7210 SAS D, E OS
OAM and Diagnostics Guide

Software Version: 7210 SAS OS 3.0 Rev. 04
April 2011
Document Part Number: 93-0226-04-04

Table of Contents

List of Tables

List of Figures

Preface

About This Guide

This guide describes service mirroring and Operations, Administration and Management (OAM) and diagnostic tools provided by the 7210 SAS D and E platforms and presents examples to configure and implement various tests.

This document is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Audience

This manual is intended for network administrators who are responsible for configuring the 7210 SAS routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols, standards, and services described in this manual include the following:

- CLI concepts
- Subscriber services
- Service mirroring
- Operation, Administration and Maintenance (OAM) operations

List of Technical Publications

The 7210-SAS D, E OS documentation set is composed of the following books:

- 7210-SAS D, E OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.

- 7210-SAS D, E OS System Management Guide

  This guide describes system security and access configurations as well as event logging and accounting logs.

- 7210-SAS D, E OS Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), and port provisioning.

- 7210-SAS D, E OS Router Configuration Guide

  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link aggregation group (LAG) as well as IP and MAC-based filtering.

- 7210-SAS D, E OS Routing Protocols Guide

  This guide provides an overview of routing concepts and provides configuration examples for protocols and route policies.

- 7210-SAS D, E OSServices Guide

  This guide describes how to configure service parameters such as, customer information and user services.

- 7210-SAS D, E OS OAM and Diagnostic Guide

  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.

- 7210-SAS D, E OS Quality of Service Guide

  This guide describes how to configure Quality of Service (QoS) policy management.

Technical Support

If you purchased a service agreement for your 7210 SAS and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your welcome center.

Web: http://www1.alcatel-lucent.com/comps/pages/carrier_support.jhtml

Getting Started

In This Chapter

This book provides process flow information to configure service mirroring and Operations, Administration and Management (OAM) tools.

Alcatel-Lucent 7210 SAS-Series Services Configuration Process

Table 1 lists the tasks necessary to configure mirroring, and perform tools monitoring functions. This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: Configuration Process

Area	Task	Chapter
Diagnostics/ Service verification	Mirroring	Mirror Services on page 13
	OAM	OAM and SAA on page 53
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 45

Mirror Services

In This Chapter

This chapter provides information to configure mirroring.

Topics in this chapter include:

Service Mirroring

When troubleshooting complex operational problems, customer packets can be examined as they traverse the network. Alcatel-Lucent's service mirroring provides the capability to mirror customer packets to allow for trouble shooting and offline analysis.

This capability also extends beyond troubleshooting services. Telephone companies have the ability to obtain itemized calling records and wire-taps where legally required by investigating authorities. The process can be very complex and costly to carry out on data networks. Service Mirroring greatly simplifies these tasks, as well as reduces costs through centralization of analysis tools and skilled technicians.

Only local mirroring is supported on the 7210 SAS D and E platforms. Additionally, only a NULL SAP can be provisioned as a mirror destination.

Original packets are forwarded while a copy is sent out the mirrored port to the mirroring (destination) port. Service mirroring allows an operator to see the actual traffic on a customer's service with a sniffer sitting in a central location. In many cases, this reduces the need for a separate, costly overlay sniffer network.

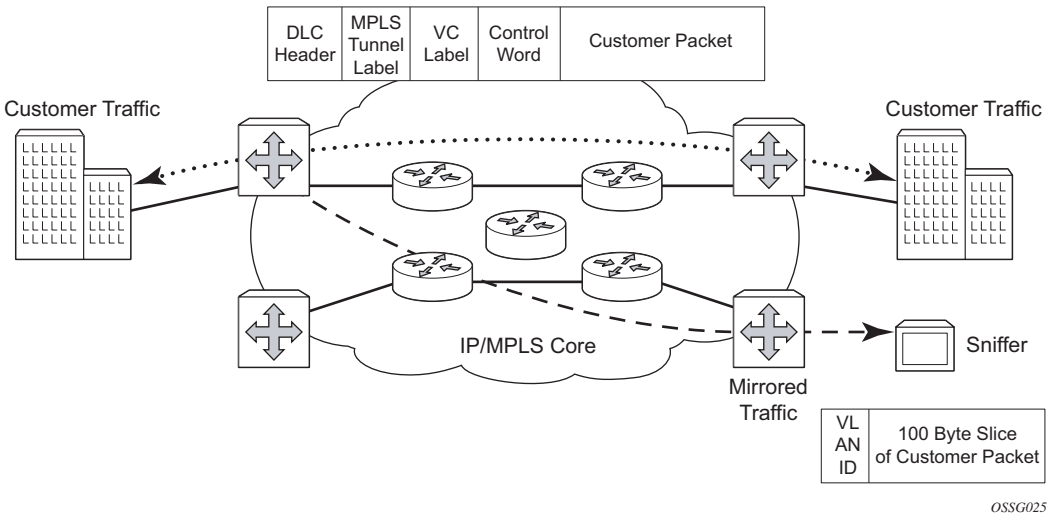

Figure 1: Service Mirroring

Mirror Implementation

Mirroring can be implemented on ingress service access points (SAPs) or ingress network interfaces as well as on ingress ports. Egress mirroring is supported only on the port. Egress mirroring is not supported for SAPs and filters.

Alcatel-Lucent's implementation of packet mirroring is based on the following assumptions:

- Ingress packets are mirrored as they appear on the wire. This is important for troubleshooting encapsulation and protocol issues.

  When mirroring at ingress the 7210 SAS node sends an exact copy of the original ingress packet to the mirror destination while normal forwarding proceeds on the original packet.

- When mirroring at egress, the packets are not an exact copy of the forwarded packet. Specifically it does not contain the SAP tags that the forwarded copy of the packet carries, but carries an internal VLAN tag.

  In the 7210 SAS node, mirroring at egress takes place before the packet is processed by egress QoS. Therefore, there exists a possibility that a packet is dropped by egress QoS mechanisms (because of RED mechanisms, etc.) and thus not forwarded but it is still mirrored.

Mirror Source and Destinations

Mirror sources and destinations have the following characteristics:

- They can only be on the same 7210 SAS node (local mirroring).
- A mirror destination can terminate on only one port (NULL SAP).
- Packets ingressing a port can have a mirror destination separate from packets egressing another or the same port.
- A total of four mirror destinations are supported (local only) per node.

Local Mirroring

Mirrored frames can be copied and sent to a specific local destination or mirror service on 7210 SAS node (local mirroring).

The 7210 SAS node allows multiple concurrent mirroring sessions so traffic from more than one ingress mirror source can be mirrored to the same or different mirror destinations. In case of port egress mirroring, only a maximum of 4 egress mirror sources are allowed and one egress mirror source can be configured to only one mirror destination.

Note: Remote mirroring is not supported on 7210 SAS D and E platforms.

Mirroring Performance

Replication of mirrored packets can, typically, affect performance and should be used carefully.

Mirroring can be performed based on the following criteria:

- Port (ingress and egress)
- SAP (ingress only)
- MAC filter (ingress only)
- IP filter (ingress only)

Mirroring Configuration

Configuring mirroring is similar to creating a uni-direction service. Mirroring requires the configuration of:

- Mirror source — The traffic on a specific point(s) to mirror.
- Mirror destination — The location to send the mirrored traffic, where the sniffer will be located.

Figure 2 depicts a local mirror service configured on ALA-A.

- Port 1/1/2 is specified as the source. Mirrored traffic ingressing and egressing this port will be sent to port 1/1/3.
- SAP 1/1/3 is specified as the destination. The sniffer is physically connected to this port. Mirrored traffic ingressing and egressing port 1/1/2 is sent here. SAP, encapsulation requirements, and mirror classification parameters are configured.

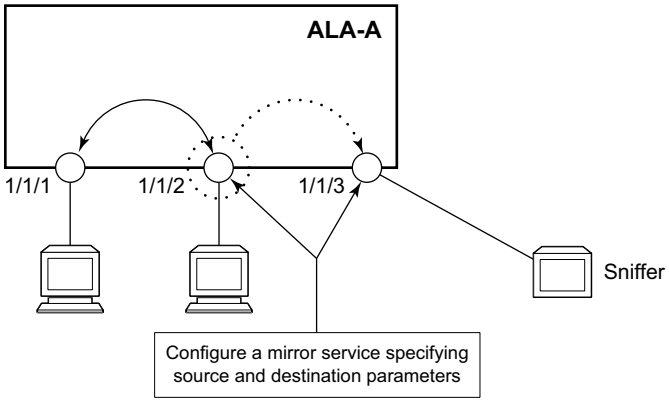

Figure 2: Local Mirroring Example

Carrier Grade NAT – Lawful Intercept

Lawful intercept for NAT is supported to mirror configured subscriber's traffic to a mirror-destination. When active, packets are mirrored from the perspective of the NAT outside interface (thus after NAT translations have occurred). All traffic for the specified subscriber, including traffic associated with static port-forwards, is mirrored.

A simplified Ethernet encapsulation (with an optional Intercept ID) is used for all NAT traffic. When mirroring NAT traffic, the mirror-destination must be of type **ether**. The customer packet from the (outside) IP Header onwards (including the IP header) is mirrored. The operator has the configuration option of embedding the Intercept ID into the LI packet through the use of an explicit intercept-id command. Both packet formats are described below:

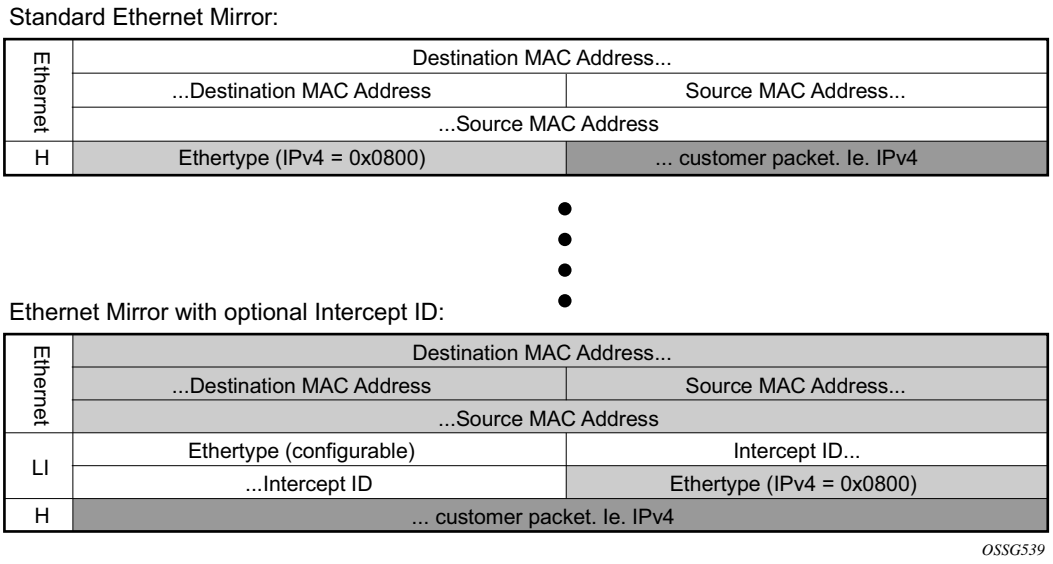

Figure 3: Ethernet Mirror Examples

The contents of the highlighted fields is configurable using the following CLI:

```
li
   li-source service-id
        nat
             classic-lsn-sub router name ip address [intercept-id id]
             dslite-lsn-sub router name b4 ipv6-address [intercept-id id]
             l2-aware-sub sub-ident [intercept-id id]
             ethernet-header [etype hex] [sa mac] [da mac]
```

The default ethernet-header is to use etype 0x600 and system MAC address for both source and destination address. The configurable Ethertype and Intercept ID is only added when an intercept-id is present for the subscriber in the NAT config.

Configuration Process Overview

Figure 4 displays the process to provision basic mirroring parameters.

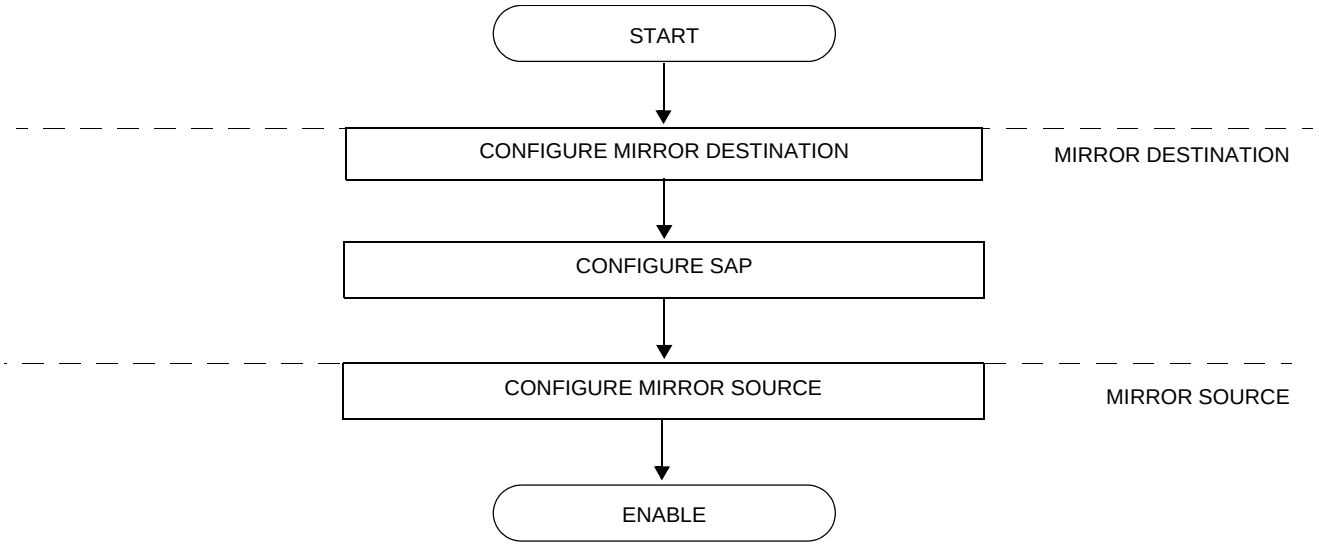

Figure 4: Mirror Configuration and Implementation Flow

Configuration Notes

This section describes mirroring configuration caveats.

- Multiple mirroring service IDs (mirror destinations) may be created within a single system.
- A mirrored source can only have one destination.
- The destination mirroring service IDs and service parameters are persistent between router (re)boots and are included in the configuration saves.

  Mirror source criteria configuration (defined in `debug>mirror>mirror-source`) is not preserved in a configuration save (admin save). Debug mirror source configuration can be saved using `admin>debug-save`.
- Physical layer problems such as collisions, jabbers, etc., are not mirrored. Typically, only complete packets are mirrored.
- Starting and shutting down mirroring:

  Mirror destinations:

  → The default state for a mirror destination service ID is shutdown. You must issue a **no shutdown** command to enable the feature.

  → When a mirror destination service ID is shutdown, mirrored packets associated with the service ID are not accepted from its mirror source. The associated mirror source is put into an operationally down mode. Mirrored packets are not transmitted out the SAP. Each mirrored packet is silently discarded.

  → Issuing the `shutdown` command causes the mirror destination service or its mirror source to be put into an administratively down state. Mirror destination service IDs must be shut down first in order to delete a service ID or SAP association from the system.

  Mirror sources:

  → The default state for a mirror source for a given mirror-dest service ID is `no shutdown`. Enter a `shutdown` command to deactivate (disable) mirroring from that mirror-source.

  → Mirror sources do not need to be shutdown to remove them from the system. When a mirror source is shutdown, mirroring is terminated for all sources defined locally for the mirror destination service ID.

Configuring Service Mirroring with CLI

This section provides information about service mirroring

Topics in this section include:

Mirror Configuration Overview

7210 SAS node mirroring can be organized in the following logical entities:

- The mirror source is defined as the location where ingress traffic specific to a port, SAP, MAC or IP filter, is to be mirrored (copied). The original frames are not altered or affected in any way. The egress traffic specific to a port can be mirrored.
- A SAP is defined in local mirror services as the mirror destination to where the mirrored packets are sent.

Defining Mirrored Traffic

In some scenarios, or when multiple services are configured on the same port, specifying the port does not provide sufficient resolution to separate traffic. In Alcatel-Lucent's implementation of mirroring, multiple source mirroring parameters can be specified to further identify traffic.

Mirroring of packets matching specific filter entries in an IP or MAC filter can be applied to refine what traffic is mirrored to flows of traffic within a service. The IP criteria can be combinations of:

- Source IP address/mask
- Destination IP address/mask
- IP Protocol value
- Source port value (for example, UDP or TCP port)
- Destination port value (for example, UDP or TCP port)
- DiffServ Code Point (DSCP) value
- ICMP code
- ICMP type
- IP fragments
- TCP ACK set/reset
- TCP SYN set/reset

The MAC criteria can be combinations of:

- IEEE 802.1p value/mask
- Source MAC address/mask
- Destination MAC address/mask
- Ethernet Type II Ethernet type value

Basic Mirroring Configuration

Destination mirroring parameters must include at least:

- A mirror destination ID (same as the mirror source service ID).
- A mirror destination SAP.

Mirror source parameters must include at least:

- A mirror service ID (same as the mirror destination service ID).
- At least one source type (port, SAP, IP filter or MAC filter) specified.

The following example displays a sample configuration of a local mirrored service (ALA-A).

```
*A:ALA-A>config>mirror# info
----------------------------------------------
        mirror-dest 103 create
            exit
            no shutdown
        exit
----------------------------------------------
*A:ALA-A>config>mirror#
```

The following displays the mirror source configuration:

```
*A:ALA-A>debug>mirror-source# show debug mirror
debug
    mirror-source 103
        no shutdown
    exit
exit
*A:ALA-A>debug>mirror-source# exit
```

Mirror Classification Rules

Alcatel-Lucent's implementation of mirroring can be performed by configuring parameters to select network traffic according to any of the following entities:

- Port
- SAP
- MAC filter
- IP filter

Port

The `port` command associates a port to a mirror source. The port is identified by the port ID. The defined port can be Ethernet or a Link Aggregation Group (LAG) ID. When a LAG ID is given as the port ID, mirroring is enabled on all ports making up the LAG.

