table continues…

OID	Notification type	Objects	Description
			d trap signifies that the SSH server is disabled.
1.3.6.1.4.1.2272.1.21.0.35	rcnHaCpuState	rc2kCardIndex rcL2RedundancyHaCpuState	An rcnHaCpuState trap signifies that the state of the HA-CPU.
1.3.6.1.4.1.2272.1.21.0.36	rcnInsufficientMemory	rc2kCardIndex	An rcnInsufficientMemory trap indicates insufficient memory on the CPU blade for proper operation.
1.3.6.1.4.1.2272.1.21.0.37	rcnSaveConfigAction	rcSysActionL1	An rcnSaveConfigAction trap indicates the switch run time or boot configuration is being saved.
1.3.6.1.4.1.2272.1.21.0.38	rcnLoopDetectOnPort	rcVlanId rcPortIndex	An rcnLoopDetectOnPort trap indicates that a loop has been detected on a port. The VLAN on that port will be disabled.
1.3.6.1.4.1.2272.1.21.0.39	rcnbgpEstablished	rcIpBgpPeerIpAddress rcIpBgpPeerLastError rcIpBgpPeerState	The BGP Established event is generated when the BGP finite state machine enters the established state.
1.3.6.1.4.1.2272.1.21.0.40	rcnbgpBackwardTransition	rcIpBgpPeerIpAddress rcIpBgpPeerLastError rcIpBgpPeerState	The rcnbgpBackwardTransition Event is generated when the BGP finite state machine moves from a higher numbered state to a lower numbered state.
1.3.6.1.4.1.2272.1.21.0.41	rcnAggLinkUp	rcMltId	An rcnAggLinkUp trap is generated when the operational state of the aggregator changes from down to up.

Table continues…

OID	Notification type	Objects	Description
1.3.6.1.4.1.2272.1.21.0.42	rcnAggLinkDown	rcMltId	An rcnAggLinkDown trap is generated when the operational state of the aggregator changes from up to down.
1.3.6.1.4.1.2272.1.21.0.43	rcnIgmpNewGroupMember	rcIgmpGroupIfIndex rcIgmpGroupIpAddress rcIgmpGroupInPort rcIgmpGroupMember	An rcnIgmpNewGroupMember trap signifies that a new member has come on an interface.
1.3.6.1.4.1.2272.1.21.0.44	rcnIgmpLossGroupMember	rcIgmpGroupMembers rcIgmpGroupIpAddress rcIgmpGroupInPort rcIgmpGroupIfIndex	An rcnIgmpLossGroupMember trap signifies that a group member has been lost on an interface.
1.3.6.1.4.1.2272.1.21.0.45	rcnIgmpNewQuerier	igmpInterfaceIfIndex igmpInterfaceQuerier	An rcnIgmpNewQuerier trap signifies that a new querier has come up on an interface.
1.3.6.1.4.1.2272.1.21.0.46	rcnIgmpQuerierChange	igmpInterfaceIfIndex rcIgmpInterfaceExtnNewQuerier igmpInterfaceQuerier	An rcnIgmpQuerierChange trap signifies that the querier has changed.
1.3.6.1.4.1.2272.1.21.0.47	rcnDvmrpIfStateChange	dvmrpInterfaceIfIndex dvmrpInterfaceOperState	An rcnDvmrpIfStateChange trap signifies that there has been a change in the state of a DVMRP interface.
1.3.6.1.4.1.2272.1.21.0.48	rcnDvmrpNewNbrChange	dvmrpNeighborIfIndex dvmrpNeighborAddress	An rcnDvmrpNewNbrChange trap signifies that a new neighbor has come up on a DVMRP interface.
1.3.6.1.4.1.2272.1.21.0.49	rcnDvmrpNbrLossChange	dvmrpNeighborIfIndex dvmrpNeighborAddress	An rcnDvmrpNbrLossChange trap signifies that a new neighbor

Table continues…

OID	Notification type	Objects	Description
			has gone down on a DVMRP interface.
1.3.6.1.4.1.2272.1.21.0.59	rcnFdbProtectViolation	rcPortIndex rcVlanId	The rcnFdbProtectViolation trap signifies that the has violated the user configured limit for total number of fdb-entries learned on that port.
1.3.6.1.4.1.2272.1.21.0.60	rcnLogMsgControl	rcSysMsgLogFrequency rcSysMsgLogText	An rcnLogMsgControl trap signifies whether the number of times of repetition of the particular Log message has exceeded the particular frequency/ count or not.
1.3.6.1.4.1.2272.1.21.0.61	rcnSaveConfigFile	rcSysActionL1 rcSysConfigFileName	An rcnSaveConfig trap signifies that either the runtime config or the boot config has been saved on the switch.
1.3.6.1.4.1.2272.1.21.0.62	rcnDNSRequestResponse	rcSysDnsServerListIpAddr rcSysDnsRequestType	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.
1.3.6.1.4.1.2272.1.21.0.63	rcnDuplicateIpAddress	ipNetToMediaNetAddress ipNetToMediaPhysAddress	An rcnDuplicateIpAddress trap signifies that a duplicate IP address is detected on the subnet.
1.3.6.1.4.1.2272.1.21.0.64	rcnLoopDetectPortDown	rcPortIndex ifAdminStatus ifOperStatus	An rcnLoopDetectPortDown trap signifies that a loop has been detected on a port

