



Fault Management Avaya Virtual Services Platform 9000

3.2
NN46250-703, 03.01
February 2012

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://support.avaya.com>.

Contents

Chapter 1: Purpose of this document.....	5
Chapter 2: New in this release.....	7
Features.....	7
Other changes.....	8
Chapter 3: Fault management fundamentals.....	9
Local alarms.....	9
Remote monitoring.....	9
Link state change control.....	12
Chapter 4: Key Health Indicators using ACLI.....	15
Displaying KHI information.....	15
Clearing KHI information.....	25
Displaying KHI performance information.....	25
Displaying KHI control processor information.....	32
Chapter 5: Key Health Indicators using EDM.....	35
Clearing KHI statistics.....	35
Viewing KHI forwarding information.....	36
Viewing protocol drop counters.....	37
Viewing COP statistics.....	39
Displaying KHI port information.....	39
Chapter 6: Link state change control using ACLI.....	41
Controlling link state changes.....	41
Displaying link state changes.....	42
Chapter 7: Link state change control using EDM.....	45
Controlling link state changes.....	45
Chapter 8: RMON configuration using ACLI.....	47
Configuring RMON.....	47
Viewing RMON settings.....	49
Chapter 9: RMON configuration using EDM.....	51
Enabling RMON globally.....	51
Enabling RMON history.....	52
Disabling RMON history.....	54
Creating an alarm.....	55
Viewing RMON alarms.....	58
Viewing RMON events.....	58
Viewing the RMON log.....	59
Deleting an alarm.....	60
Creating a default RMON event.....	61
Creating a nondefault RMON event.....	62
Deleting an event.....	63
Chapter 10: Viewing statistics using ACLI.....	65
Viewing RMON statistics.....	65
Chapter 11: Viewing statistics using EDM.....	67
Enabling RMON statistics.....	67
Disabling RMON statistics.....	68

Chapter 12: Log and trap fundamentals.....	69
Simple Network Management Protocol.....	69
Overview of traps and logs.....	70
Log message format.....	72
Log files.....	74
Log file transfer.....	75
Chapter 13: Log configuration using ACLI.....	77
Configuring a UNIX system log and syslog host.....	77
Configuring logging.....	80
Configuring the remote host address for log transfer.....	82
Configuring system logging to external storage.....	83
Configuring system message control.....	85
Extending system message control.....	86
Viewing logs.....	87
Configuring ACLI logging.....	89
Chapter 14: Log configuration using EDM.....	93
Configuring the system log.....	93
Configuring the system log table.....	94
Chapter 15: SNMP trap configuration using ACLI.....	97
Configuring an SNMP host.....	97
Configuring an SNMP notify filter table.....	99
Configuring SNMP interfaces.....	100
Enabling SNMP trap logging.....	101
Chapter 16: SNMP trap configuration using EDM.....	103
Configuring an SNMP host target address.....	103
Configuring target table parameters.....	105
Configuring an SNMP notify table.....	106
Configuring SNMP notify filter profiles.....	107
Configuring SNMP notify filter profile table parameters.....	108
Enabling SNMP trap logging.....	109
Chapter 17: RMON alarm variables.....	111
RMON alarm variables.....	111
Chapter 18: Customer service.....	135
Getting technical documentation.....	135
Getting product training.....	135
Getting help from a distributor or reseller.....	135
Getting technical support from the Avaya Web site.....	135
Glossary.....	137

Chapter 1: Purpose of this document

Fault Management provides information about how to prevent faults and improve the performance of the Avaya Virtual Services Platform 9000.

Fault Management includes procedures for RMON, link state change, key health indicators, and logs and traps.

The fault management function supports tasks related to managing or preventing faults, troubleshooting, and monitoring and improving the performance of the network or product.

Purpose of this document

Chapter 2: New in this release

The following sections detail what is new in *Avaya Virtual Services Platform 9000 Fault Management*, NN46250–703, for Release 3.2.

Features

See the following section for information about feature-related changes.

Log message format

In Release 3.2, the format of module identification in log messages is updated. Prior to Release 3.2, the log message identified which CP module logged the message, and the slot number of the affected module was embedded later. The new log message format identifies the module at the beginning of the message text. For more information, see [Log message format](#) on page 72.

System log support of IPv6

In Release 3.2, 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. For more information, see:

- [Overview of traps and logs](#) on page 70
- [Configuring a UNIX system log and syslog host](#) on page 77
- [Configuring the system log table](#) on page 94

ACLI and SNMP log consolidation

Prior to Release 3.2, the system stored the CLI log and SNMP log in two separate files on the external flash: `clilog.txt` and `snmplog.txt`. The system did not send the SNMP log and ACLI Command logs to the syslog server.

In Release 3.2, the ACLI command and SNMP logs are included in the main system log file, which can be sent to an external syslog server.

The following commands are obsolete:

- `clilog maxfilesize <64-256000>`
- `clilog syslog-host enable`
- `snmplog maxfilesize <64-256000>`

The commands `show logging file module cliilog` and `show logging file module snmplog` replace previous commands to show ACLI and SNMP logs. The following commands are only applicable to log files generated by past releases prior to Release 3.2:

- `show cliilog file`
- `save cliilog file`
- `show snmplog file`
- `save snmplog file`

For more information, see:

- [Overview of traps and logs](#) on page 70
- [Enabling SNMP trap logging](#) on page 101
- [Viewing logs](#) on page 87
- [Configuring ACLI logging](#) on page 89

Other changes

See the following sections for information about changes that are not feature-related.

ACLI and EDM chapters

ACLI and EDM chapters are grouped together to improve clarity. Fundamentals chapters are placed at the beginning of the document, followed by ACLI and then EDM procedures.

ACLI Commands

Examples for ACLI commands exist for most commands in the document.

Introduction chapter and navigation

Introduction chapters and navigation are removed.

Purpose of this document

To improve documentation usability, a brief description of the purpose of this document is now the first chapter.

Terminology

Terminology no longer exists in a separate document. Terminology is in a glossary at the end of this document.

Common procedures

Common procedures are incorporated in the document.

Chapter 3: Fault management fundamentals

Fault management includes the tools and features available to monitor and manage faults. This section provides overview for local alarms, remote monitoring (RMON), traps and logs, and link state changes (port flapping).

Local alarms

Avaya Virtual Services Platform 9000 contains a local alarms mechanism. Local alarms are raised and cleared by applications running on the switch. Active alarms are viewed using the `show alarm database` command in the ACLI. Local alarms are an automatic mechanism run by the system that do not require any additional user configuration. Check local alarms occasionally to ensure no alarms require additional operator attention. The raising and clearing of local alarms also creates a log entry for each event.

Remote monitoring

Remote monitoring (RMON) is a management information base (MIB). A MIB is a group of management objects that you can use to obtain or configure values. Use the Simple Network Management Protocol (SNMP) to manipulate the objects in MIB.

You can use Avaya command line interface (ACLI), Enterprise Device Manager (EDM), or Configuration and Orchestration Manager (COM) to globally enable RMON for devices on Avaya Virtual Services Platform 9000. After you globally enable RMON, you can enable monitoring for individual devices on a port-by-port basis.

RMON has four major functions:

- configure alarms for user-defined events
- collect Ethernet statistics
- log events
- send traps for events

Within Enterprise Device Manager, you can configure RMON alarms that relate to specific events or variables after you select variables from a list. After you configure the system to send events associated with alarms to trap or log-and-trap, tripped alarms are trapped or logged.

You can view all RMON information using EDM, ACLI, or COM. You can use all management applications that support SNMP traps to view RMON trap information.

RMON alarms

You can use RMON alarms to alert you if the value of a variable falls outside a designated range.

You can define RMON alarms on all MIB variables that resolve to an integer value, but you cannot use string variables (such as system description) as alarm variables.

All alarms share the following characteristics:

- a defined upper and lower threshold value
- a corresponding rising and falling event
- an alarm interval or polling period

After you activate alarms, you can

- view the activity in a log or a trap log
- create a script directing the system to sound an audible alert at a console
- create a script directing the system to send an e-mail
- create a script directing the system to call a pager

The alarm variable is polled and the result is compared against upper and lower limit values selected after you create the alarm. If either limit is reached or crossed during the polling period, the alarm fires and generates an event that you can view in the event log or the trap log.

The upper limit of the alarm is the rising value, and the lower limit is the falling value. RMON periodically samples data based upon the alarm interval. During the first interval that the data passes above the rising value, the alarm fires as a rising event. During the first interval that the data drops below the falling value, the alarm fires as a falling event.

The following figure shows how alarms fire:

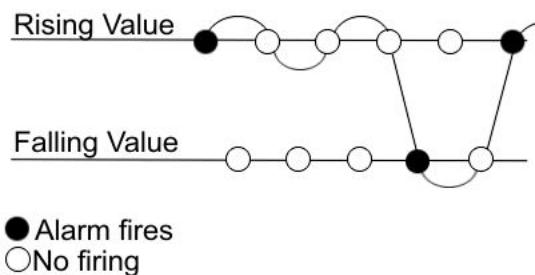


Figure 1: How alarms fire

The alarm fires during the first interval when the sample goes out of range. No additional events generate for that threshold until the opposite threshold is crossed. Therefore, it is important that you carefully define the rising and falling threshold values for alarms. Incorrect thresholds cause an alarm to fire at every alarm interval.

You can define one threshold value to an expected, baseline value, and then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value is equal to ± 1 baseline unit. For example, suppose you define an alarm with octets leaving a port as

the variable. The intent of the alarm is to notify you if excessive traffic occurs on that port. You enable spanning tree, and then 52 octets transmit from the port every 2 seconds, which is equivalent to baseline traffic of 260 octets every 10 seconds. This alarm notifies you if the lower limit of exiting octets is defined at 260 and the upper limit is defined at 320 (or at all values greater than $260 + 52 = 312$).

The first time outbound traffic other than spanning tree Bridge Protocol Data Units (BPDU) occurs, the rising alarm fires. After outbound traffic other than spanning tree ceases, the falling alarm fires. This process provides the time intervals of all nonbaseline outbound traffic.

If you define the alarm with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds), for example, 250, the rising alarm can fire only once, as shown in the following example. The falling alarm (the opposite threshold) must fire for the rising alarm to fire a second time. The falling alarm cannot fire unless the port becomes inactive or you disable spanning tree, which causes the value for outbound octets to drop to zero, because the baseline traffic is always greater than the value of the falling threshold. The failure of the falling alarm to fire prevents the rising alarm from firing a second time.

The following figure shows an example of the alarm threshold:

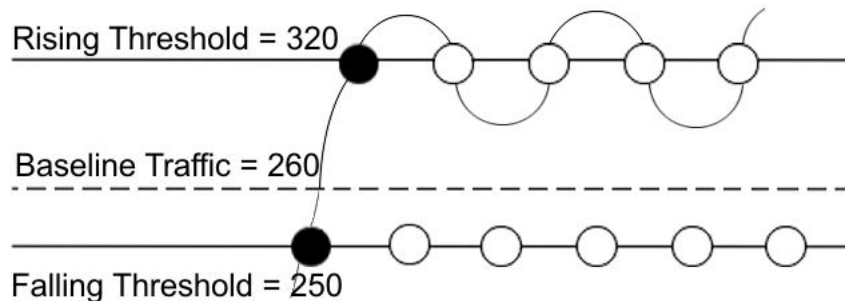


Figure 2: Alarm example, threshold less than 260

To create an alarm, you must select a variable from the variable list and a port, or another component to which it connects. Some variables require port IDs, card IDs, or other indexes (for example, spanning tree group IDs). You select a rising and a falling threshold value. The rising and falling values compare to the actual value of the variable that you choose. If the variable falls outside of the rising or falling value range, an alarm triggers and an event is logged or trapped.

To create an alarm, you must also select a sample type, which can be either absolute or delta. Define absolute alarms based on the cumulative value of the alarm variable. An example of an absolute alarm value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you configure it as the absolute value. Therefore, you can create an alarm with a rising value of 2 and a falling value of 1 to alert you whether the card is up or down.

Configure most alarm variables related to Ethernet traffic as a delta value. Define delta alarms based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice for each polling period. For each sample, the last two values are added and compared to the threshold values. This process increases precision and detects threshold crossings that span the sampling boundary. Therefore, if you track the current values of a delta-valued alarm and add them, the result is twice the actual value. This result is not an error in the software.

RMON history

The RMON history group records periodic statistical samples from a network. A sample is a history and is gathered in time intervals referred to as buckets. You enable and create histories to establish a time-dependent method to gather RMON statistics on a port. The following are the default values for history:

- Buckets are gathered at 30-minute intervals.
- The number of buckets gathered is 50.

You can configure both the time interval and the number of buckets. However, after the last bucket is reached, bucket 1 is dumped and recycled to hold a new bucket of statistics. Then buckets 2 to 50 are dumped as needed.

RMON events

RMON events and alarms work together to notify you if values in your network go out of a specified range. After a value passes the specified range, the alarm fires. The event specifies how the activity is recorded.

An event specifies whether a trap, a log, or both a trap and a log generates to view alarm activity. After you globally enable RMON, two default events generate:

- RisingEvent
- FallingEvent

The default events specify that after an alarm goes out of range, both a trap and a log track the firing of the alarm. For example, after an alarm fires at the rising threshold, the rising event specifies to send this information to both a trap and a log. Likewise, after an alarm passes the falling threshold, the falling event specifies to send this information to a trap and a log.

RMON statistics

You can use Enterprise Device Manager (EDM) to gather and graph Ethernet statistics in a variety of formats, or you can save them to a file and export them to a third-party presentation or graphing application.

This implementation of RMON requires a control row for Ethernet statistics. This control row appears as port 0/1 if you open the RMON, Control, Ethernet Statistics tab in EDM. The row ID is reserved for the control row. Therefore, some automated tests, such as ANVL, can fail if the test attempts to create a row 1.

Link state change control

Rapid fluctuation in a port link state is called link flapping.

Link flapping is detrimental to network stability because it can trigger recalculation in spanning tree and the routing table.

If the number of port down events exceeds a configured limit during a specified interval, the system forces the port out of service.

You can configure link flap detection to control link state changes on a physical port. You can set thresholds for the number and frequency of changes allowed.

You can configure the system to take one of the following actions if changes exceed the thresholds:

- send a trap
- bring down the port

If changes exceed the link state change thresholds, the system generates a log entry.

Chapter 4: Key Health Indicators using ACLI

The Key Health Indicators (KHI) feature of Avaya Virtual Services Platform 9000 provides a subset of health information that allows for quick assessment of the overall operational state of the device.

 **Note:**

The KHI feature is not intended to provide a comprehensive debugging solution. Instead, KHI identifies key information that could lead Avaya support personnel towards discovery of a specific failure. After the technician assesses the KHI information, further debugging is required to determine the specific reason for the fault.

Avaya recommends that you capture KHI information during normal operations to provide a baseline for Avaya support personnel when detecting fault situations.

Displaying KHI information

About this task

Use the commands detailed in this section to show KHI information. All commands use a slot number as an optional argument. Specifying the slot number limits command output to that slot. Leaving the slot number out of the command displays KHI information for all applicable slots. You can issue the KHI commands from any command mode.

 **Note:**

The show khi forwarding commands are only valid for IO slots.

