# Managing Faults

Release 4.3
NN47500-702
Issue 01.01
March 2016

### Notice

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

### Documentation disclaimer

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

### Link disclaimer

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

### Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

### Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

### Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

### License types

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

### Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

### Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, 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.

### Virtualization

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

### Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

### Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

### Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

### Preventing Toll Fraud

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

### Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

### Security Vulnerabilities

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

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

### Downloading Documentation

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

### Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

### Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such

# Contents

# Chapter 1: New in this document

*Managing Faults* is a new document for Release 4.3 so all the features are new in this release. See *Release Notes* for a full list of features.

# Chapter 2: 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 stage changes (port flapping).

## Local alarms

The switch 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 CLI. 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.

## 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.

# Connectivity Fault Management

The Shortest Path Bridging MAC (SPBM) network needs a mechanism to debug connectivity issues and isolate faults. This function is performed at Layer 2, not Layer 3. Connectivity Fault Management (CFM) operates at Layer 2 and provides an equivalent of the **`ping`** and **`traceroute`** commands. The switch supports a subset of CFM functionality to support troubleshooting of the SPBM cloud. For more information about CFM see *Configuring Fabric Connect*.

# Chapter 3: Key Health Indicators using CLI

The Key Health Indicators (KHI) feature of the switch 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 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.

Capture KHI information during normal operations to provide a baseline for support personnel when detecting fault situations.

## Displaying KHI performance information

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

### Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display buffer performance and utilization statistics for KHI:

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

3. 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][,...]}]
   ```

4. Display memory performance and utilization statistics for KHI on the specified slot or all slots:

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

5. Display process performance and utilization statistics for KHI on the specified slot or all slots:

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

6. Display thread performance and utilization statistics for KHI on the specified slot or all slots:

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

7. 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**

Some of the following examples include partial output only.

```
Switch:1>show khi performance buffer-pool 1
    Slot:1
      CPP:
         UsedFBuffs: 12
         FreeFBuffs: 3060
         RxQ0FBuffs: 0
         RxQ1FBuffs: 0
         RxQ2FBuffs: 0
         RxQ3FBuffs: 0
         RxQ4FBuffs: 0
         RxQ5FBuffs: 0
         RxQ6FBuffs: 0
         RxQ7FBuffs: 0
         TxQueueFBuffs: 0
         NoFbuff: 0

      Network stack system:
         UsedMbuf: 244
         FreeMbuf: 47606
         SocketMbuf: 19

      Network stack data:
         UsedMbuf: 4
         FreeMbuf: 10748

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

```
Switch:1>show khi performance cpu 1
    Slot:1
         Current utilization: 8
         5-minute average utilization: 8
         5-minute high water mark: 13 (02/13/13 14:00:47)
```

```
Switch:1>show khi performance memory 1
    Slot:1
         Used: 514560 (KB)
         Free: 521260 (KB)
         Current utilization: 49 %
         5-minute average utilization: 49 %
         5-minute high water mark: 22 (10/08/14 14:48:01)
```

```
Switch:1>show khi performance process 1
    Slot:1
--------------------------------------------------------------------------------
PID  PPID  PName           VmSize  VmLck   VmRss   VmData  VmStk   VmExe  VmLib
--------------------------------------------------------------------------------
1    0     init            1936    0       656     164     88      32     1556
2    0     kthreadd        0       0       0       0       0       0      0
3    2     migration/0     0       0       0       0       0       0      0
4    2     ksoftirqd/0     0       0       0       0       0       0      0
5    2     watchdog/0      0       0       0       0       0       0      0
```

```
6    2     migration/1     0       0       0       0       0       0      0
7    2     ksoftirqd/1     0       0       0       0       0       0      0
8    2     watchdog/1      0       0       0       0       0       0      0
9    2     events/0        0       0       0       0       0       0      0
10   2     events/1        0       0       0       0       0       0      0
11   2     khelper         0       0       0       0       0       0      0
12   2     netns           0       0       0       0       0       0      0
13   2     async/mgr       0       0       0       0       0       0      0
14   2     sync_supers     0       0       0       0       0       0      0
15   2     bdi-default     0       0       0       0       0       0      0
16   2     kblockd/0       0       0       0       0       0       0      0
17   2     kblockd/1       0       0       0       0       0       0      0
18   2     khubd           0       0       0       0       0       0      0
19   2     kmmcd           0       0       0       0       0       0      0

--More-- (q = quit)
```

```
Switch: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     kthreadd        0.0    0.0
3     3     migration/0     0.0    0.0
4     4     ksoftirqd/0     0.0    0.0
5     5     watchdog/0      0.0    0.0
6     6     migration/1     0.0    0.0
7     7     ksoftirqd/1     0.0    0.0
8     8     watchdog/1      0.0    0.0
9     9     events/0        0.0    0.0
10    10    events/1        0.1    0.0
11    11    khelper         0.0    0.0
12    12    netns           0.0    0.0
13    13    async/mgr       0.0    0.0
14    14    sync_supers     0.0    0.0
15    15    bdi-default     0.0    0.0
16    16    kblockd/0       0.0    0.0
17    17    kblockd/1       0.0    0.0
18    18    khubd           0.0    0.0

--More-- (q = quit)
```

```
Switch:1>show khi performance slabinfo
 Slot:1
--------------------------------------------------------------------------------
Name                   Active  Num     Objsize Objper  Pageper Active  Num
                       Objs    Objs            slab    slab    Slabs   Slabs
--------------------------------------------------------------------------------
merc_sock              0       0       384     21      2       0       0
cfq_queue              72      72      112     36      1       2       2
bsg_cmd                0       0       288     14      1       0       0
mqueue_inode_cache     15      15      544     15      2       1       1
nfs_direct_cache       0       0       80      51      1       0       0
nfs_inode_cache        0       0       600     13      2       0       0
fat_inode_cache        0       0       416     19      2       0       0
fat_cache              0       0       24      170     1       0       0
ext2_inode_cache       136     41      480     17      2       8       8
configfs_dir_cache     0       0       56      73      1       0       0
posix_timers_cache     0       0       104     39      1       0       0
rpc_inode_cache        17      17      480     17      2       1       1
UNIX                   57      57      416     19      2       3       3
UDP-Lite               0       0       512     16      2       0       0
UDP                    32      32      512     16      2       2       2
tw_sock_TCP            32      32      128     32      1       1       1
```

```
TCP                    28      28      1120    14      4       2       2
eventpoll_pwq          204     204     40      102     1       2       2
sgpool-128             12      12      2560    12      8       1       1
sgpool-64              12      12      1280    12      4       1       1
sgpool-32              12      12      640     12      2       1       1
scsi_data_buffer       170     170     24      170     1       1       1
blkdev_queue           48      48      1288    12      4       4       4
blkdev_requests        60      44      200     20      1       3       3
biovec-256             10      10      3072    10      8       1       1
biovec-128             0       0       1536    21      8       0       0
biovec-64              0       0       768     21      4       0       0
sock_inode_cache       304     304     416     19      2       16      16
skbuff_fclone_cache    460     290     352     23      2       20      20
file_lock_cache        72      72      112     36      1       2       2
net_namespace          24      24      320     12      1       2       2
shmem_inode_cache      1170    1144    448     18      2       65      65
proc_inode_cache       777     768     376     21      2       37      37
sigqueue               56      56      144     28      1       2       2
radix_tree_node        1222    1070    296     13      1       94      94
bdev_cache             34      34      480     17      2       2       2
sysfs_dir_cache        7055    7010    48      85      1       83      83
filp                   1700    1520    160     25      1       68      68
inode_cache            3243    3038    352     23      2       141     141
dentry                 6210    5398    136     30      1       207     207
buffer_head            280     277     72      56      1       5       5
vm_area_struct         3358    3250    88      46      1       73      73
mm_struct              126     115     448     18      2       7       7
files_cache            72      71      224     18      1       4       4
signal_cache           119     116     480     17      2       7       7
sighand_cache          108     103     1312    12      4       9       9
task_struct            260     250     1248    13      4       20      20
anon_vma               1280    1278    16      256     1       5       5
idr_layer_cache        208     208     152     26      1       8       8
kmalloc-8192           8       8       8192    4       8       2       2
kmalloc-4096           104     99      4096    8       8       13      13
kmalloc-2048           128     115     2048    16      8       8       8
kmalloc-1024           256     256     1024    16      4       16      16
kmalloc-512            288     240     512     16      2       18      18
kmalloc-256            352     351     256     16      1       22      22
kmalloc-128            896     895     128     32      1       28      28
kmalloc-64             5120    5120    64      64      1       80      80
kmalloc-32             896     883     32      128     1       7       7
kmalloc-16             1536    1535    16      256     1       6       6
kmalloc-8              2560    2558    8       512     1       5       5
kmalloc-192            273     273     192     21      1       13      13
kmalloc-96             966     900     96      42      1       23      23
```

## Variable definitions

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

| Variable | Value |
|---|---|
| {slot[-slot][,...]} | Specifies the slot number. |

# Displaying KHI control processor information

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

### Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display statistics for control packets that go to the control processor:

   ```
   show khi cpp port-statistics [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   ```

### Example