Table continues…

OID	Notification type	Objects	Description
			and the port is going to shut down.
1.3.6.1.4.1.2272.1.21.0.67	rcnLoopDetectMacDiscard	rcPortIndex rcSysMacFlapLimitTime rcSysMacFlapLimitCount	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.
1.3.6.1.4.1.2272.1.21.0.68	rcnAutoRecoverPort	rcPortIndex	An rcnAutoRecoverPort trap signifies that autorecovery has reenabled a port disabled by link flap or CP Limit.
1.3.6.1.4.1.2272.1.21.0.69	rcnAutoRecoverLoopDetectedPort	rcVlanNewLoopDetectedAction	An rcnAutoRecoverPort trap signifies that autorecovery has cleared the action taken on a port by loop detect.
1.3.6.1.4.1.2272.1.21.0.70	rcnExtCpLimitShutDown	rcPortIndex ifAdminStatus	An rcnExtCpLimitShutDown trap signifies that a port is shutdown due to extended CP-Limit.
1.3.6.1.4.1.2272.1.21.0.71	rcnExtCpLimitSopCongestion	rcSysExtCplimitSysOctapidCongested rcSysExtCplimitPortsMonitored	An rcnExtCpLimitSopCongestion trap signifies that system octapid polling determines whether system octapid is congested. • rcSysExtCplimitSysOctapidCongested signifies whether system octapid is congested. • rcSysExtCplimitPortsMonitored signifies whether ports are selected for

Table continues…

OID	Notification type	Objects	Description
			monitoring the ingress traffic utilization.
1.3.6.1.4.1.2272.1.21.0.74	rcnTacacsAuthFailure	rcTacacsGlobalLastUserName	An rcnTacacsAuthFailure trap signifies that TACACS+ authentication failed for a user.
1.3.6.1.4.1.2272.1.21.0.75	rcnTacacsNoServers	—	An rcnTacacsNoServers trap signifies that you are unable to use any TACACS+ servers for authentication.
1.3.6.1.4.1.2272.1.21.0.76	rcnTacacsRxUnsupportedFrame	rcTacacsGlobalLastAddressType rcTacacsGlobalLastAddress	An rcnTacacsRxUnsupportedFrame trap signifies that an unsupported frame was received from the TACACS+ server.
1.3.6.1.4.1.2272.1.21.0.77	rcnTacacsExceededMaxLogins	—	An rcnTacacsExceededMaxLogins trap signifies that there was an attempt to exceed the maximum number of allowed TACACS+ logins.
1.3.6.1.4.1.2272.1.21.0.78	rcnTacacsClientFailure	—	An rcnTacacsClientFailure trap signifies that the TACACS+ Client application is down.
1.3.6.1.4.1.2272.1.21.0.79	rcnBpduReceived	rcPortBpduFilteringTimeout	An rcnBpduReceived trap signifies that a notification will be generated when a BPDU is received on a port which has BPDU filtering enabled.
1.3.6.1.4.1.2272.1.21.0.80	rcnVlacpPortDown	rcPortIndex	An rcnVlacpPortDown trap signifies that

Table continues…

OID	Notification type	Objects	Description
			VLACP is down on the port specified.
1.3.6.1.4.1.2272.1.21.0.81	rcnVlacpPortUp	rcPortIndex	An rcnVlacpPortUp trap signifies that VLACP is up on the port specified.
1.3.6.1.4.1.2272.1.21.0.82	rcnExtCpLimitShutDownNormal	—	An rcnExtCpLimitShutDownNormal trap signifies that ports are shutdown due to extended CP-Limit in Normal mode.
1.3.6.1.4.1.2272.1.21.0.83	rcnEapMacIntrusion	rcSysIpAddr rcRadiusPaePortNumber rcRadiusEapLastAuthMac rcRadiusEapLastRejMac	An rcnEapMacIntrusion trap signifies that an EAP MAC intrusion has occurred on this port.
1.3.6.1.4.1.2272.1.21.0.84	rcnInterCpuCommStatus	rc2kCardIndex rcCardOperStatus	A rcnInterCpuCommStatus trap signifies the current communication status between primary and secondary CPU.
1.3.6.1.4.1.2272.1.21.0.89	rcPlugOptModTemperatureStatusTrap	rcPortIndex rcPlugOptModTemperatureStatus	A rcPlugOptModTemperatureStatusTrap is used to trap changes in the temperature status.
1.3.6.1.4.1.2272.1.21.0.90	rcPlugOptModVoltageStatusTrap	rcPortIndex rcPlugOptModVoltageStatus	A rcPlugOptModVoltageStatusTrap is used to trap changes in the voltage level.
1.3.6.1.4.1.2272.1.21.0.91	rcPlugOptModBiasStatusTrap	rcPortIndex rcPlugOptModBiasStatus	A rcPlugOptModBiasStatusTrap is used to trap changes in the laser bias status.
1.3.6.1.4.1.2272.1.21.0.92	rcPlugOptModTxPowerStatusTrap	rcPortIndex rcPlugOptModTxPowerStatus	A rcPlugOptModTxPowerStatusTrap is used