Mirror sources can be ports in either access or access uplink mode. Port mirroring is supported in the following combinations:

Table 2: Mirror Source Port Requirements

Port Type	Port Mode	Port Encap Type
faste/gige	access	dot1q, null
faste/gige	access uplink	qinq

CLI Syntax: `debug>mirror-source# port {`*`port-id`*`|lag `*`lag-id`*`} {[egress][ingress]}`

Example: `*A:ALA-A>debug>mirror-source# port 1/1/2 ingress egress`

SAP

More than one SAP can be associated within a single mirror-source. Each SAP has its own ingress parameter keyword to define which packets are mirrored to the mirror-dest service ID. A SAP that is defined within a mirror destination cannot be used in a mirror source.

CLI Syntax: `debug>mirror-source# sap `*`sap-id`*` {[ingress]}`

Example: `*A:ALA-A>debug>mirror-source# sap 1/1/4:100 ingress`

MAC filter

MAC filters are configured in the **config>filter>mac-filter** context. The **mac-filter** command causes all the packets matching the explicitly defined list of entry IDs to be mirrored to the mirror destination specified by the service-id of the mirror source.

CLI Syntax: debug>mirror-source# mac-filter *mac-filter-id* entry *entry-id* [*entry-id* …]

Example: *A:ALA-2>debug>mirror-source# mac-filter 12 entry 15 20 25

IP filter

IP filters are configured in the **config>filter>ip-filter** context. The **ip-filter** command causes all the packets matching the explicitly defined list of entry IDs to be mirrored to the mirror destination specified by the service-id of the mirror source.

Ingress mirrored packets are mirrored to the mirror destination prior to any ingress packet modifications.

CLI Syntax: debug>mirror-source# ip-filter *ip-filter-id* entry *entry-id* [*entry-id* …]

Example: *A:ALA-A>debug>mirror-source# ip-filter 1 entry 20

NOTE: An IP filter cannot be applied to a mirror destination SAP.

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure local mirror services and provides CLI command syntax. Note that the local mirror source and mirror destination components must be configured under the same service ID context.

Each local mirrored service (Figure 5) (within the same router) requires the following configurations:

1. Specify mirror destination (SAP).
2. Specify mirror source (port, SAP, IP filter, MAC filter).

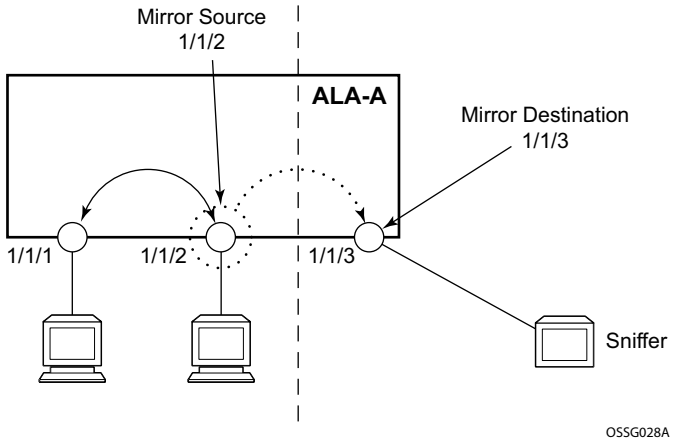

Figure 5: Local Mirrored Service Tasks

Configuring a Local Mirror Service

To configure a local mirror service, the source and destinations must be located on the same router. Note that local mirror source and mirror destination components must be configured under the same service ID context.

The **mirror-source** commands are used as traffic selection criteria to identify traffic to be mirrored at the source. Each of these criteria are independent. For example, use the **debug>mirror-source>port** {*port-id* | **lag** *lag-id*} {[**egress**] [**ingress**]} command and **debug>mirror-source ip-filter** *ip-filter-id* **entry** *entry-id* [*entry-id*…] command to capture (mirror) traffic that matches a specific IP filter entry and traffic ingressing and egressing a specific port. A filter must be applied to the SAP or interface if only specific packets are to be mirrored.

Use the CLI syntax to configure one or more mirror source parameters:

The `mirror-dest` commands are used to specify where the mirrored traffic is to be sent. Use the following CLI syntax to configure mirror destination parameters:

CLI Syntax:
```
config>mirror mirror-dest service-id [type {ether}] [create]
    description string
    sap sap-id [create]
    no shutdown
```

CLI Syntax:
```
debug# mirror-source service-id
    ip-filter ip-filter-id entry entry-id [entry-id …]
    mac-filter mac-filter-id entry entry-id [entry-id …]
    port {port-id|lag lag-id} {[egress][ingress]}
    sap sap-id {[ingress]}
    no shutdown
```

The following output displays an example of a local mirrored service. On ALA-A, mirror service 103 is mirroring traffic matching IP filter 2, entry 1 as well as egress and ingress traffic on port 1/1/23 and sending the mirrored packets to SAP 1/1/24

```
*A:ALA-A>config>mirror# info
----------------------------------------------
        mirror-dest 103 create
           sap 1/1/24 create
            exit
            no shutdown
        exit
----------------------------------------------
*A:ALA-A>config>mirror#
```

The following displays the debug mirroring information:

```
*A:ALA-A>debug>mirror-source# show debug mirror
debug
    mirror-source 103
```

```
            no shutdown
            port 1/1/23 ingress
            ip-filter 2 entry 1
        exit
    exit
    *A:ALA-A>debug>mirror-source# exit
```

Service Management Tasks

This section discusses the following service management tasks:

- Modifying a Local Mirrored Service on page 34
- Deleting a Local Mirrored Service on page 35

Use the following command syntax to modify an existing mirrored service:

CLI Syntax:
```
config>mirror#
 mirror-dest service-id [type {ether}]
    description description-string
    no description
    sap sap-id
    no sap
    [no] shutdown
```

CLI Syntax:
```
debug
[no] mirror-source service-id
    ip-filter ip-filter-id entry entry-id [entry-id...]
    no ip-filter ip-filter-id
    no ip-filter entry entry-id [entry-id...]
    mac-filter mac-filter-id entry entry-id [entry-id...]
    no mac-filter mac-filter-id
    no mac-filter mac-filter-id entry entry-id [entry-id...]
    [no] port {port-id|lag lag-id} {[egress][ingress]}
    [no] sap sap-id {[ingress]}
    [no] shutdown
```

Modifying a Local Mirrored Service

Existing mirroring parameters can be modified in the CLI. The changes are applied immediately. The service must be shut down if changes to the SAP are made.

The following example displays commands to modify parameters for a basic local mirroring service.

Example:
```
config>mirror# mirror-dest 103
config>mirror>mirror-dest# shutdown
config>mirror>mirror-dest# no sap
config>mirror>mirror-dest# sap 1/1/5 create
config>mirror>mirror-dest>sap$ exit
config>mirror>mirror-dest# no shutdown
debug# mirror-source 103
debug>mirror-source# no port 1/1/23
debug>mirror-source# port 1/1/7 ingress egress
```

The following displays the local mirrored service modifications:

```
*A:ALA-A>config>mirror# info
----------------------------------------------
mirror-dest 103 create
            no shutdown
            sap 1/1/5 create
        exit

*A:ALA-A>debug>mirror-source# show debug mirror
debug
    mirror-source 103
        no shutdown
        port 1/1/7 egress ingress
    exit
*A:ALA-A>debug>mirror-source#
```

Deleting a Local Mirrored Service

Existing mirroring parameters can be deleted in the CLI. A shutdown must be issued on a service level in order to delete the service. It is not necessary to shut down or remove SAP or port references to delete a local mirrored service.

The following example displays commands to delete a local mirrored service.

Example:ALA-A>
```
config>mirror# mirror-dest 103
config>mirror>mirror-dest# shutdown
config>mirror>mirror-dest# exit
config>mirror# no mirror-dest 103
config>mirror# exit
```

Mirror Service Command Reference

Command Hierarchies

Mirror Configuration Commands

```
config
    — mirror
        — mirror-dest service-id [type encap-type] [create]
        — no mirror-dest service-id
            — description description-string
            — no description
            — sap sap-id [create]
            — no sap
            — [no] shutdown
```

Debug Commands

```
debug
    — [no] mirror-source <service-id>
        — ip-filter ip-filter-id entry entry-id [entry-id ...]
        — no ip-filter ip-filter-id [entry entry-id] [entry-id ...]
        — mac-filter mac-filter-id entry entry-id [entry-id ...]
        — no mac-filter mac-filter-id [entry entry-id...]
        — port {port-id | lag lag-id} {[egress] [ingress]}
        — no port {port-id | lag lag-id} [egress] [ingress]
        — sap sap-id {[ingress]}
        — no sap sap-id [ingress]
        — [no] shutdown
```

Show Commands

```
show
    — debug [application]
    — mirror mirror-dest [service-id]
    — service
        — service-using mirror
```

Configuration Commands

Generic Commands

description

Syntax **description** *description-string*
no description

Context config>mirror>mirror-dest

Description This command creates a text description stored in the configuration file for a configuration context to help the administrator identify the content of the file.

The **no** form of the command removes the description string.

Default There is no default description associated with the configuration context.

Parameters *description-string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax [**no**] **shutdown**

Context config>mirror>mirror-dest
debug>mirror-source

Description The **shutdown** command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system generated configuration files.

The **no** form of the command puts an entity into the administratively enabled state.

Default See Special Cases below.

Special Cases **Mirror Destination —** When a mirror destination service ID is shutdown, mirrored packets associated with the service ID are not accepted from the mirror source device. The associated mirror source is put into an operationally down mode. Mirrored packets are not transmitted out of the SAP. Each mirrored packet is silently discarded. If the mirror destination is a SAP, the SAP's discard counters are incremented.

The **shutdown** command places the mirror destination service or mirror source into an administratively down state. The **mirror-dest** service ID must be shut down in order to delete the service ID, SAP association from the system.

The default state for a mirror destination service ID is **shutdown**. A **no shutdown** command is required to enable the service.

Mirror Source — Mirror sources do not need to be shutdown in order to remove them from the system.

When a mirror source is **shutdown**, mirroring is terminated for all sources defined locally for the **mirror-dest** service ID.

The default state for a mirror source for a given **mirror-dest** service ID is **no shutdown**. A **shutdown** command is required to disable mirroring from that mirror-source.

Mirror Destination Configuration Commands

mirror-dest

Syntax **mirror-dest** *service-id* [**type** *encap-type*] [create]
no mirror-dest

Context config>mirror

Description This command creates a context to set up a service that is intended for packet mirroring. It is configured as a service to allow mirrored packets to be directed locally (within the same device), over the core of the network and have a far end device decode the mirror encapsulation.

The **mirror-dest** service is comprised of destination parameters that define where the mirrored packets are to be sent. It also specifies whether the defined *service-id* will receive mirrored packets from far end devices over the network core.

The **mirror-dest** service IDs are persistent between boots of the router and are included in the configuration saves. The local sources of mirrored packets for the service ID are defined within the **debug mirror mirror-source** command that references the same *service-id*. Up to 4 **mirror-dest** service IDs can be created within a single system.

The **mirror-dest** command is used to create or edit a service ID for mirroring purposes. If the *service-id* does not exist within the context of all defined services, the **mirror-dest** service is created and the context of the CLI is changed to that service ID. If the *service-id* exists within the context of defined **mirror-dest** services, the CLI context is changed for editing parameters on that service ID. If the *service-id* exists within the context of another service type, an error message is returned and CLI context is not changed from the current context.

The **no** form of the command removes a mirror destination from the system. The **mirror-source** or **li-source** associations with the **mirror-dest** *service-id* do not need to be removed or shutdown first. The **mirror-dest** *service-id* must be shutdown before the service ID can be removed. When the service ID is removed, all **mirror-source** or **li-source** commands that have the service ID defined will also be removed from the system.

Default No packet mirroring services are defined.

Parameters *service-id* — The service identification identifies the service in the service domain. This ID is unique to this service and cannot be used by any other service, regardless of service type. The same service ID must be configured on every device that this particular service is defined on.

If particular a service ID already exists for a service, then the same value cannot be used to create a mirror destination service ID with the same value. For example:

If an Epipe service-ID **11** exists, then a mirror destination service-ID **11** cannot be created. If a VPLS service-ID **12** exists, then a mirror destination service-ID **12** cannot be created.
If an IES service-ID **13** exists, then a mirror destination service-ID **13** cannot be created.

Values *service-id*: 1 — 2147483647

type *encap-type* **—** The type describes the encapsulation supported by the mirror service.

Values ether

sap

Syntax **sap** *sap-id* [**create**]
no sap

Context config>mirror>mirror-dest

Description This command creates a service access point (SAP) within a mirror destination service. The SAP is owned by the mirror destination service ID.

The SAP is defined with port and encapsulation parameters to uniquely identify the (mirror) SAP on the interface and within the box. The specified SAP must define an Ethernet port with only a null encapsulation type.

Only one SAP can be created within a **mirror-dest** service ID. If the defined SAP has not been created on any service within the system, the SAP is created and the context of the CLI will change to the newly created SAP. In addition, the port cannot be a member of a multi-link bundle, LAG, APS group or IMA bundle.

If the defined SAP exists in the context of another service ID, **mirror-dest** or any other type, an error is generated.

Mirror destination SAPs can be created on Ethernet interfaces that have been defined as an access interface. If the interface is defined as network, the SAP creation returns an error.

When the **no** form of this command is used on a SAP created by a mirror destination service ID, the SAP with the specified port and encapsulation parameters is deleted.

Default No default SAP for the mirror destination service defined.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 137 for command syntax.

Mirror Source Configuration Commands

mirror-source

Syntax [**no**] **mirror-source** *service-id*

Context debug

Description This command configures mirror source parameters for a mirrored service.

The **mirror-source** command is used to enable mirroring of packets specified by the association of the **mirror-source** to sources of packets defined within the context of the *mirror-dest-service-id*. The mirror destination service must already exist within the system.

A mirrored packet cannot be mirrored to multiple destinations. If a mirrored packet is properly referenced by multiple mirror sources (for example, a SAP on one **mirror-source** and a port on another **mirror-source**), then the packet is mirrored to a single *mirror-dest-service-id* based on the following hierarchy:

1. Filter entry
2. Service access port (SAP)
3. Physical port

The hierarchy is structured so the most specific match criteria has precedence over a less specific match. For example, if a **mirror-source** defines a port and a SAP on that port, then the SAP mirror-source is accepted and the mirror-source for the port is ignored because of the hierarchical order of precedence.

The **mirror-source** configuration is not saved when a configuration is saved. A **mirror-source** manually configured within an ASCII configuration file will not be preserved if that file is overwritten by a **save** command. Define the **mirror-source** within a file associated with a **config exec** command to make a **mirror-source** persistent between system reboots.

By default, all **mirror-dest** service IDs have a **mirror-source** associated with them. The **mirror-source** is not technically created with this command. Instead the service ID provides a contextual node for storing the current mirroring sources for the associated **mirror-dest** service ID. The **mirror-source** is created for the mirror service when the operator enters the **debug>mirror-source** *svcId* for the first time.The **mirror-source** is also automatically removed when the **mirror-dest** service ID is deleted from the system.

The **no** form of the command deletes all related source commands within the context of the **mirror-source** *service-id*. The command does not remove the service ID from the system.

Default No mirror source match criteria is defined for the mirror destination service.

Parameters *service-id* — The mirror destination service ID for which match criteria will be defined. The *service-id* must already exist within the system.

Values *service-id*: 1 — 2147483647

ip-filter

Syntax **ip-filter** *ip-filter-id* **entry** *entry-id* [*entry-id …*]
no ip-filter *ip-filter-id*
no ip-filter *ip-filter-id* **entry** *entry-id* [*entry-id …*]

Context debug>mirror-source

Description This command enables mirroring of packets that match specific entries in an existing IP filter.

The **ip-filter** command directs packets which match the defined list of entry IDs to be mirrored to the mirror destination referenced by the *mirror-dest-service-id* of the **mirror-source**.

The IP filter must already exist in order for the command to execute. Filters are configured in the **config>filter** context. If the IP filter does not exist, an error will occur. If the filter exists but has not been associated with a SAP or IP interface, an error is not generated but mirroring will not be enabled (there are no packets to mirror). Once the IP filter is defined to a SAP or IP interface, mirroring is enabled.

If the IP filter is defined as ingress, only ingress packets are mirrored. Ingress mirrored packets are mirrored to the mirror destination prior to any ingress packet modifications.

If the IP filter is defined as egress, only egress packets are mirrored. Egress mirrored packets are mirrored to the mirror destination after all egress packet modifications.

An *entry-id* within an IP filter can only be mirrored to a single mirror destination. If the same *entry-id* is defined multiple times, an error occurs and only the first **mirror-source** definition is in effect.

By default, no packets matching any IP filters are mirrored. Mirroring of IP filter entries must be explicitly defined.

The **no ip-filter** command, without the **entry** keyword, removes mirroring on all *entry-id*'s within the *ip-filter-id*.

When the **no** command is executed with the **entry** keyword and one or more *entry-id*'s, mirroring of that list of *entry-id*'s is terminated within the *ip-filter-id*. If an *entry-id* is listed that does not exist, an error will occur and the command will not execute. If an *entry-id* is listed that is not currently being mirrored, no error will occur for that *entry-id* and the command will execute normally.

Default IP filter mirroring is not defined.

Parameters *ip-filter-id* — The IP filter ID whose entries are mirrored. If the *ip-filter-id* does not exist, an error will occur and the command will not execute. Mirroring of packets will commence once the *ip-filter-id* is defined on a SAP or IP interface.

entry *entry-id* [*entry-id …*] **—** The IP filter entries to use as match criteria for packet mirroring. The **entry** keyword begins a list of *entry-id*'s for mirroring. Multiple *entry-id* entries may be specified with a single command. Each *entry-id* must be separated by a space.