```
Switch:1>show khi cpp port-statistics 3/1-3/7
================================================================================
         KHI CPP Details - Port Statistics
================================================================================
Ports    Packet Type                        Rx Packets  Tx Packets
--------------------------------------------------------------------------------
-
3/1      LLC_TDP(134)                              498         498
3/1      LLC_ISIS(137)                             420         421
3/2      LLC_TDP(134)                              498         498
3/4      Ether2_ARP_Request(10)                      0           1
3/4      Ether2_IPv4_PIM_MC(24)                      0         101
3/4      Ether2_IPv4_OSPF_MC(32)                   318         320
3/4      Ether2_IPv4_OSPF_UC(34)                     5           0
3/4      LLC_TDP(134)                              496         496
3/5      Ether2_ARP_Request(10)                      4           4
3/5      Ether2_ARP_Other(11)                        0           4
3/5      Ether2_IPv4_PIM_MC(24)                      0         103
3/5      Ether2_IPv4_OSPF_MC(32)                     0         235
3/5      LLC_TDP(134)                              374         374
3/7      Ether2_ARP_Request(10)                      0           1
3/7      Ether2_ARP_Other(11)                        1           0
3/7      Ether2_IPv4_PIM_MC(24)                    153         151
3/7      Ether2_IPv4_PIM_UC(26)                      4           0
```

# Variable definitions

Use the data in the following table to use the **show khi cpp port-statistics** command.

| Variable | Value |
|---|---|
| {slot/port[/sub-port][-slot/port[/sub-port]][,...]} | Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. |

# Clearing KHI information

KHI information can be cleared for a specific slot or across the whole device. Use the command to clear the port statistics.

### Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Clear CPP statistics:

   ```
   clear khi cpp port-statistics
   ```

# Chapter 4: Key Health Indicators using EDM

The Key Health Indicators (KHI) feature of the switch 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 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.

Capture KHI information during normal operations to provide a baseline for support personnel when detecting fault situations.

## Clearing KHI statistics

### About this task

Clear KHI statistics.

### Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation pane, expand the following folders: **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **CPP Stats Control** tab.
5. Select the statistics you want to clear.
6. 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. |

# 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 pane, expand 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 5: Link state change control using CLI

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

## Controlling link state changes

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

### Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the interval for link state changes:

   ```
   link-flap-detect interval <2-600>
   ```

3. Configure the number of changes allowed during the interval:

   ```
   link-flap-detect frequency <1-9999>
   ```

4. Enable automatic port disabling:

   ```
   link-flap-detect auto-port-down
   ```

5. Enable sending a trap:

   ```
   link-flap-detect send-trap
   ```

### Example

1. Enable automatic disabling of the port:

   ```
   Switch(config)# link-flap-detect auto-port-down
   ```

2. Configure the link-flap-detect interval:

   ```
   Switch(config)# link-flap-detect interval 20
   ```

3. Enable sending traps:

   ```
   Switch(config)# link-flap-detect send-trap
   ```

## Variable definitions

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

| Variable | Value |
|---|---|
| auto-port-down | Automatically disables the port if state changes exceed the link-flap threshold. By default, auto-port-down is enabled. 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.<br>The default is 20. 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.<br>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

Displays link flap detection state changes on a physical port.

### Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display link state changes:

   ```
   show link-flap-detect
   ```

### Example

```
Switch:1>enable
Switch:1#show link-flap-detect

 Auto Port Down : enable
 Send Trap      : enable
 Interval       : 60 seconds
 Frequency      : 20
```

# Chapter 6: 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 pane, expand 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. The default is enabled. |
| **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. |
| **Interval** | Specifies the interval (in seconds) between port failures. The default is 60. |

# Chapter 7: Remote Monitoring

This section provides information on Remote Monitoring (RMON).

RMON has two versions:

- RMON1

  **Note:**

  The switch does not support RMON1.

- RMON2

## RMON 2

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).

Use CLI or EDM, to globally enable RMON on the system.

After you globally enable RMON, you enable monitoring for individual devices on a port-by-port basis.

The RMON2 feature monitors network and application layer protocols on configured network hosts, either VLAN or port interfaces, that you enable for monitoring. The RMON2 feature expands the capacity of RMON1 to upper layer protocols in the OSI model.

The following figure shows which form of RMON monitors which layers in the OSI model:

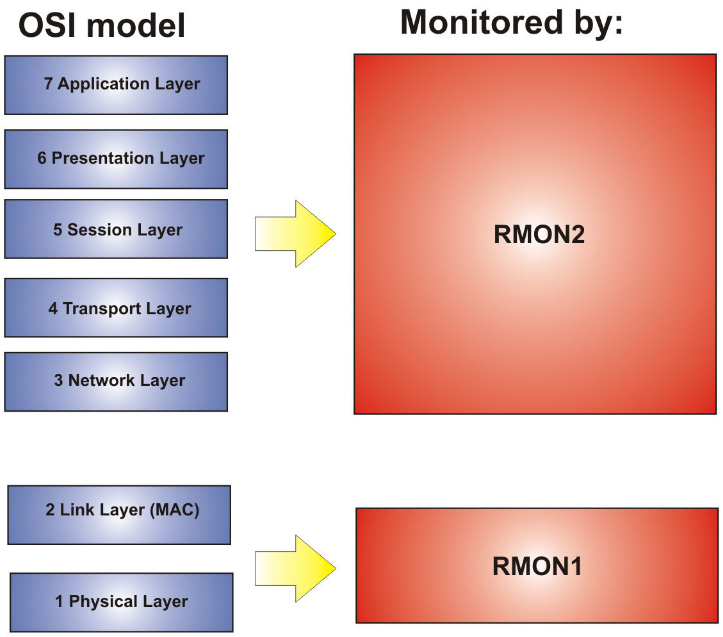

**Figure 1: OSI model and RMON**

The RMON2 feature 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). The switch supports a partial implementation of RMON2. The RMON2 feature adds the following MIBS: protocol directory, protocol distribution, address map, network-layer host and application layer host for the traffic passing through the (Control Processor) CP for these MIB tables.

The system only collects statistics for IP packets that pass through the CP. RMON2 does not monitor packets on other interfaces processed on the switch that do not pass through the CP.

After you globally enable RMON2, enable monitoring for individual devices. Identify the network hosts for the system to monitor with a manual configuration on the interfaces you want to monitor.

The RMON2 feature monitors a list of predefined protocols. The system begins to collect protocol statistics immediately after you enable RMON.

The RMON2 feature collects statistics on:

- Protocols predefined by the system.
- Address mapping between physical and network address on particular network hosts that you configure for monitoring.
- Network host statistics for particular hosts on a network layer protocol (IP) that you configure for monitoring.
- Application host statistics for a particular host on an application layer protocol that you configure for monitoring.

## RMON2 MIBs

This section describes the following MIBs, on which RMON2 can collect statistics: protocol directory, protocol distribution, address map, network-layer host, and application layer host.

### Protocol directory MIB

The protocol directory is a master directory that lists all of the protocols RMON2 can monitor. The protocols include network layer, transport layer, and application layer protocols, under the OSI model. The system only monitors statistics for the predefined protocols. You cannot delete or add additional protocols to this table. The protocol directory MIB is enabled by default for the predefined protocols.

The predefined protocols include:

- Internet Protocol (IP)
- Secure Shell version 2 (SSHv2)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Telnet
- Remote login (rlogin)
- Trivial File Transfer Protocol (TFTP)
- Simple Network Management Protocol (SNMP)

### Protocol distribution MIB

The protocol distribution MIB collects traffic statistics that each protocol generates by local area network (LAN) segment. The switch acts as the probe and the system collects protocol statistics for the entire switch as part of the group for all of the protocols predefined in the protocol directory table. The protocol distribution control table is part of this group. The protocol distribution control table is predefined with an entry for the management IP for the switch to represent the network segment where the system collects the statistics.

No CLI or EDM support exists to add or delete entries in this table.

### Address map MIB

The address map MIB maps the network layer IP to the MAC layer address.

The system populates the address map control table MIB with an entry for each host interface that you enable for monitoring on the switch.

### Network layer host MIB

The network layer host MIB monitors the Layer 3 traffic statistics for each host. The network layer host MIB monitors traffic packets in and out of hosts based on the network layer address. The network layer host controls the network and application layer host tables.

The system populates an entry for the management IP of the switch to represent the network segment where the system collects the statistics. You have to enable each host interface that you want to monitor on the switch.

The system only collects statistics for this group from packets that go to the CP.

### Application layer host MIB

The application layer host MIB monitors traffic statistics by application protocol for each host.

The system populates an entry for the management IP of the switch to represent the network segment where the system collects the statistics. You have to enable each host interface that you want to monitor on the switch.

The system only collects statistics for this group from packets that go to the CP.

# RMON configuration using CLI

This section contains procedures to configure RMON using Command Line Interface (CLI).

## Enabling RMON globally

Enable RMON globally, and then enable RMON on the host interfaces you want to monitor. By default, RMON is disabled globally.

### Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable RMON globally:

   ```
   rmon
   ```

### Example

Configure RMON globally:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#rmon
```

## Enabling Remote Monitoring on an interface

Use the following procedure to enable Remote Monitoring (RMON) on an interface.

### Before you begin

- Enable RMON globally.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable RMON on a particular VLAN:

```
vlan rmon <1-4059>
```

3. Enter GigabitEthernet Interface Configuration mode:

```
enable
configure terminal
interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
```

**Note:**

If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

4. Enable RMON on a particular port:

```
rmon
```

**Example**

Enable RMON on VLAN 2:

```
Switch:1>enable
Switch:1#configure terminal
Switch1:1(config)#vlan rmon 2
```

Enable RMON on port 3/8:

**Note:**

Slot and port information can differ depending on hardware platform. For more information, see the hardware documentation for your platform.

```
Switch:1>enable
Switch:1#configure terminal
Switch1:1(config)#interface gigabitethernet 3/8
Switch1:1(config-if)#rmon
```

## Variable definitions

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

| Variable | Value |
|---|---|
| *<1-4059>* | Specifies the VLAN ID on which to configure RMON. |

# Displaying RMON information

View RMON information on the switch such as the RMON address maps, application host statistics, control tables, network host statistics, and protocol distribution statistics.

### Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON2 information:

   ```
   show rmon {address-map|application-host-stats WORD<1–64>|ctl-table|
   network-host-stats|protocol-dist-stats}
   ```

## Variable definitions

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

| Variable | Value |
|---|---|
| address-map | Displays the RMON2 address map. This RMON2 parameter expands RMON capacity to display information on network, transport, and application layers. |
| application-host-stats *WORD<1–64>* | Displays RMON2 application host statistics from one of the following protocols: TCP, UDP, FTP, Telnet HTTP, rLogin, SSHv2, TFTP, SNMP, HTTPS. This RMON2 parameter expands RMON capacity to display network, transport, and application layers. |
| ctl-table | Displays the RMON2 control tables. This RMON2 parameter expands RMON capacity to display network, transport, and application layers. |
| network-host-stats | Displays RMON2 network-host statistics. This RMON2 parameter expands RMON capacity to display network, transport, and application layers. |
| protocol-dist-stats | Displays RMON2 protocol distribution statistics. This RMON2 parameter expands RMON capacity to display network, transport, and application layers. |

# Displaying RMON status

View the current RMON status on the switch.

### Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON status:

   ```
   show rmon
   ```

### Example

```
Switch: show rmon

RMON Info :
Status       : enable
```

# Displaying RMON address maps

View the maps of network layer address to physical address to interface.

The probe adds entries based on the source MAC and network addresses in packets without MAC-level errors.

### Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON address maps:

   ```
   show rmon address-map
   ```

### Example

```
Switch: show rmon address-map
================================================================================
                             Rmon Address Map Table
================================================================================
PROTOIDX  HOSTADDR         SOURCE  PHYADDR            LASTCHANGE
--------------------------------------------------------------------------------
1         12.1.1.1         2060    b0:ad:aa:42:a5:03  10/09/15 17:30:41
```

## Job aid

The following table describes the fields in the output for the **`show rmon address-map`** command.

| Parameter | Description |
|---|---|
| PROTOIDX | Shows a unique identifier for the entry in the table. |
| HOSTADDR | Shows the network address for this entry. The format of the value depends on the protocol portion of the local index. |
| SOURCE | Shows the interface or port on which the network address was most recently seen. |
| PHYADDR | Shows the physical address on which the network address was most recently seen. |
| LASTCHANGE | Shows when the entry was created or last changed. If this value changes frequently, it can indicate duplicate address problems. |

# Displaying RMON application host statistics

View application host statistics to see traffic statistics by application protocol for each host.

### Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON application host statistics:

   ```
   show rmon application-host-stats WORD<1-64>
   ```

### Example

```
Switch:# show rmon application-host-stats ?
  WORD<1-64>  Select one of these application protocols
              {TCP|UDP|FTP|TELNET|HTTP|RLOGIN|SSH|TFTP|SNMP|HTTPS}
Switch:# show rmon application-host-stats FTP

================================================================================
                          Rmon Application Host Stats
================================================================================
HOSTADDR         INPKT      OUTPKT     INOCT      OUTOCT     CREATETIME
--------------------------------------------------------------------------------
12.1.1.1         0          0          0          0          10/09/15 17:29:54
```

## Job aid

The following table describes the fields in the output for the **`show rmon application-host-stats`** command.

| Parameter | Description |
|---|---|
| HOSTADDR | Shows the network address for this entry. The format of the value depends on the protocol portion of the local index. |
| INPKT | Shows the number of packets for this protocol type, without errors, transmitted to this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times. |
| OUTPKT | Shows the number of packets for this protocol type, without errors, transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times. |
| INOCT | Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames. |
| OUTOCT | Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames. |
| CREATETIME | Shows when the entry was last activated. |

# Displaying RMON control tables

View RMON control tables to see the data source for both network layer and application layer host statistics.

### Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON control tables:

   ```
   show rmon ctl-table
   ```

## Job aid

The following table describes the fields in the output for the `show rmon ctl-tabl` command.

| Parameter | Description |
|---|---|
| ADDRMAPCFG | Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following:<br>• **NOT SUPPORTED**<br>• **SUPPORTED OFF**<br>• **SUPPORTED ON**<br>If the value is **SUPPORTED ON**, the probe adds entries to the address map table that maps the network layer address to the MAC layer address. |
| AHDROPFRAMES | Shows the total number of application layer host frames that the probe receives and drops. This value does not include packets that were not counted because they had MAC-layer errors. |
| CREATETIME | Shows when the entry was last activated. |
| DATASOURCE | Shows the source of data for the entry. |
| DROPFRAMES | Shows the total number of frames that the probe receives and drops. This value does not include packets that were not counted because they had MAC-layer errors. |
| HOSTCFG | Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following:<br>• **NOT SUPPORTED**<br>• **SUPPORTED OFF**<br>• **SUPPORTED ON**<br>If the value is **SUPPORTED ON**, the probe adds entries to the Host Control table to collect statistics for network layer and application layer hosts. |
| IDX | Shows a unique identifier for the entry in the table. |
| MATRIXCFG | Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following:<br>• **NOT SUPPORTED**<br>• **SUPPORTED OFF**<br>• **SUPPORTED ON** |
| NHDROPFRAMES | Shows the total number of network host frames that the probe receives and drops. This value does not include packets that were not counted because they had MAC-layer errors. |
| OWNER | Shows the entity that configured this entry. |

*Table continues…*

| Parameter | Description |
|---|---|
| PROTOCOL | Shows the protocols RMON2 can monitor:<br>• Internet Protocol (IP)<br>• Transmission Control Protocol (TCP)<br>• User Datagram Protocol (UDP)<br>• File Transfer Protocol (FTP)<br>• Secure Shell version 2 (SSHv2)<br>• Telnet<br>• Hypertext Transfer Protocol (HTTP)<br>• Remote login (RLOGIN)<br>• Trivial File Transfer Protocol (TFTP)<br>• Simple Networking Management Protocol (SNMP)<br>• Hypertext Transfer Protocol Secure (HTTPS) |

# Displaying RMON network host statistics

View network host statistics to see Layer 3 traffic statistics for each host. The network layer host MIB monitors traffic packets in and out of hosts based on the network layer address.

### Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON network host statistics:

```
show rmon network-host-stats
```

## Job aid

The following table describes the fields in the output for the **show rmon network-host-stats** command.

| Parameter | Description |
|---|---|
| HOSTADDR | Shows the host address for this entry. |
| INPKT | Shows the number of packets without errors transmitted to this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times. |
| OUTPKT | Shows the number of packets without errors transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times. |

*Table continues…*

| Parameter | Description |
|---|---|
| INOCT | Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames. |
| OUTOCT | Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames. |
| CREATETIME | Shows when the entry was last activated. |

## Displaying RMON protocol distribution statistics

View protocol distribution statistics to see traffic statistics that each protocol generates by local area network (LAN) segment.

### Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON protocol distribution statistics:

   ```
   show rmon protocol-dist-stats
   ```

### Example

```
Switch: show rmon protocol-dist-stats

================================================================================
                            Rmon Protocol Dist Stats
================================================================================
PROTOCOL  PKTS       OCTETS
--------------------------------------------------------------------------------
IP        0          0
TCP       0          0
UDP       0          0
FTP       0          0
SSH       0          0
TELNET    0          0
HTTP      0          0
RLOGIN    0          0
TFTP      0          0
SNMP      0          0
HTTPS     0          0
```

# 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

Enable RMON globally, and then enable RMON on the host interfaces you want to monitor. By default, RMON is disabled globally.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Options**.
3. Click the **Options** tab.
4. Select the **Enable** check box.
5. 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. 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. |

# Enabling RMON on a port or VLAN

Use the following procedure to enable RMON on an interface.

### Before you begin

- Enable RMON globally.

### Procedure

1. Enable RMON on a VLAN:
    a. In the navigation pane, expand the following folders: **Configuration** > **VLAN**.
    b. Click **VLANs**.
    c. Click the **Advanced** tab.
    d. In the row for the VLAN, double-click the **RmonEnable** field, and then select **enable**.
    e. Click **Apply**.
2. Enable RMON on a port:
    a. In the Device Physical View, select a port.

b. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **Port**.

c. Click **General**.

d. Click the **Interface** tab.

e. For the **RmonEnable** field, select **enable**.

f. Click **Apply**.

# Viewing the protocol directory

View the protocol directory to see the list of protocols that RMON2 can monitor. You cannot change the list of protocols.

### About this task

The protocol directory MIB is enabled by default for the predefined protocols.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Protocol Directory**.
3. Click the **Protocol Directories** tab.