Table continues…

OID	Notification type	Objects	Description
			to trap changes in the transmit power status.
1.3.6.1.4.1.2272.1.21.0.93	rcPlugOptModRxPowerStatusTrap	rcPortIndex rcPlugOptModRxPowerStatus	A rcPlugOptModRxPowerStatusTrap is used to trap changes in the received power status.
1.3.6.1.4.1.2272.1.21.0.94	rcPlugOptModAux1StatusTrap	rcPortIndex rcPlugOptModAux1Monitoring rcPlugOptModAux1Status	A rcPlugOptModAux1StatusTrap is used to trap changes in the Aux1 status.
1.3.6.1.4.1.2272.1.21.0.95	rcPlugOptModAux2StatusTrap	rcPortIndex rcPlugOptModAux2Monitoring rcPlugOptModAux2Status	A rcPlugOptModAux2StatusTrap is used to trap changes in the Aux2 status.
1.3.6.1.4.1.2272.1.21.0.110	rcnMaxRouteWarnClear	rcVrfName	An rcnMaxRouteWarnClear trap signifies that the number of routes in the routing table of the virtual router has dropped below the warning threshold.
1.3.6.1.4.1.2272.1.21.0.111	rcnMaxRouteWarnSet	rcVrfName	An rcnMaxRouteWarnSet trap signifies that the virtual router routing table is reaching its maximum size. Take action to prevent this.
1.3.6.1.4.1.2272.1.21.0.112	rcnMaxRouteDropClear	rcVrfName	An rcnMaxRouteDropClear trap signifies that the virtual router routing table is no longer dropping new routes as it is below the maximum size.
1.3.6.1.4.1.2272.1.21.0.113	rcnMaxRouteDropSet	rcVrfName	An rcnMaxRouteDropSet trap signifies that the

Table continues…

OID	Notification type	Objects	Description
			virtual router routing table has reached the maximum size, and is now dropping all new nonstatic routes.
1.3.6.1.4.1.2272.1.21.0.117	rcnMstpNewCistRoot	rcStgBridgeAddress	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.
1.3.6.1.4.1.2272.1.21.0.118	rcnMstpNewMstiRoot	rcStgBridgeAddress rcStgId	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.
1.3.6.1.4.1.2272.1.21.0.119	rcnMstpNewCistRegionalRoot	rcStgBridgeAddress	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.
1.3.6.1.4.1.2272.1.21.0.120	rcnRstpNewRoot	rcStgBridgeAddress	An rcnRstpNewRoot trap signifies that the

Table continues…

OID	Notification type	Objects	Description
			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.
1.3.6.1.4.1.2272.1.21.0.124	rcnRsmltEdgePeerModified	rcVlanId	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.
1.3.6.1.4.1.2272.1.21.0.165	rcnTmuxParityError	rc2kDeviceGlobalSlot	A rcnTmuxParityError trap identifies a problem in the FAD/SWIP based on the number of parity errors.
1.3.6.1.4.1.2272.1.21.0.167	rcnChasPowerSupplyNoRedundancy	—	An rcnChasPowerSupplyNoRedundancy trap signifies that the chassis is running on power supply without redundancy.
1.3.6.1.4.1.2272.1.21.0.168	rcnChasPowerSupplyRedundancy	—	An rcnChasPowerSupplyRedundancy trap signifies that the chassis is running on power supply with redundancy.
1.3.6.1.4.1.2272.1.21.0.171	rcnLicenseTrialPeriodExpired	—	An rcnLicenseTrialPeriodExpired trap signifies that the Trial Period License has expired.

Table continues…

OID	Notification type	Objects	Description
1.3.6.1.4.1.2272.1.21.0.172	rcnLicenseTrialPeriodExpiry	rcSysLicenseTrialDaysLeft	An rcnLicenseTrialPeriodExpiry trap signifies the time remaining, in days, before the License Trial Period expires.
1.3.6.1.4.1.2272.1.21.0.173	rcnVrfUp	rcVrfName rcVrfOperStatus	This notification is generated when the operational status of the specified VRF is toggled from down to up.
1.3.6.1.4.1.2272.1.21.0.174	rcnVrfDown	rcVrfName rcVrfOperStatus	This notification is generated when the operational status of the specified VRF is toggled from up to down.
1.3.6.1.4.1.2272.1.21.0.175	rcnMrouteIngressThresholdExceeded	rcIpResourceUsageGlobalIngressRecInUse rcIpResourceUsageGlobalIngressThreshold	This notification is generated when the number of mroute ingress records exceeds the ingress threshold.
1.3.6.1.4.1.2272.1.21.0.176	rcnMrouteEgressThresholdExceeded	rcIpResourceUsageGlobalEgressRecInUse rcIpResourceUsageGlobalEgressThreshold	This notification is generated when the number of mroute egress records exceeds the egress threshold.
1.3.6.1.4.1.2272.1.21.0.177	rcnRemoteMirroringStatus	rcPortRemoteMirroringIndex rcPortRemoteMirroringEnable rcPortRemoteMirroringMode	An rcnRemoteMirroringStatus trap signifies whether the remote mirroring is enabled or disabled on a particular port.
1.3.6.1.4.1.2272.1.21.0.182	rcnAggLinkStateChange	rcMltId rcMltAggTrapEvent	An rcnAggLinkStateChange trap signifies changes to the operational state of the LAG changes; the three events identified are local