If an *entry-id* does not exist within the IP filter, an error occurs and the command will not execute.

If the filter's *entry-id* is renumbered within the IP filter definition, the old *entry-id* is removed but the new *entry-id* must be manually added to the configuration to include the new (renumbered) entry's criteria.

mac-filter

Syntax **mac-filter** *mac-filter-id* **entry** *entry-id* [*entry-id …*]
no mac-filter *mac-filter-id*
no mac-filter *mac-filter-id* **entry** *entry-id* [*entry-id …*]

Context debug>mirror-source

Description This command enables mirroring of packets that match specific entries in an existing MAC filter.

The **mac-filter** command directs packets which match the defined list of entry IDs to be mirrored to the mirror destination referenced by the *mirror-dest-service-id* of the **mirror-source**.

The MAC filter must already exist in order for the command to execute. Filters are configured in the config>filter context. If the MAC filter does not exist, an error will occur. If the filter exists but has not been associated with a SAP or IP interface, an error is not be generated but mirroring will not be enabled (there are no packets to mirror). Once the filter is defined to a SAP or MAC interface, mirroring is enabled.

If the MAC filter is defined as ingress, only ingress packets are mirrored. Ingress mirrored packets are mirrored to the mirror destination prior to any ingress packet modifications.

The **no mac-filter** command, without the **entry** keyword, removes mirroring on all *entry-id*'s within the *mac-filter-id*.

When the **no** command is executed with the **entry** keyword and one or more *entry-id*'s, mirroring of that list of *entry-id*'s is terminated within the *mac-filter-id*. If an *entry-id* is listed that does not exist, an error will occur and the command will not execute. If an *entry-id* is listed that is not currently being mirrored, no error will occur for that *entry-id* and the command will execute normally.

Default No MAC filter mirroring defined.

Parameters *mac-filter-id* — The MAC filter ID whose entries are mirrored. If the *mac-filter-id* does not exist, an error will occur and the command will not execute. Mirroring of packets will commence once the *mac-filter-id* is defined on a SAP.

entry *entry-id* [*entry-id …*] **—** The MAC filter entries to use as match criteria for packet mirroring. The **entry** keyword begins a list of *entry-id*'s for mirroring. Multiple *entry-id* entries may be specified with a single command. Each *entry-id* must be separated by a space. Up to 8 entry IDs may be specified in a single command.

Each *entry-id* must exist within the *mac-filter-id*. If the *entry-id* is renumbered within the MAC filter definition, the old *entry-id* is removed from the list and the new *entry-id* will need to be manually added to the list if mirroring is still desired.

If no *entry-id* entries are specified in the command, mirroring will not occur for that MAC filter ID. The command will have no effect.

port

Syntax **port** {*port-id* | **lag** *lag-id*} {[**egress**] [**ingress**]}
no port {*port-id* | **lag** *lag-id*} [**egress**] [**ingress**]

Context debug>mirror-source

Description This command enables mirroring of traffic ingressing or egressing a port (Ethernet port, or Link Aggregation Group (LAG)).

The **port** command associates a port or LAG to a mirror source. The port is identified by the *port-id*. The defined port may be Ethernet, access or access uplink. access. A port may be a single port or a Link Aggregation Group (LAG) ID. When a LAG ID is given as the *port-id*, mirroring is enabled on all ports making up the LAG. Either a LAG port member *or* the LAG port can be mirrored.

The port is only referenced in the mirror source for mirroring purposes. If the port is removed from the system, the mirroring association will be removed from the mirror source.

The same port may not be associated with multiple mirror source definitions with the **ingress** parameter defined. The same port may not be associated with multiple mirror source definitions with the **egress** parameter defined.

If a SAP is mirrored on an access port, the SAP mirroring will have precedence over the access port mirroring when a packet matches the SAP mirroring criteria. Filter and label mirroring destinations will also precedence over a port-mirroring destination.

If the port is not associated with a **mirror-source**, packets on that port will not be mirrored. Mirroring may still be defined for a SAP or filter entry, which will mirror based on a more specific criteria.

The **no port** command disables port mirroring for the specified port. Mirroring of packets on the port may continue due to more specific mirror criteria. If the **egress** or **ingress** parameter keywords are specified in the **no** command, only the ingress or egress mirroring condition will be removed.

Default No ports are defined.

Parameters *port-id* — Specifies the port ID.

lag-id — The LAG identifier, expressed as a decimal integer.

egress — Specifies that packets egressing the port should be mirrored. Egress packets are mirrored to the mirror destination after egress packet modification.

ingress — Specifies that packets ingressing the port should be mirrored. Ingress packets are mirrored to the mirror destination prior to ingress packet modification.

sap

Syntax **sap** *sap-id* {[**ingress**]}
no sap *sap-id*[**ingress**]

Context debug>mirror-source

Description This command enables mirroring of traffic ingressing a service access port (SAP). A SAP that is defined within a mirror destination cannot be used in a mirror source. The mirror source SAP referenced by the *sap-*

id is owned by the service ID of the service in which it was created. The SAP is only referenced in the mirror source name for mirroring purposes. The mirror source association does not need to be removed before deleting the SAP from its service ID. If the SAP is deleted from its service ID, the mirror association is removed from the mirror source.

More than one SAP can be associated within a single **mirror-source**. Each SAP has its own **ingress** parameter keyword to define which packets are mirrored to the mirror destination.

The SAP must be valid and properly configured. If the associated SAP does not exist, an error occurs and the command will not execute.

The same SAP cannot be associated with multiple mirror source definitions for ingress packets.

If a particular SAP is not associated with a mirror source name, then that SAP will not have mirroring enabled for that mirror source.

The **no** form of the command disables mirroring for the specified SAP. All mirroring for that SAP on ingress is terminated. Mirroring of packets on the SAP can continue if more specific mirror criteria is configured. If the **ingress** parameter keyword are specified in the **no** command, only the ingress mirroring condition is removed.

Default No SAPs are defined by default.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 137 for command syntax.

ingress — Specifies that packets ingressing the SAP should be mirrored. Ingress packets are mirrored to the mirror destination prior to ingress packet modification.

Show Commands

debug

Syntax **debug** [*application*]

Context **show**

Description This command displays set debug points.

Parameters *application* — Display which debug points have been set.

Values: service, ip, ospf, mtrace, isis, mpls, rsvp, ldp, mirror, system, filter, subscriber-mgmt, radius, lag, oam

Output

```
*A:alu1# show debug
debug
    mirror-source 101
        port 1/1/1 ingress
        no shutdown
    exit
    mirror-source 102
        port 1/1/3 egress
        no shutdown
    exit
exit
*A:alu1#
```

service-using

Syntax **service-using** [**mirror**]

Context show>service

Description Displays mirror services.

If no optional parameters are specified, all services defined on the system are displayed.

Parameters **mirror** — Displays mirror services.

Output **Show Service-Using Mirror —** The following table describes service-using mirror output fields:

Label	Description
Service Id	The service identifier.
Type	Specifies the service type configured for the service ID.
Adm	The desired state of the service.
Opr	The operating state of the service.

Label	Description (Continued)
CustomerID	The ID of the customer who owns this service.
Last Mgmt Change	The date and time of the most recent management-initiated change to this service.

Sample Output

```
A:ALA-48# show service service-using mirror
===============================================================================
Services [mirror]
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
218          Mirror    Up     Down       1                 04/08/2007 13:49:57
318          Mirror    Down   Down       1                 04/08/2007 13:49:57
319          Mirror    Up     Down       1                 04/08/2007 13:49:57
320          Mirror    Up     Down       1                 04/08/2007 13:49:57
1000         Mirror    Down   Down       1                 04/08/2007 13:49:57
1216         Mirror    Up     Down       1                 04/08/2007 13:49:57
1412412      Mirror    Down   Down       1                 04/08/2007 13:49:57
-------------------------------------------------------------------------------
Matching Services : 7
===============================================================================
A:ALA-48#
```

mirror

Syntax **mirror** mirror-dest *service-id*

Context show

Description This command displays mirror configuration and operation information.

Parameters *service-id* — Specify the mirror service ID.

Output **Mirroring Output —** The following table describes the mirroring output fields:

Label	Description
Service Id	The service ID associated with this mirror destination.
Type	Entries in this table have an implied storage type of "volatile". The configured mirror source information is not persistent.
Admin State	Up – The mirror destination is administratively enabled.
	Down – The mirror destination is administratively disabled.
Oper State	Up – The mirror destination is operationally enabled.
	Down – The mirror destination is operationally disabled.
Destination SAP	The ID of the access port where the Service Access Point (SAP) associated with this mirror destination service is defined.

Sample Output

```
*A:alu1# show mirror mirror-dest 101
===============================================================================
Mirror Service
===============================================================================
Service Id       :   101                   Type          : Ether
Admin State      :   Up                    Oper State    : Up
Destination SAP  :   1/1/6
-------------------------------------------------------------------------------
Local Sources
-------------------------------------------------------------------------------
Admin State : Up
- Port 1/1/1 Egress Ingress
===============================================================================
*A:alu1#


*A:alu1# show mirror mirror-dest 102
===============================================================================
Mirror Service
===============================================================================
Service Id       :   102                   Type          : Ether
Admin State      :   Up                    Oper State    : Up
Destination SAP  :   lag-2
-------------------------------------------------------------------------------
```

```
Local Sources
-------------------------------------------------------------------------------
Admin State : Up
No Mirror Sources configured
===============================================================================
*A:alu1#
```

OAM and SAA

In This Chapter

This chapter provides information about the Operations, Administration and Management (OAM) and Service Assurance Agent (SAA) commands available in the CLI for troubleshooting services.

Topics in this chapter include:

OAM Overview

Delivery of services requires a number of operations occur properly and at different levels in the service delivery model. For example, operations such as the association of packets to a service, must be performed properly in the forwarding plane for the service to function properly. In order to verify that a service is operational, a set of in-band, packet-based Operation, Administration, and Maintenance (OAM) tools is required, with the ability to test each of the individual packet operations.

For in-band testing, the OAM packets closely resemble customer packets to effectively test the customer's forwarding path, but they are distinguishable from customer packets so they are kept within the service provider's network and not forwarded to the customer.

The suite of OAM diagnostics supplement the basic IP ping and traceroute operations with diagnostics specialized for the different levels in the service delivery model. There are diagnostics for services.

Ethernet Connectivity Fault Management (ETH-CFM)

The IEEE and the ITU-T have cooperated to define the protocols, procedures and managed objects to support service based fault management. Both IEEE 802.1ag standard and the ITU-T Y.1731 recommendation support a common set of tools that allow operators to deploy the necessary administrative constructs, management entities and functionality, Ethernet Connectivity Fault Management (ETH-CFM). The ITU-T has also implemented a set of advanced ETH-CFM and performance management functions and features that build on the proactive and on demand troubleshooting tools.

CFM uses Ethernet frames and is distinguishable by ether-type 0x8902. In certain cases the different functions will use a reserved multicast address that could also be used to identify specific functions at the MAC layer. However, the multicast MAC addressing is not used for every function or in every case. The Operational Code (OpCode) in the common CFM header is used to identify the type of function carried in the CFM packet. CFM frames are only processed by IEEE MAC bridges. With CFM, interoperability can be achieved between different vendor equipment in the service provider network up to and including customer premises bridges. The following table lists CFM-related acronyms used in this section.

This section of the guide will provide configuration example for each of the functions. It will also provide the various OAM command line options and show commands to operate the network. The individual service guides will provide the complete CLI configuration and description of the commands in order to build the necessary constructs and management points.

Acronym	Callout
1DM	One way Delay Measurement (Y.1731)
AIS	Alarm Indication Signal
CCM	Continuity check message
CFM	Connectivity fault management
DMM	Delay Measurement Message (Y.1731)
DMR	Delay Measurement Reply (Y.1731)
LBM	Loopback message
LBR	Loopback reply
LTM	Linktrace message
LTR	Linktrace reply
ME	Maintenance entity

Acronym	Callout (Continued)
MA	Maintenance association
MA-ID	Maintenance association identifier
MD	Maintenance domain
MHF	MIP half function
MIP	Maintenance domain intermediate point
OpCode	Operational Code
RDI	Remote Defect Indication
TST	Ethernet Test (Y.1731)
SLM	Synthetic Loss Message
SLR	Synthetic Loss Reply (Y.1731)

ETH-CFM Building Blocks

The IEEE and the ITU-T use their own nomenclature when describing administrative contexts and functions. This introduces a level of complexity to configuration, discussion and different vendors naming conventions. The SR and ESS OS CLI has chosen to standardize on the IEEE 802.1ag naming where overlap exists. ITU-T naming is used when no equivalent is available in the IEEE standard. In the following definitions, both the IEEE name and ITU-T names are provided for completeness, using the format IEEE Name/ITU-T Name.

Maintenance Domain (MD)/Maintenance Entity (ME) is the administrative container that defines the scope, reach and boundary for faults. It is typically the area of ownership and management responsibility. The IEEE allows for various formats to name the domain, allowing up to 45 characters, depending on the format selected. ITU-T supports only a format of “none” and does not accept the IEEE naming conventions.

0 — Undefined and reserved by the IEEE.

1 — No domain name. It is the only format supported by Y.1731 as the ITU-T specification does not use the domain name. This is supported in the IEEE 802.1ag standard but not in currently implemented for 802.1ag defined contexts.

2,3,4 — Provides the ability to input various different textual formats, up to 45 characters. The string format (2) is the default and therefore the keyword is not shown when looking at the configuration.

Maintenance Association (MA)/Maintenance Entity Group (MEG) is the construct where the different management entities will be contained. Each MA is uniquely identified by its MA-ID. The MA-ID is comprised of the by the MD level and MA name and associated format. This is another administrative context where the linkage is made between the domain and the service using the **bridging-identifier** configuration option. The IEEE and the ITU-T use their own specific formats. The MA short name formats (0-255) have been divided between the IEEE (0-31, 64-255) and the ITU-T (32-63), with five currently defined (1-4, 32). Even though the different standards bodies do not have specific support for the others formats a Y.1731 context can be configured using the IEEE format options.

1 (Primary VID) — Values 0 — 4094

2 (String) — Raw ASCII, excluding 0-31 decimal/0-1F hex (which are control characters) form the ASCII table

3 (2-octet integer) — 0 — 65535

4 (VPN ID) — Hex value as described in RFC 2685, *Virtual Private Networks Identifier*

32 (icc-format) — Exactly 13 characters from the ITU-T recommendation T.50.

Note: When a VID is used as the short MA name, 802.1ag will not support VLAN translation because the MA-ID must match all the MEPs. The default format for a short MA name is an

integer. Integer value 0 means the MA is not attached to a VID. This is useful for VPLS services on 7210 platforms because the VID is locally significant.

Maintenance Domain Level (MD Level)/Maintenance Entity Group Level (MEG Level) is the numerical value (0-7) representing the width of the domain. The wider the domain, higher the numerical value, the farther the ETH-CFM packets can travel. It is important to understand that the level establishes the processing boundary for the packets. Strict rules control the flow of ETH-CFM packets and are used to ensure proper handling, forwarding, processing and dropping of these packets. To keep it simple ETH-CFM packets with higher numerical level values will flow through MEPs on MIPs on SAPs configured with lower level values. This allows the operator to implement different areas of responsibility and nest domains within each other. Maintenance association (MA) includes a set of MEPs, each configured with the same MA-ID and MD level used verify the integrity of a single service instance.

In the following example, a Y.1731 domain context and 802.1ag context are configured. The Y.1731 context can be identified by the **none** setting for the domain format.

```
configure eth-cfm domain 3 format none level 3
configuer eth-cfm domain 4 format string name IEEE-Domain level 4

show eth-cfm domain
===============================================================================
CFM Domain Table
===============================================================================
Md-index   Level Name                                          Format
-------------------------------------------------------------------------------
3          3                                                   none
4          4     IEEE-Domain                                   charString
===============================================================================
```

The chassis does not support a domain format of **none** for the 802.1ag contexts. The domain index, the first numerical value, is not related to the level, even though in this example they do match.

The following example illustrates the creation of the association within the domain context. The association links the construct to the service using the value of the bridge-identifier. The value specified for the bridge-identifier is equivalent to the numerical value used to create the service.

```
config>eth-cfm# info
----------------------------------------------
        domain 3 format none level 3
            association 1 format icc-based name "123456789abcd"
                bridge-identifier 100
                exit
            exit
            association 2 format string name "Y1731ContextIEEEFormat"
                bridge-identifier 300
                exit
            exit
        exit
        domain 4 name "IEEE-Domain" level 4
            association 1 format string name "UpTo45CharactersForIEEEString"
                bridge-identifier 100
```

```
                exit
                ccm-interval 1
            exit
        exit
-----------------------------------------
*A:cses-E01>config>eth-cfm#  show eth-cfm association

===============================================================================
CFM Association Table
===============================================================================
Md-index   Ma-index   Name                     CCM-intrvl Hold-time Bridge-id
-------------------------------------------------------------------------------
3          1          123456789abcd            10         n/a       100
3          2          Y1731ContextIEEEFormat   10         n/a       300
4          1          UpTo45CharactersForIEEE* 1          n/a       100
===============================================================================
```

* indicates that the corresponding row element may have been truncated..

This example show how to format the association within the domain to match the domain format, Y.1731 (domain 3/association 1) or 802.1ag (domain 4/association 1), and how the 802.1ag association format can be configured within a Y.1731 domain (domain 3/association 2). The mixed configuration represented by domain 3 association 2 may be of value in mixed Y.1731 and 802.1ag environments.

The CCM-interval is also specified within the association and has a default of 10 seconds unless specifically configured with another value. When the association is created and the MEP is a facility MEP the bridge-identifier is not to be included in the configuration since the facility MEP is not bound to a service. Facility MEPs are described in this chapter.

