The bridge to possible

# Smart Monitoring and Alerting

## Cisco MDS 9000 Series Switches

# Contents

## Introduction

The Cisco MDS 9000 series of storage networking switches offer a variety of features designed to monitor fabric health, switch health, hardware components, and multiple counters. Both hardware and software sensors gather real-time metrics and logs, with hardware sensors embedded within all components.

As a progressive step, a complete overhaul has been implemented to unify and simplify the configuration and monitoring across MDS SAN switches, extending from the overall switch down to the individual interfaces or port level. This new unified capability has been introduced as Smart Monitoring and Alerting (SMA).

### Scope

This document provides step-by-step guidance to set up automated monitoring and alerting in a Cisco SAN fabric using the new Smart Monitoring and Alerting feature made production-ready in MDS NX-OS release 9.4(4). The primary audience is users of Cisco MDS 9000 switches, and NX-OS.

The command outputs, and capabilities that are described in this document are based on Cisco NX-OS 9.4(4) for MDS 9000 switches. Although the procedures and recommendations that are outlined in this document apply to MDS NX-OS releases from 9.4(1) onwards, we recommend referring to the release notes and the configuration guides for up-to-date information. Also, it is an overview document, primarily aimed at new users of SMA. For details on specific topics, please refer to the white papers and configuration guides that are listed in the references section.

## Existing Monitoring Mechanisms in a Cisco SAN Fabric

Before getting into the details of the new Smart Monitoring and Alerting feature, let’s look at the existing monitoring and alerting mechanisms in a Cisco SAN fabric that are built using MDS 9000 switches. There are three features which are used to track and monitor MDS switch health. These tools describe the counters, the techniques employed to monitor them, the monitoring capabilities available, and the configurable threshold limits for the counters, etc.

### Remote Monitoring

Remote Monitoring (RMON) is an IETF SNMP standard specification that enables network agents and console systems to exchange monitoring data. In MDS NX-OS, RMON provides support for alarms, events, and logs, thereby enabling systematic monitoring of devices.

An alarm observes a designated MIB object at specified intervals, and each alarm can be associated with an event, such as the generation of an SNMP notification or the creation of a system log entry. Notably, RMON functionality is disabled by default.

### Port Monitoring

Port Monitor (PMON) is a monitoring capability designed to track critical counters associated with physical ports and to notify external monitoring systems of potential anomalies.

This feature provides flexibility by allowing users to define and customize policies for monitoring both core and edge logical-type ports. PMON can be used to generate events and alarms on the ports.

### Embedded Event Manager

Cisco Embedded Event Manager (EEM) is an integral NX-OS component designed to monitor and respond to system events on the switch. Beyond event detection, EEM enables automated actions that assist in troubleshooting and maintaining system stability. Event Manager policies are configured on the supervisor module and can extend monitoring to parameters on additional modules and line cards.

An EEM policy operates by waiting for a predefined event to occur. When the event is triggered, the policy can execute a range of programmed actions, such as generating a syslog message, reloading the supervisor, sending an SNMP trap, or executing a VSH CLI command. This functionality provides administrators with a flexible and proactive framework for event handling and automation.

### Cisco Nexus Dashboard

While Cisco NX-OS provides management, monitoring, and alerting capabilities at the individual switch level, Cisco Nexus Dashboard extends these functions across multiple switches and fabrics. It features an intuitive, HTML5-based web interface for comprehensive visibility into the underlying SAN fabric.

Cisco Nexus Dashboard ingests hardware and software sensor data collected by Cisco MDS NX-OS firmware running on Cisco MDS 9000 switches, enabling the analysis of long-term trends and seasonal patterns. In addition, it receives event notifications generated by the switches and can forward these alerts to compatible third-party applications.

## Smart Monitoring and Alerting (SMA)

Smart Monitoring and Alerting is a feature that enables real-time monitoring and detection of important events or conditions which include various port level metrics like Fibre Channel primitive sequences, congestion signals and notifications, scalability limits for FCID, zone, etc. It proactively recognizes deviations from normal or expected behavior, facilitating timely alerts and enabling prompt responses.

### Benefits of Smart Monitoring and Alerting

This new monitoring feature brings multiple benefits for users. Some of them are listed below.

- **Unified Monitoring Infrastructure**: A centralized platform to configure various monitoring settings on the switch and view the overall system health.
- **Per Interface configuration**: SMA allows monitoring at the granularity of an interface. Interfaces can be categorized into different groups based on logical-type (edge/core/all) or a group of interfaces.
- **Port and Protocol counters**: SMA provides ease of use by grouping different types of entities monitored under the same policy.
- **Customizable Thresholds and Priorities**: SMA allows users to set personalized thresholds, priorities, and conditions based on their specific needs. This enables tailored monitoring and alerting, such as per-interface configurations, guided by user expertise.
- **Real-Time Detection**: SMA continuously analyzes data streams and system attributes for errors and anomalies in counters.
- **Proactive Alerts**: Upon detecting significant events, SMA generates notifications or alerts and triggers appropriate actions. These alerts can be delivered as syslogs, SNMP notifications, or Onboard Failure Logging (OBFL) logs.
- **Event History and Reporting**: SMA keeps a record of past events and provides comprehensive reports on overall system health.

### Supported MDS Hardware

The Smart Monitoring and Alerting feature is supported on the below MDS platforms:

- Cisco MDS 9700 with 64 Gbps, 32 Gbps Fibre Channel modules and 24/10 SAN Extension module
- Cisco MDS 9396V 64 Gbps 96-port Fibre Channel switch

- Cisco MDS 9148V 64 Gbps 48-port Fibre Channel switch
- Cisco MDS 9124V 64 Gbps 24-port Fibre Channel switch
- Cisco MDS 9396T 32 Gbps 96-port Fibre Channel switch
- Cisco MDS 9148T 32 Gbps 48-port Fibre Channel switch
- Cisco MDS 9132T 32 Gbps 32-port Fibre Channel switch
- Cisco MDS 9220i switch

## Core Components of SMA

This section outlines the core components or building blocks of the Smart Monitoring and Alerting feature. A clear understanding of these components is essential for configuring the feature on the MDS 9000 switches.

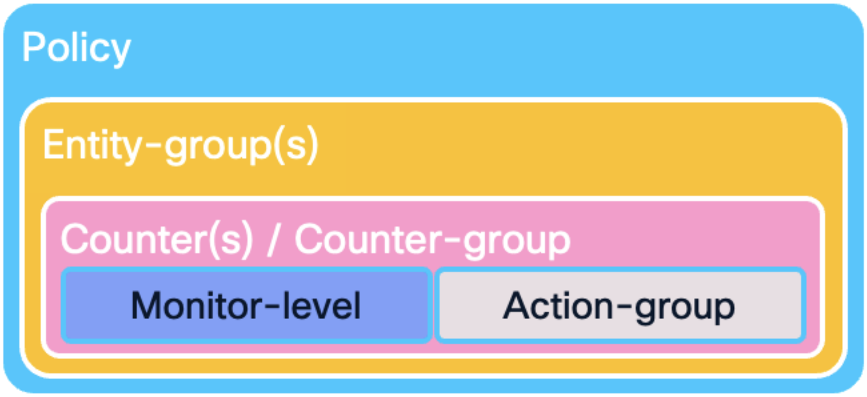


**Figure 1. Core Components of SMA**

### Policy

An SMA policy is composed of entity groups categorized by entity type. Within a given entity type, priority is determined by the order in which the entity groups are defined, with those appearing earlier in the policy assigned higher precedence. There is one default SMA policy, and the feature allows four user-defined policies.

#### Default SMA Policy

SMA maintains a system-defined default policy that incorporates supported counters. In MDS NX-OS version 9.4(4), this policy includes protocol counters and Port Monitoring (PMON) counters. In the upcoming firmware versions, the default policy will be enhanced to incorporate additional counters, ensuring broader monitoring coverage. To preserve consistency and reliability, the default policy is not user-editable.