Procedure

1. Display all KHI statistics:
`show khi forwarding [<3-12>]`
2. Display IFP statistics:
`show khi forwarding ifp [<3-12>]`
3. Display internal statistics:
`show khi forwarding k2 [<3-12>]`
4. Display MAC packet transmit, receive, and drop counts:
`show khi forwarding mac [<3-12>]`

5. Display per lane internal datapath counters:
`show khi forwarding mac-higig [<3-12>]`
6. Display internal QE statistics:
`show khi forwarding qe [<3-12>]`
7. Display internal RSP counters:
`show khi forwarding rsp [<3-12>]`
8. Display internal Zagros counters:
`show khi forwarding zagros [<3-12>]`
9. Run all KHI show commands and capture the output to the file named in the file parameter:
`show fulltech khi [file WORD<1-99>]`

Example

```
VSP-9012:1#show khi forwarding ifp 4
=====
Forwarding KHI Details - IFP Statistics - Slot 4
=====
```

RuleNo	Rulename	Ports 1-24	Ports 25-48
3	Datapath HB HG0	10434	10434
4	Datapath HB HG1	10435	10434
6	Egress Packets	13099589	5155
7	Egress Packets	6873	10322
55	BPDU	40431	35279
58	SLPP	36566	0
59	SLPP - Multicast	28	0
62	ARP request	12	0
63	ARP Other	6	0
70	IST LSM	12826155	0
117	Routed,IPv4,Other,TTL=1	31	0
138	VRRP	10328	0
143	OSPF-MC (all routers)	4174	0
145	OSPF-MC (designated routers)	1	0
221	IST (for SMLT)	20190	0
240	Bridged,IPv4,ICMP	83	0

```
VSP-9012:1#show khi forwarding k2 4
=====
Forwarding KHI Details - K2 Statistics - Slot 4
=====
```

Health Indicator	Ports 1-12	Ports 25-36
MAC->K2 If 0	38944	24959
K2 If 0->Zagros	3356144	3342153
Zagros->K2 If 0	17538	21036
K2 If 0->MAC	13289139	15798
MAC->K2 If 0 Err	0	0
K2 If 0->Zagros Err	0	0
Zagros->K2 If 0->Err	0	0
K2 If 0->MACErr	0	0
IP Multicast Drops		
Ports 1 and 25	0	0


```

IP Multicast Drops
Ports 2 and 26          0          0
IP Multicast Drops
Ports 3 and 27          0          0
IP Multicast Drops
Ports 4 and 28          0          0
IP Multicast Drops
Ports 5 and 29          0          0
IP Multicast Drops
Ports 6 and 30          0          0
IP Multicast Drops
Ports 7 and 31          0          0
IP Multicast Drops
Ports 8 and 32          0          0
IP Multicast Drops
Ports 9 and 33          0          0
IP Multicast Drops
Ports 10 and 34         0          0
IP Multicast Drops
Ports 11 and 35         0          0
IP Multicast Drops
Ports 12 and 36         0          0
-----

```

```

Health Indicator          Ports 13-24          Ports 37-48
-----
MAC->K2 If 1              13158276            32160
K2 If 1->Zagros           16496150            3370027
Zagros->K2 If 1           13372000            15900
K2 If 1->MAC              13372000            15900
MAC->K2 If 1 Err         0                   0
K2 If 1->Zagros Err      0                   0
Zagros->K2 If 1->Err     0                   0
K2 If 1->MACErr          0                   0
IP Multicast Drops
Ports 13 and 37          0                   0
IP Multicast Drops
Ports 14 and 38          0                   0
IP Multicast Drops
Ports 15 and 39          0                   0
IP Multicast Drops
Ports 16 and 40          0                   0
IP Multicast Drops
Ports 17 and 41          0                   0
IP Multicast Drops
Ports 18 and 42          0                   0
IP Multicast Drops
Ports 19 and 43          0                   0
IP Multicast Drops
Ports 20 and 44          0                   0
IP Multicast Drops
Ports 21 and 45          0                   0
IP Multicast Drops
Ports 22 and 46          0                   0
IP Multicast Drops
Ports 23 and 47          0                   0
IP Multicast Drops
Ports 24 and 48          0                   0

```

```

VSP-9012:1#show khi forwarding mac 4
=====
Forwarding KHI Details - MAC Statistics - Slot 4
=====
Ports  Rx OK          Tx OK          Rx Err          Tx Err

```

Key Health Indicators using ACLI

4/1	7568	3972	0	0
4/2	0	0	0	0
4/3	0	0	0	0
4/4	0	0	0	0
4/5	0	0	0	0
4/6	4825649	4642006	0	0
4/7	4269079	4220186	0	0
4/8	4260696	4684188	0	0
4/9	0	0	0	0
4/10	0	0	0	0
4/11	0	0	0	0
4/12	0	7137	0	0
4/13	7568	1774	0	0
4/14	0	0	0	0
4/15	0	0	0	0
4/16	0	0	0	0
4/17	0	0	0	0
4/18	0	0	0	0
4/19	0	0	0	0
4/20	7147	1779	0	0
4/21	0	0	0	0
4/22	0	0	0	0
4/23	7145	1783	0	0
4/24	7145	1783	0	0
4/25	7583	1774	0	0
4/26	0	0	0	0
4/27	7145	1783	0	0
4/28	7146	1784	0	0
4/29	0	0	0	0
4/30	0	0	0	0
4/31	0	0	0	0
4/32	0	0	0	0

4/33	0	0	0	0
4/34	0	0	0	0
4/35	0	0	0	0
4/36	0	0	0	0
4/37	7583	1774	0	0
4/38	0	0	0	0
4/39	0	0	0	0
4/40	0	0	0	0
4/41	0	0	0	0
4/42	0	0	0	0
4/43	0	0	0	0
4/44	0	0	0	0
4/45	0	7166	0	0
4/46	0	0	0	0
4/47	8238	1779	0	0
4/48	0	0	0	0

Ports ASK	RDBGCO	RDBGCO MASK	TDBGCO	TDBGCO M

4/1	0	0x0	0	0x0
4/2	0	0x0	0	0x0
4/3	0	0x0	0	0x0
4/4	0	0x0	0	0x0
4/5	0	0x0	0	0x0
4/6	40	0xc1	0	0x0
4/7	33	0xc1	0	0x0
4/8	19225	0xd1	0	0x0
4/9	0	0x0	0	0x0
4/10	0	0x0	0	0x0
4/11	0	0x0	0	0x0
4/12	0	0x0	0	0x0
4/13	0	0x0	0	0x0
4/14	0	0x0	0	0x0

Key Health Indicators using ACLI

4/15	0	0x0	0	0x0
4/16	0	0x0	0	0x0
4/17	0	0x0	0	0x0
4/18	0	0x0	0	0x0
4/19	0	0x0	0	0x0
4/20	0	0x0	0	0x0
4/21	0	0x0	0	0x0
4/22	0	0x0	0	0x0
4/23	0	0x0	0	0x0
4/24	0	0x0	0	0x0
4/25	0	0x0	0	0x0
4/26	0	0x0	0	0x0
4/27	0	0x0	0	0x0
4/28	0	0x0	0	0x0
4/29	0	0x0	0	0x0
4/30	0	0x0	0	0x0
4/31	0	0x0	0	0x0
4/32	0	0x0	0	0x0
4/33	0	0x0	0	0x0
4/34	0	0x0	0	0x0
4/35	0	0x0	0	0x0
4/36	0	0x0	0	0x0
4/37	0	0x0	0	0x0
4/38	0	0x0	0	0x0
4/39	0	0x0	0	0x0
4/40	0	0x0	0	0x0
4/41	0	0x0	0	0x0
4/42	0	0x0	0	0x0
4/43	0	0x0	0	0x0
4/44	0	0x0	0	0x0
4/45	0	0x0	0	0x0
4/46	0	0x0	0	0x0
4/47	1112	0x51	0	0x0

```

4/48  0          0x0          0          0x0

VSP-9012:1#show khi forwarding mac-higig 4
=====
          Forwarding KHI Details - MAC HIGIG Statistics - Slot 4
=====

Health Indicator          Ports 1-12          Ports 25-36
-----
MAC->K2 If 0              360228351          346478657
K2 If 0->MAC              13890172           11077
RDGBC0                    3                  0
RDGBC0 Mask               65                 0
TDGBC0                    19396              0
TDGBC0 Mask               69                 0
-----

Health Indicator          Ports 13-24         Ports 37-48
-----
MAC->K2 If 1              346583396          346471315
K2 If 1->MAC              11082              16558
RDGBC0                    0                  0
RDGBC0 Mask               0                  0
TDGBC0                    0                  0
TDGBC0 Mask               0                  0
-----

Health Indicator          Ports 1-24          Ports 25-48
-----
IFP DOS Drops             0                  0

VSP-9012:1#show khi forwarding qe 6
=====
          Forwarding KHI Details - QE Statistics - Slot 4
=====

Health Indicator          Ports 1-24          Ports 25-48
-----
Ingress qm_agr_accepted_pkt_cnt0  27775377          14009382
Ingress qm_agr_accepted_pkt_cnt1  348                348
Ingress qm_agr_dequeued_pkt_cnt   27775725          14009730
Ingress pm_switch_pkt_cnt         27775725          14009730
Ingress sr0_rx_p0_pkt_cnt         20760984          7009730
Ingress srl_rx_p0_pkt_cnt         7017100           7002359
Egress sv_pkt_cnt                 41705515          27673485
Egress st0_p0_tx_pkt_cnt          5250              5248
Egress st1_p0_tx_pkt_cnt          5250              5248
Egress st0_p2_tx_pkt_cnt          0                 1837
Egress st0_p3_tx_pkt_cnt          0                 1838
Egress st0_p5_tx_pkt_cnt          4810302           0
Egress st0_p7_tx_pkt_cnt          4831886           0
Egress st1_p7_tx_pkt_cnt          1833              0
Egress st1_p8_tx_pkt_cnt          0                 7363
Egress st1_p10_tx_pkt_cnt         1837              1829
Egress st0_p11_tx_pkt_cnt         7362              0
Egress st1_p11_tx_pkt_cnt         1837              0
Egress st0_p14_tx_pkt_cnt         45257             0
Egress st0_p15_tx_pkt_cnt         27642394          27642403
Egress st1_p15_tx_pkt_cnt         27642395          27642403
Qm_agr_non_wred_dropped_pkt_cnt   2359              2359

VSP-9012:1#show khi forwarding rsp 4
=====
          Forwarding KHI Details - RSP Statistics - Slot 4
=====

```

Key Health Indicators using ACLI

```

=====
Health Indicator          Ports 1-12          Ports 25-36
-----
LSM Drops                27886538           27886546
Exception Drops          0                   0
Frame Error Drops        0                   0
FDIB full drops          0                   0
Ingr MLT                 0                   0
All Ports Down
Egress mlt all           0                   0
Ports Down Drops
Egress IP Mcast          0                   0
Records not found
Egress IP Mcast          0                   0
MLT Wrong Port
Egress IP Mcast          0                   0
Source Knockout
Ingress DA not
Found Drops
Ingress Unknown          0                   0
Ingress Discard          0                   0
Dest Id Drops
MAC Learning             0                   0
Packet Drops
Ingress IPMC             0                   0
Supression Drops
Unsupported Feature
Drops
ACL Discards             0                   0
Ingress IPMC             0                   0
Lookup Fails
IPV4 Dest IP             0                   0
Lookup Fails
IPV4 Source IP           0                   0
Lookup Fails
L3Mirror Drops          0                   0
-----
Health Indicator          Ports 13-24         Ports 37-48
-----
LSM Drops                27886543           27886553
Exception Drops          0                   0
Frame Error Drops        0                   0
FDIB full drops          0                   0
Ingr MLT                 0                   0
All Ports Down
Egress mlt all           0                   0
Ports Down Drops
Egress IP Mcast          0                   0
Records not found
Egress IP Mcast          0                   0
MLT Wrong Port
Egress IP Mcast          0                   0
Source Knockout
Ingress DA not
Found Drops
Ingress Unknown          0                   0
Ingress Discard          0                   0
Dest Id Drops
MAC Learning             0                   0
Packet Drops
Ingress IPMC             0                   0
Supression Drops
Unsupported Feature          0                   0

```

```

Drops
ACL Discards          0          0
Ingress IPMC          0          0
Lookup Fails
IPV4 Dest IP         0          0
Lookup Fails
IPV4 Source IP       0          0
Lookup Fails
L3Mirror Drops       0          0
    
```

VSP-9012:1#show khi forwarding zagros 4

=====

Forwarding KHI Details - Zagros Statistics - Slot 4

=====

Health Indicator	Ports 1-12	Ports 25-36
K2 If 1->Zagros	17820610	3636961
Zagros->RSP	49911364	35725374
Zagros->QE If 1	21413791	7227758
QE If 1->Zagros	43022385	28518470
Zagros->K2 If 1	14431581	17157
Zagros EHP All Port down		
IST counter	1185	1185
Zagros EHP All Port down		
MLT counter	6	0
EHP IGR IST filter		
drop counter	36	0
ZAP Tx Ctl	59680679	59593801
ZAP Tx Data	46644	0
ZAP Rx Ctl	59680682	59593804
ZAP Tx HBE	28497747	28497788
Egress Esb1Count	4226	1884
Egress Esb3Count	0	1893
Egress Esb4Count	0	1894
Egress Esb6Count	4937358	0
PMM output Drop count	28497573	28497615
PMM Admission RSP		
Drop Count	28497573	28497614
PMM RSP rx count	49911364	35725372
PMM RSP tx count	35845372	7244915
PMM HAB bus rx	49911364	35725372
PMM CIF request count	35745527	35679054
PMM CIF response count	35745527	35679054
PMM page pool 3 count	131072	131072
PMM page pool 4 count	131072	131072
PMM page pool 5 count	65536	65536
PMM page pool 6 count	196608	131072
PMM page pool 7 count	131072	0
PMM page pool 8 count	196608	131072
PMM free page counters	286263258	269551578
PMM PLC threshold register	4194474	4194474
PMM RE threshold register	48	48
PMM number of pools	9	9

Health Indicator	Ports 13-24	Ports 37-48
K2 If 1->Zagros	3644552	3629361
Zagros->RSP	35732948	35717799
Zagros->QE If 1	7235354	7220161

Key Health Indicators using ACLI

QE If 1->Zagros	28520340	28524183
Zagros->K2 If 1	19047	22846
Zagros EHP All Port down		
IST counter	1185	1185
ZAP Tx Ctl	59636469	59594265
ZAP Rx Ctl	59636472	59594268
ZAP Tx HBE	28497768	28497812
Egress EsblCount	1886	1884
PMM output Drop count	28497594	28497638
PMM Admission RSP		
Drop Count	28497594	28497638
PMM RSP rx count	35732948	35717799
PMM RSP tx count	7254401	7243007
PMM HAB bus rx	35732948	35717799
PMM CIF request count	35679041	35679081
PMM CIF response count	35679041	35679081
PMM page pool 3 count	131072	131072
PMM page pool 4 count	131072	131072
PMM page pool 5 count	65536	65536
PMM page pool 6 count	131072	131072
PMM page pool 8 count	131072	131072
PMM free page counters	286394328	269617113
PMM PLC threshold register	4194474	4194474
PMM RE threshold register	48	48
PMM number of pools	9	9

Variable definitions

Use the data in the following table to use the commands in this procedure.

Table 1: Variable definitions

Variable	Value
<3-12>	Specifies the slot number.
file <i>WORD</i> <1-99>	Specifies the filename and location, from 1-99 characters, in one of the following formats: <ul style="list-style-type: none">• /intflash/<file>• /extflash/<file>• /usb/<file>

Clearing KHI information

About this task

KHI information can be cleared for a specific slot or across the whole device. Use the command to clear the statistics. Specify a slot number to clear statistics for a specific slot or leave it absent to clear information for the whole device.

Procedure

1. Clear forwarding statistics:

```
clear khi forwarding [slot <3-12>]
```

If you clear the forwarding statistics, the IFP rules do not appear in the show command output again until the specific traffic hits the rule again.

2. Clear CPP statistics:

```
clear khi cpp <iocop-statistics|port-statistics|protocol-drops>
```

Variable definitions

Use the data in the following table to use the `clear khi` command.

Table 2: Variable definitions

Variable	Value
<3-12>	Specifies the slot number.

Displaying KHI performance information

About this task

Use the following commands to display information about the performance of the Key Health Indicator feature.

 **Note:**

KHI performance commands can be used on all slots. If you do not specify a slot, information for all slots is shown.