Maintenance Endpoint (MEP)/MEG Endpoint (MEP) are the workhorses of ETH-CFM. A MEP is the unique identification within the association (0-8191). Each MEP is uniquely identified by the MA-ID, MEPID tuple. This management entity is responsible for initiating, processing and terminating ETH-CFM functions, following the nesting rules. MEPs form the boundaries which prevent the ETH-CFM packets from flowing beyond the specific scope of responsibility. A MEP has direction, **up** or **down**. Each indicates the directions packets will be generated; UP toward the switch fabric, **down** toward the SAP away from the fabric. Each MEP has an active and passive side. Packets that enter the active point of the MEP will be compared to the existing level and processed accordingly. Packets that enter the passive side of the MEP are passed transparently through the MEP. Each MEP contained within the same maintenance association and with the same level (MA-ID) represents points within a single service. MEP creation on a SAP is allowed only for Ethernet ports with NULL, q-tags, q-in-q encapsulations.

Maintenance Intermediate Point (MIP)/MEG Intermediate Point (MIP) are management entities between the terminating MEPs along the service path. These provide insight into the service path connecting the MEPs. MIPs only respond to Loopback Messages (LBM) and Linktrace Messages (LTM). All other CFM functions are transparent to these entities. Only one MIP is allowed per SAP binding. The creation of the MIPs can be done when the lower level domain is created (explicit) or manually (default). This is controlled by the use of the mhf-creation mode within the

association under the bridge-identifier. MIP creation is supported on a SAP. By default, no MIPs are created.

There are two locations in the configuration where ETH-CFM is defined. The domains, associations (including linkage to the service id), MIP creation method, common ETH-CFM functions and remote MEPs are defined under the top level **eth-cfm** command. It is important to note, when Y.1731 functions are required the context under which the MEPs are configured must follow the Y.1731 specific formats (domain format of none). Once these parameters have been entered, the MEP and possibly the MIP can be defined within the service under the SAP binding.

This is a general table that indicates the ETH-CFM support for the different services and SAP or SDP binding. It is not meant to indicate the services that are supported or the requirements for those services on the individual platforms.

Table 3: ETH-CFM Support Matrix

Service	Description	MEP/MIP Support
Epipe (Ethernet SAP)	Ethernet Point to Point	Down MEP
VPLS (Ethernet SAP)	Multipoint Ethernet	Down MEP

Note1: Ethernet-Rings are not supported on 7210 SAS-D devices. Ethernet-Rings are not configurable under all service types. Any service restrictions for MEP direction or MIP support will override the generic capability of the Ethernet-Ring MPs. Please check the applicable user guide for applicability.

MA, MEP, MIP and MD Levels

Maintenance Domain (MD) levels are used to define CFM maintenance domains, Maintenance association End Points (MEPs) and Maintenance association Intermediate Points (MIPs) only communicate within the same level. It is carried in the CFM PDU to inform management entities where maintenance association (MA) the CFM PDU belongs. There are 8 levels defined. 0 is the lowest level, 7 is the highest level. The levels are nested, not overlapping. Overlapping is not allowed.

In IEEE 802.1ag, the MD is the part of the network where services are monitored (the administrative boundaries).

The first step to configure a maintenance domain:

CLI Syntax:
```
config>eth-cfm
 domain md-index [format {dns|mac|string}] name md-name level
 level
 domain md-index
 association ma-index [format {integer|string|vid|vpn-id}]
 name ma-name
 association ma-index
```

CFM levels include:

- MEP is an actively managed functional component, which implements CFM functionalities. Together, MEPs form the maintenance association.
- MIP is the intermediate point between MEPs.
- MEP and MIP perform different CFM functionalities.

Maintenance association (MA) includes a set of MEPs, each configured with the same MA-ID and MD level, verify the integrity of a single service instance.

The follow depicts a high-level view of MEPs and MIPs in a CFM-enabled network. Two MAs are displayed.

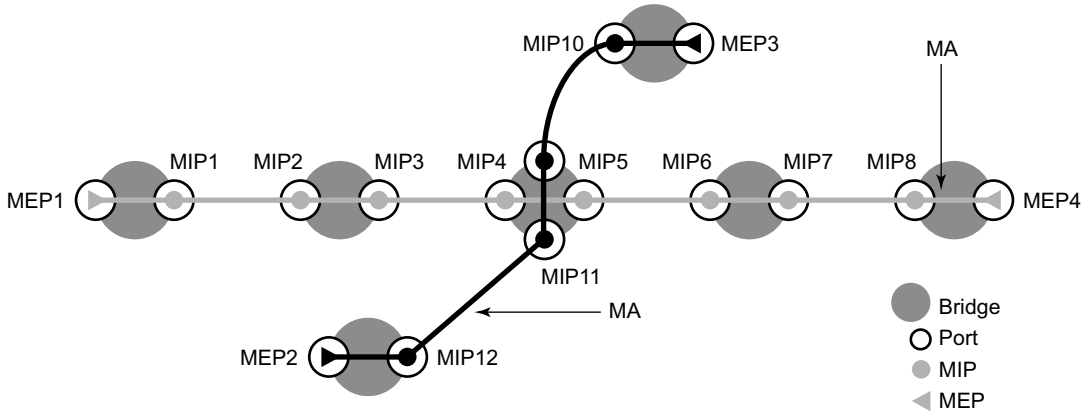

Figure 6: MEP and MIP

Figure 7 illustrates the usage of an EPIPE on two different nodes that are connected using ether SAP 1/1/2:100.31. The SAP 1/1/10:100.31 is an access port that is not used to connect the two nodes.

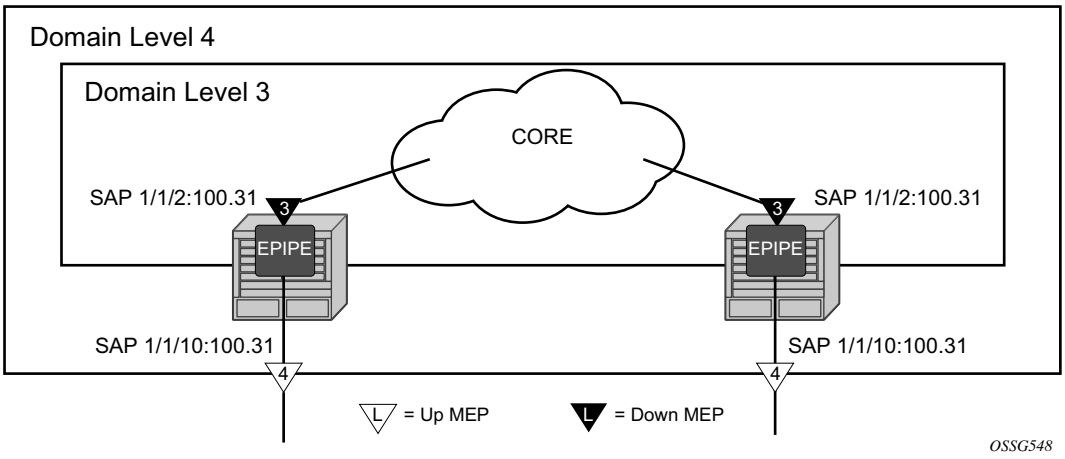

Figure 7: MEP Creation

```
NODE1
config>eth-cfm# info
----------------------------------------------
```

```
        domain 3 format none level 3
            association 1 format icc-based name "03-0000000101"
                bridge-identifier 100
                exit
            exit
        exit
        domain 4 format none level 4
            association 1 format icc-based name "04-0000000102"
                bridge-identifier 100
                exit
            exit
        exit

*A:cses-E01>config>service>epipe# info
----------------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                    mep 111 domain 3 association 1 direction down
                       mac-address d0:0d:1e:00:01:11
                        no shutdown
                    exit
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 101 domain 4 association 1 direction up
                        mac-address d0:0d:1e:00:01:01
                        no shutdown
                    exit
                exit
            exit
            no shutdown
----------------------------------------------

NODE 2
eth-cfm# info
----------------------------------------------
        domain 3 format none level 3
            association 1 format icc-based name "03-0000000101"
                bridge-identifier 100
                exit
            exit
        exit
        domain 4 format none level 4
            association 1 format icc-based name "04-0000000102"
                bridge-identifier 100
                exit
            exit
        exit
----------------------------------------------
*A:cses-E02>config>service>epipe# info
----------------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                    mep 112 domain 3 association 1 direction down
                        mac-address d0:0d:1e:00:01:12
                        no shutdown
                    exit
                exit
```

```
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 102 domain 4 association 1 direction up
                        mac-address d0:0d:1e:00:01:02
                        no shutdown
                    exit
                exit
            exit
            no shutdown
-----------------------------------------------
*A:cses-E02>config>service>epipe#
```

Examining the configuration from NODE1, MEP 101 is configured with a direction of UP causing all ETH-CFM traffic originating from this MEP to generate into the switch fabric and out the mate SAP 1/1/2:100.31. MEP 111 uses the default direction of DOWN causing all ETH-CFM traffic that is generated from this MEP to send away from the fabric and only egress the SAP on which it is configured, SAP 1/1/2:100.31.

Further examination of the domain constructs reveal that the configuration properly uses domain nesting rules. In this cas,e the Level 3 domain is completely contained in a Level 4 domain.

The following display was taken from NODE1.

```
show eth-cfm cfm-stack-table
===============================================================================
CFM Stack Table Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM, A = AisRx

===============================================================================
CFM SAP Stack Table
===============================================================================
Sap                Lvl Dir  Md-index   Ma-index   MepId  Mac-address     Defect
-------------------------------------------------------------------------------
1/1/2:100.31         3 Down          3          1  111 90:f3:01:01:00:02 ------
1/1/10:100.31        4   Up          4          1  101 d0:0d:1e:00:01:01 ------
===============================================================================
```

Figure 8 illustrates the creation of and explicit MIP.

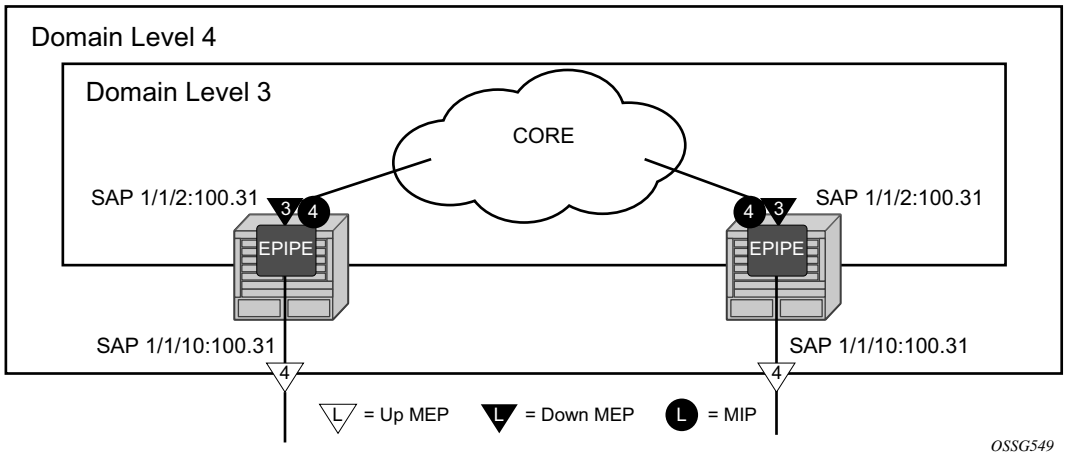

Figure 8: MIP Creation Example (NODE1)

```
NODE1
config>eth-cfm# info
----------------------------------------------
        domain 3 format none level 3
            association 1 format icc-based name "03-0000000101"
                bridge-identifier 100
                exit
            exit
        exit
        domain 4 format none level 4
            association 1 format icc-based name "04-0000000102"
                bridge-identifier 100
                exit
            exit
     association 2 format icc-based name "04-MIP0000102"
                bridge-identifier 100
                    mhf-creation explicit
                exit
            exit
        exit

config>service>epipe# info
----------------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                    mep 111 domain 3 association 1 direction down
                   mac-address d0:0d:1e:00:01:11
                            no shutdown
```

```
                    exit
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 101 domain 4 association 1 direction up
                        mac-address d0:0d:1e:00:01:01
                        no shutdown
                    exit
                exit
            exit
            no shutdown
-----------------------------------------------

NODE 2
eth-cfm# info
-----------------------------------------------
        domain 3 format none level 3
            association 1 format icc-based name "03-0000000101"
                bridge-identifier 100
                exit
            exit
        exit
        domain 4 format none level 4
            association 1 format icc-based name "04-0000000102"
                bridge-identifier 100
                exit
            exit
    association 2 format icc-based name "04-MIP0000102"
                bridge-identifier 100
                    mhf-creation explicit
                exit
            exit
        exit
-----------------------------------------------

config>service>epipe# info
-----------------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                    mep 112 domain 3 association 1 direction down
                        mac-address d0:0d:1e:00:01:12
                        no shutdown
                    exit
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 102 domain 4 association 1 direction up
                        mac-address d0:0d:1e:00:01:02
                        no shutdown
                    exit
                exit
            exit
            no shutdown
-----------------------------------------------
```

An addition of association 2 under domain four includes the **mhf-creation explicit** statement has been included. This means that when the level 3 MEP is assigned to the SAP 1/1/2:100.31 using the definition in domain 3 association 1, creating the higher level MIP on the same SAP. Since a MIP does not have directionality “Both” sides are active. The service configuration and MEP configuration within the service did not change.

The following output is from Node 1.

```
show eth-cfm cfm-stack-table
===============================================================================
CFM Stack Table Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM, A = AisRx

===============================================================================
CFM SAP Stack Table
===============================================================================
Sap                Lvl Dir  Md-index   Ma-index   MepId  Mac-address     Defect
-------------------------------------------------------------------------------
1/1/2:100.31         3 Down          3          1  111 d0:0d:1e:00:01:11 ------
1/1/2:100.31         4 Both          4          2  MIP 90:f3:01:01:00:02 ------
1/1/10:100.31        4   Up          4          1  101 d0:0d:1e:00:01:01 ------
===============================================================================
```

Figure 9 illustrates a simpler method that does not require the creation of the lower level MEP. The operator simply defines the association parameters and uses the **mhf-creation default** setting, then places the MIP on the SAP of their choice.

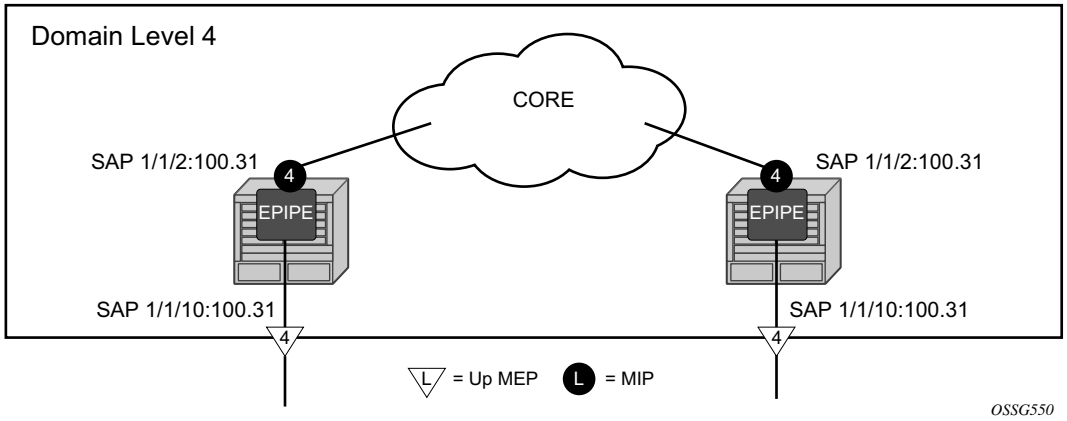

Figure 9: MIP Creation Default

```
NODE1
config>eth-cfm# info
----------------------------------------------
```

```
        domain 4 format none level 4
            association 1 format icc-based name "04-0000000102"
                bridge-identifier 100
                exit
            exit
            association 2 format icc-based name "04-MIP0000102"
                bridge-identifier 100
                    mhf-creation default
                exit
            exit
        exit
-----------------------------------------

config>service>epipe# info
-----------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                     mip mac d0:0d:1e:01:01:01
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 101 domain 4 association 1 direction up
                        mac-address d0:0d:1e:00:01:01
                        no shutdown
                    exit
                exit
            exit
            no shutdown
-----------------------------------------

# show eth-cfm cfm-stack-table
===============================================================================
CFM Stack Table Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM, A = AisRx
===============================================================================
CFM SAP Stack Table
===============================================================================
Sap                Lvl Dir  Md-index   Ma-index   MepId  Mac-address     Defect
-------------------------------------------------------------------------------
1/1/2:100.31         4 Both          4          2  MIP d0:0d:1e:01:01:01 ------
1/1/10:100.31        4   Up          4          1  101 d0:0d:1e:00:01:01 ------
===============================================================================

NODE2
config>eth-cfm# info
-----------------------------------------
        domain 4 format none level 4
            association 1 format icc-based name "04-0000000102"
                bridge-identifier 100
                exit
            exit
            association 2 format icc-based name "04-MIP0000102"
                bridge-identifier 100
                    mhf-creation default
                exit
            exit
        exit
-----------------------------------------
```

```
config>service>epipe# info
----------------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                    mip mac d0:0d:1e:01:01:02
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 102 domain 4 association 1 direction up
                        mac-address d0:0d:1e:00:01:02
                        no shutdown
                    exit
                exit
            exit
            no shutdown
----------------------------------------------

# show eth-cfm cfm-stack-table
===============================================================================
CFM Stack Table Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM, A = AisRx

===============================================================================
CFM SAP Stack Table
===============================================================================
Sap                Lvl Dir  Md-index   Ma-index   MepId  Mac-address     Defect
-------------------------------------------------------------------------------
1/1/2:100.31         4 Both          4          2  MIP d0:0d:1e:01:01:02 ------
1/1/10:100.31        4   Up          4          1  102 d0:0d:1e:00:01:02 ------
===============================================================================
```

Figure 10 shows the detailed IEEE representation of MEPs, MIPs, levels and associations, using the standards defined icons.