## Protocol Directories field descriptions

Use the data in the following table to use the **Protocol Directories** tab.

| Name | Description |
|---|---|
| **Index** | Shows a unique identifier for the entry in the table. |
| **Protocol** | Shows the protocols RMON2 can monitor:<br>• Internet Protocol (IP)<br>• Secure Shell version 2 (SSHv2)<br>• Transmission Control Protocol (TCP)<br>• User Datagram Protocol (UDP)<br>• File Transfer Protocol (FTP)<br>• Hypertext Transfer Protocol (HTTP)<br>• Telnet<br>• Remote login (rlogin)<br>• Trivial File Transfer Protocol (TFTP)<br>• Simple Networking Management Protocol (SNMP) |

*Table continues…*

| Name | Description |
|---|---|
| **AddressMapConfig** | Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following:<br>• notSupported<br>• supportedOff<br>• supportedOn<br>If the value is supportedOn, the probe adds entries to the Address Map tab that maps the network layer address to the MAC layer address. |
| **HostConfig** | Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following:<br>• notSupported<br>• supportedOff<br>• supportedOn<br>If the value is supportedOn, the probe adds entries to the Host Control tab to collect statistics for network layer and application layer hosts. |
| **MatrixConfig** | Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following:<br>• notSupported<br>• supportedOff<br>• supportedOn |
| **Owner** | Shows the entity that configured this entry. |

## Viewing the data source for protocol distribution statistics

View the Distribution Control tab to see the network segment data source on which the protocol distribution statistics are measured. The management IP mentioned as a data source represents the IP that the SNMP agent uses to access the switch.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Protocol Distribution**.
3. Click the **Distribution Control** tab.

## Distribution Control field descriptions

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

| Name | Description |
|---|---|
| **Index** | Shows a unique identifier for the entry in the table. |
| **DataSource** | Specifies the source of data for this protocol distribution. |
| **DroppedFrames** | Shows the total number of frames that the probe receives and drops but does not include in the StatsDropEvents value. This event can occur if the probe is out of resources and sheds the load from this collection. This value does not include packets that were not counted because they had MAC-layer errors. |
| **CreateTime** | Shows the value of the sysUpTime when the entry was last activated. |
| **Owner** | Shows the entity that configured this entry. |

# Viewing protocol distribution statistics

View protocol distribution statistics to see traffic statistics that each protocol generates by local area network (LAN) segment.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Protocol Distribution**.
3. Click the **Distribution Stats** tab.

## Distribution Stats field descriptions

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

| Name | Description |
|---|---|
| **LocalIndex** | Identifies the protocol distribution an entry is part of, as well as the particular protocol that it represents. |
| **Pkts** | Shows the number of packets without errors received for this protocol type. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times. |

*Table continues…*

| Name | Description |
|---|---|
| **Octets** | Shows the number of octets in packets received for this protocol type since it was added to the table. This value does not include octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames. |

# Viewing the host interfaces enabled for monitoring

View the entries in the address map control tab to see which host interfaces are enabled for monitoring on the switch. Each entry in this table enables the discovery of addresses on a new interface.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Address Map**.
3. Click the **Address Map Control** tab.

## Address Map Control field descriptions

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

| Name | Description |
|---|---|
| **Index** | Shows a unique identifier for the entry in the table. |
| **DataSource** | Shows the source of data for the entry. |
| **DroppedFrames** | Shows the total number of frames that the probe receives and drops but does not include in the StatsDropEvents value. This event can occur if the probe is out of resources and sheds the load from this collection. This value does not include packets that were not counted because they had MAC-layer errors. |
| **Owner** | Shows the entity that configured this entry. |

# Viewing address mappings

View the mappings of network layer address to physical address to interface.

### About this task

The probe adds entries on this tab based on the source MAC and network addresses in packets without MAC-level errors.

The probe populates this table for all protocols on the **Protocol Directories** tab with a value of **AddressMapConfig** equal to **supportedOn**.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Address Map**.
3. Click the **Address Map** tab.

## Address Map field descriptions

Use the data in the following table to use the **Address Map** tab.

| Name | Description |
|---|---|
| **LocalIndex** | Shows a unique identifier for the entry in the table. |
| **HostAddress** | Shows the network address for this entry. The format of the value depends on the protocol portion of the local index. |
| **Source** | Shows the interface or port on which the network address was most recently seen. |
| **PhysicalAddress** | Shows the physical address on which the network address was most recently seen. |
| **LastChange** | Shows the value of the sysUpTime when the entry was created or last changed. If this value changes frequently, it can indicate duplicate address problems. |

# Viewing the data source for host statistics

View the Host Control tab to see the data source for both network layer and application layer host statistics.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Network Layer Host**.
3. Click the **Host Control** tab.

## Host Control field descriptions

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

| Name | Description |
|---|---|
| **Index** | Shows a unique identifier for the entry in the table. |
| **DataSource** | Shows the source of data for the associated host table. The statistics in this group reflect all packets on the local network segment that attaches to the identified interface. |
| **NHDropFrames** | Shows the total number of frames that the probe receives and drops but does not include in the StatsDropEvents value. This event can occur if the probe is out of resources and sheds the load from this collection. This value does not include packets that were not counted because they had MAC-layer errors. |
| **AHDropFrames** | Shows the total number of frames that the probe receives and drops but does not include in the StatsDropEvents value. This event can occur if the probe is out of resources and sheds the load from this collection. This value does not include packets that were not counted because they had MAC-layer errors. |
| **Owner** | Shows the entity that configured this entry. |

# Viewing network host statistics

View network host statistics to see Layer 3 traffic statistics for each host. The network layer host MIB monitors traffic packets in and out of hosts based on the network layer address.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Network Layer Host**.
3. Click the **Network Host Stats** tab.

## Network Host Stats field descriptions

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

| Name | Description |
|---|---|
| **LocalIndex** | Shows a unique identifier for the entry in the table. |
| **HostAddress** | Shows the host address for this entry. |
| **InPkts** | Shows the number of packets without errors transmitted to this address. This value is the number of link-layer packets so a single, fragmented |

*Table continues…*

| Name | Description |
|---|---|
| | network-layer packet can increment the counter several times. |
| **OutPkts** | Shows the number of packets without errors transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times. |
| **InOctets** | Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames. |
| **OutOctets** | Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames. |
| **CreateTime** | Shows the value of the sysUpTime when the entry was last activated. |

# Viewing application host statistics

View application host statistics to see traffic statistics by application protocol for each host.

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Application Layer Host**.
3. Click the **Application Host Stats** tab.

## Application Host Stats field descriptions

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

| Name | Description |
|---|---|
| **Index** | Shows a unique identifier for the entry in the table. |
| **HostAddress** | Identifies the network layer address of this entry. |
| **LocalIndex** | Identifies the network layer protocol of the address. |
| **InPkts** | Shows the number of packets for this protocol type, without errors, transmitted to this address. This value is the number of link-layer packets so a single, |

*Table continues…*

| Name | Description |
|---|---|
| | fragmented network-layer packet can increment the counter several times. |
| **OutPkts** | Shows the number of packets for this protocol type, without errors, transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times. |
| **InOctets** | Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames. |
| **OutOctets** | Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames. |
| **CreateTime** | Shows the value of the sysUpTime when the entry was last activated. |

# Chapter 8: Log and trap fundamentals

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

## Overview of traps and logs

### System log messaging

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

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

The remote UNIX management workstation performs the following actions:

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

### Log consolidation

The switch generates a system log file and can forward that file to a syslog server for remote viewing, storage and analyzing.

The system log captures messages for the following components:

- Extensible Authentication Protocol (EAP)
- Remote Authentication Dial-in User Service (RADIUS)
- Remote Monitoring (RMON)
- Web
- hardware (HW)
- MultiLink Trunking (MLT)
- filter
- Quality of Service (QoS)

- Command line interface (CLI) log
- software (SW)
- Central Processing Unit (CPU)
- Internet Protocol (IP)
- Virtual Local Area Network (VLAN)
- policy
- Simple Network Management Protocol (SNMP) log

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

View logs for CLILOG module to track all CLI commands executed and for fault management purposes. The CLI 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 CLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

### System log client over IPv6 transport

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

### Log messages with enhanced secure mode

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

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

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

- **`more`**
- **`edit`**
- **`rename`**
- **`copy`**

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

The following table summarizes log file command access based on role-based access levels.

**Table 1: Log commands accessible for various users**

| Access level role | Commands |
|---|---|
| Administrator | The **`remove`** and **`delete`** commands. |
| No user at any access level. | The following commands:<br>• **`more`**<br>• **`edit`**<br>• **`rename`**<br>• **`copy`** |
| Administrator | All configuration commands can only be accessed by the individual in the administrator role. |
| Administrator and auditor | All show commands for log files. |
| All users (Administrator, auditor, security, privilege, operator) | All show commands for log configurations. |

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

### SNMP traps

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

This document only describes SNMP commands related to traps. For more information about how to configure SNMP community strings and related topics, see *Configuring Security*.

# Simple Network Management Protocol

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

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

**Important:**

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

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

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

# Log message format

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

- CPU slot number—Indicates the CP slot where the command is logged.
- timestamp—Records the date and time at which the event occurred. The format is MM/DD/YY hh:mm:ss.uuu, where uuu is milliseconds. Example: [11/01/16 11:41:21.376].
- event code—Precisely identifies the event reported.
- alarm code—Specifies the alarm code.
- alarm type—Identifies the alarm type (Dynamic or Persistent) for alarm messages.
- alarm status—Identifies the alarm status (set or clear) for alarm messages.
- VRF name—Identifies the Virtual Routing and Forwarding (VRF) instance, if applicable.
- module name—Identifies the software module or hardware from which the log is generated.
- severity level—Identifies the severity of the message.
- sequence number—Identifies a specific CLI command.
- context—Specifies the type of the session used to connect to the switch. If the session is a remote session, the remote IP address is identified.
- user name—Specifies the user name used to login to the switch.
- CLI command—Specifies the commands typed during the CLI session. The system logs anything typed during the CLI session as soon as the user presses the `Enter` key.