Procedure

1. Display buffer performance and utilization statistics for KHI:

```
show khi performance buffer-pool [{slot[-slot]][,...]}
```

Buffer pool is not supported on interface or Switch Fabric (SF) slots.
2. Show current utilization, 5-minute average utilization, and 5-minute high water mark with date and time of event:

```
show khi performance cpu [{slot[-slot]][,...]}
```
3. Display memory performance and utilization statistics for KHI on the specified slot or all slots:

```
show khi performance memory [{slot[-slot]][,...]}
```
4. Display process performance and utilization statistics for KHI on the specified slot or all slots:

```
show khi performance process [{slot[-slot]][,...]}
```
5. Display thread performance and utilization statistics for KHI on the specified slot or all slots:

```
show khi performance pthread [{slot[-slot]][,...]}
```
6. Display internal memory management resource performance and utilization statistics for KHI on the specified slot or all slots:

```
show khi performance slabinfo [{slot[-slot]][,...]}
```

Example

```
VSP-9012:1#show khi performance buffer-pool 1
```

```
Slot:1
  CPP:
    UsedFBuffs: 0
    FreeFBuffs: 1600
    NoFbuff: 0

  Network stack system:
    UsedMbuf: 120
    FreeMbuf: 47730
    SocketMbuf: 15
```

```
Network stack data:
  UsedMbuf: 4
  FreeMbuf: 5372
```

```
Letter API message queue:
  QHigh: 0
  QNormal: 0
  FreeQEntries: 51200
```

```
VSP-9012:1#show khi performance cpu 4
```

```
Slot:4
  Current utilization: 13
  5-minute average utilization: 12
  5-minute high water mark: 16 (02/08/11 09:41:04)
```

```
VSP-9012:1#show khi performance memory 4
```

```
Slot:4
```

Used: 139164 (KB)
 Free: 345276 (KB)
 Current utilization: 28 %
 5-minute average utilization: 28 %
 5-minute high water mark: 28 (02/08/11 09:41:24)

VSP-9012:1#show khi performance process 1
 Slot:1

PID	PPID	PName	VmSize	VmLck	VmRss	VmData	VmStk	VmExe	VmLib
1	0	init	2948	0	680	344	84	496	1764
2	1	ksoftirqd/0	0	0	0	0	0	0	0
3	1	events/0	0	0	0	0	0	0	0
4	1	khelper	0	0	0	0	0	0	0
5	1	kthread	0	0	0	0	0	0	0
30	5	kblockd/0	0	0	0	0	0	0	0
55	5	pdflush	0	0	0	0	0	0	0
56	5	pdflush	0	0	0	0	0	0	0
57	1	kswapd0	0	0	0	0	0	0	0
58	5	aio/0	0	0	0	0	0	0	0
624	1	mtddblockd	0	0	0	0	0	0	0
652	1	init	2948	0	244	344	84	496	1764
653	652	rcS	2868	0	1308	184	84	792	1496
674	5	wdd	0	0	0	0	0	0	0
925	1	ntpd	3536	0	1156	496	84	584	1896
929	1	portmap	1924	0	488	160	84	80	1348
931	1	inetd	3056	0	620	344	84	496	1804
933	1	syslogd	2948	0	508	344	84	496	1764
935	1	klogd	2948	0	496	344	84	496	1764
1333	5	khubd	0	0	0	0	0	0	0
1498	1	nfsd	0	0	0	0	0	0	0
1499	1	nfsd	0	0	0	0	0	0	0
1500	1	nfsd	0	0	0	0	0	0	0
1501	1	lockd	0	0	0	0	0	0	0
1502	5	rpciod/0	0	0	0	0	0	0	0
1518	1	nfsd	0	0	0	0	0	0	0
1519	1	nfsd	0	0	0	0	0	0	0
1520	1	nfsd	0	0	0	0	0	0	0
1521	1	nfsd	0	0	0	0	0	0	0
1522	1	nfsd	0	0	0	0	0	0	0
1526	1	rpc.mountd	1996	0	668	180	84	128	1352
1534	1	sshd	4612	0	928	368	84	468	2760
1560	1	tar	0	0	0	0	0	0	0
1561	653	rc.appfs	2868	0	1352	184	84	792	1496
1683	1	ckrm_cpud/0	0	0	0	0	0	0	0
1819	5	oxide	0	0	0	0	0	0	0
1897	1561	start	2868	0	1296	184	84	792	1496
1935	1897	lifecycle	75880	0	3348	68512	84	216	4900
1983	1935	patchAgent	4276	0	1372	632	180	148	2776
1984	1935	sockserv	4752	0	1548	416	84	80	3168
1985	1935	externalcf	3932	0	956	192	84	76	2256
1986	1935	oom95	109120	0	104176	102860	84	120	4672
1987	1935	oom90	109120	0	104176	102860	84	120	4672
1988	1935	imgsync.x	41236	0	3168	34196	84	164	4888
2001	1	gzip	0	0	0	0	0	0	0
2011	1	gzip	0	0	0	0	0	0	0
2014	1935	cbbcm-main.x	52716	0	12044	36416	84	9300	4232
2015	1935	cbcp-main.x	745168	32896	604720	705096	84	29352	3184
2016	1935	coreManager.x	33088	0	2872	26892	84	136	4664
2017	1935	patchmanager.x	33280	0	3384	25876	84	148	5448
2018	1935	patchAgtIf.x	33152	0	2848	26888	84	128	4676
2019	1935	remCmdAgent.x	33144	0	2844	26888	84	124	4668
2020	1935	bg_threads	40928	0	2532	35004	84	120	4552
2021	1935	logrotate	5688	0	2200	436	84	792	3376

Key Health Indicators using ACLI

```
2504 2021 sleep 3296 0 684 356 84 496 1372
```

```
VSP-9012:1#show khi performance pthread 1
Slot:1
```

```
-----
TID   PID   PName          CPU(%) 5MinAvg CPU(%) 5MinHiWater CPU(%(time stamp))
-----
1     1     init           0.0    0.0
2     2     ksoftirqd/0    0.0    0.0
3     3     events/0       0.0    0.0
4     4     khelper        0.0    0.0
5     5     kthread        0.0    0.0
30    30    kblockd/0     0.0    0.0
55    55    pdflush        0.0    0.0
56    56    pdflush        0.0    0.0
57    57    kswapd0        0.0    0.0
58    58    aio/0          0.0    0.0
624   624   mtddblockd    0.0    0.0
652   652   init           0.0    0.0
653   653   rcS            0.0    0.0
674   674   wdd            0.0    0.0
925   925   ntpd           0.0    0.0
929   929   portmap        0.0    0.0
931   931   inetd          0.0    0.0
933   933   syslogd        0.0    0.0
935   935   klogd          0.0    0.0
1333  1333  khubd          0.0    0.0
1498  1498  nfsd           0.0    0.0
1499  1499  nfsd           0.0    0.0
1500  1500  nfsd           0.0    0.0
1501  1501  lockd          0.0    0.0
1502  1502  rpciod/0       0.0    0.0
1518  1518  nfsd           0.0    0.0
1519  1519  nfsd           0.0    0.0
1520  1520  nfsd           0.0    0.0
1521  1521  nfsd           0.0    0.0
1522  1522  nfsd           0.0    0.0
1526  1526  rpc.mountd     0.0    0.0
1534  1534  sshd           0.0    0.0
1561  1561  rc.appfs       0.0    0.0
1683  1683  ckrm_cpud/0   0.0    0.0
1819  1819  oxide          0.0    0.0
1897  1897  start          0.0    0.0
1935  1935  lifecycle      0.0    0.0
1975  1935  dpmXportRxMonit 0.0    0.0
1976  1935  dpmXportTxMonit 0.0    0.0
1977  1935  ltrBulkTimerThr 0.0    0.0
1978  1935  lc_wd_exception 0.0    0.0
1979  1935  lc_hwwd_feed   0.0    0.0
1980  1935  lc_swwd_feed   0.0    0.0
1981  1935  worker_thread  0.0    0.0
1982  1935  lc_master      0.0    0.0
1983  1983  patchAgent     0.0    0.0
1984  1984  sockserv       0.0    0.0
1985  1985  externalcf     0.0    0.0
1986  1986  oom95          0.0    0.0
1987  1987  oom90          0.0    0.0
1988  1988  imgsync.x     0.0    0.0
1989  1988  dpmXportRxMonit 0.0    0.0
1990  1988  dpmXportTxMonit 0.0    0.0
1991  1988  ltrBulkTimerThr 0.0    0.0
2014  2014  cbbcm-main.x   0.0    0.0
2040  2014  tUsrRoot       0.0    0.0
2043  2014  tExcTask       0.0    0.0
-----
```

```

2044 2014 bcmtty 0.0 0.0
2045 2014 dpmXportRxMonit 0.0 0.0
2046 2014 dpmXportTxMonit 0.0 0.0
2047 2014 ltrBulkTimerThr 0.0 0.0
2048 2014 bcmtMainTask 0.0 0.0
2050 2014 bcmtLcdTask 0.0 0.0
2051 2014 bcmDPC 0.0 0.0
2052 2014 _interrupt_thre 0.0 0.0
2063 2014 bcmCNTR.1 0.0 0.0
2070 2014 bcmLINK.1 0.0 0.0
2076 2014 bcmScoreboard.0 0.0 0.0
2077 2014 bcmCNTR.0 0.0 0.0
2079 2014 bcmLINK.0 0.0 0.0
2098 2014 bcmtSfAgentTime 0.0 0.0
2099 2014 bcmtSfAgentMsgT 0.0 0.0
2015 2015 cbcP-main.x 0.0 0.0
2053 2015 tUsrRoot 0.0 0.0
2054 2015 tExcTask 0.0 0.0
2055 2015 tExcJobTask 0.0 0.0
2056 2015 tNetTask 0.0 0.0
2057 2015 traceOutput 0.0 0.0
2058 2015 profile_cmd 0.0 0.0
2059 2015 tLoggerTask 0.0 0.0
2064 2015 tTelnetd 0.0 0.0
2065 2015 tTelnetV6d 0.0 0.0
2066 2015 tRlogind 0.0 0.0
2067 2015 tRshd 0.0 0.0
2068 2015 tTftpdTask 0.0 0.0
2069 2015 tFtpdTask 0.0 0.0
2071 2015 dpmXportRxMonit 0.0 0.0
2072 2015 dpmXportTxMonit 0.0 0.0
2073 2015 tWdtTask 0.0 0.0
2074 2015 BootpServer 0.0 0.0
2075 2015 tSioMsgRx 0.0 0.0
2078 2015 tUsrRoot 0.0 0.0
2080 2015 ch_heartbeat_cp 0.0 0.0
2081 2015 chEvmTask 0.0 0.0
2082 2015 chFsmTask 0.0 0.0
2083 2015 chServiceTask 0.0 0.0
2085 2015 CpuHATask 0.0 0.0
2086 2015 tHAQTask 0.0 0.0
2087 2015 tSnmpTmr 0.0 0.0
2088 2015 tSnmpd 0.0 0.0
2089 2015 haTick 0.0 0.0
2090 2015 tMainTask 0.4 0.3 0.4(02/08/11 09:48:02)
2091 2015 rtMainTask 0.0 0.0
2092 2015 tCppSend 0.0 0.0
2093 2015 tCppInterruptTa 0.1 0.0 0.1(02/08/11 11:59:41)
2094 2015 tTrapd 0.0 0.0
2095 2015 tOspf6SpfTimer 0.0 0.0
2096 2015 tSpfTimer 0.0 0.0
2097 2015 tBgpTask 0.0 0.0
2100 2015 tTrapd 0.0 0.0

```

--More-- (q = quit)

```

VSP-9012:1#show khi performance slabinfo SF4
Slot:SF4

```

Name	Active Objs	Num Objs	Objsize	Objper slab	Pageper slab	Active Slabs	Num Slabs
TIPC	12	12	320	12	1	1	1
tipc_queue_items	0	0	16	203	1	0	0
rpc_buffers	8	8	2048	2	1	4	4

Key Health Indicators using ACLI

rpc_tasks	20	8	192	20	1	1	1
rpc_inode_cache	18	10	416	9	1	2	2
merc_sock	0	0	352	11	1	0	0
UNIX	11	2	352	11	1	1	1
tcp_bind_bucket	203	6	16	203	1	1	1
inet_peer_cache	59	1	64	59	1	1	1
ip_fib_alias	113	34	32	113	1	1	1
ip_fib_hash	113	29	32	113	1	1	1
ip_dst_cache	0	0	256	15	1	0	0
arp_cache	0	0	128	30	1	0	0
RAW	9	2	448	9	1	1	1
UDP	16	10	480	8	1	2	2
tw_sock_TCP	0	0	96	40	1	0	0
request_sock_TCP	0	0	64	59	1	0	0
TCP	8	6	960	4	1	2	2
cfq_ioc_pool	0	0	48	78	1	0	0
cfq_pool	0	0	96	40	1	0	0
crq_pool	0	0	44	84	1	0	0
deadline_drq	0	0	48	78	1	0	0
as_arq	0	0	60	63	1	0	0
rcfs_inode_cache	72	62	320	12	1	6	6
nfs_write_data	40	36	480	8	1	5	5
nfs_read_data	36	32	448	9	1	4	4
nfs_inode_cache	63	59	560	7	1	9	9
nfs_page	0	0	64	59	1	0	0
ext2_inode_cache	252	247	432	9	1	28	28
ext2_xattr	0	0	44	84	1	0	0
inotify_event_cache	0	0	28	127	1	0	0
inotify_watch_cache	0	0	36	101	1	0	0
kioctx	0	0	160	24	1	0	0
kiocb	0	0	128	30	1	0	0
fasync_cache	0	0	16	203	1	0	0
shmem_inode_cache	660	652	400	10	1	66	66
posix_timers_cache	40	1	96	40	1	1	1
uid_cache	59	1	64	59	1	1	1
relayfs_inode_cache	12	2	312	12	1	1	1
blkdev_ioc	0	0	28	127	1	0	0
blkdev_queue	30	24	380	10	1	3	3
blkdev_requests	0	0	152	26	1	0	0
biovec-(256)	54	54	3072	2	2	27	27
biovec-128	110	109	1536	5	2	22	22
biovec-64	220	218	768	5	1	44	44
biovec-16	220	218	192	20	1	11	11
biovec-4	236	218	64	59	1	4	4
biovec-1	406	218	16	203	1	2	2
bio	295	256	64	59	1	5	5
file_lock_cache	0	0	96	40	1	0	0
sock_inode_cache	44	39	352	11	1	4	4
skbuff_fclone_cache	26	26	288	13	1	2	2
skbuff_head_cache	336	336	160	24	1	14	14
proc_inode_cache	312	311	320	12	1	26	26
sigqueue	26	4	148	26	1	1	1
radix_tree_node	924	923	276	14	1	66	66
bdev_cache	9	2	416	9	1	1	1
sysfs_dir_cache	2024	1985	40	92	1	22	22
mnt_cache	40	22	96	40	1	1	1
inode_cache	910	910	304	13	1	70	70
dentry_cache	2639	2579	136	29	1	91	91
filp	384	384	160	24	1	16	16
names_cache	1	1	4096	1	1	1	1
idr_layer_cache	116	97	136	29	1	4	4
buffer_head	624	568	48	78	1	8	8
mm_struct	28	20	544	7	1	4	4
vm_area_struct	1012	928	88	44	1	23	23
fs_cache	113	19	32	113	1	1	1

files_cache	27	20	448	9	1	3	3
signal_cache	44	36	352	11	1	4	4
sighand_cache	36	35	1312	3	1	12	12
task_struct	77	72	1056	7	2	11	11
anon_vma	339	318	8	339	1	1	1
size-131072(DMA)	0	0	131072	1	32	0	0
size-131072	0	0	131072	1	32	0	0
size-65536(DMA)	0	0	65536	1	16	0	0
size-65536	0	0	65536	1	16	0	0
size-32768(DMA)	0	0	32768	1	8	0	0
size-32768	2	2	32768	1	8	2	2
size-16384(DMA)	0	0	16384	1	4	0	0
size-16384	0	0	16384	1	4	0	0
size-8192(DMA)	0	0	8192	1	2	0	0
size-8192	1	1	8192	1	2	1	1
size-4096(DMA)	0	0	4096	1	1	0	0
size-4096	42	42	4096	1	1	42	42
size-2048(DMA)	0	0	2048	2	1	0	0
size-2048	304	292	2048	2	1	152	152
size-1024(DMA)	0	0	1024	4	1	0	0
size-1024	40	37	1024	4	1	10	10
size-512(DMA)	0	0	512	8	1	0	0
size-512	136	136	512	8	1	17	17
size-256(DMA)	0	0	256	15	1	0	0
size-256	90	90	256	15	1	6	6
size-192(DMA)	0	0	192	20	1	0	0
size-192	40	27	192	20	1	2	2
size-128(DMA)	0	0	128	30	1	0	0
size-128	900	893	128	30	1	30	30
size-96(DMA)	0	0	96	40	1	0	0
size-96	560	537	96	40	1	14	14
size-64(DMA)	0	0	64	59	1	0	0
size-32(DMA)	0	0	32	113	1	0	0
size-64	472	448	64	59	1	8	8
size-32	1582	1582	32	113	1	14	14
kmem_cache	120	120	96	40	1	3	3

Variable definitions

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

Table 3: Variable definitions

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). Valid slots are 1-12, SF1-SF6, or all.

Displaying KHI control processor information

About this task

Use the following commands to display key health information about the packets generated by interface modules, the type of packets and protocols received on a port, and protocol drops.

 **Note:**

You can use KHI commands on all interface slots. If you do not specify a slot, information for all slots is shown.

Procedure

1. Display KHI statistics for packets generated by the interface modules and sent to the control processor:

```
show khi cpp iocop-statistics [<3-12>]
```
2. Display statistics for control packets that go to the control processor:

```
show khi cpp port-statistics [{slot/port[-slot/port]][, ...]}
```
3. Display KHI information about packets dropped due to CP Limit violations:

```
show khi cpp protocol-drops
```

Example

```
VSP-9012:1#show khi cpp iocop-statistics 4
```

```
=====
KHI CPP Details - IO COP Statistics - Slot 4
=====
Slot      IO Generated Packets      Rx Packets
-----
4          MAC_MGMT                   4
```

```
VSP-9012:1#show khi cpp port-statistics 4/1-4/6
```

```
=====
KHI CPP Details - Port Statistics
=====
Ports     Packet Type                Rx Packets  Tx Packets
-----
-
4/1       Ether2_EAP(140)            0           2
4/1       LLC_BPDU(456)              9882        0
4/1       LLC_TDP(464)                0          2312
4/6       Ether2_IPv4_TTL_EXP(50)    13          0
4/6       Ether2_ARP_Other(129)      3           0
4/6       LLC_BPDU(456)              2312        0
4/6       LLC_TDP(464)                0          2314
```

```
VSP-9012:1#show khi cpp protocol-drops
```

```
=====
KHI CPP Details - Protocol Drop Counters
=====
```


Protocol ID	Discard Count
LACP	12914288

Variable definitions

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

Table 4: Variable definitions

Variable	Value
<3-12>	Specifies the slot number.
slot/port[-slot/port][,...]}	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).