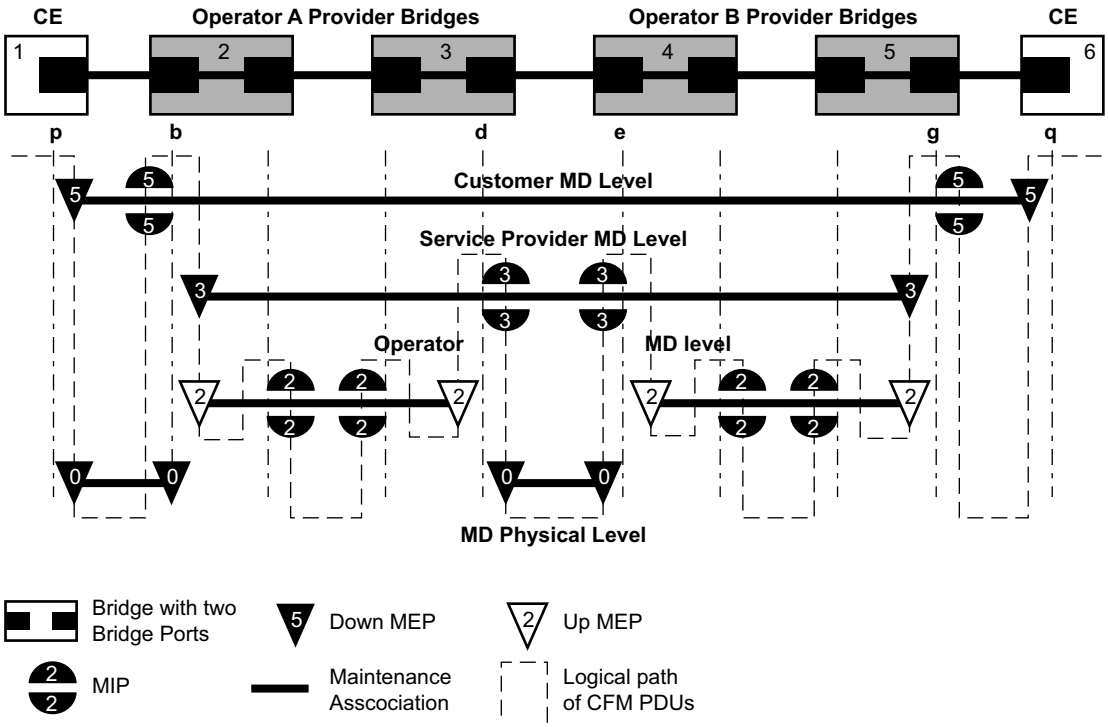

Figure 10: MEP, MIP and MD Levels

Loopback

A loopback message is generated by an MEP to its peer MEP (Figure 11). The functions are similar to an IP ping to verify Ethernet connectivity between the nodes.

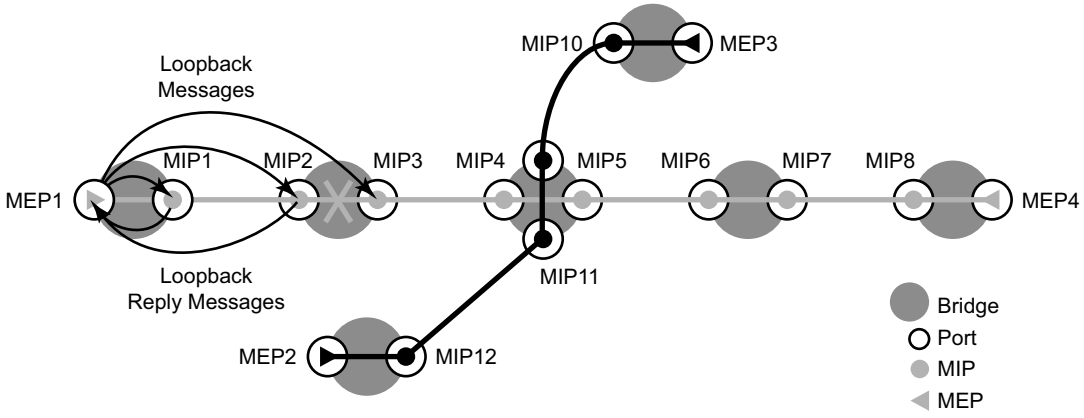

Figure 11: CFM Loopback

The following loopback-related functions are supported:

- Loopback message functionality on an MEP or MIP can be enabled or disabled.
- MEP — Supports generating loopback messages and responding to loopback messages with loopback reply messages.

- Displays the loopback test results on the originating MEP. There is a limit of ten outstanding tests per node.

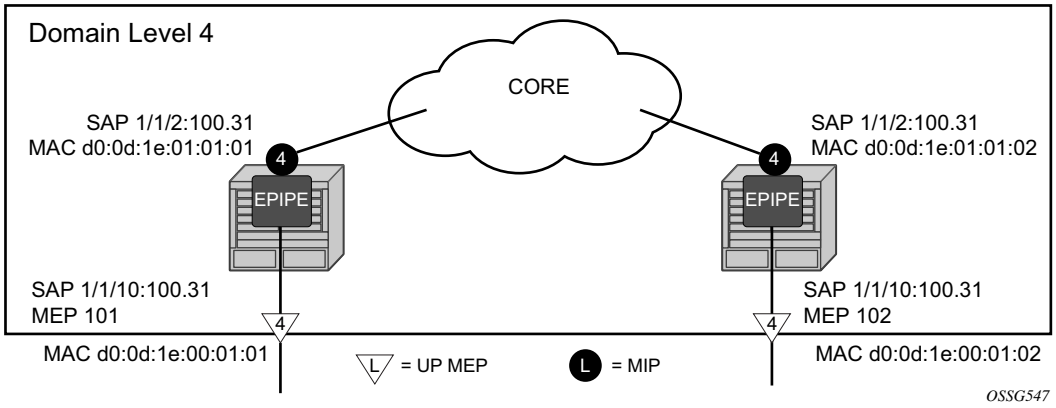

Figure 12: Loopback Configuration

```
# oam eth-cfm loopback d0:0d:1e:01:01:02 mep 101 domain 4 association
Eth-Cfm Loopback Test Initiated: Mac-Address: d0:0d:1e:01:01:02, out sap: 1/1/10:100.31
Sent 5 packets, received 5 packets [0 out-of-order, 0 Bad Msdu]

# oam eth-cfm loopback d0:0d:1e:00:01:02 mep 101 domain 4 association
Eth-Cfm Loopback Test Initiated: Mac-Address: d0:0d:1e:00:01:02, out sap: 1/1/10:100.31
Sent 5 packets, received 5 packets [0 out-of-order, 0 Bad Msdu]
```

Linktrace

A linktrace message is originated by an MEP and targeted to a peer MEP in the same MA and within the same MD level (Figure 13). Its function is similar to IP traceroute. Traces a specific MAC address through the service. The peer MEP responds with a linktrace reply message after successful inspection of the linktrace message. The MIPs along the path also process the linktrace message and respond with linktrace replies to the originating MEP if the received linktrace message that has a TTL greater than 1 and forward the linktrace message if a look up of the target MAC address in the Layer 2 FIB is successful. The originating MEP shall expect to receive multiple linktrace replies and from processing the linktrace replies, it can put together the route to the target bridge.

A traced MAC address is carried in the payload of the linktrace message, the target MAC. Each MIP and MEP receiving the linktrace message checks whether it has learned the target MAC address. In order to use linktrace the target MAC address must have been learned by the nodes in the network. If so, a linktrace message is sent back to the originating MEP. Also, a MIP forwards the linktrace message out of the port where the target MAC address was learned.

The linktrace message itself has a multicast destination address. On a broadcast LAN, it can be received by multiple nodes connected to that LAN. But, at most, one node will send a reply.

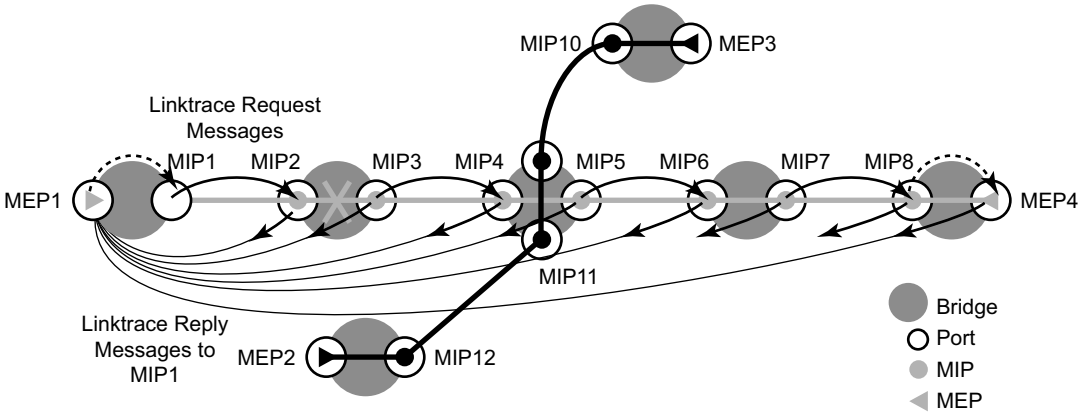

Figure 13: CFM Linktrace

The IEEE and ITU-T handle the linktrace reply slightly differently. An IEEE 802.1ag configured MEP requires the relay action field to be a valid non-zero integer. The ITU-T ignores the relay action field and will set the value to zero when when responding to the LTM. In mixed 802.ag and

Y.1731 environments the operator may chose to configure a Y.1731 context with an IEEE domain format.

The following linktrace related functions are supported:

- Enable or disables linktrace functions on an MEP.
- MEP — Supports generating linktrace messages and responding with linktrace reply messages.
- Displays linktrace test results on the originating MEP. There is a limit of ten outstanding tests per node. Storage is provided for up to ten MEPs and for the last ten responses. If more than ten responses are received older entries will be overwritten.

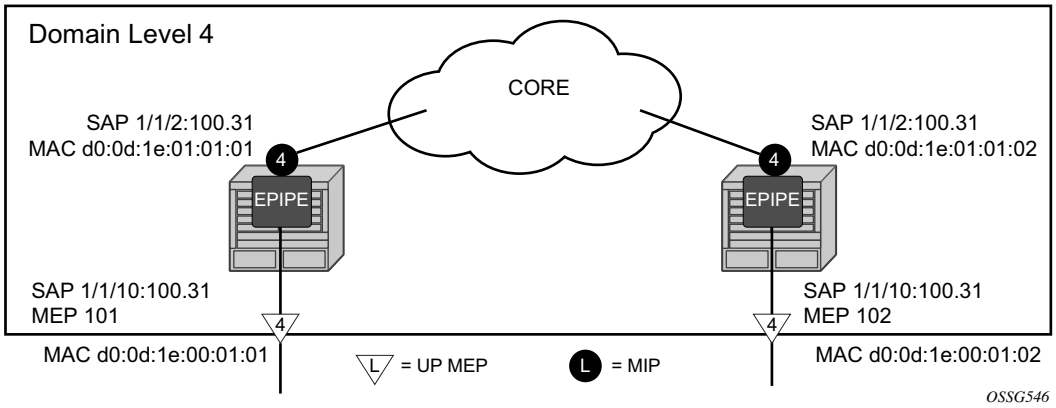

Figure 14: Linktrace Configuration

```
# oam eth-cfm linktrace d0:0d:1e:01:01:02 mep 101 domain 4 association 1

Index Ingress Mac          Egress Mac           Relay      Action
----- -------------------- -------------------- ---------- ----------
1     00:00:00:00:00:00    D0:0D:1E:01:01:01    n/a        forward
2     D0:0D:1E:01:01:02    00:00:00:00:00:00    n/a        none
----- -------------------- -------------------- ---------- ----------
No more responses received in the last 6 seconds.


# oam eth-cfm linktrace d0:0d:1e:00:01:02 mep 101 domain 4 association 1

Index Ingress Mac          Egress Mac           Relay      Action
----- -------------------- -------------------- ---------- ----------
1     00:00:00:00:00:00    D0:0D:1E:01:01:01    n/a        forward
2     D0:0D:1E:01:01:02    D0:0D:1E:00:01:02    n/a        terminate
----- -------------------- -------------------- ---------- ----------
```

```
No more responses received in the last 6 seconds.
```

Continuity Check (CC)

A Continuity Check Message (CCM) is a multicast frame that is generated by a MEP and multicast to all other MEPs in the same MA. The CCM does not require a reply message. To identify faults, the receiving MEP maintains an internal list of remote MEPs it should be receiving CCM messages from.

This list is based off of the remote-mepid configuration within the association the MEP is created in. When the local MEP does not receive a CCM from one of the configured remote MEPs within a pre-configured period, the local MEP raises an alarm.

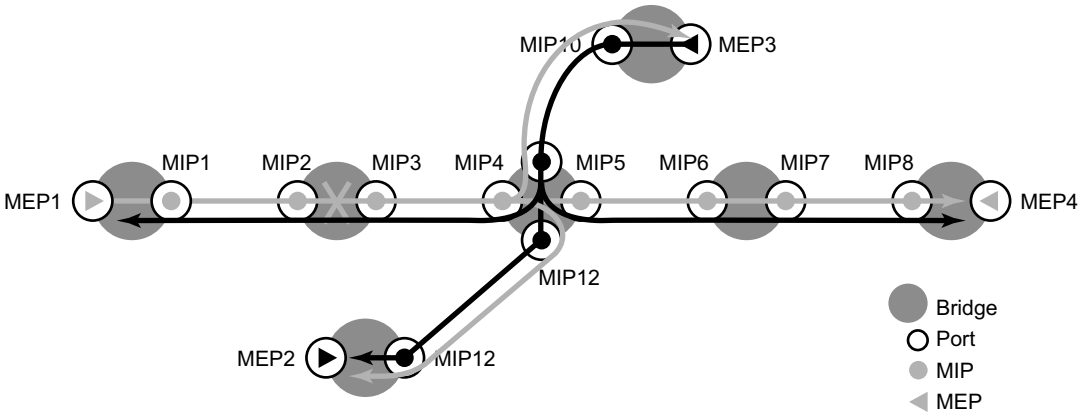

Figure 15: CFM Continuity Check

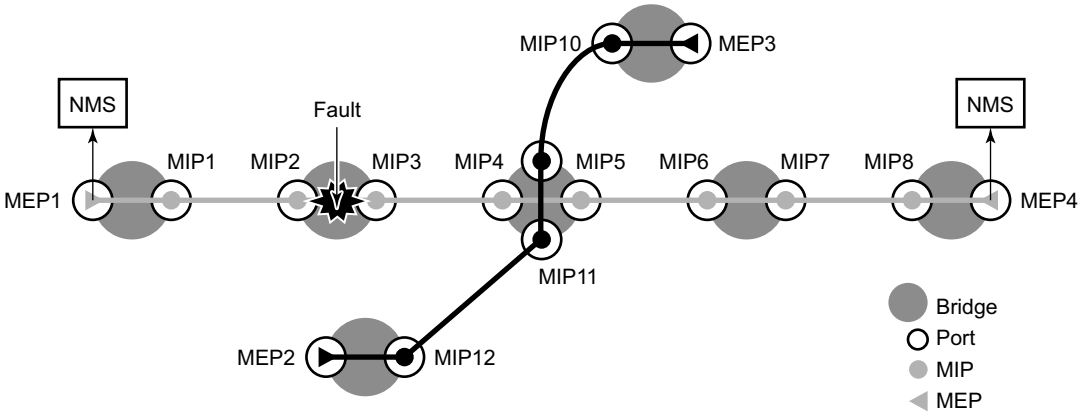

Figure 16: CFM CC Failure Scenario

The following functions are supported:

- Enable and disable CC for an MEP
- Configure and delete the MEP entries in the CC MEP monitoring database manually. It is only required to provision remote MEPs. Local MEPs shall be automatically put into the database when they are created.
- CCM transmit interval: 7210 SAS-E supports 1s,10s,60s and 600s. 7210 SAS-D supports 100ms,1s,10s,60s and 600s. Default: 10s. When configuring MEPs with sub-second CCM intervals bandwidth consumption must be taken into consideration. Each CCM PDU is 100 bytes (800 bits). Taken individually this is a small value. However, the bandwidth consumption increases rapidly as multiple MEPs are configured with 10ms timers, 100 packets per second. Sub-second enabled MEPs are supported on the following:
  - → Down MEPs configured on Ethernet SAPs.
  - → Lowest MD-level, when multiple MEPs exist on same Ethernet SAP.
  - → Individual Ethernet tunnel paths requiring EAPs but not on the Ethernet tunnel itself. This requires a the MEPs to be part of the Y.1731 context because of the EAPS.
- CCM will declare a fault, when:
  - → The CCM stops hearing from one of the remote MEPs for 3.5 times CC interval
  - → Hears from a MEP with a LOWER MD level
  - → Hears from a MEP that is not part of the local MEPs MA
  - → Hears from a MEP that is in the same MA but not in the configured MEP list
  - → Hears from a MEP in the same MA with the same MEP id as the receiving MEP
  - → The CC interval of the remote MEP does not match the local configured CC interval
  - → The remote MEP is declaring a fault
- An alarm is raised and a trap is sent if the defect is greater than or equal to the configured low-priority-defect value.
- Remote Defect Indication (RDI) is supported but by default is not recognized as a defect condition because the low-priority-defect setting default does not include RDI.

NODE1:

```
Config>eth-cfm# info
----------------------------------------------
        domain 4 format none level 4
            association 1 format icc-based name "04-0000000102"
                bridge-identifier 100
                exit
                ccm-interval 1
                remote-mepid 102
            exit
        exit
----------------------------------------------
```

NODE2:

```
config>eth-cfm# info
----------------------------------------------
        domain 4 format none level 4
            association 1 format icc-based name "04-0000000102"
                bridge-identifier 100
                exit
                ccm-interval 1
                remote-mepid 101
            exit
        exit
----------------------------------------------
```

Common CCM attributes are defined within the association, including the list of remote peers and interval. Once this is complete, the MEP configured on the SAP within the service must enabled CCM and the priority of the packet can be set.