Below is a snippet of the default SMA policy. Note that the policy is not active by default, and the user needs to activate it.

```
switch# show sma policy name default

Policy: default
Class:  system
Status: not active

Entity group:  eg-switch (system)
Entity type:   switch
---------------------------------------------------------------------------------------------------------------
                               | Period    |           Threshold          |
Counter                        | seconds   | Warning  | Alarm     | Falling  | Action group name (class)
---------------------------------------------------------------------------------------------------------------
max-fcns-entries-per-switch    |       na |      90% |      95% |      85% | ag-syslog-warning (system)
max-zone-members-per-switch    |       na |      90% |      95% |      85% | ag-syslog-warning (system)
max-zonesets-per-switch        |       na |      90% |      95% |      85% | ag-syslog-warning (system)
zone-member-ratio              |       na |       na |      100 |       na | ag-syslog-warning (system)
max-zone-dbsize-per-vsan       |       na |      80% |      90% |      75% | ag-syslog-warning (system)
max-zones-per-switch           |       na |      90% |      95% |      85% | ag-syslog-warning (system)
max-fcids-per-switch           |       na |      90% |      95% |      85% | ag-syslog-warning (system)
max-fcids-per-interface        |       na |      90% |      95% |      85% | ag-syslog-warning (system)

Entity group:  eg-fcport-edge (system)
Entity type:   fc-port
---------------------------------------------------------------------------------------------------------------
                               | Period    |           Threshold          |
Counter                        | seconds   | Warning  | Alarm     | Falling  | Action group name (class)
---------------------------------------------------------------------------------------------------------------
tx-overutilization             |       10 |   50@80% |   80@80% |   30@80% | ag-fpin-congestion-signals (system)
tx-wait                        |        1 |      20% |      30% |       0% | ag-fpin-congestion-signals (system)
rx-invalid-words               |       60 |        2 |        5 |        0 | ag-fpin-link-integrity (system)
rx-invalid-crc                 |       60 |        1 |        2 |        0 | ag-fpin-link-integrity (system)
credit-loss-recovery           |       10 |        1 |        2 |        0 | ag-error-disable (system)

Entity group:  eg-fcport-all (system)
Entity type:   fc-port
---------------------------------------------------------------------------------------------------------------
                               | Period    |           Threshold          |
Counter                        | seconds   | Warning  | Alarm     | Falling  | Action group name (class)
---------------------------------------------------------------------------------------------------------------
tx-wait                        |        1 |      20% |      30% |       0% | ag-syslog-trap-error (system)
tx-discards                    |       60 |        1 |        2 |        0 | ag-syslog-trap-error (system)
tx-datarate-burst              |       10 |    4@80% |    6@80% |    0@80% | ag-syslog-trap-obfl (system)
tx-credit-not-available        |        1 |      10% |      20% |       0% | ag-syslog-trap-warning (system)
tx-timeout-discards            |       60 |        1 |        2 |        0 | ag-syslog-trap-error (system)
sync-loss                      |       60 |        2 |        5 |        0 | ag-error-disable (system)
signal-loss                    |       60 |        2 |        5 |        0 | ag-error-disable (system)
rx-datarate-burst              |       10 |    4@80% |    6@80% |    0@80% | ag-syslog-trap-obfl (system)
rx-lr                          |       60 |        1 |        2 |        0 | ag-syslog-trap-critical (system)
link-loss                      |       60 |        2 |        5 |        0 | ag-error-disable (system)
rx-invalid-words               |       60 |        2 |        5 |        0 | ag-syslog-trap-error (system)
rx-invalid-crc                 |       60 |        1 |        2 |        0 | ag-syslog-error (system)
rx-input-errors                |       60 |        1 |        2 |        0 | ag-syslog-trap-error (system)
credit-loss-recovery           |       10 |        1 |        2 |        0 | ag-syslog-trap-critical (system)
```

### User-defined SMA Policy

Users can create a custom, user-defined policy either by cloning the system-defined default policy or by authoring a new policy from the ground up. In MDS NX-OS version 9.4(4), support is limited to four user-defined policies.

## Entity-group

An entity group is a collection of entities defined by an entity type and, optionally, by sub-entity types. A set of predefined entity groups is available, and users also have the flexibility to create custom groups as needed. Predefined entity groups, such as eg-fcport-all, eg-fcport-edge, and eg-fcport-core, are used for configuring port counters. Similarly, the predefined entity group eg-switch is used for configuring protocol counters.

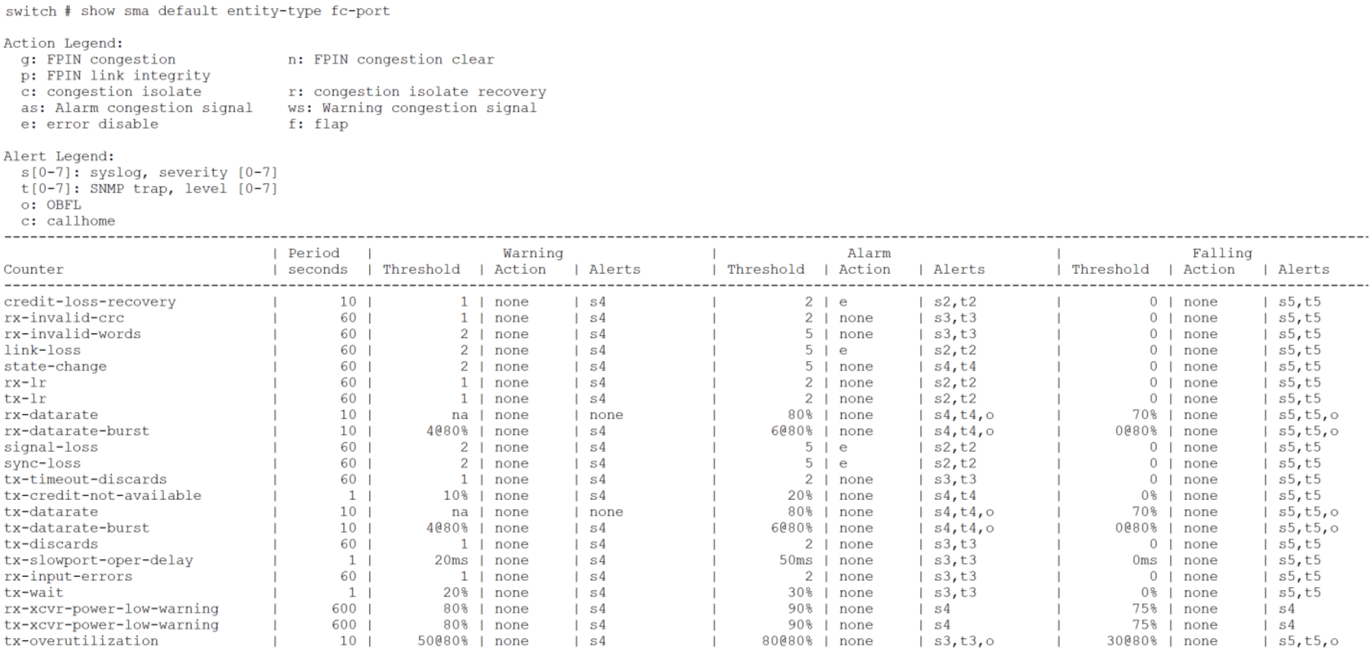
Below snippet lists the four-default entity-groups – eg-fcport-all, eg-fcport-core, eg-fcport-edge and eg-switch.

```
switch# show sma entity-group class system

Entity group:               eg-fcport-all
    Class:                  system
    Entity type:            fc-port
    Subentity type:         all
    Configured entity list: fc1/1-48,fc3/1-48,fc4/1-48,fc7/1-48,fc8/1-48,fc9/1-48,fc11/1-48

Entity group:               eg-fcport-core
    Class:                  system
    Entity type:            fc-port
    Subentity type:         core
    Configured entity list: fc1/4-10,fc1/17,fc1/20,fc1/28,fc1/33,fc1/37-39,
                            fc3/1-2,fc3/7,fc3/15,fc4/1-2,fc4/7,fc4/15,fc7/1-3,
                            fc9/5-8,fc10/40-48

Entity group:               eg-fcport-edge
    Class:                  system
    Entity type:            fc-port
    Subentity type:         edge
    Configured entity list: fc4/42,fc9/1-6,fc9/17-22,fc9/33-38,fc10/39,fc11/3-8

Entity group:               eg-switch
    Class:                  system
    Entity type:            switch
    Subentity type:         -
    Configured entity list: switch
switch#
```

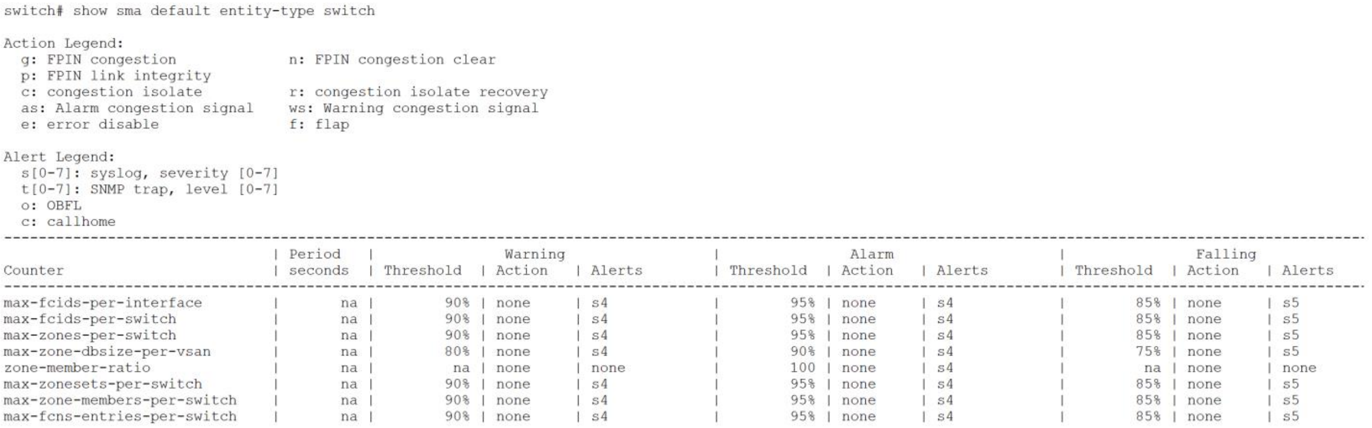
### Entity-type

An Entity-type defines an object which needs to be monitored. This is where the SMA policy will be applied. fc-port and switch are the currently supported entity-types. Under the fc-port entity-type, users have an option to configure the subentity-types – interface, core, edge or all.