Table continues…

OID	Notification type	Objects	Description
			down, remote down, or up.
1.3.6.1.4.1.2272.1.21.0.185	rcnChasPowerSupplyRunningLow	—	An rcnChasPowerSupplyRunningLow trap signifies that the chassis is running on low power supply.
1.3.6.1.4.1.2272.1.21.0.192	rcnIsisPlsbMetricMismatchTrap	rcIsisLocalLspId rcIsisLocalL1Metric rcIsisNgbLspId rcIsisNgbL1Metric rcIsisPlsbTrapType rcIsisTrapIndicator rcIsisLocalHostName rcIsisNgbHostName	An rcnIsisPlsbMetricMismatchTrap signifies that an Link State Packet (LSP) with a different value of Level 1 metric is received.
1.3.6.1.4.1.2272.1.21.0.193	rcnIsisPlsbDuplicateSysidTrap	rcIsisLocalSysId rcIsisLocalInterface rcIsisPlsbTrapType rcIsisTrapIndicator	An rcnIsisPlsbduplicateSysidTrap signifies that a Hello packet with a duplicate system ID is received.
1.3.6.1.4.1.2272.1.21.0.194	rcnIsisPlsbLsdbUpdateTrap	rcIsisPlsbTrapType	An rcnIsisPlsbLsdbUpdateTrap signifies that link state database (LSDB) information has changed.
1.3.6.1.4.1.2272.1.21.0.196	rcnChasFanCoolingLow	rcChasFanOperStatus rcChasFanType rcErrorLevel rcErrorText	An rcnaChasFanCoolingLow trap signifies that the chassis is running on low fan cooling.
1.3.6.1.4.1.2272.1.21.0.269	rcnCardInsert	rc2kCardIndex rcSlotType	An rcnCardInsert trap signifies that a module is inserted into the chassis.
1.3.6.1.4.1.2272.1.21.0.270	rcnCardRemove	rc2kCardIndex rcSlotType	An rcnCardRemove trap signifies that a module is removed from the chassis.
1.3.6.1.4.1.2272.1.21.0.271	rcnChasFanFail	rcFanZoneType rcFanTrayId rcFanUnitId	An rcnChasFanFail trap indicates that a fan unit of a fan tray

Table continues…

OID	Notification type	Objects	Description
			in a fan zone has a fault.
1.3.6.1.4.1.2272.1.21.0.272	rcnChasFanOk	rcFanZoneType rcFanTrayId rcFanUnitId	An rcnChasFanOk trap indicates that a fan unit of a fan tray in a fan zone has recovered from a previously detected fan fault.
1.3.6.1.4.1.2272.1.21.0.273	rcnCardOverheat	rc2kCardIndex rcSlotType rcCardTemp	An rcnCardOverheat trap indicates that a card temperature has exceeded the alarm threshold temperature. Although you may still see this trap, Avaya recommends that you monitor rcn2kCardOverheat.
1.3.6.1.4.1.2272.1.21.0.274	rcnCardNormalTemp	rc2kCardIndex rcSlotType rcCardTemp	An rcnCardNormalTemp trap indicates that a card temperature has cooled down from previously detected overheat condition. Although you may still see this trap, Avaya recommends that you monitor rcn2kCardNormalTemp.
1.3.6.1.4.1.2272.1.21.0.275	rcnCardOverheatShutDown	rc2kCardIndex rcSlotType rcCardTemp	An rcnCardOverheatShutDown trap indicates that a card has been shut down due to persistent temperature overheat for 15 minutes or temperature has exceeded the shutdown threshold temperature.

Table continues…

OID	Notification type	Objects	Description
			Although you may still see this trap, Avaya recommends that you monitor rcn2kCardOverheatShutDown.
1.3.6.1.4.1.2272.1.21.0.276	rcnCardCpuUtilizationHigh	rc2kCardIndex rcSlotType rcCpuUtilization	An rcnCardCpuUtilizationHigh trap indicates that a 5-minute CPU utilization average on this slot is above 90%.
1.3.6.1.4.1.2272.1.21.0.277	rcnCardCpuUtilizationNormal	rc2kCardIndex rcSlotType rcCpuUtilization	An rcnCardCpuUtilizationNormal trap indicates that 5-minute CPU utilization average on this slot is below 75%.
1.3.6.1.4.1.2272.1.21.0.278	rcnIsisPlsbBvidMismatchTrap	rcIsisLocalSysId rcIsisLocalPrimaryBvid rcIsisLocalPrimaryTieBrkAlg rcIsisLocalSecondaryBvid rcLocalSecondaryTieBrkAlg rcIsisNgbSysId rcIsisNgbPrimaryBvid rcIsisNgbPrimaryTieBrkAlg rcIsisNgbSecondaryBvid rcIsisNgbSecondaryTieBrkAlg rcIsisLocalBvidCounter rcIsisNgbBvidCounter rcIsisPlsbTrapType rcIsisTrapIndicator rcIsisNgbHostName	An rcnIsisPlsbBvidMismatchTrap signifies when a backbone VLAN ID (BVID) Type-Length-Value (TLV) from a neighbor node does not match the local configuration.
1.3.6.1.4.1.2272.1.21.0.279	rcnIsisPlsbSmltVirtBmacMismatchTrap	rcIsisLocalVirtualBmac rcIsisPeerVirtualBmac rcIsisPlsbTrapType rcIsisTrapIndicator	An rcnIsisPlsbSmltVirtBmacMismatchTrap signifies that the virtual Backbone MAC (BMAC) configured in the switch is different from the virtual BMAC configured on