Chapter 5: Key Health Indicators using EDM

The Key Health Indicators (KHI) feature of Avaya Virtual Services Platform 9000 provides a subset of health information that allows for quick assessment of the overall operational state of the device.

 **Note:**

The KHI feature is not intended to provide a comprehensive debugging solution. Instead, KHI identifies key information that could lead Avaya support personnel towards discovery of a specific failure. After the technician assesses the KHI information, further debugging is required to determine the specific reason for the fault.

Avaya recommends that you capture KHI information during normal operations to provide a baseline for Avaya support personnel when detecting fault situations.

Clearing KHI statistics

About this task

Clear KHI statistics.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit**
 2. Click **Chassis**.
 3. Click the **CPP Stats Control** tab.
 4. Select the statistics you want to clear.
 5. Click **Apply**.
-

CPP Stats Control field descriptions

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

Name	Description
PortStatsClear	Clears port statistics.
IoCopStatsClear	Clears statistics for the processors on the interface modules.

Name	Description
ProtocolDropsClear	Clears dropped protocol statistics.

Viewing KHI forwarding information

About this task

View KHI forwarding information to see statistics and counters for each lane. Use these statistics to know which IFP rules are hit and to understand why packets are dropped.

Procedure

1. In the Device Physical View, select a module.
 2. In the navigation tree, open the following folders: **Configuration > Edit**.
 3. Click **Card**.
 4. Click the **IFP** tab.
-

IFP field descriptions

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

Name	Description
Index	Shows the index number for the IFP rule.
Name	Shows the name of the IFP rule.
Slice0Ports	Shows the range of ports 1-24 or 1-8 based on the module type.
Slice0Cnt	Shows the counter for the range of ports 1-24 or 1-8 based on the module type..
Slice1Ports	Shows the range of ports 25-48 or 9-16 based on the module type.
Slice1Cnt	Shows the counter for the range of ports 25-48 or 9-16 based on the module type.
Slice2Ports	Shows the range of ports 17-24 based on the module type. This field appears only for 24-port modules.

Name	Description
Slice2Cnt	Shows the counter for ports 17-24 based on the module type.. This field appears only for 24-port modules.

Viewing protocol drop counters

About this task

View protocol drop counters to see the number of packets dropped due to CP Limit violations.

Procedure

1. In the Device Physical View, select the chassis.
 2. In the navigation tree, open the following folders: **Configuration > Graph**.
 3. Click **Chassis**.
 4. Click the **Protocol Drop** tab.
-

Protocol Drop field descriptions

The **Protocol Drop** tab shows the number of packets dropped for the following protocol-violation counters:

- **DataExpCnt**
- **TtlExpCnt**
- **IpmcDataCnt**
- **MacLearningCnt**
- **IsIsCnt**
- **BgpCnt**
- **RipV1Cnt**
- **RipV2Cnt**
- **OspfMcCnt**
- **FtpCnt**
- **TftpCnt**
- **SnmpCnt**

- **TelnetCnt**
- **SshCnt**
- **RshCnt**
- **IstCtlCnt**
- **RadiusCnt**
- **NtpCnt**
- **DhcpCnt**
- **IcmpV4Cnt**
- **IcmpV6Cnt**
- **IgmpCnt**
- **PimMcCnt**
- **VrrpCnt**
- **ArpReqCnt**
- **ArpOtherCnt**
- **RarpReqCnt**
- **RarpOtherCnt**
- **SlppCnt**
- **BpduCnt**
- **TdpCnt**
- **EapCnt**
- **LacpCnt**
- **VlaccpCnt**
- **MldV2Cnt**
- **LldpCnt**
- **HttpCnt**
- **PimUcCnt**
- **OspfUcCnt**
- **DnsCnt**
- **IcmpBcCnt**
- **IpfixCnt**
- **TestPktCnt**

Viewing COP statistics

About this task

View COP statistics for packets generated on interface modules.

Procedure

1. In the Device Physical View, select a module.
 2. In the navigation tree, open the following folders: **Configuration > Graph**.
 3. Click **Card**.
 4. Click the **COP Stats** tab.
 5. To graph the statistics, select the information you want to graph, and then click the type of graph you want to create.
-

COP Stats field descriptions

Use the data in the following table to use the **COP Stats** tab.

Name	Description
MacMgmtRxPackets	Shows the number of received MAC management packets.
IpFixRxPackets	Shows the number of received IPFIX packets.

Displaying KHI port information

About this task

Use the following commands to display key health information about the types of control packets and protocols received on a port and sent to the control processor.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation tree, open the following folders: **Configuration > Graph**.
3. Click **Port**.

4. Click the **CPP Stats** tab.

CPP Stats field descriptions

Use the data in the following table to use the **CPP Stats** tab.

Name	Description
Port	Identifies the slot and port.
Packet	Shows the packet type.
PacketName	Shows the name of the packet.
RxPackets	Indicates the number of received packets on the port for the packet type.
TxPackets	Indicates the number of transmitted packets on the port for the packet type.

Chapter 6: Link state change control using ACLI

Detect and control link flapping to bring more stability to your network.

Controlling link state changes

Before you begin

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

About this task

Configure link flap detection to control state changes on a physical port.

Procedure

1. Configure the interval for link state changes:
`link-flap-detect interval <2-600>`
2. Configure the number of changes allowed during the interval:
`link-flap-detect frequency <1-9999>`
3. Enable automatic port disabling:
`link-flap-detect auto-port-down`
4. Enable sending a trap:
`link-flap-detect send-trap`

Example

1. Enable automatic disabling of the port:
`VSP-9012:1(config)# link-flap-detect auto-port-down`
2. Configure the link-flap-detect interval:
`VSP-9012:1(config)# link-flap-detect interval 20`
3. Enable sending traps:
`VSP-9012:1(config)# link-flap-detect send-trap`

Variable definitions

Use the data in the following table to use the `link-flap-detect` command.

Table 5: Variable definitions

Variable	Value
<auto-port-down>	Automatically disables the port if state changes exceed the link-flap threshold. By default, auto-port-down is disabled. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
frequency <1-9999>	Configures the number of changes that are permitted during the time specified by the interval command. The default is 10. To set this option to the default value, use the default operator with the command.
interval <2-600>	Configures the link-flap-detect interval in seconds. The default value is 60. To set this option to the default value, use the default operator with the command.
send-trap	Activates traps transmission. The default setting is activated. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.

Displaying link state changes

Before you begin

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

About this task

Displays link flap detection state changes on a physical port.

Procedure

Display link state changes:
`show link-flap-detect`

Example

```
VSP-9012:1>enable
VSP-9012:#show link-flap-detect

Auto Port Down : enable
Send Trap      : enable
```

```
Interval      : 60  
Frequency     : 20
```


Chapter 7: Link state change control using EDM

Detect and control link flapping to bring more stability to your network.

Controlling link state changes

About this task

Configure link flap detection to control link state changes on a physical port.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit > Diagnostics**.
 2. Click **General**.
 3. Click the **Link Flap** tab.
 4. Configure the parameters as required.
 5. Click **Apply**.
-

Link Flap field descriptions

Use the data in the following table to use the **Link Flap** tab.

Name	Description
AutoPortDownEnable	Enables or disables Link Flap Detect. If you enable Link Flap Detect, the system monitors the number of times a port goes down during a designated interval. If the number of drops exceeds a specified limit, the system forces the port out-of-service.
SendTrap	Specifies that a trap is sent if the port is forced out-of-service.
Frequency	Specifies the number of times the port can go down. The default is 20.

Link state change control using EDM

Name	Description
Interval	Specifies the interval (in seconds) between port failures. The default is 60.

Chapter 8: RMON configuration using ACLI

This chapter contains procedures to configure remote monitoring (RMON) on Avaya Virtual Services Platform 9000 by using Avaya Command Line Interface (ACLI).

Configuring RMON

Before you begin

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

About this task

Configure RMON functions on Virtual Services Platform 9000 to set alarms and capture events.

Procedure

1. Enable RMON globally:

```
rmon
```

2. Configure an RMON alarm:

```
rmon alarm <1-65535> WORD <1-1536> <1-3600> {absolute|delta}
[falling-threshold <-2147483647-2147483647> event <1-65535>]
[owner WORD<1-127>] [rising-threshold <-
2147483647-2147483647> event <1-65535>]
```

3. Configure an RMON event:

```
rmon event <1-65535> [community WORD<1-127>] [description
WORD<1-127>] [log] [owner WORD<1-127>] [trap] [trap_dest
[{A.B.C.D}]] [trap_src [{A.B.C.D}]]
```

Example

```
VSP-9012:1(config)#rmon
```

```
VSP-9012:1(config)#rmon alarm 4 rcCliNumAccessViolations.0 10
absolute rising-threshold 2 event 60000
```

```
VSP-9012:1(config)#rmon event 60534 community public description
"Rising Event" log trap
```

Variable definitions

Use the data in this table to use the `rmon` command.

Table 6: Variable definitions

Variable	Value
<pre>alarm <1-65535> WORD <1-1536> <1-3600> {absolute delta} [falling-threshold <-2147483647-2147483647> event <1-65535>] [owner WORD<1-127>] [rising-threshold <-2147483647-2147483647> event <1-65535>]</pre>	<p>Create an alarm interface.</p> <ul style="list-style-type: none"> • <code><1-65535></code> is the interface index number from 1–65535. • <code>WORD <1-1536></code> is the variable name or OID, case sensitive (string length 1–1536). • <code>{absolute delta}</code> is the sample type. • <code>rising-threshold <-2147483648-2147483647> [<code><event:1-65535></code>]</code> is the rising threshold (–2147483648–2147483647) and the rising event number (1–65535). • <code>falling-threshold <-2147483648-2147483647> [<code><event:1-65535></code>]</code> is the falling threshold (–2147483648–2147483647) and the falling event number (1–65535). • <code>owner WORD<1-127></code> is the name of the owner (string length 1–127). <p>Use the default operator to reset the RMON alarms to their default configuration:<code>default rmon alarm <65535></code></p> <p>Use the no operator to disable RMON alarms: <code>no rmon alarm [<1-65535>]</code></p>
<pre>event <1-65535> [community WORD<1-127>] [description WORD<1-127>] [log] [owner WORD<1-127>] [trap] [trap_dest {{A.B.C.D}}] [trap_src {{A.B.C.D}}]</pre>	<p>Create an event.</p> <ul style="list-style-type: none"> • <code><1-65535></code> is the event index number. • <code>[log]</code> display information about configured traps. • <code>[trap]</code> specify trap source and destination IP addresses. • <code>description WORD<1-127></code> is the event description (string length 0–127). • <code>owner WORD<1-127></code> is the name of the owner (string length 1–127). • <code>trap_src {A.B.C.D}</code> is the trap source ip address.

Variable	Value
	<ul style="list-style-type: none"> • trap_dest {A.B.C.D} is the trap destination ip address. • community WORD<1-127> is the event community (string length 1–127). <p>Use the no operator to delete a RMON event: no rmon event [<1-65535>] [log]</p>

Viewing RMON settings

About this task

View RMON settings to see information about alarms, statistics, events, or the status of RMON on Virtual Services Platform 9000.

Procedure

View RMON settings:

```
show rmon {alarm|event|history|log|stats}
```

Example

```
CB-SWB:1(config)#show rmon event
```

```
=====
                        Rmon Event
=====
INDEX DESCRIPTION          TYPE          COMMUNITY OWNER          LAST_TIME_SENT
-----
60534 Rising Event        log-and-trap public         47.17.142.155 none
60535 Falling Event      log-and-trap public         47.17.142.155 8 day(s), 19:14:32
```

```
CB-SWB:1(config)#show rmon log
```

```
=====
                        Rmon Log
=====
INDEX    TIME                DESCRIPTION
-----
60535. 1 8 day(s), 19:14:45  1.3.6.1.4.1.2272.1.19.14.0 (absValue = 0, Falling
                        Threshold = 2, interval = 10)[alarmIndex.1][trap]
                        "Falling Event"
60535. 2 8 day(s), 19:14:45  1.3.6.1.4.1.2272.1.19.14.0 (absValue = 0, Falling
                        Threshold = 1, interval = 10)[alarmIndex.2][trap]
                        "Falling Event"
```

```
VSP-9012:1(config)#show rmon stats
```

```
=====
                        Rmon Ether Stats
=====
```

```
=====
INDEX  PORT   OWNER
-----
1      cpp    monitor
```

Variable definitions

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

Table 7: Variable definitions

Variable	Value
alarm	Display the RMON Alarm table.
event	Display the RMON event table.
history	Display the RMON history table.
log	Display the RMON log table.
stats	Display the RMON statistics table.

Chapter 9: RMON configuration using EDM

Remote monitoring (RMON) is a management information base (MIB) or a group of management objects that you use to obtain or configure values using the Simple Network Management Protocol (SNMP).

Enabling RMON globally

About this task

You must globally enable RMON before you can use an RMON function. If you attempt to enable an RMON function before the global flag is disabled, EDM informs you that the flag is disabled and prompts you to enable the flag.

If you want to use nondefault RMON parameter values, you can configure them before you enable RMON, or as you configure the RMON functions.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Options**.
 3. Click the **Options** tab.
 4. Select the **Enable** check box.
 5. In the **UtilizationMethod** option, select a utilization method.
 6. In the **TrapOption** option, select a trap option.
 7. In the **MemSize** box, type a memory size.
 8. Click **Apply**.
-

Options field descriptions

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

Name	Description
Enable	Enables RMON. If you select the Enable check box, the RMON agent starts immediately if the amount of memory

Name	Description
	specified by MemSize is currently available in the device. To disable RMON, clear the Enable check box and click Apply to save the new setting to NVRAM, and then restart the device. The default is disabled.
UtilizationMethod	Controls whether RMON uses a half-duplex or full-duplex formula to calculate port usage. After you select halfDuplex, RMON uses InOctets and the speed of the port to calculate port usage (this is the standard RMON RFC1271 convention). After you select fullDuplex, RMON uses InOctets and OutOctets and 2X the speed of the port to calculate port usage. If you select fullDuplex, but the port operates in half-duplex mode, the calculation defaults to the RFC1271 convention. The default is halfDuplex.
TrapOption	Indicates whether the system sends RMON traps to the owner of the RMON alarm (the manager that created the alarm entry) or to all trap recipients in the system trap receiver table. The default value is toOwner.
MemSize	Specifies the RAM size, in bytes, available for RMON to use. The default value is 250 Kilobytes.

Enabling RMON history

About this task

Use RMON to establish a history for a port and configure the bucket interval. For example, to gather RMON statistics over the weekend, you must have enough buckets to cover two days. Configure the history to gather one bucket every hour, and cover a 48 hour period. After you configure history characteristics, you cannot modify them; you must delete the history and create another one.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
2. Click **Control**.
3. In the **History** tab, click **Insert**.
4. In the **Port** box, click the ellipsis (...) button.
5. Select a port.
6. Click **OK**.
7. In the **Buckets Requested** box, type the number of discrete time intervals to save data.

8. In the **Interval** box, type the interval in seconds.
9. In the **Owner** box, type the owner information.
10. Click **Insert**.

History field descriptions

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

Name	Description
Index	Specifies an index that uniquely identifies an entry in the historyControl table. Each entry defines a set of samples at a particular interval for an interface on the device. Index value ranges from 1–65535. The default value is 1.
Port	Identifies the source for which historical data is collected and placed in a media-specific table on behalf of this historyControlEntry. The source is an interface on this device. To identify a particular interface, the object identifies the instance of the ifIndex object, defined in (4,6), for the desired interface. For example, if an entry receives data from interface 1, the object is ifIndex 1. The statistics in this group reflect all packets on the local network segment attached to the identified interface. You cannot modify this object if the associated historyControlStatus object is equal to valid(1).
BucketsRequested	Specifies the requested number of discrete time intervals over which data is saved in the part of the media-specific table associated with this historyControlEntry. After this object is created or modified, the probe configures historyControlBucketsGranted as closely to this object as possible for the particular probe implementation and available resources. Values range from 1–65535. The default value is 50.
BucketsGranted	Specifies the number of discrete sampling intervals over which data is saved in the part of the media-specific table associated with this historyControlEntry. After the associated BucketsRequested object is created or modified, the probe sets this object as closely to the requested value as possible for the particular probe implementation and available resources. The probe must not lower this value except as a result of a modification to the associated BucketsRequested object. Occasionally, the actual number of buckets associated with this entry is less than the value of this object. In this case, at the end of each sampling interval, a new bucket is added to the media-specific table. After the number of buckets reaches the value of this object and a new bucket

Name	Description
	<p>is to be added to the media-specific table, the oldest bucket associated with this entry is deleted by the agent so that the new bucket can be added. After the value of this object changes to a value less than the current value, entries are deleted from the media-specific table associated with this entry. The agent deletes the oldest of these entries so that their number remains less than or equal to the new value of this object. After the value of this object changes to a value greater than the current value, the number of associated media-specific entries is allowed to grow.</p>
Interval	<p>Specifies the interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this historyControlEntry. You can set this interval between 1–3600 seconds (1 hour). Because the counters in a bucket can overflow at their maximum value with no indication, you must take into account the possibility of overflow in all of the associated counters. Consider the minimum time in which a counter can overflow on a particular media type, and then set the historyControlInterval object to a value less than this interval, which is typically most important for the octets counter in a media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter can overflow in approximately 1 hour at the maximum utilization. You cannot modify this object if the associated historyControlStatus object is equal to valid. The default value is 1800.</p>
Owner	<p>Specifies the entity that configured this entry and is using the assigned resources.</p>

Disabling RMON history

About this task

Disable RMON history on a port if you do not want to record a statistical sample from that port.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
2. Click **Control**.
3. In the **History** tab, select the row that contains the port ID to delete.