Below snippet lists the two, default, entity-types – fc-port and switch.



```
switch # show sma default entity-type fc-port

Action Legend:
  g: FPIN congestion            n: FPIN congestion clear
  p: FPIN link integrity
  c: congestion isolate         r: congestion isolate recovery
  as: Alarm congestion signal   ws: Warning congestion signal
  e: error disable              f: flap

Alert Legend:
  s[0-7]: syslog, severity [0-7]
  t[0-7]: SNMP trap, level [0-7]
  o: OBFL
  c: callhome
----------------------------------------------------------------------------------------------------------------------------------------------
                                | Period  |              Warning                |                Alarm                |             Falling
Counter                         | seconds | Threshold   | Action   | Alerts     | Threshold   | Action   | Alerts     | Threshold  | Action   | Alerts
----------------------------------------------------------------------------------------------------------------------------------------------
credit-loss-recovery            |      10 |           1 | none     | s4         |           2 | e        | s2,t2      |          0 | none     | s5,t5
rx-invalid-crc                  |      60 |           1 | none     | s4         |           2 | none     | s3,t3      |          0 | none     | s5,t5
rx-invalid-words                |      60 |           2 | none     | s4         |           5 | none     | s3,t3      |          0 | none     | s5,t5
link-loss                       |      60 |           2 | none     | s4         |           5 | e        | s2,t2      |          0 | none     | s5,t5
state-change                    |      60 |           2 | none     | s4         |           5 | none     | s4,t4      |          0 | none     | s5,t5
rx-lr                           |      60 |           1 | none     | s4         |           2 | none     | s2,t2      |          0 | none     | s5,t5
tx-lr                           |      60 |           1 | none     | s4         |           2 | none     | s2,t2      |          0 | none     | s5,t5
rx-datarate                     |      10 |          na | none     | none       |         80% | none     | s4,t4,o    |        70% | none     | s5,t5,o
rx-datarate-burst               |      10 |       4@80% | none     | s4         |       6@80% | none     | s4,t4,o    |      0@80% | none     | s5,t5,o
signal-loss                     |      60 |           2 | none     | s4         |           5 | e        | s2,t2      |          0 | none     | s5,t5
sync-loss                       |      60 |           2 | none     | s4         |           5 | e        | s2,t2      |          0 | none     | s5,t5
tx-timeout-discards             |      60 |           1 | none     | s4         |           2 | none     | s3,t3      |          0 | none     | s5,t5
tx-credit-not-available         |       1 |         10% | none     | s4         |         20% | none     | s4,t4      |         0% | none     | s5,t5
tx-datarate                     |      10 |          na | none     | none       |         80% | none     | s4,t4,o    |        70% | none     | s5,t5,o
tx-datarate-burst               |      10 |       4@80% | none     | s4         |       6@80% | none     | s4,t4,o    |      0@80% | none     | s5,t5,o
tx-discards                     |      60 |           1 | none     | s4         |           2 | none     | s3,t3      |          0 | none     | s5,t5
tx-slowport-oper-delay          |       1 |        20ms | none     | s4         |        50ms | none     | s3,t3      |        0ms | none     | s5,t5
rx-input-errors                 |      60 |           1 | none     | s4         |           2 | none     | s3,t3      |          0 | none     | s5,t5
tx-wait                         |       1 |         20% | none     | s4         |         30% | none     | s3,t3      |         0% | none     | s5,t5
rx-xcvr-power-low-warning       |     600 |         80% | none     | s4         |         90% | none     | s4         |        75% | none     | s4
tx-xcvr-power-low-warning       |     600 |         80% | none     | s4         |         90% | none     | s4         |        75% | none     | s4
tx-overutilization              |      10 |      50@80% | none     | s4         |      80@80% | none     | s3,t3,o    |     30@80% | none     | s5,t5,o
```



```
switch# show sma default entity-type switch

Action Legend:
  g: FPIN congestion            n: FPIN congestion clear
  p: FPIN link integrity
  c: congestion isolate         r: congestion isolate recovery
  as: Alarm congestion signal   ws: Warning congestion signal
  e: error disable              f: flap

Alert Legend:
  s[0-7]: syslog, severity [0-7]
  t[0-7]: SNMP trap, level [0-7]
  o: OBFL
  c: callhome
----------------------------------------------------------------------------------------------------------------------------------------------
                                | Period  |              Warning                |                Alarm                |             Falling
Counter                         | seconds | Threshold   | Action   | Alerts     | Threshold   | Action   | Alerts     | Threshold  | Action   | Alerts
----------------------------------------------------------------------------------------------------------------------------------------------
max-fcids-per-interface         |      na |         90% | none     | s4         |         95% | none     | s4         |        85% | none     | s5
max-fcids-per-switch            |      na |         90% | none     | s4         |         95% | none     | s4         |        85% | none     | s5
max-zones-per-switch            |      na |         90% | none     | s4         |         95% | none     | s4         |        85% | none     | s5
max-zone-dbsize-per-vsan        |      na |         80% | none     | s4         |         90% | none     | s4         |        75% | none     | s5
zone-member-ratio               |      na |          na | none     | none       |         100 | none     | s4         |         na | none     | none
max-zonesets-per-switch         |      na |         90% | none     | s4         |         95% | none     | s4         |        85% | none     | s5
max-zone-members-per-switch     |      na |         90% | none     | s4         |         95% | none     | s4         |        85% | none     | s5
max-fcns-entries-per-switch     |      na |         90% | none     | s4         |         95% | none     | s4         |        85% | none     | s5
```

## Counter group

Counter groups are used to define consistent or common behavior across a set of counters. A set of predefined counter groups is available for use. Users cannot create custom counter groups.

Users have the option to monitor an individual counter too. In that case, the feature will only allow the actions and monitor level which are applicable for that counter.

Below snippet lists the default counter groups available under SMA. Table 1 lists the counters which constitute the default counter-groups.

```
switch(config)# show sma counter-group name ?
*** No matching command found in current mode, matching in (exec) mode ***
  cg-all                        Configure all port and protocol counters
  cg-congestion                 Show default values for congestion counters group
  cg-core-fcport                Configure counters supported for core fc port
  cg-datarate                   Show default values for datarate counters group
  cg-default-policy-fcport-all  Configure fc port counters part of default policy
  cg-edge-fcport                Configure counters supported for edge fc port
  cg-fpin-congestion-signals    Show default values for fpin-congestion-signals counters group
  cg-link-integrity             Show default values for link integrity counters group
  cg-protocol-all               Show all action groups configured for protocol counters group
  cg-slowdrain                  Show default values for slowdrain counters group
```

### Default Counter groups

**Table 1.** Default Counter-groups under SMA

| Sl No. | Counter-group | Counters |
|---|---|---|
| 1 | cg-default-policy-fcport-all | credit-loss-recovery<br>rx-input-errors<br>rx-invalid-crc<br>rx-invalid-words<br>link-loss<br>rx-lr<br>rx-datarate-burst<br>signal-loss<br>sync-loss<br>tx-timeout-discards<br>tx-credit-not-available<br>tx-datarate-burst<br>tx-discards<br>tx-wait |
| 2 | cg-core-fcport | credit-loss-recovery<br>rx-input-errors<br>rx-invalid-crc<br>rx-invalid-words<br>link-loss<br>rx-lr<br>tx-lr<br>rx-datarate<br>rx-datarate-burst<br>signal-loss<br>state-change<br>sync-loss |

| SI No. | Counter-group | Counters |
|---|---|---|
| | | tx-timeout-discards<br>tx-credit-not-available<br>tx-datarate<br>tx-datarate-burst<br>tx-discards<br>tx-slowport-oper-delay<br>tx-wait<br>rx-xcvr-power-low-warning<br>tx-xcvr-power-low-warning |
| 3 | cg-edge-fcport | credit-loss-recovery<br>rx-input-errors<br>rx-invalid-crc<br>rx-invalid-words<br>link-loss<br>rx-lr<br>tx-lr<br>rx-datarate<br>rx-datarate-burst<br>signal-loss<br>state-change<br>sync-loss<br>tx-timeout-discards<br>tx-credit-not-available<br>tx-datarate<br>tx-datarate-burst<br>tx-discards<br>tx-slowport-oper-delay<br>tx-wait<br>rx-xcvr-power-low-warning<br>tx-xcvr-power-low-warning<br>tx-overutilization |
| 4 | cg-link-integrity | link-loss<br>sync-loss<br>signal-loss<br>rx-invalid-words<br>rx-invalid-crc |
| 5 | cg-datarate | tx-datarate |

| Sl No. | Counter-group | Counters |
|---|---|---|
| | | tx-datarate-burst<br>rx-datarate<br>rx-datarate-burst<br>tx-overutilization |
| 6 | cg-congestion | tx-wait<br>tx-datarate<br>tx-datarate-burst<br>tx-overutilization |
| 7 | cg-slowdrain | tx-credit-not-available<br>credit-loss-recovery<br>tx-wait<br>tx-slowport-oper-delay |
| 8 | cg-fpin-congestion-signals | tx-wait<br>tx-overutilization |
| 9 | cg-protocol-all | max-fcns-entries-per-switch<br>max-fcids-per-switch<br>max-fcids-per-interface<br>max-zone-dbsize-per-vsan<br>zone-member-ratio<br>max-zone-members-per-switch<br>max-zones-per-switch<br>max-zonesets-per-switch |
| 10 | cg-all | All the port and protocol counters |