NODE1:

```
config>service>epipe# info
----------------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                    mip mac D0:0D:1E:01:01:01
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 101 domain 4 association 1 direction up
                        ccm-enable
                        mac-address d0:0d:1e:00:01:01
                        no shutdown
                    exit
                exit
            exit
            no shutdown
----------------------------------------------
```

NODE2:

```
config>service>epipe# info
----------------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                    mip mac D0:0D:1E:01:01:02
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 102 domain 4 association 1 direction up
                        ccm-enable
                        mac-address d0:0d:1e:00:01:02
                        no shutdown
                    exit
                exit
            exit
            no shutdown
----------------------------------------------
```

There are various display commands that are available to show the status of the MEP and the list of remote peers. The following illustrates the output from a few of these display commands, taken from NODE1.

No defect conditions are raised. The **Defect** column in the first display is clear and the **Defect Flags** is the second display is also clear.

```
show eth-cfm cfm-stack-table
===============================================================================
CFM Stack Table Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM, A = AisRx

===============================================================================
CFM SAP Stack Table
===============================================================================
Sap                Lvl Dir  Md-index   Ma-index   MepId  Mac-address     Defect
-------------------------------------------------------------------------------
1/1/2:100.31         4 Both          4          2  MIP d0:0d:1e:01:01:01 ------
1/1/10:100.31        4   Up          4          1  101 d0:0d:1e:00:01:01 ------
===============================================================================

show eth-cfm mep 101 domain 4 association 1
===============================================================================
Eth-Cfm MEP Configuration Information
===============================================================================
Md-index           : 4                       Direction         : Up
Ma-index           : 1                       Admin             : Enabled
MepId              : 101                     CCM-Enable        : Enabled
IfIndex            : 35979264                PrimaryVid        : 2031716
Description        : (Not Specified)
FngState           : fngReset                ControlMep        : False
LowestDefectPri    : macRemErrXcon           HighestDefect     : none
Defect Flags       : None
Mac Address        : d0:0d:1e:00:01:01       ControlMep        : False
CcmLtmPriority     : 7
CcmTx              : 1639                    CcmSequenceErr    : 0
Fault Propagation  : disabled                FacilityFault     : n/a
MA-CcmInterval     : 1                       MA-CcmHoldTime    : 0ms
```

```
Eth-1Dm Threshold  : 3(sec)                   MD-Level          : 4
Eth-Ais:           : Disabled
Eth-Tst:           : Disabled

Redundancy:
    MC-LAG State   : n/a

CcmLastFailure Frame:
    None

XconCcmFailure Frame:
    None
===============================================================================
```

The **all-remote-mepids** is the appropriate command to show the details for each configured peer, including the MAC address.

```
show eth-cfm mep 101 domain 4 association 1 all-remote-mepids

===============================================================================
Eth-CFM Remote-Mep Table
===============================================================================
R-mepId Rx CC  Rx Rdi Port-Tlv If-Tlv Peer Mac Addr     CCM status since
-------------------------------------------------------------------------------
102     True   False  Up       Up     d0:0d:1e:00:01:02 02/02/2011 13:37:42
===============================================================================
```

CCM Hold Timers

In some cases the requirement exists to prevent a MEP from entering the defRemoteCCM defect, remote peer timeout, from more time than the standard 3.5 times the CCM-interval. Both the IEEE 802.1ag standard and ITU-T Y.1731 recommendation provide a non-configurable 3.5 times the CCM interval to determine a peer time out. However, when sub second CCM timers (10ms/ 100ms) are enabled the carrier may want to provide additional time for different network segments to converge before declaring a peer lost because of a timeout. In order to maintain compliance with the specifications the `ccm-hold-timer down <delay-down>` option has been introduced to artificially increase the amount of time it takes for a MEP to enter a failed state should the peer time out. This timer is only additive to CCM timeout conditions. All other CCM defect conditions, like defMACStatus, defXconCCM, and so on, will maintain their existing behavior of transitioning the MEP to a failed state and raising the proper defect condition without delay.

When the **ccm-hold-timer down** *delay-down* option is configured the following calculation is used to determine the remote peer time out (3.5 times the CCM-Interval + ccm-hold-timer delay-down).

This command is configured under the association. Only sub second CCM enabled MEPs support this hold timer. Ethernet-Tunnel Paths use a similar but slightly different approach and will continue to utilize the existing method. Ethernet-tunnels will be blocked from using this new hold timer.

It is possible to change this command on the fly without deleting it first. Simply entering the command with the new values will change to values without having to delete the command prior to the change.

It is possible to change the ccm-interval of a MEP on the fly without first deleting it. This means it is possible to change a sub second CCM enabled MEP to 1 second or above. The operator will be prevented from changing an association from a sub second CCM interval to a non-sub second CCM interval when a `ccm-hold-timer` is configured in that association. The `ccm-hold-timer` must be removed using the `no` option prior to allowing the transition from sub second to non-sub second CCM interval.

Alarm Indication Signal (ETH-AIS Y.1731)

Alarm Indication Signal (AIS) provides an Y.1731 capable MEP the ability to signal a fault condition in the reverse direction of the MEP, out the passive side. When a fault condition is detected the MEP will generate AIS packets at the configured client levels and at the specified AIS interval until the condition is cleared. Currently a MEP configured to generate AIS must do so at a level higher than its own. The MEP configured on the service receiving the AIS packets is required to have the active side facing the receipt of the AIS packet and must be at the same level the AIS, The absence of an AIS packet for 3.5 times the AIS interval set by the sending node will clear the condition on the receiving MEP.

AIS generation is also not subject to the low-priority-defect setting. AIS, when enabled, generates when the MEP enters any defect condition, including RDI.

AIS configuration has two components: receive and transmit. AIS reception is enabled when the command **ais-enable** is configured under the MEP. The transmit function is enabled when the **client-meg-level** is configured.

Alarm Indication Signal function is used to suppress alarms at the client (sub) layer following detection of defect conditions at the server (sub) layer. Due to independent restoration capabilities provided within the Spanning Tree Protocol (STP) environments, ETHAIS is not expected to be applied in the STP environment.

Transmission of frames with ETH-AIS information can be enabled or disabled on a MEP. Frames with ETH-AIS information can be issued at the client MEG Level by a MEP, including a Server MEP, upon detecting the following conditions:

- Signal failure conditions in the case that ETH-CC is enabled.
- AIS condition in the case that ETH-CC is disabled.

For a point-to-point ETH connection at the client (sub) layer, a client layer MEP can determine that the server (sub) layer entity providing connectivity to its peer MEP has encountered defect condition upon receiving a frame with ETH-AIS information. Alarm suppression is straightforward since a MEP is expected to suppress defect conditions associated only with its peer MEP.

For multipoint ETH connectivity at the client (sub) layer, a client (sub) layer MEP cannot determine the specific server (sub)layer entity that has encountered defect conditions upon receiving a frame with ETH-AIS information. More importantly, it cannot determine the associated subset of its peer MEPs for which it should suppress alarms since the received ETHAIS information does not contain that information. Therefore, upon reception of a frame with ETH-AIS information, the MEP will suppress alarms for all peer MEPs whether there is still connectivity or not.

Only a MEP, including a Server MEP, is configured to issue frames with ETH-AIS information. Upon detecting a defect condition the MEP can immediately start transmitting periodic frames with ETHAIS information at a configured client MEG Level. A MEP continues to transmit periodic frames with ETH-AIS information until the defect condition is removed. Upon receiving a frame with ETH-AIS information from its server (sub) layer, a client (sub) layer MEP detects AIS condition and suppresses alarms associated with all its peer MEPs. A MEP resumes alarm generation upon detecting defect conditions once AIS condition is cleared.

Specific configuration information required by a MEP to support ETH-AIS is the following:

- Client MEG Level — MEG level at which the most immediate client layer MIPs and MEPs exist.
- ETH-AIS transmission period — Determines transmission periodicity of frames with ETH-AIS information.
- Priority — Identifies the priority of frames with ETH-AIS information.
- Drop Eligibility — Frames with ETH-AIS information are always marked as drop ineligible.

A MIP is transparent to frames with ETH-AIS information and therefore does not require any information to support ETH-AIS functionality.

It is important to note that Facility MEPs do not support the generation of AIS to an explicitly configured endpoint. An explicitly configured endpoint is an object that contains multiple individual endpoints, as in PW redundancy.

AIS is enabled under the service and has two parts, receive and transmit. Both of the components have their own configuration option. The **ais-enable** command under the SAP allows for the processing of received AIS packets at the MEP level. The **client-meg-level** command is the transmit portion that generates AIS if the MEP enter a fault state. AIS is independent of the **low-priority-defect** setting, so that any fault in the MEP causes AIS to be generated.

```
config>service>epipe# info
----------------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                    mip mac D0:0D:1E:01:01:01
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 101 domain 4 association 1 direction up
                        ais-enable
                            client-meg-level 5
                        exit
                        ccm-enable
                        mac-address d0:0d:1e:00:01:01
                        no shutdown
                    exit
                exit
```

```
            exit
            no shutdown
-----------------------------------------------
```

When MEP 101 enters a defect state, it starts to generate AIS out the passive side of the MEP, away from the fault. In this case, the AIS generates out sap 1/1/10:100.31 since MEP 101 is an up MEP on that SAP. The **Defect Flag** indicates that an RDI error state has been encountered and even though the **LowestDefectPri** setting is higher than the existing defect AIS is being transmitted. The **Eth-Ais Tx Counted** value is increasing, indicating that AIS is actively being sent.

```
# show eth-cfm mep 101 domain 4 association 1
===============================================================================
Eth-Cfm MEP Configuration Information
===============================================================================
Md-index           : 4                        Direction         : Up
Ma-index           : 1                        Admin             : Enabled
MepId              : 101                      CCM-Enable        : Disabled
IfIndex            : 35979264                 PrimaryVid        : 2031716
Description        : (Not Specified)
FngState           : fngReset                 ControlMep        : False
LowestDefectPri    : macRemErrXcon            HighestDefect     : none
Defect Flags       : bDefRDICCM
Mac Address        : d0:0d:1e:00:01:01        ControlMep        : False
CcmLtmPriority     : 7
CcmTx              : 2578                     CcmSequenceErr    : 0
Fault Propagation  : disabled                 FacilityFault     : n/a
MA-CcmInterval     : 1                        MA-CcmHoldTime    : 0ms
Eth-1Dm Threshold  : 3(sec)                   MD-Level          : 4
Eth-Ais:           : Enabled                  Eth-Ais Rx Ais:   : No
Eth-Ais Tx Priorit*: 7                        Eth-Ais Rx Interv*: 1
Eth-Ais Tx Interva*: 1                        Eth-Ais Tx Counte*: 288
Eth-Ais Tx Levels  : 5
Eth-Tst:           : Disabled

Redundancy:
    MC-LAG State   : n/a

CcmLastFailure Frame:
    None

XconCcmFailure Frame:
    None
===============================================================================
```

Test (ETH-TST Y.1731)

Ethernet test affords operators an Y.1731 capable MEP the ability to send an in service on demand function to test connectivity between two MEPs. The test is generated on the local MEP and the results are verified on the destination MEP. Any ETH-TST packet generated that exceeds the MTU will be silently dropped by the lower level processing of the node.

Specific configuration information required by a MEP to support ETH-test is the following:

- MEG level — MEG level at which the MEP exists
- Unicast MAC address of the peer MEP for which ETH-test is intended.
- Data - Optional element whose length and contents are configurable at the MEP.
- Priority — Identifies the priority of frames with ETH-Test information.
- Drop Eligibility — Identifies the eligibility of frames with ETHTest information to be dropped when congestion conditions are encountered.

A MIP is transparent to the frames with ETH-Test information and does not require any configuration information to support ETH-Test functionality.

Both nodes require the eth-test function to be enabled in order to successfully execute the test. Since this is a dual-ended test, initiate on sender with results calculated on the receiver, both nodes need to be check to see the results.

```
NODE1
config>service>epipe# info
----------------------------------------------
            sap 1/1/2:100.31 create
                eth-cfm
                    mip mac D0:0D:1E:01:01:01
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 101 domain 4 association 1 direction up
                        eth-test-enable
                        exit
                        mac-address d0:0d:1e:00:01:01
                        no shutdown
                    exit
                exit
            exit
            no shutdown
----------------------------------------------
# oam eth-cfm eth-test d0:0d:1e:00:01:02 mep 101 domain 4 association 1 data-length 1000
# oam eth-cfm eth-test d0:0d:1e:00:01:02 mep 101 domain 4 association 1 data-length 1000
# oam eth-cfm eth-test d0:0d:1e:00:01:02 mep 101 domain 4 association 1 data-length 1000

NODE2
config>service>epipe# info
----------------------------------------------
```

```
            sap 1/1/2:100.31 create
                eth-cfm
                    mip mac D0:0D:1E:01:01:02
                exit
            exit
            sap 1/1/10:100.31 create
                eth-cfm
                    mep 102 domain 4 association 1 direction up
                        eth-test-enable
                        exit
                        mac-address d0:0d:1e:00:01:02
                        no shutdown
                    exit
                exit
            exit
            no shutdown
-----------------------------------------------

# show eth-cfm mep 102 domain 4 association 1 eth-test-results
===============================================================
Eth CFM ETH-Test Result Table
===============================================================
                                Current        Accumulate
                  FrameCount    ErrBits        ErrBits
Peer Mac Addr     ByteCount     CrcErrs        CrcErrs
---------------------------------------------------------------
d0:0d:1e:00:01:01 3             0              0
                  3000          0              0
===============================================================
```

One-Way Delay Measurement (ETH-1DM Y.1731)

Note: 7210 SAS-D devices do not support One-Way Delay Measurement.

One-way delay measurement allows the operator the ability to check unidirectional delay between MEPs. An ETH-1DM packet is time stamped by the generating MEP and sent to the remote node. The remote node time stamps the packet on receipt and generates the results. The results, available from the receiving MEP, will indicate the delay and jitter. Jitter, or delay variation, is the difference in delay between tests. This means the delay variation on the first test will not be valid. It is important to ensure that the clocks are synchronized on both nodes to ensure the results are accurate. NTP can be used to achieve a level of wall clock synchronization between the nodes.

Note: Accuracy relies on the nodes ability to timestamp the packet in hardware. 7210 SAS-E devices support only software based time stamping. Network elements that do not support hardware time stamping like 7210 SAS-E, display different results than hardware time-stamp capable devices.

Two-Way Delay Measurement (ETH-DMM Y.1731)

Note: 7210 SAS-D devices do not support Two-Way Delay Measurement.

Two-way delay measurement is similar to one way delay measurement except it measures the round trip delay from the generating MEP. In this case wall clock synchronization issues will not influence the test results because four timestamps are used. This allows the remote nodes time to be removed from the calculation and as a result clock variances are not included in the results. The same consideration for first test and hardware based time stamping stated for one way delay measurement are applicable to two-way delay measurement.

Delay can be measured using one-way and two-way on demand functions. The two-way test results are available single-ended, test initiated, calculation and results viewed on the same node. There is no specific configuration under the MEP on the SAP in order to enabled this function. An example of an on demand test and results are below. The latest test result is stored for viewing. Further tests will overwrite the previous results. Delay Variation is only valid if more than one test has been executed.

```
oam eth-cfm two-way-delay-test d0:0d:1e:00:01:02 mep 101 domain 4 association 1

Two-Way-Delay-Test Response:
Delay 2955 microseconds        Variation 111 microseconds

# show eth-cfm mep 101 domain 4 association 1 two-way-delay-test
===============================================================
Eth CFM Two-way Delay Test Result Table
===============================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
---------------------------------------------------------------
```

```
d0:0d:1e:00:01:02     2955                111
===============================================================================
```

Service Assurance Agent Overview

In the last few years, service delivery to customers has drastically changed. Services such as are offered. The introduction of Broadband Service Termination Architecture (BSTA) applications such as Voice over IP (VoIP), TV delivery, video and high speed Internet services force carriers to produce services where the health and quality of Service Level Agreement (SLA) commitments are verifiable to the customer and internally within the carrier.

SAA is a feature that monitors network operations using statistics such as jitter, latency, response time, and packet loss. The information can be used to troubleshoot network problems, problem prevention, and network topology planning.

The results are saved in SNMP tables are queried by either the CLI or a management system. Threshold monitors allow for both rising and falling threshold events to alert the provider if SLA performance statistics deviate from the required parameters.

SAA allows two-way timing for several applications. This provides the carrier and their customers with data to verify that the SLA agreements are being properly enforced.

Traceroute Implementation

In the 7210 SAS, for various applications, such as IP traceroute, control CPU inserts the timestamp in software.

When interpreting these timestamps care must be taken that some nodes are not capable of providing timestamps, as such timestamps must be associated with the same IP-address that is being returned to the originator to indicate what hop is being measured.

NTP

Because NTP precision can vary (+/- 1.5ms between nodes even under best case conditions), SAA one-way latency measurements might display negative values, especially when testing network segments with very low latencies. The one-way time measurement relies on the accuracy of NTP between the sending and responding nodes.