4. Click **Delete**.
-

Creating an alarm

Before you begin

- You must globally enable RMON.

About this task

After you enable RMON globally, you also create a default rising and falling event. The default for the events is log-and-trap, which means that you receive notification through a trap as well as through a log file.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Alarms**.
 3. Click the **Alarms** tab.
 4. Click **Insert**.
 5. In the **Variable** option, select a variable for the alarm.
If you select some variables, the system will prompt you for a port (or other object) on which you want to set an alarm.
 6. In the **SampleType** option, select a sample type.
 7. In the **Interval** box, type a sample interval in seconds.
 8. In the **Index** box, type an index number.
 9. In the **RisingThreshold** box, type a rising threshold value.
 10. In the **RisingEventIndex** box, type a rising threshold event index.
 11. In the **FallingThreshold** box, type a falling threshold value.
 12. In the **FallingEventIndex** box, type a falling threshold event index.
 13. In the **Owner** box, type the owner of the alarm.
 14. Click **Insert**.
-

Alarms field descriptions

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

Name	Description
Index	Uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The default is 1.
Interval	Specifies the interval, in seconds, over which the data is sampled and compared with the rising and falling thresholds. deltaValue sampling—configure the interval short enough that the sampled variable is unlikely to increase or decrease by more than $2^{31}-1$ during a single sampling interval. The default is 10.
Variable	<p>Specifies the object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) can be sampled. Alarm variables exist in three formats, depending on the type:</p> <ul style="list-style-type: none"> • A chassis, power supply, or fan-related alarm ends in x where the x index is hard-coded. No further information is required. • A card, spanning tree group (STG), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or EtherStat alarm ends with a dot (.). You must enter a card number, STG ID, IP address, or EtherStat information. • A port alarm ends with no dot or index and requires that you use the port shortcut menu. An example of a port alarm is ifInOctets (interface incoming octet count). <p>Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists to restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is no acceptable means of restricting the read access that is obtained through the alarm mechanism exists, the probe must grant only write access to this object in those views that have read access to all objects on the probe.</p> <p>After you configure a variable, if the supplied variable name is not available in the selected MIB view, a badValue error will be returned. After the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe will change the status of this alarmEntry to invalid.</p> <p>You cannot modify this object if the associated alarmStatus object is equal to valid.</p>
SampleType	Specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue, the value of the selected

Name	Description
	variable is compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. You cannot modify this object if the associated alarmStatus object is equal to valid. The default is deltaValue.
Value	Specifies the value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value is the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value is the sampled value at the end of the period. This value is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and remains available until the next period is complete.
StartUpAlarm	Specifies the alarm that is sent after this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to the risingAlarm or the risingOrFallingAlarm, then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to the fallingAlarm or the risingOrFallingAlarm, then a single falling alarm is generated. You cannot modify this object if the associated alarmStatus object is equal to valid.
Rising Threshold	Specifies a threshold for the sampled statistic. After the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm or risingOrFallingAlarm. After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold. You cannot modify this object if the associated alarmStatus object is equal to valid.
RisingEventIndex	Specifies the index of the eventEntry that is used after a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, no association exists. In particular, if this value is zero, no associated event is generated, as zero is not a valid event index. You cannot modify this object if the associated alarmStatus object is equal to valid. The default is 60534.
FallingThreshold	Specifies a threshold for the sampled statistic. If the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single event is also generated if the first sample after

Name	Description
	this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm or risingOrFallingAlarm. After a falling event is generated, another such event is not generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold. You cannot modify this object if the associated alarmStatus object is equal to valid.
FallingEventIndex	Specifies the index of the eventEntry that is used after a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, no association exists. In particular, if this value is zero, no associated event is generated, as zero is not a valid event index. You cannot modify this object if the associated alarmStatus object is equal to valid. The default is 60535.
Owner	Specifies the entity that configured this entry and is therefore using the resources assigned to it.
Status	Specifies the status of this alarm entry.

Viewing RMON alarms

About this task

View the RMON alarm information to see alarm activity.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Alarms**.
-

Viewing RMON events

About this task

View RMON events to see how many events occurred.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Alarms**.
 3. Click the **Events** tab.
-

Events field descriptions

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

Name	Description
Index	Uniquely identifies an entry in the event table. Each such entry defines one event that is generated after the appropriate conditions occur.
Description	Specifies a comment describing this event entry.
Type	Specifies the type of notification that the probe makes about this event. In the case of a log, an entry is made in the log table for each event. In the case of SNMP traps, an SNMP trap is sent to one or more management stations.
Community	Specifies the SNMP community to where you can send SNMP traps.
LastTimeSent	Specifies the value of sysUpTime at the time this event entry last generated an event. If this entry has not generated events, this value is zero.
Owner	Specifies the entity that configured this entry and is therefore using the assigned resources. If this object contains a string starting with monitor and has associated entries in the log table, all connected management stations retrieve those log entries, as they have significance to all management stations connected to this device.

Viewing the RMON log

About this task

View the trap log to see which activity occurred.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Alarms**.
 3. Click the **Log** tab.
-

Log field descriptions

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

Name	Description
Time	Specifies the creation time for this log entry.
Description	Specifies an implementation dependent description of the event that activated this log entry.

Deleting an alarm

About this task

Delete an alarm if you no longer want it to appear in the log.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Alarms**.
 3. Select the alarm you must delete.
 4. Click **Delete**.
-

Creating a default RMON event

About this task

Create a default rising and falling event to specify if alarm information is sent to a trap, a log, or both.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Alarms**.
 3. Click the **Events** tab.
 4. Click **Insert**.
 5. In the **Description** box, type a description for the event.
 6. In the **Owner** box, type the owner of the event.
 7. In the **Insert Events** dialog box, click **Insert**.
If Rmon is not globally enabled, the following message appears:
RMON is currently disabled. Do you want to enable it now?
 8. Click **Yes**.
-

Events field descriptions

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

Name	Description
Index	Uniquely identifies an entry in the event table. Each such entry defines one event that is generated after the appropriate conditions occur.
Description	Specifies a comment describing this event entry.
Type	Specifies the type of notification that the probe makes about this event. In the case of a log, an entry is made in the log table for each event. In the case of SNMP traps, an SNMP trap is sent to one or more management stations.
Community	Specifies the SNMP community to where you can send SNMP traps.

Name	Description
LastTimeSent	Specifies the value of sysUpTime at the time this event entry last generated an event. If this entry has not generated events, this value is zero.
Owner	Specifies the entity that configured this entry and is therefore using the assigned resources. If this object contains a string starting with monitor and has associated entries in the log table, all connected management stations retrieve those log entries, as they have significance to all management stations connected to this device.

Creating a nondefault RMON event

About this task

Create a custom rising and falling event to specify if alarm information is sent to a trap, a log, or both.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
2. Click **Alarms**.
3. Click the **Events** tab.
4. Click **Insert**.
5. In the **Description** box, type an event name.
6. In the **Type** option, select an event type.
 The default configuration is log-and-trap. To save memory, configure the event type to log. To reduce traffic from the system, configure the event type to snmp-log.
 If you select snmp-trap or log, you must configure trap receivers.
7. In the **Community** box, type an SNMP community.
8. In the **Owner** box, type the owner of this event.
9. Click **Insert**.

Events field descriptions

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

Name	Description
Index	Uniquely identifies an entry in the event table. Each such entry defines one event that is generated after the appropriate conditions occur.
Description	Specifies a comment describing this event entry.
Type	Specifies the type of notification that the probe makes about this event. In the case of a log, an entry is made in the log table for each event. In the case of SNMP traps, an SNMP trap is sent to one or more management stations.
Community	Specifies the SNMP community to where you can send SNMP traps.
LastTimeSent	Specifies the value of sysUpTime at the time this event entry last generated an event. If this entry has not generated events, this value is zero.
Owner	Specifies the entity that configured this entry and is therefore using the assigned resources. If this object contains a string starting with monitor and has associated entries in the log table, all connected management stations retrieve those log entries, as they have significance to all management stations connected to this device.

Deleting an event

About this task

Delete an event after you no longer require the alarm information.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Alarms**.
 3. Click the **Events** tab.
 4. Select the event you must delete.
 5. Click **Delete**.
-

Chapter 10: Viewing statistics using ACLI

Use remote monitoring (RMON) statistics on Ethernet ports to remotely monitor network performance.

Viewing RMON statistics

About this task

View RMON statistics to manage network performance.

Procedure

View RMON statistics:

```
show rmon stats
```

Example

```
VSP-9012:1(config)#show rmon stats
```

```
=====
                        Rmon Ether Stats
=====
INDEX  PORT    OWNER
-----
1      cpp     monitor
```

Job aid

Use the data in the following table to use the `show rmon stats` command output.

Table 8: show rmon stats command output

Parameter	Description
Index	Uniquely identifies an entry in the Ethernet Statistics table.
Port	Identifies the source of the data that this etherStats entry analyzes.
Owner	Specifies the entity that configured this entry and is therefore using the assign resources.

Chapter 11: Viewing statistics using EDM

Use remote monitoring (RMON) statistics on Ethernet ports to remotely monitor network performance.

Enabling RMON statistics

About this task

Enable Ethernet statistics collection for RMON.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Control**.
 3. Click the **Ethernet Statistics** tab.
 4. Click **Insert**.
 5. Next to the **Port** box, click the ellipsis (...) button.
 6. Select a port.
 7. Click **OK**.
 8. In the **Owner** box, type the name of the owner entity.
 9. Click **OK**.
 10. Click **Insert**.
-

Ethernet Statistics field descriptions

Use the data in the following table to use the **Ethernet Statistics** tab.

Name	Description
Index	Uniquely identifies an entry in the Ethernet Statistics table. The default is 1.
Port	Identifies the source of the data that this etherStats entry is configured to analyze.

Name	Description
Owner	Specifies the entity that configured this entry and therefore uses the assigned resources.

Disabling RMON statistics

About this task

Disable RMON statistics on a port after you do not need to gather statistics on that port.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Serviceability > RMON**.
 2. Click **Control**.
 3. Click the **Ethernet Statistics** tab.
 4. Select the row that contains the port ID for which you must disable statistics.
 5. Click **Delete**.
-

Chapter 12: 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 9000 System Messaging Platform.

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 used by SNMP agents and managers 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:**

Virtual Services Platform 9000 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

This message is sent by an SNMP agent in response to a get request, get next request, or set request message.

- trap

An SNMP trap is a notification triggered by events at the agent.

Overview of traps and logs

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 Virtual Services Platform 9000 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 *Avaya Virtual Services Platform 9000 Security*, NN46250–601.

System log messaging

On a UNIX-based management platform, you can use system log (syslog) messaging to manage event messages. The Virtual Services Platform 9000 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 Virtual Services Platform 9000 that run in a network accessible to the workstation.

The remote UNIX management workstation performs the following actions:

- receives system log messages from Virtual Services Platform 9000
- 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:

- Simple Network Management Protocol (SNMP)
- Extensible Authentication Protocol (EAP)
- Remote Authentication Dial-in User Service (RADIUS)
- Remote Monitoring (RMON)
- Web
- Internet Group Management Protocol (IGMP)
- 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)
- Internet Protocol Multicast (IPMC)
- Internet Protocol-Routing Information Protocol (IP-RIP)
- Open Shortest Path First (OSPF)
- policy
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP) log

Avaya Virtual Services Platform 9000 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, under the System Log Table tab, you must select either IPv4 or IPv6.

Log message format

The log messages for Virtual Services Platform 9000 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
- module—identifies the software module or hardware from which the log is generated
- 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
- event instance or alarm ID—identified the instance of the event or alarm ID for alarm messages
- 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
- severity level—identifies the severity of the message
- terse message—represents the event and provides additional information
- probable cause—describes the possible conditions that trigger the event

The following messages are examples of an informational message, warning message, and alarm messages:

```
I05 [08/17/11 11:38:04.875] 0x0009059e 00000000 GlobalRouter QOS INFO QOS profile
set to 0
SF4 [08/17/11 11:38:04.875] 0x0009059e 00000000 GlobalRouter QOS INFO QOS profile
set to 0
CP1 [08/16/11 11:38:04.875] 0x00043fff 00000000 GlobalRouter WEB INFO HTTPS: Server
Cert/Key Generated Successfully
```

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 9: Severity levels

Severity level	Definition
INFO	Information only. No action is required.

Severity level	Definition
ERROR	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.
WARNING	A nonfatal condition occurred. No immediate action is needed.
FATAL	A fatal condition occurred. The system cannot recover without restarting. For example, a fatal message is generated after the configuration database is corrupted.

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, under the System Log Table tab, you must select either IPv4 or IPv6.

Internally, Virtual Services Platform 9000 has four severity levels for log messages: Info, Warning, Error, Fatal. The system log supports eight different severity levels:

- Debug
- Info
- Notice
- Warning
- Critical
- Error
- Alert
- Emergency

The following table shows the default mapping of internal severity levels to syslog severity levels.

Table 10: Default and system log severity level mapping

UNIX system error codes	System log severity level	Internal VSP 9000 severity level
0	Emergency	Fatal

UNIX system error codes	System log severity level	Internal VSP 9000 severity level
1	Alert	—
2	Critical	—
3	Error	Error
4	Warning	Warning
5	Notice	—
6	Info	Info
7	Debug	—

Log files

The log file captures hardware and software log messages, and alarm messages. Virtual Services Platform 9000 can log to external flash. Avaya strongly recommends that you configure logging to an external flash and keep an external card in each CP module at all times. The system supports 2 GB Compact Flash cards. By default, the system logs to external flash. If the external flash does not exist or the system configuration does not log to external flash, the system logs to internal flash instead.

To log to a file on external or internal flash, the used disk space on the flash must be below 75%. If the used disk space of the flash is more than 75%, the system stops logging to a file on the flash and raises an alarm even though the system always saves logs in internal memory. 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.xxxxxxx.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 specify the slot number of the CP module that generated the logs. 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 both external flash and 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 for logging. If the newest

log file exists on the flash that is not used for logging, the system creates a new log file with incremented sequence number on the flash that is used for logging.

Log file transfer

The system logs contain important information for debugging and maintaining Virtual Services Platform 9000. After the current log file reaches the configured maximum size, a new log file is created 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 external flash or 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.

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 .xxxxxxx.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 specify the slot number of the CP module that generated the logs. 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 on flash 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. Virtual Services Platform 9000 does not support the minimum size and percentage of free disk space parameters. The flash must be less than 75% full for the system to log a file. If the flash is more than 75% full, logging to a file stops to prevent exhausting disk space.