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

```
CP1  [07/18/14 13:23:11.253] 0x002c0600 00000000 GlobalRouter CLILOG INFO    13   TELNET:
135.55.40.200 rwa show log file name-of-file log.40300001.1806

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

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

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

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

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

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

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

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

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

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

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

```
CP1  [07/24/14 18:04:10.651] 0x00034594 00000000 GlobalRouter SW INFO System boot
CP1  [07/24/14 18:04:10.779] 0x0001081c 00400010.2 DYNAMIC SET GlobalRouter HW INFO Slot
2 is initializing.
CP1  [07/24/14 18:04:10.780] 0x0001081c 00400010.1 DYNAMIC SET GlobalRouter HW INFO Slot
1 is initializing.
CP1  [07/24/14 18:04:10.810] 0x00010729 00000000 GlobalRouter HW INFO Detected   Power
Supply in slot PS 1. Adding 800 watts to available power
```

Only a Customer Service engineer can decrypt the encrypted information. CLI commands display the logs without the encrypted information. Do not edit the log file.

The following table describes the system message severity levels.

**Table 2: Severity levels**

| Severity level | Definition |
|---|---|
| EMERGENCY | A panic condition that occurs when the system becomes unusable. Usually a severity level of emergency is usually a condition where multiple applications or server are affected. You must correct a severity level of alert immediately. |
| ALERT | Any condition requiring immediate attention and correction. You must correct a severity level of alert immediately, but usually indicates failure of a secondary system, such as an Internet Service Provider connection. |

*Table continues…*

| Severity level | Definition |
|---|---|
| CRITICAL | Any critical condition such as a hard drive error. |
| 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. An indication that an error can occur if action is not taken within a given amount of time. |
| NOTIFICATION | Significant event of a normal and normal nature. An indication that unusual, but not error, conditions have occurred. No immediate action is required. |
| INFO | Information only. No action is required. |
| DEBUG | Message containing information useful for debugging. |
| 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 in EDM, under the System Log Table tab, you must select either IPv4 or IPv6.

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

- DEBUG
- INFO
- NOTICE
- WARNING
- CRITICAL
- ERROR
- ALERT
- EMERGENCY

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

**Table 3: Default and system log severity level mapping**

| UNIX system error codes | System log severity level | Internal severity level |
|---|---|---|
| 0 | EMERGENCY | Fatal |
| 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. The switch saves log messages to internal flash.

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

## Log file naming conventions

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

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

# Log file transfer

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

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

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

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

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

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

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

  The system appends a suffix of .xxxxxxxx.sss to the file name. The first six characters of the suffix contain the last three bytes of the chassis base MAC address. The next two characters are 01. The last three characters (sss) denote the sequence number of the log file. For example, if you configure the name prefix as mylog, a possible file name is mylog. 90000001.001.
- The user name and password, if using File Transfer Protocol (FTP) for file transfer. Use the following commands to configure the user name and password:

  ```
  boot config host user WORD<0-16>
  ```

  ```
  boot config host password WORD<0-16>
  ```

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

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

Three parameters exist to configure the log file:

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

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

### Log file transfer using a wildcard filename

Use the command **`attribute WORD<1-99> [+/-] R`** to change the permissions of a file. To change permissions for all log files, use the **`attribute`** command with the wildcard filename `log.*`. Using the command in the wildcard form `attribute log.* [+/-]R` changes permissions for log files with names that begin with the characters “log.”.

**Important:**

You cannot use a wildcard pattern other than `log.*` for this command.

## Email notification

The switch can send email notification for failed components or other critical log-event conditions. The switch can also send periodic health status notifications.

Enable and configure a Simple Mail Transfer Protocol (SMTP) client on the switch for one SMTP server by specifying the server hostname or IPv4 address. To use a hostname, you must also configure a Domain Name System (DNS) client on the switch.

You must configure at least one email recipient and can create a maximum of five email recipients.

The switch can periodically send general health status notifications. Status email messages include information about the following items:

- General switch
- Chassis
- Card
- Temperature
- Power supplies
- Fans
- LEDs
- System errors
- Port lock
- Message control

- Operational configuration changes
- Current Uboot
- Port interfaces
- Port statistics

The switch maintains a default list of event IDs for which it generates an email notification. You can add specific event IDs to this list. To see the default list of event IDs, run the **`show smtp event-id`** command.

The following example shows an email that the switch sends for log events.

```
Subject: Logs from LabSwitch - 50712100008
From: <LabSwitch@default.com>
To: <test1@default.com>
CP1  [08/04/15 21:48:04.527:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR GlobalRouter
SNMP INFO 2k card up(CardNum=1 AdminStatus=1 OperStatus=1)
CP1  [08/04/15 21:48:04.527:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR GlobalRouter
SNMP INFO 2k card up(CardNum=1 AdminStatus=1 OperStatus=1)
CP1  [08/04/15 21:48:04.527:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR GlobalRouter
SNMP INFO 2k card up(CardNum=2 AdminStatus=1 OperStatus=1)
CP1  [08/04/15 21:50:03.511:UTC] 0x00088524 00000000 GlobalRouter SW INFO Boot sequence
successful
```

If you enable the SMTP client but the switch cannot reach the SMTP server, the switch generates an alarm. The switch holds log and status information in a queue until the connection with the SMTP server is restored. The message queue holds a maximum of 2,000 messages. If the queue fills, the switch drops new messages.

The following text is an example of the alarm that the switch generates when it cannot connect to the SMTP server.

```
CP1  [06/10/15 19:27:07.901:EST] 0x00398600 0e600000 DYNAMIC SET GlobalRouter SMTP
WARNING SMTP: Unable to establish connection with server: mailhost.usae.company.com, port:
25
```

If the switch cannot establish a connection to the SMTP server, verify that the server IP address or hostname, and the TCP port are correct. If you specify the server hostname, confirm that the IP address for the DNS server is correct. Check for network issues such as unplugged cables.

If the SMTP server rejects the email message, the switch generates a log message.

# Chapter 9: Log configuration using CLI

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

## Configuring a UNIX system log and syslog host

Configure the syslog to control a facility in UNIX machines that logs SNMP messages and assigns each message a severity level based on importance.

### About this task

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 CLI.

### Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable the system log:

   ```
   syslog enable
   ```

3. Specify the IP header in syslog packets:

   ```
   syslog ip-header-type <circuitless-ip|default>
   ```

4. Configure the maximum number of syslog hosts:

   ```
   syslog max-hosts <1-10>
   ```

5. Create the syslog host:

   ```
   syslog host <1-10>
   ```

6. Configure the IP address for the syslog host:

   ```
   syslog host <1-10> address WORD <0-46>
   ```

7. Enable the syslog host:

   ```
   syslog host <1-10> enable
   ```

Configure optional syslog host parameters by using the variables in the following variable definition tables.

8. View the configuration to ensure it is correct:

   ```
   show syslog [host <1-10>]
   ```

**Example**

```
Switch:1(config)# syslog enable
```

```
Switch:1(config)# syslog host 1 address 47.17.143.52
```

```
Switch:1(config)# syslog host 1 enable
```

```
Switch: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
```

```
Switch: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
```

## Variable definitions

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

| Variable | Value |
|---|---|
| enable | Enables the sending of syslog messages on the device. The default is disabled. Use the no operator before this parameter, no syslog enable to disable the sending of syslog messages on the device. The default is enabled. |
| ip-header-type <circuitless-ip\|default> | Specifies the IP header in syslog packets to circuitless-ip or default.<br>• If the value is default, the IP address of the VLAN is used for syslog packets that are transmitted in-band using I/O ports. |

*Table continues…*

| Variable | Value |
|---|---|
| | • 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.

| Variable | Value |
|---|---|
| *1–10* | Creates and configures a host instance. Use the no operator before this parameter, no syslog host 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 x:x:x:x:x:x:x:x. You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration using CLI. |
| 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> | Specifies the severity levels for which to send syslog messages. 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

Configure logging to determine the types of messages to log and where to store the messages.

### About this task

**Note:**

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

### Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Define which messages to log:

   ```
   logging level <0-4>
   ```

3. Write the log file from memory to a file:

   ```
   logging write WORD<1-1536>
   ```

4. Show logging on the screen:

   ```
   logging screen
   ```

### Example

```
Switch:1 logging level 0
Switch:1 logging write log2
Switch:1 logging screen
```

## Variable definitions

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

| Variable | Value |
|---|---|
| level <0-4> | Shows and configures the logging level. The level is one of the following values:<br>• 0: Information—all messages are recorded<br>• 1: Warning—only warning and more serious messages are recorded<br>• 2: Error—only error and more serious messages are recorded |

*Table continues…*

| Variable | Value |
|---|---|
| | • 3: Manufacturing—this parameter is not available for customer use<br>• 4: Fatal—only fatal messages are recorded |
| 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: `no logging screen` |
| 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

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.

### Before you begin

The IP address you configure for the remote host must be reachable at the time of configuration.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure the remote host address for log transfer:

```
logging transferFile {1-10} address {A.B.C.D} [filename-prefix
WORD<0-200>]
```

### Example

```
Switch: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.

| 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-prefix WORD<0-200> | 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

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

### About this task

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

Configure logging to a flash file at all times as a best practice.

### Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable system logging to a PC card file:

   ```
   boot config flags logging
   ```

3. Configure the logfile parameters:

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

### Example

```
Switch:1>enable
```

```
Switch:1#configure terminal
```

```
Switch:1(config)#boot config logfile 64 600 10
```

# Variable definitions

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

| Variable | Value |
|---|---|
| flags logging | Enables or disables logging to a file or a flash file. The log file is named using the format log.xxxxxxxx.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. The last three characters denote the sequence number of the log file. |
| logfile <64-500> <500-16384> <10-90> | Configures the logfile parameters<br>• *<64-500>* specifies the minimum free memory space on the external storage device from 64–500 KB. The switch does not support this parameter.<br>• *<500-16384>* specifies the maximum size of the log file from 500–16384 KB.<br>• *<10-90>* specifies the maximum percentage, from 10–90%, of space on the external storage device the logfile can use. The switch does not support this parameter. |

# Configuring system message control

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

### Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure system message control action:

   ```
   sys msg-control action <both|send-trap|suppress-msg>
   ```

3. Configure the maximum number of messages:

   ```
   sys msg-control max-msg-num <2-500>
   ```

4. Configure the interval:

   ```
   sys msg-control control-interval <1-30>
   ```

5. Enable message control:

   ```
   sys msg-control
   ```

### Example

```
Switch:1(config)# sys msg-control action suppress-msg
```

```
Switch:1(config)# sys msg-control max-msg-num 10
```

```
Switch:1(config)# sys msg-control control-interval 15
```

```
Switch:1(config)# sys msg-control
```

## Variable definitions

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

| 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

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

### About this task

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

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the force message control option:

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

### Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

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

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

## Variable definitions

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

| Variable | Value |
|---|---|
| *WORD<4-4>* | Adds a forced message control pattern, where *WORD<4-4>* 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

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

### About this task

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

### Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Show log information:

   ```
   show logging file [alarm] [cpu WORD<0-100>] [event-code WORD<0-10>]
   [module WORD<0-100>] [name-of-file WORD<1-99>] [save-to-file
   WORD<1-99>] [severity WORD<0-25>] [tail] [vrf WORD<0-32>]
   ```

### Example

Display log file information:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#show logging file
CP1  [02/06/15 22:38:20.678:UTC] 0x00270428 00000000 GlobalRouter SW INFO Lifecy
cle: Start
CP1  [02/06/15 22:38:21.770:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s sockserv started, pid:4794
CP1  [02/06/15 22:38:21.771:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s oom95 started, pid:4795
CP1  [02/06/15 22:38:21.771:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
```

```
s oom90 started, pid:4796
CP1  [02/06/15 22:38:21.772:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s imgsync.x started, pid:4797
CP1  [02/06/15 22:38:22.231:UTC] 0x0026452f 00000000 GlobalRouter SW INFO No pat
ch set.
CP1  [02/06/15 22:38:22.773:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s logServer started, pid:4840
CP1  [02/06/15 22:38:22.774:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s trcServer started, pid:4841
CP1  [02/06/15 22:38:22.774:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s oobServer started, pid:4842
CP1  [02/06/15 22:38:22.775:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s cbcp-main.x started, pid:4843
CP1  [02/06/15 22:38:22.776:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s rssServer started, pid:4844
CP1  [02/06/15 22:38:22.777:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s dbgServer started, pid:4845
CP1  [02/06/15 22:38:22.777:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s dbgShell started, pid:4846
CP1  [02/06/15 22:38:22.778:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s coreManager.x started, pid:4847
CP1  [02/06/15 22:38:22.779:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s ssio started, pid:4848
CP1  [02/06/15 22:38:22.780:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s hckServer started, pid:4849
CP1  [02/06/15 22:38:22.780:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s remCmdAgent.x started, pid:4850
CP1  [02/06/15 22:38:24.717:UTC] 0x000006cc 00000000 GlobalRouter SW INFO rcStar
t:  FIPS Power Up Self Test SUCCESSFUL - 0
CP1  [02/06/15 22:38:24.718:UTC] 0x000006c2 00000000 GlobalRouter SW INFO rcStar
t:  Security Stack Init SUCCESSFUL - 0
CP1  [02/06/15 22:38:24.718:UTC] 0x000006c3 00000000 GlobalRouter SW INFO rcStar
t:  IPSEC Init SUCCESSFUL
CP1  [02/06/15 22:38:24.718:UTC] 0x000006bf 00000000 GlobalRouter SW INFO rcStar
t: Security Stack Log init SUCCESSFUL - 0
CP1  [02/06/15 22:38:26.111:UTC] 0x000005c0 00000000 GlobalRouter SW INFO Licens
eLoad = ZERO, loading premier license for developer debugging
IO1  [02/06/15 22:38:26.960:UTC] 0x0011054a 00000000 GlobalRouter COP-SW INFO De
tected Master CP in slot 1

--More-- (q = quit)

Switch:1(config)#show logging file module SNMP
CP1  [02/06/15 22:39:58.530:UTC] 0x00004595 00000000 GlobalRouter SNMP INFO Boot
ed with file
CP1  [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=1 AdminStatus=1 OperStatus=1)
CP1  [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=2 AdminStatus=1 OperStatus=1)
CP1  [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=3 AdminStatus=1 OperStatus=1)
CP1  [02/06/15 22:40:45.839:UTC] 0x000045e5 00400005 DYNAMIC SET GlobalRouter SN
MP INFO Sending Cold-Start Trap
```

## Variable definitions

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

| Variable | Value |
|---|---|
| alarm | Displays alarm log entries. |
| cpu WORD<0-100> | Displays logs for the specified CPU. |
| event-code *WORD<0–10>* | Specifies a number that precisely identifies the event reported. |
| module *WORD<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, HW, MLT, FILTER, QOS, CLILOG, SW, CPU, IP, VLAN, IPMC, and SNMPLOG. To specify multiple filters, separate each category by the vertical bar (\|), for example, \|FILTER\|QOS. |
| name-of-file *WORD<1-99>* | Displays the valid logs from this file. For example, /intflash/logcopy.txt. You cannot use this command on the current log file, which is the file into which the messages are currently logged. Specify a string length of 1 to 99 characters.<br>If you enable enhanced secure mode, the system encrypts the entire log file. After you use the **`show log file name-of-file WORD<1-99>`** command, the system takes the encrypted log file name as input, then decrypts it, and prints the output to the screen. You can then redirect the decrypted output to a file that you can store onto the flash.<br>If enhanced secure mode is disabled, the system only encrypts the proprietary portion of the log file. |
| save-to-file *WORD<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. |
| severity *WORD<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 *WORD<0–32>* | Specifies the name of a VRF instance to show log messages that only pertain to that VRF. |

# Configuring CLI logging

Use CLI logging to track all CLI commands executed and for fault management purposes. The CLI commands are logged to the system log file as CLILOG module.

## About this task

**Note:**

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

## Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Enable CLI logging:

   `clilog enable`

3. **(Optional)** Disable CLI logging:

   `no clilog enable`

4. Ensure that the configuration is correct:

   `show clilog`

5. View the CLI log:

   `show logging file module clilog`

### Example

Enable CLI logging, and view the CLI log:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#clilog enable
Switch:1(config)#show logging file module clilog
CP1  [02/13/13 17:27:25.956] 0x002c0600 00000000 GlobalRouter CLILOG INFO     1 CONSOLE
rwa show snmp-server host
CP1  [02/13/13 17:28:10.100] 0x002c0600 00000000 GlobalRouter CLILOG INFO     2 CONSOLE
rwa show snmp-server notif
CP1  [02/13/13 17:28:45.732] 0x002c0600 00000000 GlobalRouter CLILOG INFO     3 CONSOLE
rwa snmp-server force-trap
CP1  [02/13/13 17:29:30.628] 0x002c0600 00000000 GlobalRouter CLILOG INFO     4 CONSOLE
rwa show logging file modug
CP1  [02/14/13 19:39:11.648] 0x002c0600 00000000 GlobalRouter CLILOG INFO     5 CONSOLE
rwa ena
CP1  [02/14/13 19:39:13.420] 0x002c0600 00000000 GlobalRouter CLILOG INFO     6 CONSOLE
rwa conf t
CP1  [02/14/13 19:49:21.044] 0x002c0600 00000000 GlobalRouter CLILOG INFO     7 CONSOLE
rwa filter acl 2 enable
CP1  [02/14/13 19:50:08.540] 0x002c0600 00000000 GlobalRouter CLILOG INFO     8 CONSOLE
rwa filter acl 2 type inpo1
CP1  [02/14/13 19:50:38.444] 0x002c0600 00000000 GlobalRouter CLILOG INFO     9 CONSOLE
rwa filter acl 2 type inpoe
CP1  [02/14/13 19:50:52.968] 0x002c0600 00000000 GlobalRouter CLILOG INFO    10 CONSOLE
rwa filter acl enable 2
CP1  [02/14/13 19:51:08.908] 0x002c0600 00000000 GlobalRouter CLILOG INFO    11 CONSOLE
rwa filter acl 2 enable
CP1  [02/15/13 06:50:25.972] 0x002c0600 00000000 GlobalRouter CLILOG INFO    14 CONSOLE
rwa ena
CP1  [02/15/13 06:50:30.288] 0x002c0600 00000000 GlobalRouter CLILOG INFO    15 CONSOLE
rwa conf t
CP1  [02/15/13 06:50:39.412] 0x002c0600 00000000 GlobalRouter CLILOG INFO    16 CONSOLE
rwa show vlan basic
CP1  [02/15/13 06:51:09.488] 0x002c0600 00000000 GlobalRouter CLILOG INFO    17 CONSOLE
rwa show isis spbm
CP1  [02/15/13 06:56:00.992] 0x002c0600 00000000 GlobalRouter CLILOG INFO    19 CONSOLE
rwa spbm 23 b-vid 2 primar1
```

```
CP1  [02/15/13 06:56:59.092] 0x002c0600 00000000 GlobalRouter CLILOG INFO    20 CONSOLE
rwa show isis
CP1  [02/15/13 07:10:54.928] 0x002c0600 00000000 GlobalRouter CLILOG INFO    21 CONSOLE
rwa show isis interface
CP1  [02/15/13 07:12:33.404] 0x002c0600 00000000 GlobalRouter CLILOG INFO    22 CONSOLE
rwa show isis spbm
CP1  [02/15/13 07:45:28.596] 0x002c0600 00000000 GlobalRouter CLILOG INFO    23 CONSOLE
rwa ena
CP1  [02/15/13 07:45:30.236] 0x002c0600 00000000 GlobalRouter CLILOG INFO    24 CONSOLE
rwa conf t
CP1  [02/15/13 07:46:29.456] 0x002c0600 00000000 GlobalRouter CLILOG INFO    25 CONSOLE
rwa interface gigabitEther0
CP1  [02/15/13 07:47:28.476] 0x002c0600 00000000 GlobalRouter CLILOG INFO    26 CONSOLE
rwa encapsulation dot1q

--More-- (q = quit)
```

## Variable definitions

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

| Variable | Value |
|---|---|
| enable | Activates CLI logging. To disable, use the `no clilog enable` command. |

# Configuring email notification

Configure the SMTP feature to generate email notifications for component failures, critical conditions, or general system health status.