Configuring SAA Test Parameters

The following example displays an SAA configuration:

```
*A:7210 SAS>config>saa# info
----------------------------------------------
        test "abc"
            shutdown
            description "test"
            jitter-event rising-threshold 100 falling-threshold 10
            loss-event rising-threshold 300 falling-threshold 30
            latency-event rising-threshold 100 falling-threshold 20
        exit
----------------------------------------------
*A:7210 SAS>config>saa#
```

Diagnostics Command Reference

OAM Commands

Base Operational Commands

GLOBAL

— **ping** [*ip-address* | *dns-name*] [**rapid** | **detail**] [**ttl** *time-to-live*] [**tos** *type-of-service*] [**size** *bytes*] [**pattern** *pattern*] [**source** *ip-address*] [**interval** *seconds*] [{**next-hop** *ip-address*} | {**interface** *interface-name*} | **bypass-routing**] [**count** *requests*] [**do-not-fragment**] [**router** *router-instance*] [**timeout** *timeout*]

— **traceroute** [*ip-address* | *dns-name*] [**ttl** *ttl*] [**wait** *milli-seconds*] [**no-dns**][**source** *src-ip-address*] [**tos** *type-of-service*] [**router** [*router-instance*]

— **oam**

— **dns target-addr** *dns-name* **name-server** *ip-address* [**source** *ip-address*] [**send-count** *send-count*] [**timeout** *timeout*] [**interval** *interval*]

— **saa** *test-name* [**owner** *test-owner*] {**start** | **stop**}

Ethernet in the First Mile (EFM) Commands

GLOBAL

— **oam**

— **efm** *port-id* **local-loopback** {**start** | **stop**}

— **efm** *port-id* **remote-loopback** {**start** | **stop**}

ETH-CFM OAM Commands

oam

— **eth-cfm eth-test** ***mac-address*** **mep** ***mep-id*** **domain** ***md-index*** **association** ***ma-index*** [**priority** *priority*] [**data-length** *data-length*]

— **eth-cfm linktrace** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**ttl** *ttl-value*]

— **eth-cfm loopback** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**send-count** *send-count*] [**size** *data-size*] [**priority** *priority*]

— **eth-cfm one-way-delay-test** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*]

— **eth-cfm two-way-delay-test** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*]

— **eth-cfm two-way-slm-test** ***mac-address*** **mep** ***mep-id*** **domain** ***md-index*** **association** ***ma-index*** **[priority** *priority***]] [send-count** ***send-count*** **][size data-size][timeout** ***timeout***] [interval** ***interval***]**

SAA Commands

config
- **saa**
  - [**no**] **test** *test-name* [**owner** *test-owner*]
    - **description** *description-string*
    - **no description**
    - [**no**] **jitter-event** **rising-threshold** *threshold* [**falling-threshold** *threshold*] [*direction*]
    - [**no**] **latency-event** **rising-threshold** *threshold* [**falling-threshold** *threshold*] [*direction*]
    - [**no**] **loss-event** **rising-threshold** *threshold* [**falling-threshold** *threshold*] [*direction*]
    - [**no**] **shutdown**
    - **trap-gen**
      - [**no**] **probe-fail-enable**
      - [**no**] **probe-fail-threshold** *0..15*
      - [**no**] **test-completion-enable**
      - [**no**] **test-fail-enable**
      - [**no**] **test-fail-threshold** *0..15*
    - [**no**] **type**
      - **dns** **target-addr** *dns-name* **name-server** *ip-address* [**source** *ip-address*] [**send-count** *send-count*] [**timeout** *timeout*] [**interval** *interval*]
      - **icmp-ping** [*ip-address* | *dns-name*] [**rapid** | **detail**] [**ttl** *time-to-live*] [**tos** *type-of-service*] [**size** *bytes*] [**pattern** *pattern*] [**source** *ip-address*] [**interval** *seconds*] [{**next-hop** *ip-address*}|{**interface** *interface-name*}|**bypass-routing**] [**count** *requests*] [**do-not-fragment**] [**router** *router-instance*] [**timeout** *timeout*]
      - **icmp-trace** [*ip-address* | *dns-name*] [**ttl** *time-to-live*] [**wait** *milli-seconds*] [**source** *ip-address*] [**tos** *type-of-service*] [**router** *router-instance*]

Show Commands

show

- **eth-cfm**
  - **association** [*ma-index*] [**detail**]
  - **cfm-stack-table** [**port** [*port-id* [**vlan** *vlan-id*]][**level** 0..7] [**direction down**]
  - **cfm-stack-table**
  - **cfm-stack-table port** [**{all-ports**[**level** <0..7>][**direction** < **down**>]
  - **cfm-stack-table** <*port-id*> [**vlan** <**qtag**[*.qtag*]>] [**level** <0..7>] **[direction < down>]**
  - **cfm-stack-table facility [{all-ports|all-lags|all-lag-ports|all-tunnel-meps| all-router-interfaces}] [level** <0..7>**] [direction <down>]**
  - **cfm-stack-table facility lag** <*id*> **[tunnel** <1..4094>**] [level** <0..7>**] [direction <down>]**
  - **cfm-stack-table facility port** <*id*> **[level** <0..7>**] [direction <down>]**
  - **cfm-stack-table facility router-interface** <*ip-int-name*> **[level** <0..7>**] [direction <down>]**
  - **domain** [*md-index*] [**association** *ma-index* | **all-associations**] [**detail**]
  - **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**loopback**] [**linktrace**]
  - **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**remote-mepid** *mep-id* | **all-remote-mepids**]
  - **mep** *mep-id* **domain** *md-index* **association** *ma-index* **eth-test-results** [**remote-peer** *mac-address*]
  - **mep** *mep-id* **domain** *md-index* **association** *ma-index* **one-way-delay-test** [**remote-peer** *mac-address*]
  - **mep** *mep-id* **domain** *md-index* **association** *ma-index* **two-way-delay-test** [**remote-peer** *mac-address*]
  - **mep** *mep-id* **domain** *md-index* **association** *ma-index* **two-way-slm-test** [**remote-peer** *mac-address*]
- **saa** [*test-name* [**owner** *test-owner*]]

Clear Commands

clear

- **saa** [*test-name* [**owner** *test-owner*]]

OAM and SAA Commands

Command Hierarchies

Operational Commands

shutdown

Syntax [**no**] **shutdown**

Context config>saa>test

Description In order to modify an existing test it must first be shut down. When a test is created it will be in shutdown mode until a **no shutdown** command is executed.

A **shutdown** can only be performed if a test is not executing at the time the command is entered.

Use the **no** form of the command to set the state of the test to operational.

dns

Syntax **dns target-addr** *dns-name* **name-server** *ip-address* [**source** *ip-address*] [**send-count** *send-count*] [**timeout** *timeout*] [**interval** *interval*]

Context oam

Description This command performs DNS name resolution. If ipv4-a-record is specified, dns-names are queried for A-records only.

Parameters *ip-address* — The IP address of the primary DNS server.

ipv4-address - a.b.c.d

timeout *timeout* **—** The **timeout** parameter in seconds, expressed as a decimal integer. This value is used to override the default **timeout** value and is the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. Any response received after the request times out will be silently discarded.

Default 5

Values 1 — 120

interval *interval* **—** The **interval** parameter in seconds, expressed as a decimal integer. This parameter is

used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Default 1

Values 1 — 10

ping

Syntax **ping** [*ip-address* | *dns-name*] [**rapid** | **detail**] [**ttl** *time-to-live*] [**tos** *type-of-service*] [**size** *bytes*] [**pattern** *pattern*] [**source** *ip-address* | *dns-name*] [**interval** *seconds*] [{**next-hop** *ip-address*} | {**interface** *interface-name*} | **bypass-routing**] [**count** *requests*] [**do-not-fragment**] [**router** *router-instance*] [**timeout** *timeout*]

Context <GLOBAL>

Description This command verifies the reachability of a remote host.

Parameters *ip-address* — The far-end IP address to which to send the **icmp-ping** request message in dotted decimal notation.

Values ipv4-address: a.b.c.d

dns-name — The DNS name of the far-end device to which to send the **icmp-ping** request message, expressed as a character string.

rapid — Packets will be generated as fast as possible instead of the default 1 per second.

detail — Displays detailed information.

ttl *time-to-live* **—** The TTL value for the IP TTL, expressed as a decimal integer.

Values 1 — 128

tos *type-of-service* **—** Specifies the service type.

Values 0 — 255

size *bytes* **—** The request packet size in bytes, expressed as a decimal integer.

Values 0 — 16384

pattern *pattern* **—** The date portion in a ping packet will be filled with the pattern value specified. If not specified, position info will be filled instead.

Values 0 — 65535

source *ip-address* **—** Specifies the IP address to be used.

Values ipv4-address: a.b.c.d

router *router-instance* **—** Specifies the router name or service ID.

Values *router-name*: Base

Default Base

bypass-routing — Specifies whether to send the ping request to a host on a directly attached network bypassing the routing table.

interface *interface-name* — Specifies the name of an IP interface. The name must already exist in the **config>router>interface** context.

next-hop *ip-address* **—** Only displays static routes with the specified next hop IP address.

Values ipv4-address: a.b.c.d (host bits must be 0)

count *requests* **—** Specifies the number of times to perform an OAM ping probe operation. Each OAM echo message request must either timeout or receive a reply before the next message request is sent.

Values 1 — 100000

Default 5

do-not-fragment — Sets the DF (Do Not Fragment) bit in the ICMP ping packet.

timeout *seconds* **—** Overrides the default **timeout** value and is the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. A 'request timeout' message is displayed by the CLI for each message request sent that expires. Any response received after the request times out will be silently discarded.

Default 5

Values 1 — 10

traceroute

Syntax **traceroute** [*ip-address* |*dns-name*] [**ttl** *ttl*] [**wait** *milli-seconds*] [**no-dns**] [**source** *ip-address*] [tos *type-of-service*] [**router** *router-instance*]

Context oam

Description The TCP/IP traceroute utility determines the route to a destination address. DNS lookups of the responding hosts is enabled by default.

```
*A:ALA-1# traceroute 192.168.xx.xx4
traceroute to 192.168.xx.xx4, 30 hops max, 40 byte packets
 1  192.168.xx.xx4 0.000 ms  0.000 ms  0.000 ms
*A:ALA-1#
```

Parameters *ip-address* — The far-end IP address to which to send the traceroute request message in dotted decimal notation.

Values ipv4-address : a.b.c.d

d*ns-name* — The DNS name of the far-end device to which to send the traceroute request message, expressed as a character string.

ttl *ttl* **—** The maximum Time-To-Live (TTL) value to include in the traceroute request, expressed as a decimal integer.

Values 1 — 255

wait *milliseconds* **—** The time in milliseconds to wait for a response to a probe, expressed as a decimal integer.

Default 5000

Values 1 — 60000

no-dns — When the **no-dns** keyword is specified, DNS lookups of the responding hosts will not be performed, only the IP addresses will be printed.

Default DNS lookups are performed

source *ip-address* **—** The source IP address to use as the source of the probe packets in dotted decimal notation. If the IP address is not one of the device's interfaces, an error is returned.

tos *type-of-service* **—** The type-of-service (TOS) bits in the IP header of the probe packets, expressed as a decimal integer.

Values 0 — 255

router *router-name* **—** Specify the alphanumeric character string up to 32 characters.

Default Base

Values

EFM Commands

efm

Syntax *port-id*

Context oam>efm

Description This command enables Ethernet in the First Mile (EFM) OAM tests loopback tests on the specified port. The EFM OAM remote loopback OAMPDU will be sent to the peering device to trigger remote loopback.

Parameters *port-id* — Specify the port ID in the slot/mda/port format.

local-loopback

Syntax **local-loopback** {**start** | **stop**}

Context oam>efm

Description This command enables local loopback tests on the specified port.

remote-loopback

Syntax **remote-loopback** {**start** | **stop**}

Context oam>efm

Description This command enables remote Ethernet in the First Mile (EFM) OAM loopback tests on the specified port. The EFM OAM remote loopback OAMPDU will be sent to the peering device to trigger remote loopback.

ETH-CFM OAM Commands

linktrace

Syntax **linktrace** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**ttl** *ttl-value*]

Context oam>eth-cfm

Default The command specifies to initiate a linktrace test.

Parameters *mac-address* — Specifies a unicast destination MAC address.

mep *mep-id* **—** Specifies the target MAC address.

Values 1 — 8191

domain *md-index* **—** Specifies the MD index.

Values 1 — 4294967295

association *ma-index* **—** Specifies the MA index.

Values 1 — 4294967295

ttl *ttl-value* **—** Specifies the TTL for a returned linktrace.

Values 0 — 255

loopback

Syntax **loopback** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**send-count** *send-count*] [**size** *data-size*] [**priority** *priority*]

Context oam>eth-cfm

Default The command specifies to initiate a loopback test.

Parameters *mac-address* — Specifies a unicast MAC address.

mep *mep-id* **—** Specifies target MAC address.

Values 1 — 8191

domain *md-index* **—** Specifies the MD index.

Values 1 — 4294967295

association *ma-index* **—** Specifies the MA index.

Values 1 — 4294967295

send-count *send-count* **—** Specifies the number of messages to send, expressed as a decimal integer. Loopback messages are sent back to back, with no delay between the transmissions.

Default 1

Values 1 — 5

size *data-size* **—** This is the size of the data portion of the data TLV. If 0 is specified no data TLV is added to the packet.

Values 0 — 1500

priority *priority* **—** Specifies a 3-bit value to be used in the VLAN tag, if present, in the transmitted frame.

Values 0 — 7

eth-test

Syntax *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*] [**data-length** *data-length*]

Context oam>eth-cfm

Description This command issues an ETH-CFM test.

Parameters *mac-address* — Specifies a unicast MAC address.

mep *mep-id* **—** Specifies target MAC address.

Values 1 — 8191

domain *md-index* **—** Specifies the MD index.

Values 1 — 4294967295

association *ma-index* **—** Specifies the MA index.

Values 1 — 4294967295

data-length *data-length* **—** Indicates the UDP data length of the echo reply, the length starting after the IP header of the echo reply.

Values 64 — 1500

Default 64

one-way-delay-test

Syntax **one-way-delay-test** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*]

Context oam>eth-cfm

Description This command issues an ETH-CFM one-way delay test.

Parameters *mac-address* — Specifies a unicast MAC address.

mep *mep-id* **—** Specifies target MAC address.

Values 1 — 8191

domain *md-index* **—** Specifies the MD index.

Values 1 — 4294967295

association *ma-index* **—** Specifies the MA index.

Values 1 — 4294967295

priority *priority* **—** Specifies the priority.

Values 0 — 7

Default The CCM and LTM priority of the MEP.

two-way-delay-test

Syntax **two-way-delay-test** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*]

Context oam>eth-cfm

Description This command issues an ETH-CFM two-way delay test.

Parameters *mac-address* — Specifies a unicast MAC address.

mep *mep-id* **—** Specifies target MAC address.

Values 1 — 8191

domain *md-index* **—** Specifies the MD index.

Values 1 — 4294967295

association *ma-index* **—** Specifies the MA index.

Values 1 — 4294967295

priority *priority* **—** Specifies the priority.

Values 0 — 7

Default The CCM and LTM priority of the MEP.

two-way-slm-test

Syntax **two-way-slm-test** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*] [**send-count** *send-count*] [**size** *data-size*] [**timeout** *timeout*] [**interval** *interval*]

Context oam>eth-cfm

Description This command configures an Ethernet CFM two-way SLM test in SAA.

mac-address — Specifies a unicast destination MAC address.

mep *mep-id* **—** Specifies the target MAC address.

Values 1 — 8191

domain *md-index* **—** Specifies the MD index.

Values 1 — 4294967295

association *ma-index* **—** Specifies the MA index.

Values 1 — 4294967295

priority *priority* **—** Specifies the priority.

Values 0—7

send-count *send-count* **—** The number of messages to send, expressed as a decimal integer. The **count** parameter is used to override the default number of message requests sent. Each message request must either timeout or receive a reply before the next message request is sent. The message **interval** value must be expired before the next message request is sent.

Default 1

Values 1 — 100

size *data-size* **—** This is the size of the data portion of the data TLV. If 0 is specified no data TLV is added to the packet.

Default 0

Values 0 — 1500

timeout *timeout* **—** The **timeout** parameter in seconds, expressed as a decimal integer. This value is used to override the default **timeout** value and is the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. Any response received after the request times out will be silently discarded. The **timeout** value must be less than the **interval**.

Default 5

Values 1 — 10

interval *interval* **—** The **interval** parameter in seconds, expressed as a decimal integer. This parameter is used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request. The **timeout** value must be less than the **interval**.

Default 5

Values 1 — 10

Service Assurance Agent (SAA) Commands

saa

Syntax **saa**

Context config

Description This command creates the context to configure the Service Assurance Agent (SAA) tests.

test

Syntax **test** *name* [**owner** *test-owner*]
no test *name*

Context config>saa

Description This command identifies a test and create/modify the context to provide the test parameters for the named test. Subsequent to the creation of the test instance the test can be started in the OAM context.

A test can only be modified while it is shut down.

The **no** form of this command removes the test from the configuration. In order to remove a test it can not be active at the time.

Parameters *name* — Identify the saa test name to be created or edited.

owner *test-owner* **—** Specifies the owner of an SAA operation up to 32 characters in length.

Values If a *test-owner* value is not specified, tests created by the CLI have a default owner "TiMOS CLI".

description

Syntax **description** *description-string*
no description

Context config>saa>test

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default No description associated with the configuration context.

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed

of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

jitter-event

Syntax **jitter-event rising-threshold** *threshold* [**falling-threshold** *threshold*] [**direction**]
no jitter-event

Context config>saa>test

Description Specifies that at the termination of an SAA test probe, the calculated jitter value is evaluated against the configured rising and falling jitter thresholds. SAA threshold events are generated as required.

Once the threshold (rising/falling) is crossed, it is disabled from generating additional events until the opposite threshold is crossed. If a falling-threshold is not supplied, the rising threshold will be re-enabled when it falls below the threshold after the initial crossing that generate the event.

The configuration of jitter event thresholds is optional.

Parameters **rising-threshold** *threshold* **—** Specifies a rising threshold jitter value. When the test run is completed, the calculated jitter value is compared to the configured jitter rising threshold. If the test run jitter value is greater than the configured rising threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Default 0

Values 0 — 2147483 milliseconds

falling-threshold *threshold* **—** Specifies a falling threshold jitter value. When the test run is completed, the calculated jitter value is compared to the configured jitter falling threshold. If the test run jitter value is greater than the configured falling threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Default 0

Values 0 — 2147483 milliseconds

direction — Specifies the direction for OAM ping responses received for an OAM ping test run.