Chapter 13: 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|management-virtual-ip>`
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

```
VSP-9012:1(config)#syslog enable
```

```
VSP-9012:1(config)#syslog host 1 address 47.17.143.52
```

```
VSP-9012:1(config)#syslog host 1 enable
```

```
VSP-9012:1(config)#show syslog host 1
```

```
      Id : 1
      IpAddr : 47.17.143.52
      UdpPort : 515
      Facility : local7
      Severity : info|warning|error|fatal
      MapInfoSeverity : info
      MapWarningSeverity : warning
      MapErrorSeverity : error
      MapMfgSeverity : notice
      MapFatalSeverity : emergency
      Enable : true
```

```
VSP-9012:1(config)#show syslog
```

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

```
VSP-9012:(config)# syslog host 2 address fe80:0:0:0:22b:4eee:fe5e:73fd udp-port 515
```

```
VSP-9012:(config)# syslog host 2 udp-port 515
```

```
VSP-9012:(config)# syslog host 2 enable
```

```
VSP-9012:(config)#
```

```
VSP-9012:1(config)#show syslog host 2
```

```
      Id : 2
      IpAddr : fe80:0:0:0:22b:4eee:fe5e:73fd
      UdpPort : 515
      Facility : local7
      Severity : info|warning|error|fatal
      MapInfoSeverity : info
      MapWarningSeverity : warning
      MapErrorSeverity : error
      MapMfgSeverity : notice
      MapFatalSeverity : emergency
      Enable : true
```

Variable definitions

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

Table 11: Variable definitions

Variable	Value
enable	Enables the sending of syslog messages on the device. The default is disabled. Use the <code>no</code> operator before this parameter, <code>no syslog enable</code> to disable the sending of syslog messages on the device. The default is enabled.
ip-header-type <circuitless-ip default management-virtual-ip>	<p>Specifies the IP header in syslog packets to circuitless-ip, default, or management-virtual-ip.</p> <ul style="list-style-type: none"> • 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. For syslog packets that are transmitted out-of-band through the management port, the physical IP address of the master CPU is used in the IP header. • If the value is management-virtual-ip, the virtual management IP address of the device is used in the IP header for syslog packets that are transmitted out-of-band only through the management port. • 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 12: Variable definitions

Variable	Value
1–10	Creates and configures a host instance. Use the <code>no</code> operator before this parameter, <code>no syslog host</code> to delete a host instance.
address WORD <0–46>	Configures a host location for the syslog host. WORD <0–46> is the IPv4 or IPv6 address of the UNIX system syslog host in the format A.B.C.D or

Variable	Value
	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.
enable	Enables the syslog host. Use the no operator before this parameter, no syslog host enable to disable syslog host. The default is disabled.
facility {local0 local1 local2 local3 local4 local5 local6 local7}	Specifies the UNIX facility in messages to the syslog host. {local0 local1 local2 local3 local4 local5 local6 local7} is the UNIX system syslog host facility. The default is local7.
maperror {emergency alert critical error warning notice info debug}	Specifies the syslog severity to use for error messages. The default is error.
mapfatal {emergency alert critical error warning notice info debug}	Specifies the syslog severity to use for fatal messages. The default is emergency.
mapinfo {emergency alert critical error warning notice info debug}	Specifies the syslog severity level to use for information messages. The default is info.
mapwarning {emergency alert critical error warning notice info debug}	Specifies the syslog severity to use for warning messages. The default is warning.
severity <info warning error fatal> [<info warning error fatal>] [<info warning error fatal>]	Specifies the severity levels for which to send syslog messages for the specified modules. The default is info.
udp-port <514-530>	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.

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-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#logging level 0
VSP-9012:1(config)#logging write log2
VSP-9012:1(config)#logging screen
```

Variable definitions

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

Table 13: Variable definitions

Variable	Value
level <0-4>	Shows and configures the logging level. The level is one of the following values: <ul style="list-style-type: none"> • 0: Information; all messages are recorded • 1: Warning; only warning and more serious messages are recorded • 2: Error; only error and more serious messages are recorded • 3: Manufacturing; this parameter is not available for customer use • 4: Fatal; only fatal messages are recorded
logToExtFlash	Starts logging system messages to the external flash. The default logging location is the external flash device. Avaya recommends that you use logging to the

Variable	Value
	external flash. Use the no form of the command to stop logging to external flash and log to internal flash instead: <code>no logging logToExtFlash</code>
screen	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>
transferFile <1-10> address {A.B.C.D} filename-prefix WORD<0-200	Transfers the syslog file to a remote FTP/TFTP server. <1-10> specifies the file ID. The address {A.B.C.D} option specifies the IP address. The filename-prefix WORD<0-200> option sets the filename prefix for the log file at the remote host.
write WORD<1-1536>	Writes the log file with the designated string. WORD<1-1536> 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 (").

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-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

```
VSP-9012:1(config)#logging transferFile 1 address 172.16.120.10
```

Variable definitions

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

Table 14: Variable definitions

Variable	Value
1–10	Specifies the file ID to transfer.
address {A.B.C.D}	Specifies the IP address of the host to which to transfer the log file. The remote host must be reachable or the configuration fails.
filename WORD<0-255>	Specifies the name of the file on the remote host. If you do not configure a name, the current log file name is the default.

Configuring system logging to external storage

Before you begin

- You must install a CF card in the CP module before you can log to external storage.
- You must log on to the Global Configuration mode in ACLI.

Caution:

Risk of data loss

Before you remove the CF card from the master CP module, you must stop the logging of system messages. Failure to do so can corrupt the file system on the CF card and cause the log file to be permanently lost.

About this task

System logs are a valuable diagnostic tool. You can send log messages to external flash for later retrieval.

Define the maximum log file sizes to bound the file storage size on the Compact Flash (CF) card. The system transfers the current log file to a remote host after the log file size reaches the maximum size.

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

Avaya recommends that you configure logging to an external flash and keep an external flash in each CP module at all times. If external flash does not exist, the system raises an alarm, and then logs to internal flash instead.

Procedure

1. Enable system logging to a CF card:

```
boot config flags logging
```
2. Configure the logfile parameters:

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

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#boot config logfile 64 600 10
```

Variable definitions

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

Table 15: Variable definitions

Variable	Value
flags logging	Enables or disables logging to a file on external flash. The log file is named using the format log.xxxxxxx.sss. 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 of the CP module that generated 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 you replace or reinsert the CP module, or if the maximum log file size is reached.
logfile <64-500> <500-16384> <10-90>	Configures the logfile parameters <ul style="list-style-type: none"> • <64-500> specifies the minimum free memory space on the external storage device from 64–500 KB. Virtual Services Platform 9000 does not support this parameter. • <500-16384> specifies the maximum size of the log file from 500–16384 KB. • <10-90> specifies the maximum percentage, from 10–90%, of space on the external storage device the logfile can use. Virtual Services Platform 9000 does not support this parameter.

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`

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#sys msg-control action suppress-msg
VSP-9012:1(config)#sys msg-control max-msg-num 10
VSP-9012:1(config)#sys msg-control control-interval 15
VSP-9012:1(config)#sys msg-control
```

Variable definitions

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

Table 16: Variable definitions

Variable	Value
action <both send-trap suppress-msg>	Configures the message control action. You can either suppress the message or send a trap notification, or both. The default is suppress.
control-interval <1-30>	Configures the message control interval in minutes. The valid options are 1–30. The default is 5.
max-msg-num <2-500>	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.

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-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

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

```
VSP-9012:1(config)# sys force-msg ****
```

Variable definitions

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

Table 17: Variable definitions

Variable	Value
<i>WORD<4-4></i>	Adds a forced message control pattern, where <i>WORD<4-4></i> 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.

Viewing logs

About this task

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

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

Procedure

Show log information:

```
show logging file [alarm][CPU WORD<0-25>] [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

```
VSP-9012:1>show logging file module cliilog
CP1 [08/21/11 14:29:57.231] 0x002c0600 00000000 GlobalRouter CLILOG INFO 1
CONSOLE rwa en
CP1 [08/21/11 14:29:58.771] 0x002c0600 00000000 GlobalRouter CLILOG INFO 2
CONSOLE rwa config t
CP1 [08/21/11 14:30:06.743] 0x002c0600 00000000 GlobalRouter CLILOG INFO 3
CONSOLE rwa source basic.cfg
CP1 [08/21/11 14:30:07.018] 0x002c0600 00000000 GlobalRouter CLILOG INFO 4
CONSOLE rwa config terminal
CP1 [08/21/11 14:30:07.026] 0x002c0600 00000000 GlobalRouter CLILOG INFO 5
```

Log configuration using ACLI

```
CONSOLE rwa boot config flags fabric-profile 1
CP1 [08/21/11 14:30:07.027] 0x002c0600 00000000 GlobalRouter CLILOG INFO 6
CONSOLE rwa boot config flags ftpd
CP1 [08/21/11 14:30:07.028] 0x002c0600 00000000 GlobalRouter CLILOG INFO 7
CONSOLE rwa boot config flags rlogind
CP1 [08/21/11 14:30:07.029] 0x002c0600 00000000 GlobalRouter CLILOG INFO 8
CONSOLE rwa boot config flags sshd
CP1 [08/21/11 14:30:07.030] 0x002c0600 00000000 GlobalRouter CLILOG INFO 9
CONSOLE rwa boot config flags telnetd
CP1 [08/21/11 14:30:07.031] 0x002c0600 00000000 GlobalRouter CLILOG INFO 10
CONSOLE rwa cli timeout 65535
CP1 [08/21/11 14:30:07.032] 0x002c0600 00000000 GlobalRouter CLILOG INFO 11
CONSOLE rwa password password-history 3
CP1 [08/21/11 14:30:07.033] 0x002c0600 00000000 GlobalRouter CLILOG INFO 12
CONSOLE rwa cli log enable
CP1 [08/21/11 14:30:07.034] 0x002c0600 00000000 GlobalRouter CLILOG INFO 13
CONSOLE rwa snmplog enable
CP1 [08/21/11 14:30:07.036] 0x002c0600 00000000 GlobalRouter CLILOG INFO 14
CONSOLE rwa no sys ecn-compatibility
CP1 [08/21/11 14:30:07.046] 0x002c0600 00000000 GlobalRouter CLILOG INFO 15
CONSOLE rwa interface mgmtEthernet 1/1
CP1 [08/21/11 14:30:07.047] 0x002c0600 00000000 GlobalRouter CLILOG INFO 16
CONSOLE rwa ip address 47.17.159.49 255.255.255.0
CP1 [08/21/11 14:30:07.049] 0x002c0600 00000000 GlobalRouter CLILOG INFO 17
CONSOLE rwa exit
CP1 [08/21/11 14:30:07.050] 0x002c0600 00000000 GlobalRouter CLILOG INFO 18
CONSOLE rwa interface GigabitEthernet 10/11
CP1 [08/21/11 14:30:07.051] 0x002c0600 00000000 GlobalRouter CLILOG INFO 19
CONSOLE rwa no shutdown
CP1 [08/21/11 14:30:07.053] 0x002c0600 00000000 GlobalRouter CLILOG INFO 20
CONSOLE rwa exit
CP1 [08/21/11 14:30:07.054] 0x002c0600 00000000 GlobalRouter CLILOG INFO 21
CONSOLE rwa interface gigabitethernet 10/11
CP1 [08/21/11 14:30:07.056] 0x002c0600 00000000 GlobalRouter CLILOG INFO 22
CONSOLE rwa ipv6 interface vlan 3
CP1 [08/21/11 14:30:07.079] 0x002c0600 00000000 GlobalRouter CLILOG INFO 23
CONSOLE rwa ipv6 interface enable
```

Variable definitions

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

Table 18: Variable definitions

Variable	Value
alarm	Displays alarm log entries.
CPU <i>WORD</i> <0-25>	Filters and lists the logs according to the CP module that generated the message. Specify a string length of 0–25 characters. To specify multiple filters, separate each CP module by the vertical bar (), for example, <code>show logging file CPU CP1 CP2 IO1</code> . Following are some of the available CPU qualifiers: <ul style="list-style-type: none">• CP1• CP2

Variable	Value
	<ul style="list-style-type: none"> • IO1 • IO2 • SF1 • SF6
event-code <i>WORD</i> <0–10>	Specifies a number that precisely identifies the event reported.
module <i>WORD</i> <0-100>	Filters and lists the logs according to module. Specifies a string length of 0–100 characters. Categories include SNMP, EAP, RADIUS, RMON, WEB, IGMP, HW, MLT, FILTER, QOS, CLILOG, SW, CPU, IP, VLAN, IPMC, IP-RIP, OSPF, PIM, POLICY, RIP and SNMPLOG. To specify multiple filters, separate each category by the vertical bar (), for example, OSPF FILTER QOS.
name-of-file <i>WORD</i> <1-99>	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.
save-to-file <i>WORD</i> <1-99>	Redirects the output to the specified file and removes all encrypted information. You cannot use the tail option with the save-to-file option. Specify a string length of 1–99 characters. The format for the file name is: /intflash/<filename>, /extflash/<filename>, or /usb/<filename>.
severity <i>WORD</i> <0-25>	Filters and lists the logs according to severity. Choices include INFO, ERROR, WARNING, and FATAL. To specify multiple filters, separate each severity by the vertical bar (), for example, ERROR WARNING FATAL.
tail	Shows the last results first.
vrf <i>WORD</i> <0–32>	Specifies the name of a VRF instance to show log messages that only pertain to that VRF.

Configuring ACLI logging

Before you begin

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

About this task

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 CLILOG module.

 **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. Enable ACLI logging:

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

```
no clilog enable
```
3. Ensure that the configuration is correct:

```
show clilog
```
4. View the ACLI log:

```
show logging file module clilog
```
5. View the ACLI log. The following command only applies to log files generated by releases prior to Release 3.2:

```
show clilog file [grep WORD<1-256>] [tail]
```

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

```
VSP-9012:1(config)#clilog enable
```

```
VSP-9012:1(config)#show logging file module clilog
CP1 [08/21/11 14:29:57.231] 0x002c0600 00000000 GlobalRouter CLILOG INFO 1
CONSOLE rwa en
CP1 [08/21/11 14:29:58.771] 0x002c0600 00000000 GlobalRouter CLILOG INFO 2
CONSOLE rwa config t
CP1 [08/21/11 14:30:06.743] 0x002c0600 00000000 GlobalRouter CLILOG INFO 3
CONSOLE rwa source basic.cfg
CP1 [08/21/11 14:30:07.018] 0x002c0600 00000000 GlobalRouter CLILOG INFO 4
CONSOLE rwa config terminal
CP1 [08/21/11 14:30:07.026] 0x002c0600 00000000 GlobalRouter CLILOG INFO 5
CONSOLE rwa boot config flags fabric-profile 1
CP1 [08/21/11 14:30:07.027] 0x002c0600 00000000 GlobalRouter CLILOG INFO 6
CONSOLE rwa boot config flags ftpd
CP1 [08/21/11 14:30:07.028] 0x002c0600 00000000 GlobalRouter CLILOG INFO 7
CONSOLE rwa boot config flags rlogind
CP1 [08/21/11 14:30:07.029] 0x002c0600 00000000 GlobalRouter CLILOG INFO 8
CONSOLE rwa boot config flags sshd
CP1 [08/21/11 14:30:07.030] 0x002c0600 00000000 GlobalRouter CLILOG INFO 9
CONSOLE rwa boot config flags telnetd
CP1 [08/21/11 14:30:07.031] 0x002c0600 00000000 GlobalRouter CLILOG INFO 10
CONSOLE rwa cli timeout 65535
CP1 [08/21/11 14:30:07.032] 0x002c0600 00000000 GlobalRouter CLILOG INFO 11
CONSOLE rwa password password-history 3
CP1 [08/21/11 14:30:07.033] 0x002c0600 00000000 GlobalRouter CLILOG INFO 12
```

```

CONSOLE rwa cliilog enable
CP1 [08/21/11 14:30:07.034] 0x002c0600 00000000 GlobalRouter CLILOG INFO 13
CONSOLE rwa snmplog enable
CP1 [08/21/11 14:30:07.036] 0x002c0600 00000000 GlobalRouter CLILOG INFO 14
CONSOLE rwa no sys ecn-compatibility
CP1 [08/21/11 14:30:07.046] 0x002c0600 00000000 GlobalRouter CLILOG INFO 15
CONSOLE rwa interface mgmtEthernet 1/1
CP1 [08/21/11 14:30:07.047] 0x002c0600 00000000 GlobalRouter CLILOG INFO 16
CONSOLE rwa ip address 47.17.159.49 255.255.255.0
CP1 [08/21/11 14:30:07.049] 0x002c0600 00000000 GlobalRouter CLILOG INFO 17
CONSOLE rwa exit
CP1 [08/21/11 14:30:07.050] 0x002c0600 00000000 GlobalRouter CLILOG INFO 18
CONSOLE rwa interface GigabitEthernet 10/11
CP1 [08/21/11 14:30:07.051] 0x002c0600 00000000 GlobalRouter CLILOG INFO 19
CONSOLE rwa no shutdown
CP1 [08/21/11 14:30:07.053] 0x002c0600 00000000 GlobalRouter CLILOG INFO 20
CONSOLE rwa exit
CP1 [08/21/11 14:30:07.054] 0x002c0600 00000000 GlobalRouter CLILOG INFO 21
CONSOLE rwa interface gigabitethernet 10/11
CP1 [08/21/11 14:30:07.056] 0x002c0600 00000000 GlobalRouter CLILOG INFO 22
CONSOLE rwa ipv6 interface vlan 3
CP1 [08/21/11 14:30:07.079] 0x002c0600 00000000 GlobalRouter CLILOG INFO 23
CONSOLE rwa ipv6 interface enable

```

Variable definitions

Use the data in the following table to use the `cliilog` commands.

Table 19: Variable definitions

Variable	Value
enable	Activates ACLI logging. To disable, use the <code>no cliilog enable</code> command.