Table continues…

OID	Notification type	Objects	Description
			the interswitch trunking (IST) peer.
1.3.6.1.4.1.2272.1.21.0.280	rcnIsisPlsbSmltPeerBmacMismatchTrap	rcIsisSysId rcIsisSmltPeerSysId rcIsisPlsbTrapType rcIsisTrapIndicator	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.
1.3.6.1.4.1.2272.1.21.0.281	rcnIsisPlsbAdjStateTrap	rcIsisNgbSysId rcIsisLocalInterface rcIsisPlsbTrapType rcIsisAdjState rcIsisNgbHostName	An rcnIsisPlsbAdjStateTrap signifies when IS-IS adjacency state changes.
1.3.6.1.4.1.2272.1.21.0.282	rcnIsisPlsbDuplicateNNameTrap	rcIsisNgbNickname rcIsisPlsbTrapType rcIsisTrapIndicator rcIsisNgbSysId rcIsisDuplicateNnameCounter rcIsisNgbHostName	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.
1.3.6.1.4.1.2272.1.21.0.283	rcnIsisPlsbSmltSplitBebMismatchTrap	rcIsisLocalSmltSplitBeb rcIsisPeerSmltSplitBeb rcIsisPlsbTrapType rcIsisTrapIndicator	An rcnIsisPlsbSmltSplitBebMismatchTrap signifies that the SMLT Split Backbone Edge Bridge (BEB) configured on the local switch and the

Table continues…

OID	Notification type	Objects	Description
			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.
1.3.6.1.4.1.2272.1.21.0.284	rcnIsisPlsbMultiLinkAdjTrap	rcIsisNgbSysId rcIsisLocalInterface rcIsisPrevInterface rcIsisPlsbTrapType rcIsisNgbHostName rcIsisTrapIndicator	An rcnIsisPlsbMultiLinkAdjTrap signifies when the Intermediate-System-to-Intermediate-System (IS-IS) protocol forms more than one adjacency with the same IS-IS.
1.3.6.1.4.1.2272.1.21.0.285	rcnaSshSessionLogout	rcSshGlobalHostIpAddr	An rcnaSshSessionLogout trap signifies a Secure Shell (SSH) session logout.
1.3.6.1.4.1.2272.1.21.0.286	rcnaSshUnauthorizedAccess	rcSshGlobalHostIpAddr	An rcnaSshUnauthorizedAccess trap signifies that an unauthorized access has occurred. It is deprecated by rcnaSshUnauthorizedAccess.
1.3.6.1.4.1.2272.1.21.0.287	rcnaAuthenticationSuccess	rcLoginUserName rcLoginHostIpAddress	An rcnaAuthenticationSuccess trap signifies that a login is successful. The Trap includes the login username and the host IP address. It is deprecated by rcnaAuthenticationSuccess.
1.3.6.1.4.1.2272.1.21.0.288	rcnaSshSessionLogin	rcSshGlobalHostIpAddr	An rcnaSshSessionLogin trap signifies that there is a Secure

Table continues…

OID	Notification type	Objects	Description
			Shell (SSH) session login.
1.3.6.1.4.1.2272.1.21.0.295	rcnSlotPowerAvailableTrap	rc2kCardIndex rcSlotType rcSlotPowerStatus	A rcnSlotPowerAvailable trap signifies whether there is sufficient power to boot up the module in slot.
1.3.6.1.4.1.2272.1.21.0.298	rcn2kCardShutDownTrap	rc2kCardIndex, rcSlotType rc2kCardShutDownReason	An rcn2kCardShutDown trap signifies that both high-speed fans are not installed and second generation module shuts down.
1.3.6.1.4.1.2272.1.21.0.300	rcn2kCardOverheat	rc2kCardIndex rcSlotType	An rcn2kCardOverheat trap indicates that a card temperature has exceeded the alarm threshold temperature. This trap will be followed by the rcn2kCardZoneOverheat trap that specifies which zone temperature has crossed the alarm threshold.
1.3.6.1.4.1.2272.1.21.0.301	rcn2kCardZoneOverheat	rc2kCardIndex rcSlotType rc2kCardZoneTemperature rc2kCardTemperatureZoneInfo	An rcn2kCardZoneOverheat trap indicates which zone on the card has exceeded the alarm threshold temperature.
1.3.6.1.4.1.2272.1.21.0.302	rcn2kCardZoneNormalTemp	rc2kCardIndex rcSlotType rc2kCardZoneTemperature rc2kCardTemperatureZoneInfo	An rcn2kCardZoneNormalTemp trap indicates that a zone temperature on the card has cooled down from a previously

Table continues…

OID	Notification type	Objects	Description
			detected overheat condition.
1.3.6.1.4.1.2272.1.21.0.303	rcn2kCardNormalTemp	rc2kCardIndex rcSlotType	An rcn2kCardNormalTemp trap indicates that a card temperature has cooled down from a previously detected overheat condition. This trap is generated only after the temperature on all the zones on the card have dropped below the alarm thresholds.
1.3.6.1.4.1.2272.1.21.0.304	rcn2kCardOverheatShutDown	rc2kCardIndex rcSlotType rc2kCardZoneTemperature rc2kCardTemperatureZoneInfo	An rcn2kCardOverheatShutDown trap indicates that a card has been shut down because the temperature has exceeded the shutdown threshold temperature.
1.3.6.1.4.1.2272.1.21.0.305	RcIsisPlsbSmltVirtBmacMisconfigTrap	rcIsisSmltVirtBmacMisconfigNodeSysId rcIsisPlsbTrapType rcIsisSmltVirtBmacMisconfigNodeHostName rcIsisTrapIndicator	An SPBM ISIS trap signifies that SMLT virtual BMAC has been used by nodes other than the SMLT nodes as system-id or MAC.