### About this task

The SMTP feature is disabled by default.

### Before you begin

- To identify the SMTP server by hostname, you must first configure a DNS client on the switch. For more information about how to configure a DNS client, see *Administering*.

### Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the TCP port the client uses to open a connection with the SMTP server:

   ```
   smtp port <1-65535>
   ```

> **Note:**
>
> The port you specify must match the port that the SMTP server uses.

3. Configure email recipients:

   `smtp receiver-email add WORD<3-1274>`

   `smtp receiver-email remove WORD<3-1274>`

   > **Note:**
   >
   > You must configure at least one recipient.

4. Configure the SMTP server hostname or IPv4 address:

   `smtp server WORD<1-256>`

5. **(Optional)** Configure a sender email address:

   `smtp sender-email WORD<3-254>`

6. **(Optional)** Add or remove log events to the default list that generate email notification:

   `smtp event-id add WORD<1-1100>`

   `smtp event-id remove WORD<1-1100>`

7. **(Optional)** Configure the status update interval:

   `smtp status-send-timer <0 | 30-43200>`

8. Enable the SMTP client:

   `smtp enable`

9. Verify the configuration:

   `show smtp [event-id]`

### Example

Configure the SMTP client to use TCP port 26 to communicate with an SMTP server that is using port 26. Add two receiver email addresses, and configure the server information using an IPv4 address. Finally, enable the SMTP feature, and then verify the configuration.

```
LabSwitch:1>enable
LabSwitch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
LabSwitch:1(config)#smtp port 26
LabSwitch:1(config)#smtp receiver-email add test1@default.com,test2@default.com
LabSwitch:1(config)#smtp server 192.0.2.1
LabSwitch:1(config)#smtp enable
LabSwitch:1(config)#show smtp
================================================================================
                                SMTP Information
================================================================================
        SMTP Status:  Enabled
     Server Address:  192.0.2.1
        Server Port:  26
  Status send Timer:  30 (seconds)
       Sender Email:  LabSwitch@default.com
```

```
    Receiver Emails:  test1@default.com
                      test2@default.com
```

Add an event ID to the list for which the switch sends email notification on a log event. Verify the configuration.

```
LabSwitch:1(config)#smtp event-id add 0x0000c5ec
LabSwitch:1(config)#show smtp event-id
================================================================================
                           SMTP Event IDs Information
================================================================================
Log Event IDs: (total: 51)
           0x000045e3,0x00004602,0x00004603,0x0000c5ec,0x000106ce,0x000106cf
           0x000106d0,0x000106d1,0x000106d2,0x000106d4,0x000106d8,0x000106d9
           0x000106da,0x000106f8,0x000106f9,0x000106fb,0x00010775,0x00010776
           0x000107f5,0x000107f6,0x000305c8,0x000305ca,0x000305f1,0x00030637
           0x00040506,0x00040507,0x00040508,0x00040509,0x000646da,0x000646db
           0x00088524,0x000d8580,0x000d8586,0x000d8589,0x000e4600,0x000e4601
           0x000e4602,0x000e4603,0x000e4604,0x000e4605,0x000e4606,0x000e4607
           0x000e4608,0x000e4609,0x001985a0,0x00210587,0x00210588,0x00210595
           0x00210596,0x0027458a,0x0027458d

Default Event IDs: (total: 50)
           0x000045e3,0x00004602,0x00004603,0x000106ce,0x000106cf,0x000106d0
           0x000106d1,0x000106d2,0x000106d4,0x000106d8,0x000106d9,0x000106da
           0x000106f8,0x000106f9,0x000106fb,0x00010775,0x00010776,0x000107f5
           0x000107f6,0x000305c8,0x000305ca,0x000305f1,0x00030637,0x00040506
           0x00040507,0x00040508,0x00040509,0x000646da,0x000646db,0x00088524
           0x000d8580,0x000d8586,0x000d8589,0x000e4600,0x000e4601,0x000e4602
           0x000e4603,0x000e4604,0x000e4605,0x000e4606,0x000e4607,0x000e4608

           0x000e4609,0x001985a0,0x00210587,0x00210588,0x00210595,0x00210596
           0x0027458a,0x0027458d

Remove From Default: (total: 0)

Add List: (total: 1)
           0x0000c5ec
```

## Variable definitions

Use the data in the following table to use the **`smtp port`** command.

| Variable | Value |
|---|---|
| <1–65535> | Specifies the TCP port on the switch that the SMTP client uses to communicate with the SMTP server. The default value is 25.<br>**Note:**<br>You must disable the SMTP feature before you can change an existing SMTP port configuration.<br>The port you specify must match the port that the SMTP server uses. |

Use the data in the following table to use the **`smtp receiver-email`** command.

| **Variable** | **Value** |
|---|---|
| add *WORD<3-1274>* | Adds an email address to the recipient list. The recipients receive the email notification generated by the switch.<br>You must configure at least one email recipient and can create a maximum of five email recipients. You can specify multiple addresses in a single command by separating them with a comma.<br>You cannot use quotation marks (“) or commas (,) in email addresses. Other restrictions for the format of the email address follow RFC 5321.<br>The maximum length for the address is 254 characters. |
| remove *WORD<3-1274>* | Removes an email address from the recipient list. The recipients receive the email notification generated by the switch. You can specify multiple addresses in a single command by separating them with a comma.<br>You cannot use quotation marks (“) or commas (,) in email addresses. Other restrictions for the format of the email address follow RFC 5321.<br>The maximum length for the address is 254 characters. |

Use the data in the following table to use the **`smtp server`** command.

| **Variable** | **Value** |
|---|---|
| *WORD<1-256>* | Specifies the SMTP server address. You can use either a hostname or IPv4 address. If you use a hostname, you must configure the DNS client on the switch. |

Use the data in the following table to use the **`smtp sender-email`** command.

| **Variable** | **Value** |
|---|---|
| *WORD<3-254>* | Specifies the email address that appears in the From field of the message that the switch generates. By default, the switch uses <*SystemName*>@default.com. |

Use the data in the following table to use the **`smtp event-id`** command.

| Variable | Value |
|---|---|
| add *WORD<1-1100>* | Adds a log event to the list of events that generate email notification. You can specify multiple event IDs in a single command by separating them with a comma.<br>The event ID can be up to 10 digits in hexadecimal format. |
| remove *WORD<1-1100>* | Removes a log event from the list of events that generate email notification. You can specify multiple event IDs in a single command by separating them with a comma.<br>The event ID can be up to 10 digits in hexadecimal format. |

Use the data in the following table to use the **`smtp status-send-timer`** command.

| Variable | Value |
|---|---|
| *<0 \| 30-43200>* | Specifies the interval, in seconds, at which the switch sends status information. The default is 30 seconds. A value of 0 means the switch does not send status information. |

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

| Variable | Value |
|---|---|
| event-id | Shows a list of active event IDs for which the switch generates email notification. The command output includes the default list of IDs and IDs you specifically add or remove. |

# Chapter 10: Log configuration using EDM

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

## Configuring the system log

### About this task

Configure the system log to track all user activity on the device. The system log can send messages of up to 10 syslog hosts.

### Procedure

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

## System Log field descriptions

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

| 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. |
| **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. |

*Table continues…*

| Name | Description |
|---|---|
| **OperState** | Specifies the operational state of the syslog service. The default is active. |
| **Header** | Specifies the IP header in syslog packets to circuitlessIP or default.<br>• 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.<br>• 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.<br>The default value is default. |

# Configuring the system log table

## About this task

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

You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration except in the following case. When you configure the system log table, under the **System Log Table** tab, you must select **ipv4** or **ipv6**, in the **AddressType** box. The **Address** box supports both IPv4 and IPv6 addresses.

## Procedure

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

# System Log Table field descriptions

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

| Name | Description |
|---|---|
| **Id** | Specifies the ID for the syslog host. The range is 1–10. |
| **AddressType** | Specifies if the address is an IPv4 or IPv6 address. |
| **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. The default is disabled. |
| **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\|warning\|error\|fatal. |
| **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. |
| **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 notice. |

# Configuring email notification

Configure the SMTP feature to generate email notifications for component failures, critical conditions, or general system health status.

## About this task

The SMTP feature is disabled by default.

## Before you begin

- To identify the SMTP server by hostname, you must first configure a DNS client on the switch. For more information about how to configure a DNS client, see *Administering*.

## Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Edit**.
2. Click **SMTP**.
3. Click the **Globals** tab.