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

 **Note:**

The `show cliilog file` command only applies to log files generated by releases prior to Release 3.2.

Table 20: Variable definitions

Variable	Value
tail	Shows the last results first.
grep WORD<1-256>	Performs a string search in the log file. <i>WORD<1-256></i> is the string, of up to 256 characters in length, to match.

Log configuration using ACLI

Chapter 14: 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, open 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.

Name	Description
Enable	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.

Name	Description
MaxHosts	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.
OperState	Specifies the operational state of the syslog service. The default is active.
Header	<p>Specifies the IP header in syslog packets to circuitlessIP, default, or managementVIP.</p> <ul style="list-style-type: none"> • 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. For syslog packets that are transmitted out-of-band through the management port, the physical IP address of the master CPU is used in the IP header. • If the value is managementVIP, the virtual management IP address of the device is used in the IP header for syslog packets that are transmitted out-of-band only through the management port. • 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. <p>The default value is default.</p>

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, open 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.

Name	Description
Id	Specifies the ID for the syslog host. The range is 1–10.
AddressType	Specifies if the address is an IPv4 or an IPv6 address. 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.
Address	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.
UdpPort	Specifies the UDP port to use to send messages to the syslog host (514–530). The default is 514.
Enable	Enables or disables the sending of messages to the syslog host.
HostFacility	Specifies the syslog host facility used to identify messages (LOCAL0 to LOCAL7). The default is LOCAL7.
Severity	Specifies the message severity for which syslog messages are sent. The default is INFO.
MapInfoSeverity	Specifies the syslog severity to use for INFO messages. The default is INFO.
MapWarningSeverity	Specifies the syslog severity to use for WARNING messages. The default is WARNING.
MapErrorSeverity	Specifies the syslog severity to use for ERROR messages. The default is ERROR.

Name	Description
MapFatalSeverity	Specifies the syslog severity to use for FATAL messages. The default is EMERGENCY.
MapMfgSeverity	Specifies the syslog severity to use for Accelar manufacturing messages. The default is ERROR.

Chapter 15: 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 *Avaya Virtual Services Platform 9000 Security*, NN46250–601.

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 <0-2147483647>] [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 <0-2147483647>] [retries <0-255>]] [filter
WORD<1-32>]
```

4. Ensure that the configuration is correct:

```
show snmp-server host
```

Example

1. Configure the target table entry:

```
VSP-9012:1(config)# snmp-server host 198.202.188.207 port 162
v2c ReadView inform timeout 1500 retries 3 mms 484
```


2. Configure an SNMPv3 host:

```
VSP-9012:(config)# snmp-server host 4717:0:0:0:0:0:7933:6
port 163 v3 authPriv Lab3 inform timeout 1500 retries 3
```

Variable definitions

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

Table 21: Variable definitions

Variable	Value
inform [timeout <0-2147483647>] [retries <0-255>] [mms <0-2147483647>]	Sends SNMP notifications as inform (rather than trap). To use all three options in one command, you must use them in the following order: <ol style="list-style-type: none"> 1. timeout <0-2147483647> specifies the timeout value in seconds with a range of 0–214748364. 2. retries <0-255> specifies the retry count value with a range of 0–255. 3. mms <0-2147483647> specifies the maximum message size as an integer with a range of 0–2147483647.
filter WORD<1-32>	Specifies the filter profile to use.
noAuthNoPriv authNoPriv AuthPriv	Specifies the security level.
port <1-65535>	Specifies the host server port number.
WORD<1-32>	Specifies the security name, which identifies the principal that generates SNMP messages.
WORD<1-256>	Specifies either an IPv4 or IPv6 address. <p> Note: The SNMP server host IPv6 format should be 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.</p>

Configuring an SNMP notify filter table

Before you begin

- You must log on to the Global Configuration mode in ACLI.
- For more information about the notify filter table, see RFC3413.

About this task

Configure the notify table to select management targets to receive notifications, as well as the type of notification to send to each management target.

Procedure

1. Create a new notify filter table:

```
snmp-server notify-filter WORD<1-32> WORD<1-32>
```
2. Ensure that the configuration is correct:

```
show snmp-server notify-filter
```

Example

```
VSP-9012:1(config)#snmp-server notify-filter profile3
99.3.6.1.6.3.1.1.4.1
```

```
VSP-9012:1#show snmp-server notify-filter
```

```
=====
Notify Filter Configuration
=====
Profile Name          Subtree                Mask
-----
profile1              +99.3.6.1.6.3.1.1.4.1  0x7f
profile2              +99.3.6.1.6.3.1.1.4.1  0x7f
profile3              +99.3.6.1.6.3.1.1.4.1  0x7f
```

Variable definitions

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

Table 22: Variable definitions

Variable	Value
<code>WORD<1-32> WORD<1-32></code>	Creates a notify filter table. The first instance of <code>WORD<1-32></code> specifies the name of the filter profile with a string length of 1–32.

Variable	Value
	<p>The second instance of <i>WORD</i><1-32> identifies the filter subtree OID with a string length of 1–32.</p> <p>If the subtree OID parameter uses a plus sign (+) prefix (or no prefix), this indicates include. If the subtree OID uses the minus sign (–) prefix, it indicates exclude.</p> <p>You do not calculate the mask because it is automatically calculated. You can use the wildcard character, the asterisk (*), to specify the mask within the OID. You do not need to specify the OID in the dotted decimal format; you can alternatively specify that the MIB parameter names and the OIDs are automatically calculated.</p>

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 Avaya Virtual Services Platform 9000 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-9012:1(config)#snmp-server sender-ip 172.16.120.2 172.16.120.5
VSP-9012:1(config)#no snmp-server force-iphdr-sender enable
```

Variable definitions

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

Table 23: Variable definitions

Variable	Value
agent-conformance enable	Enables the agent conformance mode. Conforms to MIB standards if disabled. If you activate this option, feature configuration is stricter and error handling less informative. Avaya recommends that you do not activate this option; it is not a normally supported mode of operation.
authentication-trap enable	Activates the generation of authentication traps.
force-iphdr-sender enable	Automatically configures the SNMP and IP sender to the same value. The default is disabled.
force-trap-sender enable	Sends the configured source address (sender IP) as the sender network in the notification message.
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.

Enabling SNMP trap logging

Before you begin

- You must log on to the Global Configuration mode in ACLI.
- You must configure and enable the syslog server.

About this task

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

 **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. Enable SNMP trap logging:

```
snmplog enable
```
2. Disable SNMP trap logging:

```
no snmplog enable
```
3. View the contents of the SNMP log:

```
show logging file module snmplog
```
4. View the contents of the SNMP log. The following command only applies to log files generated by releases prior to Release 3.2:

```
show snmplog [file [grep WORD<1-255>|tail]]
```

Example

```
VSP-9012:1> enable
VSP-9012:1# configure terminal
VSP-9012:1(config)# snmplog enable
VSP-9012:1(config)# show logging file module snmplog
```

Variable definitions

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

Table 24: Variable definitions

Variable	Value
enable	Enables the logging of traps. Use the command <code>no snmplog enable</code> to disable the logging of traps.
file [grep WORD<1-255> tail]	The parameter only applies to log files generated by releases prior to Release 3.2: Shows the trap log file stored on external flash. You can optionally specify search or display parameters: <ul style="list-style-type: none"> • <code>grep WORD<1-255></code> performs a string search in the log file. <code>WORD<1-255></code> is the string, of up to 255 characters in length, to match. • <code>tail</code> shows the last results first.

Chapter 16: 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 *Avaya Virtual Services Platform 9000 Security*, NN46250–601.

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, open 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.

Name	Description
Name	Specifies a unique identifier for this table. The name is a community string.
TDomain	Specifies the transport type of the address. ipv4Tdomain specifies the transport type of address is an IPv4 address and ipv6Tdomain specifies the transport type of address is IPv6.
TAddress	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.
Timeout	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.
RetryCount	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.
TagList	Contains a list of 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.
Params	Contains SNMP parameters used to generate messages to send to this transport address. For example, to receive SNMPv2C traps, use TparamV2.
TMask	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.
MMS	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.

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, open 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.

Name	Description
Name	Identifies the target table.
MPModel	Specifies the message processing model to use to generate messages: SNMPv1, SNMPv2c, or SNMPv3/USM.
SecurityModel	Specifies the security model to use to generate messages: SNMPv1, SNMPv2c, or USM. You can receive an <code>inconsistentValue</code> error if you try to configure this variable to a value for a security model that the implementation does not support.

Name	Description
SecurityName	Identifies the principal on whose behalf SNMP messages are generated.
SecurityLevel	Specifies the security level used to generate SNMP messages: noAuthNoPriv, authNoPriv, or authPriv.

Configuring an SNMP notify table

About this task

Configure the notify table to select management targets to receive notifications, as well as the type of notification to send to each management target.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit > SnmpV3**.
 2. Click **Notify Table**.
 3. In the **Notify Table** tab, click **Insert**.
 4. In the **Name** box, type a notify table name.
 5. In the **Tag** box, type the transport tag for the table.
 6. From the **Type** options, select a type.
 7. Click **Insert**.
-

Notify Table field descriptions

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

Name	Description
Name	Specifies a unique identifier.
Tag	Specifies the tag.
Type	Determines the type of notification generated. This value is only used to generate notifications, and is ignored for other purposes. If an SNMP entity only supports generation of Unconfirmed-Class protocol data unit (PDU), this parameter can be read-only. The possible values are

Name	Description
	<ul style="list-style-type: none"> • trap—messages generated contain Unconfirmed-Class Protocol Data Units (PDU) • inform—messages generated contain Confirmed-Class PDUs <p>The default value is trap.</p>

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, open 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.

Name	Description
NotifyFilterProfileName	Specifies the name of the filter profile used to generate notifications.
Subtree	Specifies the MIB subtree that, if you combine it with the mask, defines a family of subtrees, which are included in

Name	Description
	or excluded from the filter profile. For more information, see RFC2573.
Mask	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.
Type	Indicates whether the family of filter subtrees are included in or excluded from a filter.

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, open 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.

Name	Description
TargetParamsName	Specifies the unique identifier associated with this entry.

Name	Description
NotifyFilterProfileName	Specifies the name of the filter profile to use to generate notifications.

Enabling SNMP trap logging

About this task

Enable trap logging to save a copy of all SNMP traps.

Procedure

1. In the navigation tree, open 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.

Name	Description
AuthenticationTraps	Enables or disables the sending of traps after an error occurs.
LastErrorCode	Specifies the last reported error code.
LastErrorSeverity	Specifies the last reported error severity: 0= Informative Information 1= Warning Condition 2= Error Condition 3= Manufacturing Information 4= Fatal Condition

Chapter 17: RMON alarm variables

This reference section describes remote monitoring (RMON) alarm variables.

RMON alarm variables are divided into three categories.

- Security
- Errors
- Traffic

Each category can have subcategories.

For more information on how to configure and view RMON alarm variables, see:

- [RMON configuration using ACLI](#) on page 47
- [RMON configuration using EDM](#) on page 51

RMON alarm variables

RMON alarm variables are divided into three categories. Each category has subcategories.

The following table lists the alarm variable categories and provides a brief variable description.

Table 25: RMON alarm variables

Category	Subcategory	Variable	Definition
Security		rcCliNumAccessViolations.0	The number of CLI access violations detected by the system.
		rcWebNumAccessBlocks.0	The number of accesses the Web server blocked.
		snmpInBadCommunityNames.0	The total number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation not allowed by the SNMP community named in the message.
Errors	Interface	ifInDiscards	The number of inbound packets discarded even

Category	Subcategory	Variable	Definition
			though no errors were detected to prevent the packets being deliverable to a higher-layer protocol. One possible reason for discarding a packet is to free buffer space.
		ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors, preventing them from being deliverable to a higher-layer protocol.
		ifOutDiscards	The number of outbound packets discarded even though no errors were detected to prevent the packets being transmitted. One possible reason for discarding such a packet is to free buffer space.
		ifOutErrors	For packet-oriented interfaces, the number of outbound packets that were not transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that were not transmitted because of errors.
	Ethernet	dot3StatsAlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object increments when the

Category	Subcategory	Variable	Definition
			alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions exist are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
		dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object increments when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
		dot3StatsSingleCollisionFrames	A count of successfully transmitted frames on a particular interface where transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts object, the ifOutMulticastPkts object, or the ifOutBroadcastPkts object, and is not counted by the corresponding instance of the

Category	Subcategory	Variable	Definition
			dot3StatsMultipleCollisionFrames object.
		dot3StatsMultipleCollisionFrames	A count of successfully transmitted frames on a particular interface where transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts object, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.
		dot3StatsSQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
		dot3StatsDeferredTransmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
		dot3StatsLateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet; 512 bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late)

Category	Subcategory	Variable	Definition
			collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
		dot3StatsExcessiveCollisions	A count of frames where the transmission on a particular interface fails due to excessive collisions.
		dot3StatsInternalMacTransmit Errors	A count of frames where the transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object can represent a count of transmission errors on a particular interface that are not otherwise counted.
		dot3StatsCarrierSenseErrors	The number of times the carrier sense condition was lost or never asserted when the switch attempted to transmit a frame on a particular interface. The count represented by an instance of this object increments at most once for each transmission attempt, even if the carrier sense

Category	Subcategory	Variable	Definition
			condition fluctuates during a transmission attempt.
		dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceeds the maximum permitted frame size. The count represented by an instance of this object increments when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
		dot3StatsInternalMacReceiveErrors	A count of frames where the transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is counted by an instance of this object only if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object can represent a count of transmission errors on a particular interface that are not otherwise counted.

Category	Subcategory	Variable	Definition
	IP	ipInHdrErrors.0	The number of input datagrams discarded due to errors in the datagram IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, and errors discovered in processing IP options.
		ipInDiscards.0	The number of discarded input IP datagrams where no problems were encountered to prevent continued processing. An example of why they were discarded can be lack of buffer space. This counter does not include any datagrams discarded while awaiting reassembly.
		ipOutDiscards.0	The number of output IP datagrams where no problems were encountered to prevent transmission to the destination, but that were discarded (for example, for lack of buffer space). This counter includes datagrams counted in ipForwDatagrams if packets meet this (discretionary) discard criterion.
		ipFragFails.0	The number of IP datagrams discarded because they needed to be fragmented at this entity but were not, for example, because the Don't Fragment flag was set.
		ipReasmFails.0	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so forth). This is not necessarily a count of discarded IP fragments because some algorithms

Category	Subcategory	Variable	Definition
			(notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
		icmplnParmProbs.0	The number of ICMP In parameter problem messages received.
		icmpOutParmProbs.0	The number of ICMP Out parameter problem messages received.
	MLT	rcStatMltEtherAlignmentErrors	The number of frames received on an MLT that are not an integral number of octets in length, but do not pass the FCS check.
		rcStatMltEtherFCSErrors	The number of frames received on an MLT that are an integral number of octets in length, but do not pass the FCS check.
		rcStatMltEtherSingleCollFrames	The number of successfully transmitted frames on a particular MLT where transmission is inhibited by exactly one collision.
		rcStatMltEtherMultipleCollFrames	The number of successfully transmitted frames on a particular MLT where transmission is inhibited by more than one collision.
		rcStatMltEtherSQETestError	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT.
		rcStatMltEtherDeferredTransmiss	A count of frames where the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object.

Category	Subcategory	Variable	Definition
		rcStatMltEtherLateCollisions	The number of times that a late collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet; 512-bit-times corresponds to 51.2-microseconds on a 10 Mb/s system.
		rcStatMltEtherExcessiveCollis	The number of times that excessive collisions are detected on a particular MLT later than 512 bit-times into the transmission of a packet; 512 bit-times corresponds to 51.2 microseconds on a 10-Mb/s system.
		rcStatMltEtherMacTransmitErr or	A count of frames where the transmission on a particular MLT fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
		rcStatMltEtherCarrierSenseErr or	The number of times the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular MLT. The count represented by an instance of this object increments at most once for each transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
		rcStatMltEtherFrameTooLong	A count of frames received on a particular MLT that exceeds the maximum permitted frame size. The count represented by an instance of this object

Category	Subcategory	Variable	Definition
			increments when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user).
		rcStatMltEtherMacReceiveError	A count of frames for which reception on a particular MLT fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object.
	Other	rcTblArNoSpace	The number of entries not added to the address translation table due to lack of space.
		snmpInAsnParseErrs.0	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when it decodes received SNMP messages.
		rcStgPortInBadBpdus	The number of bad BPDUs received by this port.
		dot1dTpPortInDiscards	Count of valid frames received that were discarded (that is, filtered) by the forwarding process.
		rip2ifStatRcvBadPackets	The number of routes in valid RIP packets that were ignored for any reason.
		rip2ifStatRcvBadRoutes	The number of RIP response packets received by the RIP process that were subsequently discarded for any reason.
		rcStatOspfBufferAllocFailures.0	The number of times that OSPF failed to allocate buffers.