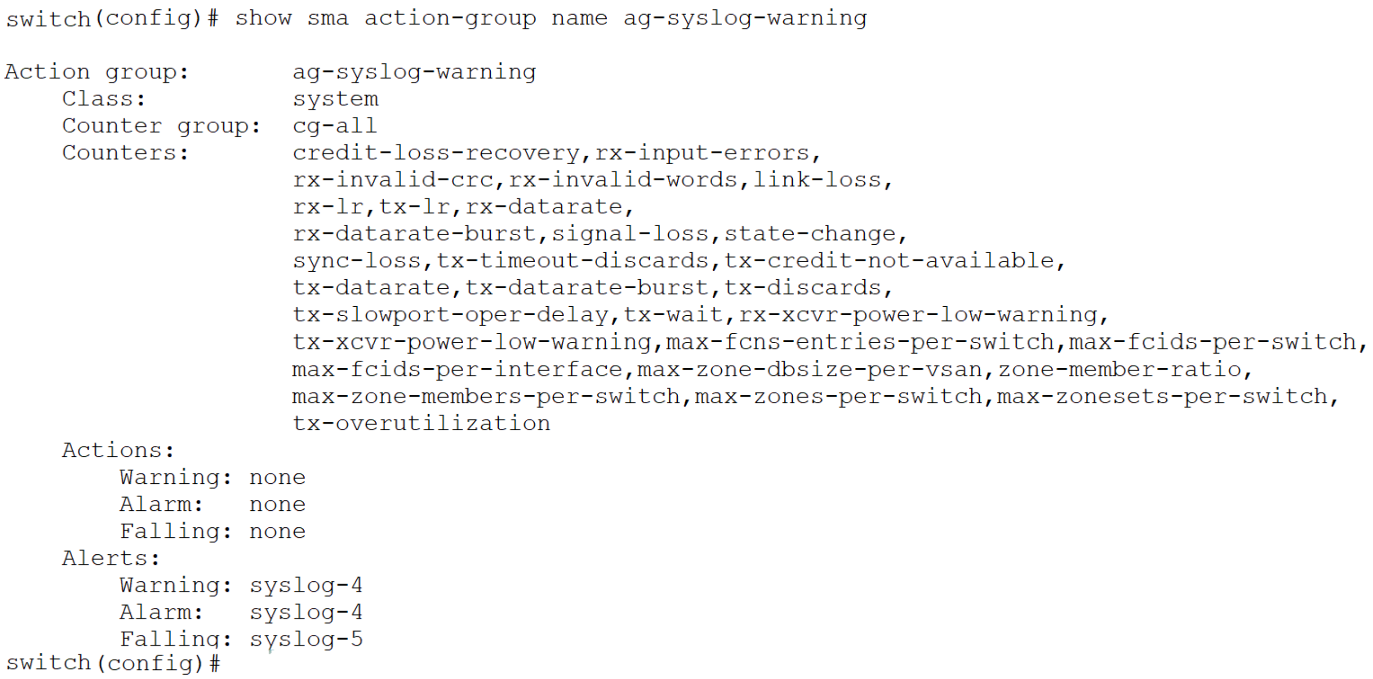
## Monitor level

Monitor levels define the threshold values and sampling periods for different conditions, such as warning, alarm, and falling states. Each counter is assigned default monitor levels appropriate for the counter; however, users have the option to configure custom values as required.

## Action group

Action groups define the alerts and responses/actions associated with various threshold levels. A set of predefined action groups is available, and each counter is assigned a default action group. Users also have the flexibility to create custom action groups as needed. These groups are reusable and can be applied across multiple counters within different entity groups. Some valid actions include flap, error-disable, congestion-signal, FPIN (Fabric Performance Impact Notification), etc. SNMP trap, syslog, OBFL (Onboard Failure Logging) are some alerts.

Below is a snippet for the default action-group: ag-syslog-warning.



```
switch(config)# show sma action-group name ag-syslog-warning

Action group:       ag-syslog-warning
    Class:          system
    Counter group:  cg-all
    Counters:       credit-loss-recovery,rx-input-errors,
                    rx-invalid-crc,rx-invalid-words,link-loss,
                    rx-lr,tx-lr,rx-datarate,
                    rx-datarate-burst,signal-loss,state-change,
                    sync-loss,tx-timeout-discards,tx-credit-not-available,
                    tx-datarate,tx-datarate-burst,tx-discards,
                    tx-slowport-oper-delay,tx-wait,rx-xcvr-power-low-warning,
                    tx-xcvr-power-low-warning,max-fcns-entries-per-switch,max-fcids-per-switch,
                    max-fcids-per-interface,max-zone-dbsize-per-vsan,zone-member-ratio,
                    max-zone-members-per-switch,max-zones-per-switch,max-zonesets-per-switch,
                    tx-overutilization
    Actions:
        Warning: none
        Alarm:   none
        Falling: none
    Alerts:
        Warning: syslog-4
        Alarm:   syslog-4
        Falling: syslog-5
switch(config)#
```

## Priority of Entity-groups

The priority of an entity group within a policy is determined by its position. For a given entity type, groups defined earlier in the policy are assigned higher precedence. When the same entity is included in multiple groups, the configuration associated with the highest-priority entity group is applied to that counter.

In the below example, SMA policy “test-sma” has three entity-groups. One entity-group named eg-switch for protocol counters. And 2 entity-groups, eg-fcport-edge and eg-fcport-all for FC ports. Entity-group eg-fcport-edge includes only those fc ports that are of logical-type edge. For credit-loss-recovery counter, the action is different only for edge ports, so it is added to eg-fcport-edge. Entity-group eg-fcport-all includes all fc ports with a counter-group cg-fcport-all which includes all counters for FC ports.

Since entity-group eg-fcport-edge appears above entity-group eg-fcport-all in the policy, credit-loss-recovery counter config under entity-group eg-fcport-edge take precedence for the edge ports over the same counter configured in eg-fcport-all. As a result, when credit-loss-recovery counter threshold is hit for an edge port or F-port, error-disable action will be applied on that port. Whereas for core ports or E-ports, a syslog warning message will be logged.

```
sma policy name test-sma

    entity-group name eg-switch

        counter-group cg-protocol-all monitor-level default action-group ag-default

    entity-group name eg-fcport-edge

        counter credit-loss-recovery monitor-level default action-group ag-error-disable

    entity-group name eg-fcport-all

        counter-group cg-fcport-all monitor-level default action-group ag-syslog-warning
```

## Creating a User-defined SMA Policy

This section describes the detailed step-by-step procedure for creating a user-defined Smart Monitoring and Alerting (SMA) policy that includes a custom entity group, a custom action group, and a default counter group. The custom entity group and action group must be created independently before they are referenced within an SMA policy.

## High-level procedure

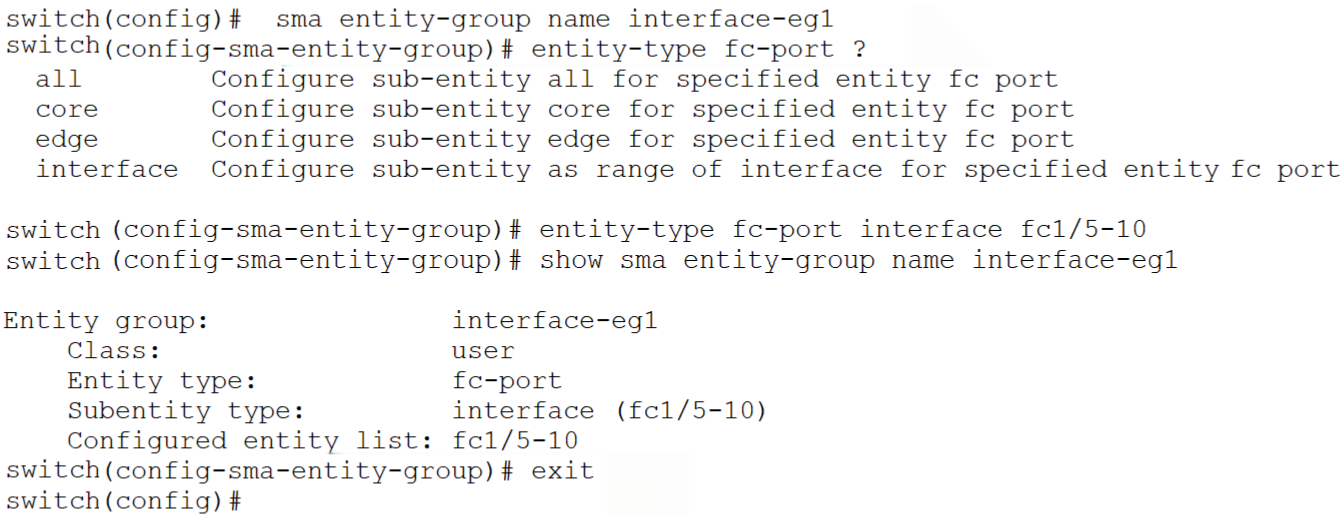
1. Entity-group configuration
    a. Create an entity-group with a valid name
    b. Under the config-sma-entity-group mode, add entity-type along with subentity-types for the entity-group
2. Action-group configuration
    a. Create an action-group with an appropriate name
    b. Under config-action-group mode, configure actions for each threshold level (alarm, warning and falling)
3. SMA policy creation
    a. Create an SMA policy with an appropriate name
    b. Under config-sma-policy mode, configure entity-group (pre-defined or user-defined from Step 1)
    c. Under config-sma-policy-entity mode, configure counters for entity-group
4. Activate the SMA policy

## Detailed procedure

The following CLI commands illustrate how to create a user-defined SMA policy. This policy monitors a set of port counters on specific interfaces of a Cisco 9000 Series switch. Configuring an MDS 9000 switch requires read-write access privileges.