1.3.6.1.4.1.2272.1.63.9.x.xx series

The following table describes 1.3.6.1.4.1.2272.1.63.9.x.xx series traps.

OID	Notification type	Objects	Description
1.3.6.1.4.1.2272.1.63.9.1	rcIsisLocalLsp		Indicates the 8–byte Local LSP ID, which consists of the System ID, Circuit ID, and Fragment Number.

Table continues…

OID	Notification type	Objects	Description
1.3.6.1.4.1.2272.1.63.9.2	rcIsisLocalI1Metric		Indicates the I1-metric for the IS-IS interface on the local Node.
1.3.6.1.4.1.2272.1.63.9.3	rcIsisNgbLspId		Indicates the 8–byte neighbor LSP ID, which consists of the System ID, Circuit ID, and Fragment Number.
1.3.6.1.4.1.2272.1.63.9.4	rcIsisNgbI1Metric		Indicates the I1-metric for the IS-IS interface on the neighbor Node.
1.3.6.1.4.1.2272.1.63.9.5	rcIsisPlsbTrapType	metricMismatch(1), duplicateSysid(2), lsdbUpdate(3), duplicateNickname(4), bvidMismatch(5), smltVirtBmacMismatch(6),smltPeerBmacMismatch(7), adjState(8), smltSplitBebMismatch(9),multiLinkAdj(10)	An SPBM IS-IS trap is generated when a mismatch or duplicate ID is received.
1.3.6.1.4.1.2272.1.63.9.6	rcIsisLocalSysId		Indicates the IS-IS local node system-id.
1.3.6.1.4.1.2272.1.63.9.7	rcIsisLocalInterface		Indicates the IS-IS local interface index.
1.3.6.1.4.1.2272.1.63.9.8	rcIsisTrapIndicator	alarm(1) clear(2)	The value 1 indicates that an alarm has been raised; value 2 indicates an alarm has been cleared.
1.3.6.1.4.1.2272.1.63.9.9	rcIsisLocalNickname		Indicates the IS-IS local node nickname.
1.3.6.1.4.1.2272.1.63.9.10	rcIsisNgbNickname		Indicates the IS-IS neighbor node nickname.
1.3.6.1.4.1.2272.1.63.9.11	rcIsisNgbSysId		Indicates the IS-IS neighbor node system ID.
1.3.6.1.4.1.2272.1.63.9.12	rcIsisLocalPrimaryBvid		Indicates the IS-IS local primary BVID.
1.3.6.1.4.1.2272.1.63.9.13	rcIsisLocalPrimaryTieBrkAlg		Indicates the tie breaking algorithm applied to the local primary B-VID.
1.3.6.1.4.1.2272.1.63.9.14	rcIsisLocalSecondaryBvid		Indicates the IS-IS local secondary B-VID.

Table continues…

OID	Notification type	Objects	Description
1.3.6.1.4.1.2272.1.63.9.15	rcIsisLocalSecondaryTieBrk Alg		Indicates the tie breaking algorithm applied to the local secondary B-VID.
1.3.6.1.4.1.2272.1.63.9.16	rcIsisNgbPrimaryBvid		Indicates the IS-IS neighbor primary B-VID.
1.3.6.1.4.1.2272.1.63.9.17	rcIsisNgbPrimaryTieBrkAlg		Indicates the neighbor tie breaking algorithm applied to the primary BVID.
1.3.6.1.4.1.2272.1.63.9.18	rcIsisNgbSecondaryBvid		Indicates the IS-IS neighbor secondary B-VID.
1.3.6.1.4.1.2272.1.63.9.19	rcIsisNgbSecondaryTieBrkAl g		Indicates the neighbor tie breaking algorithm applied to the secondary B-VID.
1.3.6.1.4.1.2272.1.63.9.20	rcIsisLocalVirtualBmac		Indicates the SMLT Virtual BMAC configured in the local IST switch.
1.3.6.1.4.1.2272.1.63.9.21	rcIsisPeerVirtualBmac		Indicates the SMLT Virtual BMAC configured in the IST Peer.
1.3.6.1.4.1.2272.1.63.9.22	rcIsisSysId		Indicates the IS-IS system ID configured in the local switch or IST peer.
1.3.6.1.4.1.2272.1.63.9.23	rcIsisSmltPeerSysId		Indicates the SMLT Peer system ID configured in the local switch or IST peer.
1.3.6.1.4.1.2272.1.63.9.24	rcIsisAdjState	init(2), up(3), down(4)	Indicates different IS-IS adjacency states.
1.3.6.1.4.1.2272.1.63.9.25	rcIsisDuplicateNnameCounter		Indicates how many nodes in the network share the nickname.
1.3.6.1.4.1.2272.1.63.9.26	rcIsisLocalBvidCounter		Indicates how many B-VIDs are configured on local nodes.
1.3.6.1.4.1.2272.1.63.9.26	rcIsisLocalBvidCounter		Indicates how many B-VIDs are configured on local nodes.
1.3.6.1.4.1.2272.1.63.9.27	rcIsisNgbBvidCounter		Indicates how many B-VIDs are configured on neighbor nodes.
1.3.6.1.4.1.2272.1.63.9.28	rcIsisLocalSmltSplitBeb	primary(1), secondary(2)	Indicates the SMLT Split-BEB configured in the local IST switch.