Category	Subcategory	Variable	Definition
		rcStatOspfBufferFreeFailures .0	The number of times that OSPF failed to free buffers.
Traffic	Interface	ifInOctets	The total number of octets received on the interface, including framing characters.
		ifInMulticastPkts	The number of packets, delivered by this sublayer to a higher sublayer, that are addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
		ifInBroadcastPkts	The number of packets, delivered by this sublayer to a higher (sub) layer, that are addressed to a broadcast address at this sublayer.
		ifInUnkownProtos	For packet-oriented interfaces, the number of packets received through the interface that are discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received through the interface that are discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always 0.
		ifOutOctets	The total number of octets transmitted from the interface, including framing characters.
		ifOutMulticastPkts	The total number of packets that higher-level protocols requested be transmitted, and that are addressed to a

Category	Subcategory	Variable	Definition
			multicast address at this sublayer, including those that are discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
		ifoutBroadcastPkts	The total number of packets that higher level protocols requested transmitted, and that were addressed to a broadcast address at this sublayer, including those discarded or not sent.
		ifLastChange	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, this object contains a value of zero.
	RmonEther Stats	etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). Use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
		etherStatsPkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
		etherStatsBroadcastPkts	The total number of good packets received that are directed to the broadcast address. This number does

Category	Subcategory	Variable	Definition
			not include multicast packets.
		etherStatsMulticastPkts	The total number of good packets received that are directed to a multicast address. This number does not include packets directed to the broadcast address.
		etherStatsCRCAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of 64 to 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
		etherStatsUndersizePkts	The total number of packets received that are less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
		etherStatsOversizePkts	The total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
		etherStatsFragments	The total number of packets received that are less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal

Category	Subcategory	Variable	Definition
			occurrences due to collisions) and noise hits.
		etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
	IP	ipInReceives.0	All incoming IP packets.
		ipInAddrErrors.0	The number of bad IP destination addresses.
		ipForwDatagrams.0	IP packets forwarded.
		ipInUnknownProtos.0	Number of unsupported IP protocols.
		ipInDelivers.0	The number of IP In packets delivered.
		ipOutRequests.0	The total number of IP datagrams that local IP user protocols supplied to IP in request for transmission.
		ipOutNoRoutes.0	The number of IP datagrams discarded because no route was found to transmit to the destination.
		ipFragOKs.0	The number of IP datagrams successfully fragmented.
		ipFragCreates.0	The number of IP datagram fragments generated as a result of fragmentation.
		ipReasmReqds.0	The number of requests to reassemble fragments.
		ipReasmOKs.0	The number of fragments reassembled successfully.
	ICMP	icmpInSrcQuenchs.0	The number of ICMP Source Quench messages received.
		icmpInRedirects.0	The number of ICMP redirect messages.
		icmpInEchos.0	The number of ICMP Echo requests messages received.
		icmpInEchosReps.0	The number of ICMP Echo reply messages received.

Category	Subcategory	Variable	Definition
		icmpInTimeStamps.0	The number of ICMP timestamp request messages received.
		icmpInTimeStampsReps.0	The number of ICMP timestamp reply messages received.
		icmpInAddrMasks.0	The number of ICMP mask request messages reviewed.
		icmpInAddrMasksReps.0	The number of ICMP mask reply messages reviewed.
		icmpInDestUnreachs.0	The number of ICMP destinations unreachable messages received.
		icmpInTimeExcds.0	The number of ICMP Time Exceeded messages received.
		icmpOutSrcQuenchs.0	The number of ICMP Source Quench messages sent.
		icmpOutRedirects.0	The number of ICMP redirect messages sent.
		icmpOutEchos.0	The number of ICMP Echo request messages sent.
		icmpOutEchosReps.0	The number of ICMP Echo reply messages sent.
		icmpOutTimeStamps.0	The number of ICMP Timestamp request messages sent.
		icmpOutTimeStampsReps.0	The number of ICMP Timestamp reply messages sent.
		icmpOutAddrMasks.0	The number of ICMP Address mask messages sent.
		icmpOutAddrMasksReps.0	The number of ICMP Address mask reply messages sent.
		icmpOutDestUnreachs.0	The number of ICMP destination unreachable messages sent.

Category	Subcategory	Variable	Definition
		icmpOutTimeExcds.0	The number of ICMP time exceeded messages sent.
	Snmp	snmpInPkts.0	The total number of messages delivered to the SNMP entity from the transport service.
		snmpOutPkts.0	The total number of SNMP messages passed from the SNMP protocol entity to the transport service.
		snmpInBadVersions.0	The total number of SNMP messages delivered to the SNMP protocol entity that were intended for an unsupported SNMP version.
		snmpInBadCommunityUses.0	The total number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation that was not allowed by the SNMP community named in the message.
		snmpInTooBigs.0	The total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig.
		snmpInNoSuchNames.0	The total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.
		snmpInBadValues. 0	The total number of SNMP PDUs received that were generated by the SNMP protocol entity and for which the value of the error-status field is badValue.
		snmpInReadOnlys.0	The total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the

Category	Subcategory	Variable	Definition
			error-status field is readOnly. It is a protocol error to generate an SNMP PDU that contains the value readOnly in the error-status field; as such, this object is provided as a means of detecting incorrect implementations of the SNMP.
		snmpInGenErrs.0	The total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
		snmpInTotalReqVars.0	The total number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
		snmpInTotalSetVars.0	The total number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
		snmpInGetRequests.0	The total number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.
		snmpInGetNexts.0	The total number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol entity.
		snmpInSetRequests.0	The total number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol entity.
		snmpInGetResponses.0	The total number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol entity.

Category	Subcategory	Variable	Definition
		snmpInTraps.0	The total number of SNMP Trap PDUs accepted and processed by the SNMP protocol entity.
		snmpOutTooBig.0	The total number of SNMP PDUs generated by the SNMP protocol entity and for which the value of the error-status field is tooBig.
		snmpOutNoSuchNames.0	The total number of SNMP PDUs generated by the SNMP protocol entity and for which the value of the error-status field is noSuchName.
		snmpOutBadValues.0	The total number of SNMP PDUs sent that were generated by the SNMP protocol entity and for which the value of the error-status field is badValue.
		snmpOutGenErrs.0	The total number of SNMP PDUs generated by the SNMP protocol entity and for which the value of the error-status field is genErr.
		snmpOutGetRequests.0	The total number of SNMP Get-Request PDUs generated by the SNMP protocol entity.
		snmpOutGetNexts.0	The total number of SNMP Get-Next PDUs generated by the SNMP protocol entity.
		snmpOutSetRequests.0	The total number of SNMP Set-Request PDUs generated by the SNMP protocol entity.
		snmpOutGetResponses.0	The total number of SNMP Get-Response PDUs generated by the SNMP protocol entity.
		snmpOutTraps.0	The total number of SNMP Trap PDUs generated by the SNMP protocol entity.

Category	Subcategory	Variable	Definition
	Bridge	rcStgTimeSinceTopologyChange	The time (in hundredths of a second) since the last topology change was detected by the bridge entity.
		rcStgTopChanges	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
		rcStgMaxAge	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in hundredths of a second. This is the actual value that this bridge is currently using.
		rcStgPortForwardTransitions	The number of times this port transitioned from the Learning state to the Forwarding state.
		rcStgPortInConfigBpdus	The number of Config BPDUs received by this port.
		rcStgPortInTcnBpdus	The number of Topology Change Notification BPDUs received by this port.
		rcStgPortOutConfigBpdus	The number of Config BPDUs transmitted by this port.
		rcStgPortOutTcnBpdus	The number of Topology Change Notification BPDUs transmitted by this port.
		dot1dTpPortInFrames	The number of frames received by this port from its segment. A frame received on the interface corresponding to this port is counted by this object only if it is for a protocol being processed by the local bridging function, including

Category	Subcategory	Variable	Definition
			bridge management frames.
		dot1dTpPortOutFrames	The number of frames transmitted by this port to its segment. A frame transmitted on the interface corresponding to this port is counted by this object if and only if it is for a protocol processed by the local bridging function, including bridge management frames.
		dot1dTpLearnedEntryDiscards.0	The total number of Forwarding Database entries learned but discarded due to a lack of space to store them in the Forwarding Database. If this counter increases, it indicates that the forwarding database is regularly becoming full (a condition that has negative performance effects on the subnetwork). If this counter has a significant value but does not increase, it indicates that the problem occurred but is not persistent.
	Utilization	rcSysCpuUtil.0	Percentage of SF/CPU utilization.
		rcSysSwitchFabricUtil.0	Percentage of switching fabric utilization.
		rcSysBufferUtil.0	Buffer utilization as a percentage of the total amount of buffer space in the system. A high value indicates congestion.
		rcSysNVRamUsed.0	Nonvolatile RAM (NVRAM) in use in kilobytes.
		rcSysLastChange.0	Last management-initiated configuration change since sysUpTime.

Category	Subcategory	Variable	Definition
		rcSysLastVlanChange.0	Last management-initiated VLAN configuration change since sysUpTime.
		rcSysLastSaveToNVRam.0	SysUpTime of the last time the NVRAM on the SF/CPU board was written to.
		rcSysLastSaveToStandbyNVRam.0	SysUpTime of the last time the standby NVRAM (on the backup SF/CPU board) was written to.
	RIP	rip2GlobalRoute Changes.0	The number of changes made to the IP Route database by RIP.
		rip2GlobalQueries.0	The number of responses sent to RIP queries from other systems.
		rip2IfStatSentUpdates	The number of triggered RIP updates actually sent on this interface.
	OSPF	ospfExternLSACount.0	The number of external (LSA type 5) link-state advertisements in the link-state database.
		ospfOriginateNewLSAs.0	The number of new link-state advertisements that have originated. The number increments each time the router originates a new LSA.
		ospfrxNewLSAs.0	The number of link-state advertisements received determined to be new installations.
		ospfSpfRuns	Indicates the number of SPF calculations performed by OSPF.
		ospfAreaBdrRtrCount	The total number of area border routers reachable within this area.
		ospfASBdrRtrCount	The total number of autonomous system border routers reachable within this area.

Category	Subcategory	Variable	Definition
		ospfAreaLSACount	The total number of link-state advertisements in this area's link state database.
		ospflfState	This signifies a change in the state of an OSPF virtual interface.
		ospflfEvents	The number of times this OSPF interface changed the state or an error occurred.
		ospfVirtlfState	The number of times this OSPF interface.
		ospfVirtlfEvents	The number of state changes or error events on this virtual link.
		ospfVirtNbrState	The state of the Virtual Neighbor Relationship.
		ospfVirtNbrEvents	The number of times this virtual link changed the state or an error occurred.
	Igmp	igmpInterfaceWrongVersions	The number of queries received whose IGMP version does not match. IGMP requires that all routers on the LAN are configured to run the same version of IGMP.
		igmpInterfaceJoins	The number of times a group membership was added on this interface.
		igmpInterfaceLeaves	The number of times a group membership was deleted on this interface.
	MLT	rcStatMltlfExtnlfnMulticastPkts	The total number of multicast packets delivered to this MLT interface.
		rcStatMltlfExtnlfnBroadcastPkts	The total number of broadcast packets delivered to this MLT interface.
		rcStatMltlfExtnlfnOutMulticastPkts	The total number of MLT interface multicast packets delivered to this MLT interface.

Category	Subcategory	Variable	Definition
		rcStatMltIfExtnIfOutBroadcastPkts	The total number of MLT interface broadcast packets delivered to this MLT interface.
		rcStatMltIfExtnIfHCInOctets	The total number of octets received on this MLT interface including framing characters detected by the high-count (64-bit) register.
		rcStatMltIfExtnIfHCInUcastPkts	The number of packets delivered by this MLT interface to a higher MLT that were not addressed to a multicast or broadcast address as detected by the high-count (64-bit) register.
		rcStatMltIfExtnIfHCInMulticastPkt	The total number of multicast packets delivered to this MLT interface detected by the high-count (64-bit) register.
		rcStatMltIfExtnIfHCInBroadcastPkt	The total number of broadcast packets delivered to this MLT interface detected by the high-count (64-bit) register.
		rcStatMltIfExtnIfHCOctets	The total number of octets transmitted from the MLT interface, including framing characters.
		rcStatMltIfExtnIfHCOutUcastPkts	The number of packets transmitted by this MLT interface to a higher MLT that were not addressed to a multicast or broadcast address as detected by the high-count (64-bit) register.
		rcStatMltIfExtnIfHCOutMulticast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this sublayer, including those that were discarded or not

RMON alarm variables

Category	Subcategory	Variable	Definition
			sent registered by the high-count (64-bit) register.
		rcStatMltlfExtnIfHCOutBroadcast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent registered by the high-count (64-bit) register.

Chapter 18: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Glossary

Application Programming Interface (API)	Defines how to access a software-based service. An API is a published specification that describes how other software programs can access the functions of an automated service.
Autonomous System Number (ASN)	A two-byte number that is used to identify a specific AS.
Avaya command line interface (ACLI)	A textual user interface. When you use ACLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.
bit error rate (BER)	The ratio of the number of bit errors to the total number of bits transmitted in a given time interval.
Bridge Protocol Data Unit (BPDU)	A data frame used to exchange information among the bridges in local or wide area networks for network topology maintenance.
Enterprise Device Manager (EDM)	A Web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.
Frame Check Sequence (FCS)	Frames are used to send upper-layer data and ultimately the user application data from a source to a destination.
Generalized Regular Expression Parser (grep)	A Unix command used to search files for lines that match a given regular expression (RE).
Institute of Electrical and Electronics Engineers (IEEE)	An international professional society that issues standards and is a member of the American National Standards Institute, the International Standards Institute, and the International Standards Organization.
Internet Control Message Protocol (ICMP)	A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.
Internet Group Management Protocol (IGMP)	A host membership protocol used to arbitrate membership in multicast services.

Internet Protocol multicast (IPMC)	The technology foundation for audio and video streaming, push applications, software distribution, multipoint conferencing, and proxy and caching solutions.
link-state advertisement (LSA)	Packets that contain state information about directly connected links (interfaces) and adjacencies. Each Open Shortest Path First (OSPF) router generates the packets.
Logical Link Control (LLC)	A protocol used in LANs to transmit protocol data units between two end stations. This LLC layer addresses and arbitrates data exchange between two endpoints.
mask	A bit string that is used along with an IP address to indicate the number of leading bits in the address that correspond with the network part.
media	A substance that transmits data between ports; usually fiber optic cables or category 5 unshielded twisted pair (UTP) copper wires.
Media Access Control (MAC)	Arbitrates access to and from a shared medium.
MultiLink Trunking (MLT)	A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.
port	A physical interface that transmits and receives data.
quality of service (QoS)	Use QoS features to reserve resources in a congested network. For example, you can configure a higher priority to IP deskphones, which need a fixed bit rate, and, split the remaining bandwidth between data connections if calls in the network are important than the file transfers.
Random Access Memory (RAM)	Memory into which you can write and read data. A solid state memory device used for transient memory stores. You can enter and retrieve information from storage position.
remote monitoring (RMON)	A remote monitoring standard for Simple Network Management Protocol (SNMP)-based management information bases (MIB). The Internetwork Engineering Task Force (IETF) proposed the RMON standard to provide guidelines for remote monitoring of individual LAN segments.
reverse path checking (RPC)	Prevents packet forwarding for incoming IP packets with incorrect or forged (spoofed) IP addresses.
Routing Information Protocol (RIP)	A distance vector protocol in the IP suite, used by IP network-layer protocol, that enables routers in the same AS to exchange routing information by means of periodic updates. The RIP is most often used as a very simple IGP within small networks.

shortest path first (SPF)	A class of routing protocols that use Dijkstra's algorithm to compute the shortest path through a network, according to specified metrics, for efficient transmission of packet data.
Simple Network Management Protocol (SNMP)	Administratively monitors network performance through agents and management stations.
spanning tree	A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.
Spanning Tree Group (STG)	A collection of ports in one spanning tree instance.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.
user-based security model (USM)	A security model that uses a defined set of user identities for authorized users on a particular Simple Network Management Protocol (SNMP) engine.
User Datagram Protocol (UDP)	In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.
virtual router (VR)	An abstract object managed by the Virtual Router Redundancy Protocol (VRRP) that acts as a default router for hosts on a shared LAN.
virtual router forwarding (VRF)	Provides traffic isolation between customers operating over the same node. Each virtual router emulates the behavior of a dedicated hardware router by providing separate routing functionality, and the network treats each VRF as a separate physical router.
Virtual Router Redundancy Protocol (VRRP)	A protocol used in static routing configurations, typically at the edge of the network. This protocol operates on multiple routers on an IP subnet and elects a primary gateway router. When the primary router fails, a backup router is quickly available to take its place.