### Entity-group configuration

A user-defined entity-group “interface-eg1” is created and then for entity-type fc-port, interfaces fc 1/5 - 10 are added as subentity-type.



```
switch(config)#  sma entity-group name interface-eg1
switch(config-sma-entity-group)# entity-type fc-port ?
  all        Configure sub-entity all for specified entity fc port
  core       Configure sub-entity core for specified entity fc port
  edge       Configure sub-entity edge for specified entity fc port
  interface  Configure sub-entity as range of interface for specified entity fc port

switch (config-sma-entity-group)# entity-type fc-port interface fc1/5-10
switch (config-sma-entity-group)# show sma entity-group name interface-eg1

Entity group:               interface-eg1
    Class:                  user
    Entity type:            fc-port
    Subentity type:         interface (fc1/5-10)
    Configured entity list: fc1/5-10
switch(config-sma-entity-group)# exit
switch(config)#
```

### Action-group configuration

Next, a user-defined action-group named “link-itw-ag1” is created to monitor the counter-group “cg-link-integrity”. The action-group can be configured with alerts as well as actions for the warning, alarm and falling threshold levels. In this example, once the threshold level reaches the alarm value, an “error-disable” action will be executed on the monitored interface. Note that a user-defined action-group cannot be created without associating it with a counter or counter-group.

```
switch(config)# sma action-group name link-itw-ag1 counter-group cg-link-integrity
switch(config-sma-action-group)# threshold-level warning alerts severity-level 4 syslog
switch(config-sma-action-group)# threshold-level alarm action error-disable alerts severity-level 2 snmp-trap syslog
switch(config-sma-action-group)# threshold-level falling alerts severity-level 4 snmp-trap syslog
switch(config-sma-action-group)# exit
switch(config)# show sma action-group name link-itw-ag1

Action group:       link-itw-ag1
    Class:          user
    Counter group:  cg-link-integrity
    Counters:       link-loss,sync-loss,
                    signal-loss,rx-invalid-words,rx-invalid-crc
    Actions:
        Warning: none
        Alarm:   error-disable
        Falling: none
    Alerts:
        Warning: syslog-4
        Alarm:   snmp-trap-2,syslog-2
        Falling: snmp-trap-4,syslog-4
switch(config)#
```

### Creating the SMA Policy

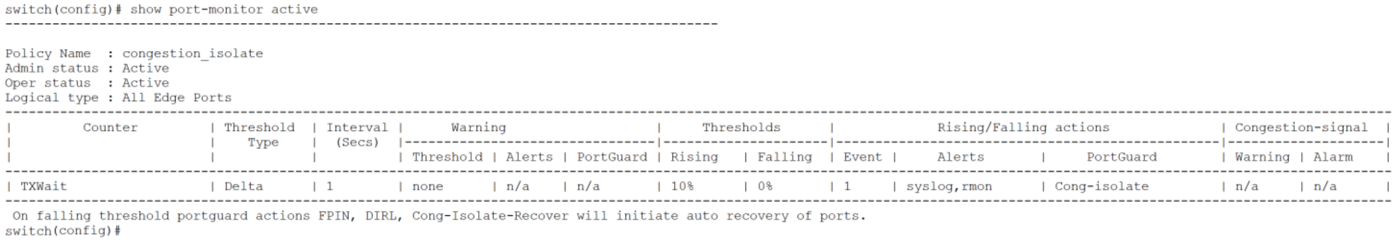
In this step, a user-defined SMA policy named “ud-sma-1” is created. The user-defined entity-group created in Step 1 is added to this SMA policy. The counter-group “cg-link-integrity” is then added with the default monitor level and the user-defined action-group created in the previous step. The policy alerts when there are 2 or more sync-loss, signal-loss, link-loss, invalid-words or 1 or more invalid-crc events in a 60 second period. Note that since we are monitoring a pre-defined counter-group that consists of five different port counters, the monitor-level can only be set to default, and the user cannot modify it. If the user wants to configure different values for the monitor-level, individual counters must be added to the policy. Additionally, in an SMA policy, there can be a maximum of 10 entity-groups with the entity-type fc-port and 1 entity-group with the entity-type switch, for a total of 11 entity-groups.

```
switch(config)# sma policy name ud-sma-1
switch(config-sma-policy)#
switch(config-sma-policy)# entity-group name interface-eg1
switch(config-sma-policy-entity)#
switch(config-sma-policy-entity)# counter-group cg-link-integrity monitor-level default action-group link-itw-ag1
switch(config-sma-policy-entity)#
switch(config-sma-policy-entity)# exit
switch(config-sma-policy)#
switch(config-sma-policy)# show sma policy name ud-sma-1

Policy: ud-sma-1
Class:  user
Status: not active

Entity group:  interface-eg1 (user)
Entity type:   fc-port
---------------------------------------------------------------------------------------------------------
                               | Period   |           Threshold            |
Counter                        | seconds  | Warning  | Alarm    | Falling  | Action group name (class)
---------------------------------------------------------------------------------------------------------
sync-loss                      |       60 |        2 |        5 |        0 | link-itw-ag1 (user)
signal-loss                    |       60 |        2 |        5 |        0 | link-itw-ag1 (user)
link-loss                      |       60 |        2 |        5 |        0 | link-itw-ag1 (user)
rx-invalid-words               |       60 |        2 |        5 |        0 | link-itw-ag1 (user)
rx-invalid-crc                 |       60 |        1 |        2 |        0 | link-itw-ag1 (user)
switch(config-sma-policy)#
```

### Activating the SMA Policy

Finally, the user-defined SMA policy can be activated. Note that a port-monitor (PMON) and an SMA policy cannot be active at the same time. Any existing active port-monitor policy must be deactivated before activating the SMA policy.

```
switch(config-sma-policy)# exit

switch (config)# sma policy activate name ud-sma-1

Error: SMA policy is not activated. Port Monitor policy errdy is already active. SMA and
Port Monitor policies cannot be active at the same time.

switch (config)#
```



```
switch(config)# show port-monitor active
-------------------------------------------------------------------------------------------

Policy Name  : congestion_isolate
Admin status : Active
Oper status  : Active
Logical type : All Edge Ports
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|         Counter          | Threshold | Interval |       Warning                  |      Thresholds      |              Rising/Falling actions              | Congestion-signal  |
|                          |   Type    |  (Secs)  |--------------------------------|----------------------|--------------------------------------------------|--------------------|
|                          |           |          | Threshold | Alerts | PortGuard | Rising     | Falling | Event |      Alerts        |      PortGuard      | Warning | Alarm    |
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| TXWait                   | Delta     | 1        | none      | n/a    | n/a       | 10%        | 0%      | 1     | syslog,rmon        | Cong-isolate        | n/a     | n/a      |
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
 On falling threshold portguard actions FPIN, DIRL, Cong-Isolate-Recover will initiate auto recovery of ports.
switch(config)#
```

```
switch(config)# no port-monitor activate congestion_isolate

WARNING: Ports which are cong-isolated or either in DIRL or FPIN will be recovered.

switch (config)#

switch (config)# show port-monitor active

switch (config)#
```