Table continues…

OID	Notification type	Objects	Description
1.3.6.1.4.1.2272.1.63.9.29	rcIsisPeerSmltSplitBeb	primary(1), secondary(2)	Indicates the SMLT Split-BEB configured in the IST Peer switch.
1.3.6.1.4.1.2272.1.63.9.30	rcIsisLocalHostName		Indicates the IS-IS local host name.
1.3.6.1.4.1.2272.1.63.9.31	rcIsisNgbHostName		Indicates the IS-IS neighbor host name.
1.3.6.1.4.1.2272.1.63.9.32	rcIsisPrevInterface		Indicates the IS-IS local interface index for a previously found adjacency.

1.3.6.1.4.1.2272.1.64.1.x series

The following table describes 1.3.6.1.4.1.2272.1.64.1.x series traps.

OID	Notification type	Objects	Description
1.3.6.1.4.1.2272.1.64.1.0.1	rcnSlppPortDownEvent	rcSlppPortSlppEnable rcSlppVlanSlppEnable rcSlppIncomingVlanId rcSlppSrcMacAddress	This notification is generated whenever a port down event occurs due to Simple Loop Prevention Protocol (SLPP). The user is notified of the expected VLAN ID along with the VLAN ID and source MAC address of the packet coming in on the port identified. The first two objects can be used to lookup instance info for port ID and VLAN ID.
1.3.6.1.4.1.2272.1.64.1.0.2	rcnSlppPortDownEventNew	rcSlppRxPortIndex rcSlppRxVlanId rcSlppIncomingVlanId rcSlppSrcMacAddress	This notification is generated whenever a port down event occurs due to SLPP. The user is notified of the expected VLAN ID along with the VLAN ID and source MAC address of the packet coming in on the port identified.

1.3.6.1.4.1.2272.1.206.x.x.x series

The following table describes 1.3.6.1.4.1.2272.1.206.x.x.x series traps.

OID	Notification type	Objects	Description
1.3.6.1.4.1.2272.1.206.1.0.1	rcVrrpTmpTrapNewMaster	rcVrrpTmpOperationsMasterIpAddr rcVrrpTmpNewMasterReason	This notification is generated when Virtual Router Redundancy Protocol (VRRP) transitions to the master.
1.3.6.1.4.1.2272.1.206.2.2.1	rcVrrpExtTrapStateTransition	ifIndex rcVrrpExtTrapStateTransitionType rcVrrpExtTrapStateTransitionCause rcVrrpExtOperationsVrId rcVrrpTmpOperationsPrimaryIpAddr rcVrrpTmpOperationsMasterIpAddr	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.

Standard traps

The following table describes standard traps that Virtual Services Platform 9000 can generate.

Table 1: Standard traps

OID	Notification type	Objects	Description
1.3.6.1.2.1.14.16.2.1	ospfVirtIfStateChange	ospfRouterId ospfVirtIfAreaId ospfVirtIfNeighbor ospfVirtIfState	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual interface. This trap is generated after the interface state regresses, for example, goes from Point-to-Point to Down, or progresses to a terminal state, for example, Point-to-Point.
1.3.6.1.2.1.14.16.2.2	ospfNbrStateChange	ospfRouterId ospfNbrIpAddr ospfNbrAddressLessIndex ospfNbrRtrId ospfNbrStat	An ospfNbrStateChange trap signifies a change in the state of a non-virtual OSPF neighbor. This trap is generated after the neighbor state regresses, for example, goes from Attempt or Full to 1-Way or Down. or progresses to a terminal state, for example, 2-Way or Full. When a neighbor transitions from or to Full on non-broadcast multiple access and broadcast networks, the trap is