4. In the **ServerAddress** field, configure the SMTP server address.
5. In the **ReceiverEmailsList** field, add email recipients.

   **Note:**

   You must configure at least one recipient.
6. In the **Port** field, configure the TCP port the client uses to open a connection with the SMTP server.
7. **(Optional)** In the **SenderEmail** field, configure a sender email address to use an address other than the default.
8. **(Optional)** In the **LogEventIds** field, add or remove log events to the default list that generate email notification.
9. **(Optional)** In the **SystemStatusSendTimer** field, configure the status update interval.
10. Click **enable** to enable the SMTP client.
11. Click **Apply**.

## Globals field descriptions

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

| Name | Description |
|---|---|
| **ServerAddressType** | Specifies the type of server address as either an IPv4 address or a hostname. If you use a hostname, you must configure the DNS client on the switch. |
| **ServerAddress** | Specifies the SMTP server address. You can use either a hostname or IPv4 address. If you use a hostname, you must configure the DNS client on the switch. |
| **ReceiverEmailsList** | Specifies the recipient list. The recipients receive the email notification generated by the switch.<br>You must configure at least one email recipient and can create a maximum of five email recipients. You can specify multiple addresses in a single command by separating them with a comma.<br>You cannot use quotation marks (“) or commas (,) in email addresses. Other restrictions for the format of the email address follow RFC5321.<br>The maximum length for the address is 254 characters. |
| **NumOfEmails** | Shows the total number of addresses in **ReceiverEmailsList**. |

*Table continues…*

| Name | Description |
|---|---|
| **SenderEmail** | Specifies the email address that appears in the From field of the message that the switch generates. By default, the switch uses *SystemName*@default.com. |
| **Port** | Specifies the TCP port on the switch that the SMTP client uses to communicate with the SMTP server. The default value is 25.<br>**Note:**<br>You must disable the SMTP feature before you can change an existing SMTP port configuration.<br>The port you specify must match the port that the SMTP server uses. |
| **SystemStatusSendTimer** | Specifies the interval, in seconds, at which the switch sends status information. The default is 30 seconds. A value of 0 means the switch does not send status information. |
| **Enable** | Enables or disables the SMTP feature. Be default, SMTP is disabled. |
| **LogEventIds** | Specifies the list of events that generate email notification. You can specify multiple event IDs in a single command by separating them with a comma.<br>The event ID can be up to 10 digits in hexadecimal format. |
| **NumOfEventIds** | Shows the total number of IDs in **LogEventIds**. |
| **DefaultLogEventIds** | Shows the default list of event IDs that generate email notification. |
| **NumOfDefaultEventIds** | Shows the total number of IDs in **DefaultLogEventIds**. |

# Chapter 11: SNMP trap configuration using CLI

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 *Configuring Security*.

## Configuring an SNMP host

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. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure an SNMPv1 host:

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

3. Configure an SNMPv2c host:

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

4. Configure an SNMPv3 host:

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

5. Ensure that the configuration is correct:

   ```
   show snmp-server host
   ```

**Example**

Configure the target table entry. Configure an SNMPv3 host.

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

| Variable | Value |
|---|---|
| inform [timeout <1-2147483647>] [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:<br>1. timeout <1-2147483647> specifies the timeout value in seconds with a range of 0–214748364.<br>2. retries <0-255> specifies the retry count value with a range of 0–255.<br>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. |

# Configuring an SNMP notify filter table

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

### Before you begin

- For more information about the notify filter table, see RFC3413.

### Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Create a new notify filter table:

   `snmp-server notify-filter` *`WORD<1-32> WORD<1-32>`*

3. Ensure that the configuration is correct:

   `show snmp-server notify-filter`

**Example**

```
Switch(config)# snmp-server notify-filter profile3 99.3.6.1.6.3.1.1.4.1
```

```
Switch(config)#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.

| Variable | Value |
|---|---|
| *WORD<1-32> WORD<1-32>* | Creates a notify filter table.<br>The first instance of *WORD<1-32>* specifies the name of the filter profile with a string length of 1–32.<br>The second instance of *WORD<1-32>* identifies the filter subtree OID with a string length of 1–32.<br>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.<br>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. |

## Configuring SNMP interfaces

Configure an interface to send SNMP traps. If the switch has multiple interfaces, configure the IP interface from which the SNMP traps originate.

### Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the destination and source IP addresses for SNMP traps:

   ```
   snmp-server sender-ip {A.B.C.D} {A.B.C.D}
   ```

3. If required, send the source address (sender IP) as the sender network in the notification message:

   ```
   snmp-server force-trap-sender enable
   ```

4. If required, force the SNMP and IP sender flag to use the same value:

   ```
   snmp-server force-iphdr-sender enable
   ```

### Example

```
Switch(config)# snmp-server sender-ip 172.16.120.2 172.16.120.5
```

```
Switch(config)# no snmp-server force-iphdr-sender enable
```

## Variable definitions

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

| 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. 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. |

*Table continues…*

| Variable | Value |
|---|---|
|  | 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

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

## Before you begin

You must configure and enable the syslog server.

## About this task

**Note:**

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

## Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable SNMP trap logging:

   ```
   snmplog enable
   ```

3. **(Optional)** Disable SNMP trap logging:

   ```
   no snmplog enable
   ```

4. View the contents of the SNMP log:

   ```
   show logging file module snmplog
   ```

## Example

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

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#snmplog enable
Switch:1(config-app)#show logging file module snmp
CP1  [02/06/15 22:39:58.530:UTC] 0x00004595 00000000 GlobalRouter SNMP INFO Boot
ed with file
CP1  [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=1 AdminStatus=1 OperStatus=1)
```

```
CP1  [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=2 AdminStatus=1 OperStatus=1)
CP1  [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=3 AdminStatus=1 OperStatus=1)
CP1  [02/06/15 22:40:45.839:UTC] 0x000045e5 00400005 DYNAMIC SET GlobalRouter SN
MP INFO Sending Cold-Start Trap
```

# Variable definitions

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

| Variable | Value |
|---|---|
| enable | Enables the logging of traps.<br>Use the command `no snmplog enable` to disable the logging of traps. |

# Chapter 12: SNMP trap configuration using EDM

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

For information about how to configure SNMP community strings and related topics, see *Configuring Security*.

## Configuring an SNMP host target address

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

### Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **Target Table**.
3. In the **Target Table** tab, click **Insert**.
4. In the **Name** box, type a unique identifier.
5. In the **TDomain** box, select the transport type of the address.
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.<br>**ipv4Tdomain** specifies the transport type of address is an IPv4 address. |
| **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.<br>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.<br>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 pane, expand the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **Target Table**.
3. Click the **Target Params Table** tab.
4. Click **Insert**.
5. In the **Name** box, type a target table name.
6. From the **MPModel** options, select an SNMP version.
7. From the **Security Model** options, select the security model.
8. In the **SecurityName** box, type `readview` or `writeview`.
9. From the **SecurityLevel** options, select the security level for the table.
10. Click **Insert**.

## Target Params Table field descriptions

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

| 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 inconsistentValue error if you try to configure this variable to a value for a security model that the implementation does not support. |
| **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 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 pane, expand the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **Notify Table**.
3. Click the **Notify Filter Table** tab.
4. Click **Insert**.
5. In the **NotifyFilterProfileName** box, type a name for the notify filter profile.
6. In the **Subtree** box, type subtree location information in x.x.x.x.x.x.x.x.x.x. format.
7. In the **Mask** box, type the mask location in hex string format.
8. From the **Type** options, select **included** or **excluded**.
9. Click **Insert**.

## Notify Filter Table field descriptions

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

| 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 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. The default is included. |

# 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 pane, expand the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **Notify Table**.

3. Click the **Notify Filter Profile Table** tab.
4. Click **Insert**.
5. In the **TargetParamsName** box, type a name for the target parameters.
6. In the **NotifyFilterProfileName** box, type a name for the notify filter profile.
7. Click **Insert**.

## Notify Filter Profile Table field descriptions

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

| Name | Description |
|---|---|
| **TargetParamsName** | Specifies the unique identifier associated with this entry. |
| **NotifyFilterProfileName** | Specifies the name of the filter profile to use to generate notifications. |

# Enabling authentication traps

### About this task

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

### Procedure

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

## Error field descriptions

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

| Name | Description |
|---|---|
| **AuthenticationTraps** | Enables or disables the sending of traps after an error occurs. The default is disabled. |
| **LastErrorCode** | Specifies the last reported error code. |
| **LastErrorSeverity** | Specifies the last reported error severity: |

*Table continues…*

| Name | Description |
|---|---|
| | 0= Informative Information<br>1= Warning Condition<br>2= Error Condition<br>3= Manufacturing Information<br>4= Fatal Condition |

# 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.

**bit error rate (BER)**
The ratio of the number of bit errors to the total number of bits transmitted in a specific 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.

**command line interface (CLI)**
A textual user interface. When you use CLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.

**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 certain 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 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 the device uses 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)**
QoS features reserve resources in a congested network, allowing you to configure a higher priority for certain devices. For example, you can configure a higher priority for IP deskphones, which need a fixed bit rate and split the remaining bandwidth between data connections if calls in the network are more 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 Network Monitoring (RMON)**
Creates and displays alarms for user-defined events, gathers cumulative statistics for Ethernet interfaces, and tracks statistical history for Ethernet interfaces.

**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. You often use RIP as a very simple interior gateway protocol (IGP) within small networks.

**shortest path first (SPF)**
A class of routing protocols that use Djikstra'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)**

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 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.

**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.

**virtual router**

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.