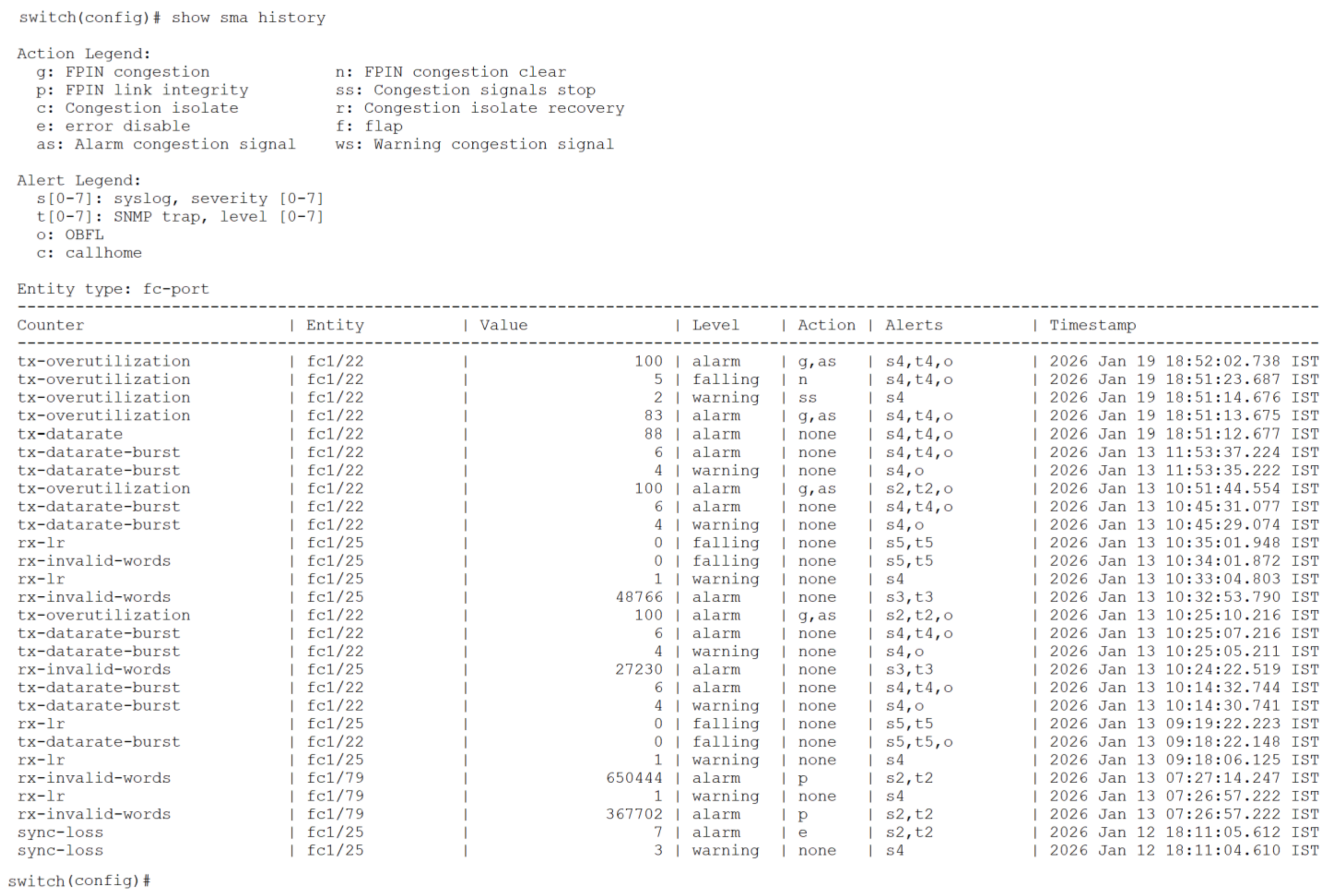
```
switch(config-sma-policy)# sma policy activate name ud-sma-1
switch(config)#
switch(config)# show sma policy active

Policy: ud-sma-1
Class:  user
Status: active - Activated at 2026 Jan 20 14:01:28.343 IST

Entity group:  interface-eg1 (user)
Entity type:   fc-port
-------------------------------------------------------------------------------------------------------
                               | Period    |           Threshold            |
Counter                        | seconds   | Warning  | Alarm    | Falling  | Action group name (class)
-------------------------------------------------------------------------------------------------------
sync-loss                      |       60 |        2 |        5 |        0 | link-itw-ag1 (user)
signal-loss                    |       60 |        2 |        5 |        0 | link-itw-ag1 (user)
link-loss                      |       60 |        2 |        5 |        0 | link-itw-ag1 (user)
rx-invalid-words               |       60 |        2 |        5 |        0 | link-itw-ag1 (user)
rx-invalid-crc                 |       60 |        1 |        2 |        0 | link-itw-ag1 (user)

-------------------------------------------------------------------------------------------------------
Counter                        | Effective entity list
-------------------------------------------------------------------------------------------------------
sync-loss                      | fc1/5-10
signal-loss                    | fc1/5-10
link-loss                      | fc1/5-10
rx-invalid-words               | fc1/5-10
rx-invalid-crc                 | fc1/5-10
switch(config)#
```

Customers also have the option to copy the default (or a user-defined) SMA policy using the command **sma policy copy default <new name>** and modify it according to their requirements.

As of NX-OS release 9.4(4), up to four user-defined SMA policies and one default SMA policy are supported. The default SMA policy can be activated or deactivated but cannot be deleted. For more details about the SMA guidelines, please refer to the References section to access the Cisco MDS 9000 Series Interfaces Configuration Guide.

## SMA Event History

Another major benefit of SMA is its ability to maintain a historical record of past threshold events. This feature allows Storage administrators to review when specific thresholds were crossed, analyze recurring patterns, and correlate these events with network conditions or configuration changes. By preserving this event history, SMA enables more effective troubleshooting, and long-term trend analysis compared to the other monitoring methods that only provide real-time alerts.



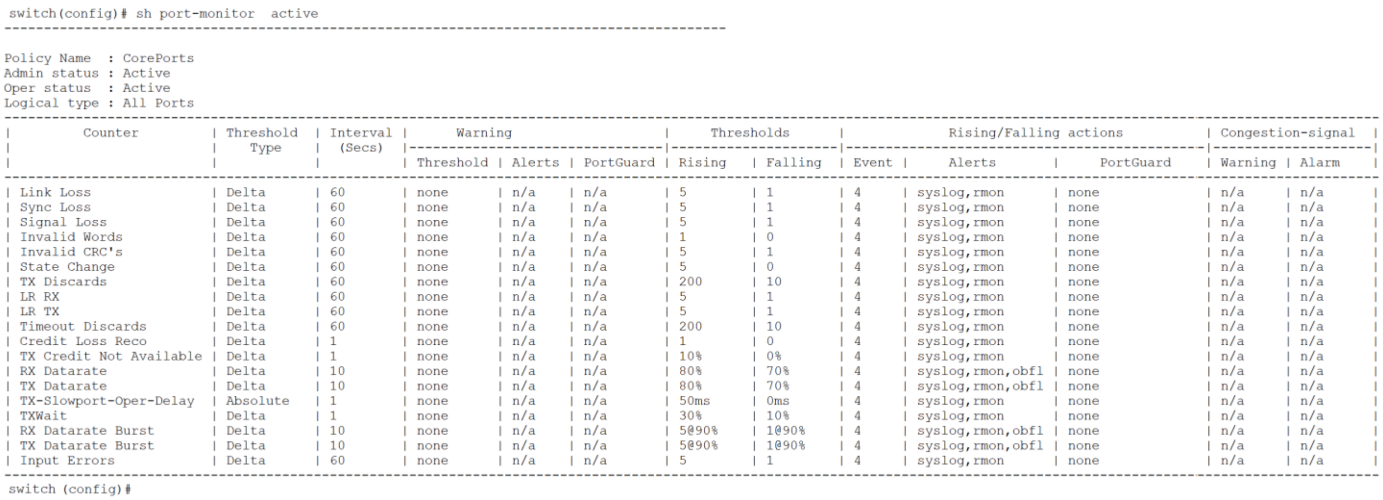
```
switch(config)# show sma history

Action Legend:
  g: FPIN congestion             n: FPIN congestion clear
  p: FPIN link integrity         ss: Congestion signals stop
  c: Congestion isolate          r: Congestion isolate recovery
  e: error disable               f: flap
  as: Alarm congestion signal    ws: Warning congestion signal

Alert Legend:
  s[0-7]: syslog, severity [0-7]
  t[0-7]: SNMP trap, level [0-7]
  o: OBFL
  c: callhome

Entity type: fc-port
---------------------------------------------------------------------------------------------------------------------------------------
Counter                     | Entity          | Value                  | Level    | Action | Alerts          | Timestamp
---------------------------------------------------------------------------------------------------------------------------------------
tx-overutilization          | fc1/22          |                    100 | alarm    | g,as   | s4,t4,o         | 2026 Jan 19 18:52:02.738 IST
tx-overutilization          | fc1/22          |                      5 | falling  | n      | s4,t4,o         | 2026 Jan 19 18:51:23.687 IST
tx-overutilization          | fc1/22          |                      2 | warning  | ss     | s4              | 2026 Jan 19 18:51:14.676 IST
tx-overutilization          | fc1/22          |                     83 | alarm    | g,as   | s4,t4,o         | 2026 Jan 19 18:51:13.675 IST
tx-datarate                 | fc1/22          |                     88 | alarm    | none   | s4,t4,o         | 2026 Jan 19 18:51:12.677 IST
tx-datarate-burst           | fc1/22          |                      6 | alarm    | none   | s4,t4,o         | 2026 Jan 13 11:53:37.224 IST
tx-datarate-burst           | fc1/22          |                      4 | warning  | none   | s4,o            | 2026 Jan 13 11:53:35.222 IST
tx-overutilization          | fc1/22          |                    100 | alarm    | g,as   | s2,t2,o         | 2026 Jan 13 10:51:44.554 IST
tx-datarate-burst           | fc1/22          |                      6 | alarm    | none   | s4,t4,o         | 2026 Jan 13 10:45:31.077 IST
tx-datarate-burst           | fc1/22          |                      4 | warning  | none   | s4,o            | 2026 Jan 13 10:45:29.074 IST
rx-lr                       | fc1/25          |                      0 | falling  | none   | s5,t5           | 2026 Jan 13 10:35:01.948 IST
rx-invalid-words            | fc1/25          |                      0 | falling  | none   | s5,t5           | 2026 Jan 13 10:34:01.872 IST
rx-lr                       | fc1/25          |                      1 | warning  | none   | s4              | 2026 Jan 13 10:33:04.803 IST
rx-invalid-words            | fc1/25          |                  48766 | alarm    | none   | s3,t3           | 2026 Jan 13 10:32:53.790 IST
tx-overutilization          | fc1/22          |                    100 | alarm    | g,as   | s2,t2,o         | 2026 Jan 13 10:25:10.216 IST
tx-datarate-burst           | fc1/22          |                      6 | alarm    | none   | s4,t4,o         | 2026 Jan 13 10:25:07.216 IST
tx-datarate-burst           | fc1/22          |                      4 | warning  | none   | s4,o            | 2026 Jan 13 10:25:05.211 IST
rx-invalid-words            | fc1/25          |                  27230 | alarm    | none   | s3,t3           | 2026 Jan 13 10:24:22.519 IST
tx-datarate-burst           | fc1/22          |                      6 | alarm    | none   | s4,t4,o         | 2026 Jan 13 10:14:32.744 IST
tx-datarate-burst           | fc1/22          |                      4 | warning  | none   | s4,o            | 2026 Jan 13 10:14:30.741 IST
rx-lr                       | fc1/25          |                      0 | falling  | none   | s5,t5           | 2026 Jan 13 09:19:22.223 IST
tx-datarate-burst           | fc1/22          |                      0 | falling  | none   | s5,t5,o         | 2026 Jan 13 09:18:22.148 IST
rx-lr                       | fc1/25          |                      1 | warning  | none   | s4              | 2026 Jan 13 09:18:06.125 IST
rx-invalid-words            | fc1/79          |                 650444 | alarm    | p      | s2,t2           | 2026 Jan 13 07:27:14.247 IST
rx-lr                       | fc1/79          |                      1 | warning  | none   | s4              | 2026 Jan 13 07:26:57.222 IST
rx-invalid-words            | fc1/79          |                 367702 | alarm    | p      | s2,t2           | 2026 Jan 13 07:26:57.222 IST
sync-loss                   | fc1/25          |                      7 | alarm    | e      | s2,t2           | 2026 Jan 12 18:11:05.612 IST
sync-loss                   | fc1/25          |                      3 | warning  | none   | s4              | 2026 Jan 12 18:11:04.610 IST

switch(config)#
```