Table continues…

OID	Notification type	Objects	Description
			generated by the designated router. A designated router transitioning to Down will be noted by ospfIfStateChange.
1.3.6.1.2.1.14.16.2.3	ospfVirtNbrStateChange	ospfRouterId ospfVirtNbrArea ospfVirtNbrRtrId ospfVirtNbrState	An ospfIfStateChange trap signifies a change in the state of an OSPF virtual neighbor. This trap is generated after the neighbor state regresses, for example, goes from Attempt or Full to 1-Way or Down, or progresses to a terminal state, for example, Full.
1.3.6.1.2.1.14.16.2.4	ospfIfConfigError	ospfRouterId ospfIfIpAddress ospfAddressLessIf ospfPacketSrc ospfConfigErrorType ospfPacketType	An ospfIfConfigError trap signifies that a packet has been received on a nonvirtual interface from a router whose configuration parameters conflict with the configuration parameters of this router. Note that the event optionMismatch should cause a trap only if it prevents an adjacency from forming.
1.3.6.1.2.1.14.16.2.5	ospfVirtIfConfigError	ospfRouterId ospfVirtIfAreaId ospfVirtIfNeighbor ospfConfigErrorType ospfPacketType	An ospfConfigError trap signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with the configuration parameters of this router. Note that the event optionMismatch should cause a trap only if it prevents an adjacency from forming.
1.3.6.1.2.1.14.16.2.6	ospfIfAuthFailure	ospfRouterId ospfIfIpAddress ospfAddressLessIf ospfPacketSrc ospfConfigErrorType authTypeMismatch authFailure ospfPacketType	An ospfIfAuthFailure trap signifies that a packet has been received on a nonvirtual interface from a router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
1.3.6.1.2.1.14.16.2.7	ospfVirtIfAuthFailure	ospfRouterId ospfVirtIfAreaId ospfVirtIfNeighbor ospfConfigErrorType authTypeMismatch authFailure ospfPacketType	An ospfVirtIfAuthFailure trap signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
1.3.6.1.2.1.14.16.2.16	ospfIfStateChange	ospfRouterId ospfIfIpAddress ospfAddressLessIf ospfIfState	An ospfIfStateChange trap signifies a change in the state of a nonvirtual OSPF interface. This trap is generated after the interface state regresses, for example, goes from Dr to Down, or progresses to

Table continues…

OID	Notification type	Objects	Description
			a terminal state, for example, Point-to-Point, DR Other, Dr, or Backup.
1.3.6.1.2.1.16.0.1	risingAlarm	alarmIndex alarmVariable alarmSampleType alarmValue alarmRisingThreshold	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
1.3.6.1.2.1.16.0.2	fallingAlarm	alarmIndex alarmVariable alarmSampleType alarmValue alarmFallingThreshold	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
1.3.6.1.2.1.46.1.3.0.3	vrrpTrapStateTransition	ifIndex vrrpTrapStateTransitionType vrrpTrapStateTransitionCause vrrpOperVrId vrrpOperIpAddr ipAdEntAddr	A vrrpTrapStateTransition 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.
1.3.6.1.2.1.68.0.1	vrrpTrapNewMaster	vrrpOperMasterIpAddr	The newMaster trap indicates that the sending agent has transitioned to Master state.
1.3.6.1.2.1.68.0.2	vrrpTrapAuthFailure	vrrpTrapPacketSrc vrrpTrapAuthErrorType	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.
1.3.6.1.2.1.80.0.1	pingProbeFailed	pingCtlTargetAddressType pingCtlTargetAddress pingResultsOperStatus pingResultsIpTargetAddressType pingResultsIpTargetAddress pingResultsMinRtt pingResultsMaxRtt pingResultsAverageRtt pingResultsProbeResponse pingResultsSentProbes pingResultsRttSumOfSquares	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.

Table continues…

OID	Notification type	Objects	Description
		pingResultsLastGoodProbe	
1.3.6.1.2.1.80.0.2	pingTestFailed	pingCtlTargetAddressType pingCtlTargetAddress pingResultsOperStatus pingResultsIpTargetAddressType pingResultsIpTargetAddress pingResultsMinRtt pingResultsMaxRtt pingResultsAverageRtt pingResultsProbeResponses pingResultsSentProbes pingResultsRttSumOfSquares pingResultsLastGoodProbe	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.
1.3.6.1.2.1.80.0.3	pingTestCompleted	pingCtlTargetAddressType pingCtlTargetAddress pingResultsOperStatus pingResultsIpTargetAddressType pingResultsIpTargetAddress pingResultsMinRtt pingResultsMaxRtt pingResultsAverageRtt pingResultsProbeResponses pingResultsSentProbes pingResultsRttSumOfSquares pingResultsLastGoodProbe	This trap is generated at the completion of a ping test when the corresponding pingCtlTrapGeneration object is configured to testCompletion(4).
1.3.6.1.2.1.81.0.1	traceRoutePathChange	traceRouteCtlTargetAddressType traceRouteCtlTargetAddress traceRouteResultsIpTgtAddrType traceRouteResultsIpTgtAddr	This trap is generated after the path to a target changes.

Table continues…

OID	Notification type	Objects	Description
1.3.6.1.2.1.81.0.2	traceRouteTestFailed	traceRouteCtlTargetAddressType traceRouteCtlTargetAddress traceRouteResultsIpTgtAddrType traceRouteResultsIpTgtAddr	This trap is generated is traceroute cannot determine the path to a target (traceRouteNotifications 2).
1.3.6.1.2.1.81.0.3	traceRouteTestCompleted	traceRouteCtlTargetAddressType traceRouteCtlTargetAddress traceRouteResultsIpTgtAddrType traceRouteResultsIpTgtAddr	This trap is generated after the path to a target is determined.
1.3.6.1.6.3.1.1.5.1	coldStart	—	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing and that its configuration may have been altered.
1.3.6.1.6.3.1.1.5.2	warmStart	—	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing such that its configuration is unaltered.
1.3.6.1.6.3.1.1.5.3	linkDown	—	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
1.3.6.1.6.3.1.1.5.4	linkUp	—	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
1.3.6.1.6.3.1.1.5.5	authenticationFailure	—	—