## Migration from PMON to SMA

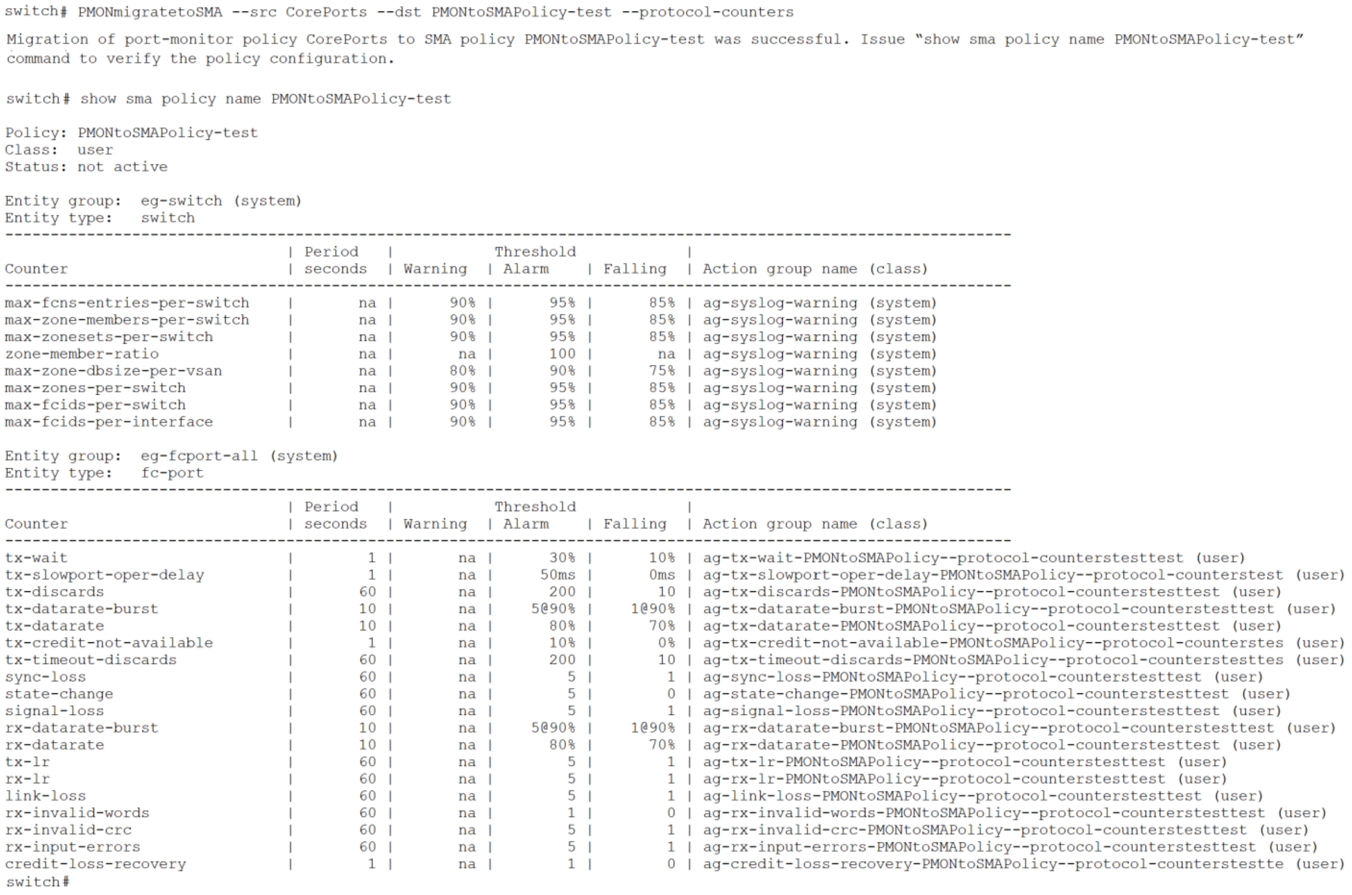
To accelerate and simplify the adoption of SMA, Cisco MDS NX-OS provides an overlay CLI command to migrate from Port Monitoring (PMON) policies (either default or user-defined) to SMA. An overlay CLI is a Python script that acts as a wrapper around the standard NX-OS CLI command. This command converts all PMON policy configurations into an equivalent SMA policy configuration. Note that the migrated SMA policy will not be activated by default. User will need to activate the SMA policy.

This section describes how to use this feature to convert PMON policies to SMA policies. For more information about the prerequisites and constraints, please refer to the references section to access the SMA section in Cisco MDS 9000 Congestion Alerting guide.

In this example, a user-defined PMON policy named “CorePorts” is active. It has multiple port counters with defined monitor-levels and associated actions or alerts. To migrate this PMON policy to a SMA policy, execute the following command: “PMONmigratetoSMA --src CorePorts --dst PMONtoSMAPolicy-test –protocol-counters”. The command also takes an argument --protocol-counters, which will create a entity-group eg-switch with the respective protocol counters.



```
 switch(config)# sh port-monitor  active
-------------------------------------------------------------------------------------------

Policy Name  : CorePorts
Admin status : Active
Oper status  : Active
Logical type : All Ports
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|         Counter          | Threshold | Interval |        Warning                 |     Thresholds     |              Rising/Falling actions            | Congestion-signal  |
|                          |   Type    |  (Secs)  |--------------------------------|--------------------|------------------------------------------------|--------------------|
|                          |           |          | Threshold | Alerts | PortGuard | Rising   | Falling | Event |       Alerts       |      PortGuard     | Warning | Alarm    |
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| Link Loss                | Delta     | 60       | none      | n/a    | n/a       | 5        | 1       | 4     | syslog,rmon        | none               | n/a     | n/a      |
| Sync Loss                | Delta     | 60       | none      | n/a    | n/a       | 5        | 1       | 4     | syslog,rmon        | none               | n/a     | n/a      |
| Signal Loss              | Delta     | 60       | none      | n/a    | n/a       | 5        | 1       | 4     | syslog,rmon        | none               | n/a     | n/a      |
| Invalid Words            | Delta     | 60       | none      | n/a    | n/a       | 1        | 0       | 4     | syslog,rmon        | none               | n/a     | n/a      |
| Invalid CRC's            | Delta     | 60       | none      | n/a    | n/a       | 5        | 1       | 4     | syslog,rmon        | none               | n/a     | n/a      |
| State Change             | Delta     | 60       | none      | n/a    | n/a       | 5        | 0       | 4     | syslog,rmon        | none               | n/a     | n/a      |
| TX Discards              | Delta     | 60       | none      | n/a    | n/a       | 200      | 10      | 4     | syslog,rmon        | none               | n/a     | n/a      |
| LR RX                    | Delta     | 60       | none      | n/a    | n/a       | 5        | 1       | 4     | syslog,rmon        | none               | n/a     | n/a      |
| LR TX                    | Delta     | 60       | none      | n/a    | n/a       | 5        | 1       | 4     | syslog,rmon        | none               | n/a     | n/a      |
| Timeout Discards         | Delta     | 60       | none      | n/a    | n/a       | 200      | 10      | 4     | syslog,rmon        | none               | n/a     | n/a      |
| Credit Loss Reco         | Delta     | 1        | none      | n/a    | n/a       | 1        | 0       | 4     | syslog,rmon        | none               | n/a     | n/a      |
| TX Credit Not Available  | Delta     | 1        | none      | n/a    | n/a       | 10%      | 0%      | 4     | syslog,rmon        | none               | n/a     | n/a      |
| RX Datarate              | Delta     | 10       | none      | n/a    | n/a       | 80%      | 70%     | 4     | syslog,rmon,obfl   | none               | n/a     | n/a      |
| TX Datarate              | Delta     | 10       | none      | n/a    | n/a       | 80%      | 70%     | 4     | syslog,rmon,obfl   | none               | n/a     | n/a      |
| TX-Slowport-Oper-Delay   | Absolute  | 1        | none      | n/a    | n/a       | 50ms     | 0ms     | 4     | syslog,rmon        | none               | n/a     | n/a      |
| TXWait                   | Delta     | 1        | none      | n/a    | n/a       | 30%      | 10%     | 4     | syslog,rmon        | none               | n/a     | n/a      |
| RX Datarate Burst        | Delta     | 10       | none      | n/a    | n/a       | 5@90%    | 1@90%   | 4     | syslog,rmon,obfl   | none               | n/a     | n/a      |
| TX Datarate Burst        | Delta     | 10       | none      | n/a    | n/a       | 5@90%    | 1@90%   | 4     | syslog,rmon,obfl   | none               | n/a     | n/a      |
| Input Errors             | Delta     | 60       | none      | n/a    | n/a       | 5        | 1       | 4     | syslog,rmon        | none               | n/a     | n/a      |
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------
 switch (config)#
```



```
switch# PMONmigratetoSMA --src CorePorts --dst PMONtoSMAPolicy-test --protocol-counters
 Migration of port-monitor policy CorePorts to SMA policy PMONtoSMAPolicy-test was successful. Issue “show sma policy name PMONtoSMAPolicy-test”
 command to verify the policy configuration.

 switch# show sma policy name PMONtoSMAPolicy-test

Policy: PMONtoSMAPolicy-test
Class:  user
Status: not active

Entity group:  eg-switch (system)
Entity type:   switch
-------------------------------------------------------------------------------------------------------------
                               | Period   |           Threshold          |
Counter                        | seconds  | Warning  | Alarm     | Falling  | Action group name (class)
-------------------------------------------------------------------------------------------------------------
max-fcns-entries-per-switch    |       na |      90% |       95% |      85% | ag-syslog-warning (system)
max-zone-members-per-switch    |       na |      90% |       95% |      85% | ag-syslog-warning (system)
max-zonesets-per-switch        |       na |      90% |       95% |      85% | ag-syslog-warning (system)
zone-member-ratio              |       na |       na |       100 |       na | ag-syslog-warning (system)
max-zone-dbsize-per-vsan       |       na |      80% |       90% |      75% | ag-syslog-warning (system)
max-zones-per-switch           |       na |      90% |       95% |      85% | ag-syslog-warning (system)
max-fcids-per-switch           |       na |      90% |       95% |      85% | ag-syslog-warning (system)
max-fcids-per-interface        |       na |      90% |       95% |      85% | ag-syslog-warning (system)

Entity group:  eg-fcport-all (system)
Entity type:   fc-port
-------------------------------------------------------------------------------------------------------------
                               | Period   |           Threshold          |
Counter                        | seconds  | Warning  | Alarm     | Falling  | Action group name (class)
-------------------------------------------------------------------------------------------------------------
tx-wait                        |        1 |       na |       30% |      10% | ag-tx-wait-PMONtoSMAPolicy--protocol-counterstesttest (user)
tx-slowport-oper-delay         |        1 |       na |      50ms |      0ms | ag-tx-slowport-oper-delay-PMONtoSMAPolicy--protocol-counterstest (user)
tx-discards                    |       60 |       na |       200 |       10 | ag-tx-discards-PMONtoSMAPolicy--protocol-counterstesttest (user)
tx-datarate-burst              |       10 |       na |     5@90% |    1@90% | ag-tx-datarate-burst-PMONtoSMAPolicy--protocol-counterstesttest (user)
tx-datarate                    |       10 |       na |       80% |      70% | ag-tx-datarate-PMONtoSMAPolicy--protocol-counterstesttest (user)
tx-credit-not-available        |        1 |       na |       10% |       0% | ag-tx-credit-not-available-PMONtoSMAPolicy--protocol-counterstes (user)
tx-timeout-discards            |       60 |       na |       200 |       10 | ag-tx-timeout-discards-PMONtoSMAPolicy--protocol-counterstesttes (user)
sync-loss                      |       60 |       na |         5 |        1 | ag-sync-loss-PMONtoSMAPolicy--protocol-counterstesttest (user)
state-change                   |       60 |       na |         5 |        0 | ag-state-change-PMONtoSMAPolicy--protocol-counterstesttest (user)
signal-loss                    |       60 |       na |         5 |        1 | ag-signal-loss-PMONtoSMAPolicy--protocol-counterstesttest (user)
rx-datarate-burst              |       10 |       na |     5@90% |    1@90% | ag-rx-datarate-burst-PMONtoSMAPolicy--protocol-counterstesttest (user)
rx-datarate                    |       10 |       na |       80% |      70% | ag-rx-datarate-PMONtoSMAPolicy--protocol-counterstesttest (user)
tx-lr                          |       60 |       na |         5 |        1 | ag-tx-lr-PMONtoSMAPolicy--protocol-counterstesttest (user)
rx-lr                          |       60 |       na |         5 |        1 | ag-rx-lr-PMONtoSMAPolicy--protocol-counterstesttest (user)
link-loss                      |       60 |       na |         5 |        1 | ag-link-loss-PMONtoSMAPolicy--protocol-counterstesttest (user)
rx-invalid-words               |       60 |       na |         1 |        0 | ag-rx-invalid-words-PMONtoSMAPolicy--protocol-counterstesttest (user)
rx-invalid-crc                 |       60 |       na |         5 |        1 | ag-rx-invalid-crc-PMONtoSMAPolicy--protocol-counterstesttest (user)
rx-input-errors                |       60 |       na |         5 |        1 | ag-rx-input-errors-PMONtoSMAPolicy--protocol-counterstesttest (user)
credit-loss-recovery           |        1 |       na |         1 |        0 | ag-credit-loss-recovery-PMONtoSMAPolicy--protocol-counterstestte (user)
switch#
```

## Comparison of SMA and PMON

The following section provides a detailed comparison of SMA and PMON, emphasizing the enhancements and benefits that SMA introduces. This comparison highlights how SMA not only extends visibility and control but also streamlines monitoring and alerting workflows, making it a superior solution for managing Cisco MDS 9000 storage networks.

**Table 2.** Comparison between SMA and PMON

| Feature | Smart Monitoring and Alerting (SMA) | Port Monitoring (PMON) |
|---|---|---|
| Monitoring Flexibility | Provides granular control over monitored entities and thresholds | Limited ability to customize monitored entities. |
| Monitoring granularity | Enables precise interface-level monitoring | Monitoring is restricted to logical core and edge-types |
| Policy Structure | Unified policy for monitoring different type of entities port-level and protocol-level counters | A single policy applies to all core and edge ports without per-group customization. EEM feature-set to be configured for protocol counters |
| Counter Grouping | Provides a hierarchical monitoring model with individual counters and counter groups, enabling efficient organization and management of related metrics by entity group | Flat monitoring structure with no hierarchy |
| Actions and Alerting Capabilities | Supports multiple actions and alerts for each threshold level (Alarm/Warning/Falling) | Single action and alert applied to all thresholds |
| Event logging and Debuggability | Maintains event history with show SMA history, including counters, actions, alerts, and timestamps | No support for detailed event logging |
| Entity Group Priority | Entity group priority follows policy order; topmost group has highest priority. Matching entities adopt the highest-priority group's configuration | No concept of entity groups |
| Monitoring of SFP-related counters | Only the percentage is monitored and not count simplifying the monitoring of SFP-related counters | Count and percentage of these SFP counters are monitored |

## Conclusion

This document provides step-by-step guidance for configuring the new Smart Monitoring and Alerting (SMA) feature in a Cisco SAN fabric. This feature establishes a unified and scalable framework for monitoring Cisco MDS switch infrastructure. It integrates port-level and protocol-level observability within a centralized platform, enabling precise configuration, proactive monitoring, and efficient system health management—resulting in reduced downtime and improved SLAs. The comparison between PMON and SMA clearly demonstrates the numerous advantages that SMA provides over PMON. SMA offers more granular control over monitored entities and thresholds, supports hierarchical organization with counters and counter groups, enables per-threshold actions and alerts, and maintains a detailed history of events, actions, and alerts. Additionally, the overlay CLI command that migrates existing Port Monitoring (PMON) policies into SMA policies ensures a seamless transition and enhances operational efficiency. Collectively, these benefits make a strong case for customers to adopt SMA as their preferred monitoring and alerting solution in Cisco SAN environments.

## References

- Release Notes for Cisco MDS 9000 Series, Release 9.4(4)

- Cisco MDS 9000 Series Interfaces Configuration Guide
- Cisco MDS 9000 Congestion Alerting

## Legal Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.