Values **inbound** — Monitor the value of jitter calculated for the inbound, one-way, OAM ping responses received for an OAM ping test run.
outbound — Monitor the value of jitter calculated for the outbound, one-way, OAM ping requests sent for an OAM ping test run.
roundtrip — Monitor the value of jitter calculated for the round trip, two-way, OAM ping requests and replies for an OAM ping test run.

Default roundtrip

latency-event

Syntax **latency-event rising-threshold** *threshold* [**falling-threshold** *threshold*] [**direction**]
no latency-event

Context config>saa>test

Description Specifies that at the termination of an SAA test probe, the calculated latency event value is evaluated against the configured rising and falling latency event thresholds. SAA threshold events are generated as required.

Once the threshold (rising/falling) is crossed, it is disabled from generating additional events until the opposite threshold is crossed. If a falling-threshold is not supplied, the rising threshold will be re-enabled when it falls below the threshold after the initial crossing that generate the event.

The configuration of latency event thresholds is optional.

Parameters **rising-threshold** *threshold* **—** Specifies a rising threshold latency value. When the test run is completed, the calculated latency value is compared to the configured latency rising threshold. If the test run latency value is greater than the configured rising threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Default 0

Values 0 — 2147483 milliseconds

falling-threshold *threshold* **—** Specifies a falling threshold latency value. When the test run is completed, the calculated latency value is compared to the configured latency falling threshold. If the test run latency value is greater than the configured falling threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Default 0

Values 0 — 2147483 milliseconds

direction — Specifies the direction for OAM ping responses received for an OAM ping test run.

Values **inbound** — Monitor the value of jitter calculated for the inbound, one-way, OAM ping responses received for an OAM ping test run.
outbound — Monitor the value of jitter calculated for the outbound, one-way, OAM ping requests sent for an OAM ping test run.
roundtrip — Monitor the value of jitter calculated for the round trip, two-way, OAM ping requests and replies for an OAM ping test run.

Default roundtrip

loss-event

Syntax **loss-event rising-threshold** *threshold* [**falling-threshold** *threshold*] [**direction**]
no loss-event

Context config>saa>test

Description Specifies that at the termination of an SAA testrun, the calculated loss event value is evaluated against the configured rising and falling loss event thresholds. SAA threshold events are generated as required.

The configuration of loss event thresholds is optional.

Parameters **rising-threshold** *threshold* **—** Specifies a rising threshold loss event value. When the test run is completed, the calculated loss event value is compared to the configured loss event rising threshold. If the test run loss event value is greater than the configured rising threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Default 0

Values 0 — 2147483647 packets

falling-threshold *threshold* **—** Specifies a falling threshold loss event value. When the test run is completed, the calculated loss event value is compared to the configured loss event falling threshold. If the test run loss event value is greater than the configured falling threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Default 0

Values 0 — 2147483647 packets

direction — Specifies the direction for OAM ping responses received for an OAM ping test run.

Values **inbound** — Monitor the value of jitter calculated for the inbound, one-way, OAM ping responses received for an OAM ping test run.
outbound — Monitor the value of jitter calculated for the outbound, one-way, OAM ping requests sent for an OAM ping test run.
roundtrip — Monitor the value of jitter calculated for the round trip, two-way, OAM ping requests and replies for an OAM ping test run.

Default roundtrip

trap-gen

Syntax **trap-gen**

Context config>saa>test

Description This command enables the context to configure trap generation for the SAA test.

probe-fail-enable

Syntax [**no**] **probe-fail-enable**

Context config>saa>test>trap-gen

Description This command enables the generation of an SNMP trap when probe-fail-threshold consecutive probes fail during the execution of the SAA ping test. This command is not applicable to SAA trace route tests.

The **no** form of the command disables the generation of an SNMP trap.

probe-fail-threshold

Syntax [**no**] **probe-fail-threshold** *0..15*

Context config>saa>test>trap-gen

Description This command has no effect when probe-fail-enable is disabled. This command is not applicable to SAA trace route tests.

The **probe-fail-enable** command enables the generation of an SNMP trap when the probe-fail-threshold consecutive probes fail during the execution of the SAA ping test. This command is not applicable to SAA trace route tests.

The **no** form of the command returns the threshold value to the default.

Default 1

test-completion-enable

Syntax [**no**] **test-completion-enable**

Context config>saa>test>trap-gen

Description This command enables the generation of a trap when an SAA test completes.

The **no** form of the command disables the trap generation.

test-fail-enable

Syntax [**no**] **test-fail-enable**

Context config>saa>test>trap-gen

Description This command enables the generation of a trap when a test fails. In the case of a ping test, the test is considered failed (for the purpose of trap generation) if the number of failed probes is at least the value of the **test-fail-threshold** parameter.

The **no** form of the command disables the trap generation.

test-fail-threshold

Syntax [**no**] **test-fail-threshold** *0..15*

Context config>saa>test>trap-gen

Description This command configures the threshold for trap generation on test failure.

This command has no effect when test-fail-enable is disabled. This command is not applicable to SAA trace route tests.

The **no** form of the command returns the threshold value to the default.

Default 1

type

Syntax **type**
no type

Context config>saa>test

Description This command creates the context to provide the test type for the named test. Only a single test type can be configured.

A test can only be modified while the test is in shut down mode.

Once a test type has been configured the command can be modified by re-entering the command, the test type must be the same as the previously entered test type.

To change the test type, the old command must be removed using the **config>saa>test>no type** command.

dns

Syntax **dns target-addr** *dns-name* **name-server** *ip-address* [**source** *ip-address*] [**send-count** *send-count*] [**timeout** *timeout*] [**interval** *interval*]

Context <GLOBAL>
config>saa>test>type

Description This command configures a DNS name resolution test.

Parameters **target-addr —** Is a keyword to specify the domain name or IP address to be looked up.

dns-name — Specifies the domain name or IP address to be looked up.

name-server *ip-address* **—** Specifies the server connected to a network that resolves network names into network addresses.

source *ip-address* **—** Specifies the IP address to be used as the source for performing an OAM ping operation.

send-count *send-count* **—** The number of messages to send, expressed as a decimal integer. The **send-count** parameter is used to override the default number of message requests sent. Each message request must either timeout or receive a reply before the next message request is sent. The message **interval** value must be expired before the next message request is sent.

Default 1

Values 1 — 100

timeout *timeout* **—** The **timeout** parameter in seconds, expressed as a decimal integer. This value is used to override the default **timeout** value and is the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router

assumes that the message response will not be received. Any response received after the request times out will be silently discarded.

Default 5

Values 1 — 120

interval *interval* **—** The **interval** parameter in seconds, expressed as a decimal integer. This parameter is used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Default 1

Values 1 — 10

icmp-ping

Syntax **icmp-ping** [*ip-address* | *dns-name*] [**rapid** | **detail**] [**ttl** *time-to-live*] [**tos** *type-of-service*] [**size** *bytes*] [**pattern** *pattern*] [**source** *ip-address*] [**interval** *seconds*] [{**next-hop** *ip-address*} | {**interface** *interface-name*} | **bypass-routing**] [**count** *requests*] [**do-not-fragment**] [**router** *router-instance* | **service-name** *service-name*] [**timeout** *timeout*]

Context config>saa>test>type

Description This command configures an ICMP traceroute test.

Parameters *ip-address* — The far-end IP address to which to send the **icmp-ping** request message in dotted decimal notation.

Values ipv4-address: a.b.c.d

dns-name — The DNS name of the far-end device to which to send the **icmp-ping** request message, expressed as a character string up to 63 characters maximum.

rapid — Packets will be generated as fast as possible instead of the default 1 per second.

detail — Displays detailed information.

ttl *time-to-live* **—** The TTL value for the IP TTL, expressed as a decimal integer.

Values 1 — 128

tos *type-of-service* **—** Specifies the service type.

Values 0 — 255

size *bytes* **—** The request packet size in bytes, expressed as a decimal integer.

Values 0 — 16384

pattern *pattern* **—** The date portion in a ping packet will be filled with the pattern value specified. If not specified, position info will be filled instead.

Values 0 — 65535

source *ip-address* **—** Specifies the IP address to be used.

Values ipv4-address: a.b.c.d

interval *seconds* **—** This parameter is used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Default 1

Values 1 — 10

next-hop *ip-address* **—** Only displays static routes with the specified next hop IP address.

Values ipv4-address: a.b.c.d (host bits must be 0)

interface *interface-name* — The name used to refer to the interface. The name must already exist in the **config>router>interface** context.

bypass-routing — Specifies whether to send the ping request to a host on a directly attached network bypassing the routing table.

count *requests* **—** Specifies the number of times to perform an OAM ping probe operation. Each OAM echo message request must either timeout or receive a reply before the next message request is sent.

Values 1 — 100000

Default 5

do-not-fragment — Sets the DF (Do Not Fragment) bit in the ICMP ping packet.

router *router-instance* **—** Specifies the router name or service ID.

Values *router-name*: Base , management
service-id: 1 — 2147483647

Default Base

service-name *service-name* **—** Specifies the service name as an integer.

Values *service-id*: 1 — 2147483647

timeout *timeout* **—** Overrides the default **timeout** value and is the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. Any response received after the request times out will be silently discarded.

Default 5

Values 1 — 10

icmp-trace

Syntax **icmp-trace** [*ip-address* | *dns-name*] [**ttl** *time-to-live*] [**wait** *milli-seconds*] [**tos** *type-of-service*] [**source** *ip-address*] [**tos** *type-of-service*] [**router** *router-instance* | **service-name** *service-name*]

Context config>saa>test>type

Description This command configures an ICMP traceroute test.

Parameters *ip-address* — The far-end IP address to which to send the **icmp-ping** request message in dotted decimal notation.

Values ipv4-address: a.b.c.d

dns-name — The DNS name of the far-end device to which to send the **icmp-ping** request message, expressed as a character string to 63 characters maximum.

ttl *time-to-live* **—** The TTL value for the IP TTL, expressed as a decimal integer.

Values 1 — 255

wait *milliseconds* **—** The time in milliseconds to wait for a response to a probe, expressed as a decimal integer.

Default 5000

Values 1 — 60000

tos *type-of-service* **—** Specifies the service type.

Values 0 — 255

source *ip-address* **—** Specifies the IP address to be used.

Values ipv4-address: a.b.c.d

router *router-instance* **—** Specifies the router name or service ID.

Values *router-name*: 7210 SAS E supports: Base, management
7210 SAS D supports: Base
service-id: 1 — 2147483647

Default Base

OAM SAA Commands

saa

Syntax **saa** *test-name* [**owner** *test-owner*] {**start** | **stop**}

Context oam

Description Use this command to start or stop an SAA test.

test-name — Name of the SAA test. The test name must already be configured in the **config>saa>test** context.

owner *test-owner* **—** Specifies the owner of an SAA operation up to 32 characters in length.

Values If a *test-owner* value is not specified, tests created by the CLI have a default owner "TiMOS CLI".

start — This keyword starts the test. A test cannot be started if the same test is still running.

A test cannot be started if it is in a shut-down state. An error message and log event will be generated to indicate a failed attempt to start an SAA test run. A test cannot be started if it is in a continous state.

stop — This keyword stops a test in progress. A test cannot be stopped if it is not in progress. A log message will be generated to indicate that an SAA test run has been aborted. A test cannot be stopped if it is in a continous state.

Show Commands

saa

Syntax **saa** [*test-name*] [**owner** *test-owner*]

Context show>saa

Description Use this command to display information about the SAA test.

If no specific test is specified a summary of all configured tests is displayed.

If a specific test is specified then detailed test results for that test are displayed for the last three occurrences that this test has been executed, or since the last time the counters have been reset via a system reboot or clear command.

Parameters *test-name* — Enter the name of the SAA test for which the information needs to be displayed. The test name must already be configured in the **config>saa>test** context.

This is an optional parameter.

owner *test-owner* **—** Specifies the owner of an SAA operation up to 32 characters in length.

Values 32 characters maximum.

Default If a *test-owner* value is not specified, tests created by the CLI have a default owner "TiMOS CLI".

Output **SAA Output —** The following table provides SAA field descriptions.

Label	Description
Test Name	Specifies the name of the test.
Owner Name	Specifies the owner of the test.
Description	Specifies the description for the test type.
Accounting policy	Specifies the associated accounting policy ID.
Administrative status	Specifies whether the administrative status is enabled or disabled.
Test type	Specifies the type of test configured.
Trap generation	Specifies the trap generation for the SAA test.
Test runs since last clear	Specifies the total number of tests performed since the last time the tests were cleared.
Number of failed tests run	Specifies the total number of tests that failed.

Label	Description (Continued)
Last test run	Specifies the last time a test was run.
Threshold type	Indicates the type of threshold event being tested, jitter-event, latency-event, or loss-event, and the direction of the test responses received for a test run: in — inbound out — outbound rt — roundtrip
Direction	Indicates the direction of the event threshold, rising or falling.
Threshold	Displays the configured threshold value.
Value	Displays the measured crossing value that triggered the threshold crossing event.
Last event	Indicates the time that the threshold crossing event occurred.
Run #	Indicates what test run produced the specified values.

```
*A:7210 SAS>show# saa

===============================================================================
SAA Test Information
===============================================================================
Test name                    : abc
Owner name                   : TiMOS CLI
Description                  : test
Accounting policy            : None
Administrative status        : Disabled
Test type                    : Not configured
Trap generation              : None
Test runs since last clear   : 0
Number of failed test runs   : 0
Last test result             : Undetermined
-------------------------------------------------------------------------------
Threshold
Type        Direction Threshold  Value      Last Event          Run #
-------------------------------------------------------------------------------
Jitter-in   Rising    None       None       Never               None
            Falling   None       None       Never               None
Jitter-out  Rising    None       None       Never               None
            Falling   None       None       Never               None
Jitter-rt   Rising    100        None       Never               None
            Falling   10.0       None       Never               None
Latency-in  Rising    None       None       Never               None
            Falling   None       None       Never               None
Latency-out Rising    None       None       Never               None
            Falling   None       None       Never               None
Latency-rt  Rising    100        None       Never               None
            Falling   20.0       None       Never               None
Loss-in     Rising    None       None       Never               None
            Falling   None       None       Never               None
Loss-out    Rising    None       None       Never               None
            Falling   None       None       Never               None
```

```
Loss-rt     Rising    300        None       Never              None
            Falling   30         None       Never              None

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

===============================================================================
*A:7210 SAS>show#
```

eth-cfm

Syntax **eth-cfm**

Context show

Description This command enables the context to display CFM information.

association

Syntax **association** [*ma-index*] [**detail**]

Context show>eth-cfm

Description This command displays eth-cfm association information.

Parameters *ma-index* — Specifies the MA index.

Values 1— 4294967295

detail — Displays detailed information for the eth-cfm association.

Sample Output

```
ALU-IPD# show eth-cfm association

===============================================================================
CFM Association Table
===============================================================================
Md-index   Ma-index   Name                    CCM-intrvl Hold-time Bridge-id
-------------------------------------------------------------------------------
3          1          03-0000000100           1          n/a       100
10         1          FacilityPrt01           1          n/a       none
===============================================================================
ALU-IPD#
```

cfm-stack-table

Syntax **cfm-stack-table [port [***port-id* **[vlan** *vlan-id***]][level** 0..7**] [direction down]**

Context show>eth-cfm

Description This command displays stack-table information. This stack-table is used to display the various management points MEPs and MIPs that are configured on the system. These can be Service based or facility based. The various option allow the operator to be specific. If no parameters are include then the entire stack-table will be displayed.

Parameters **port** *port-id* **—** Displays the bridge port or aggregated port on which MEPs or MHFs are configured.

vlan *vlan-id* **—** Displays the associated VLAN ID.

level — Display the MD level of the maintenance point.

Values 0 — 7

direction down — Displays the direction in which the MP faces on the bridge port.

facility — Displays the CFM stack table information for facility MEPs. The base command will display all the facility MEPs. Options may be included in order to further parse the table for specific facility MEP information.

Sample Output

```
*ALU-IPD# show eth-cfm cfm-stack-table
===============================================================================
CFM SAP Stack Table
===============================================================================
Sap            Level Dir  Md-index   Ma-index   Mep-id Mac-address
-------------------------------------------------------------------------------
lag-1:1.1      0     Down 2          1          10     00:f3:f0:98:97:1b
lag-1:1.1      6     Down 1          1          1      00:f3:f0:98:97:1b
lag-1:2.2      0     Down 2          2          20     00:f3:f0:98:97:1b
lag-1:2.2      6     Down 1          2          2      00:f3:f0:98:97:1b
===============================================================================
*ALU-IPD#
```

domain

Syntax **domain** [*md-index*] [**association** *ma-index* | **all-associations**] [**detail**]

Context show>eth-cfm

Description This command displays domain information.

Parameters *md-index* — Displays the index of the MD to which the MP is associated, or 0, if none.

association *ma-index* — Displays the index to which the MP is associated, or 0, if none.

all-associations — Displays all associations to the MD.

detail — Displays detailed domain information.

Sample Output

```
*ALU-IPD#  show eth-cfm domain
===============================================================================
CFM Domain Table
===============================================================================
Md-index   Level Name                                          Format
-------------------------------------------------------------------------------
1          6                                                   none
2          0                                                   none
===============================================================================
*ALU-IPD#
```

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**loopback**] [**linktrace**]
mep *mep-id* **domain** *md-index* **association** *ma-index* [**remote-mepid** *mep-id* | **all-remote-mepids**]
mep *mep-id* **domain** *md-index* **association** *ma-index* **eth-test-results** [**remote-peer** *mac-address*]
mep *mep-id* **domain** *md-index* **association** *ma-index* **one-way-delay-test** [**remote-peer** *mac-address*]
mep *mep-id* **domain** *md-index* **association** *ma-index* **two-way-delay-test** [**remote-peer** *mac-address*]
mep *mep-id* **domain** *md-index* **association** *ma-index* **two-way-slm-test [remote-peer** *mac-address*]

Context show>eth-cfm

Description This command displays Maintenance Endpoint (MEP) information.

Parameters **domain** *md-index* **—** Displays the index of the MD to which the MP is associated, or 0, if none.

association *ma-index* — Displays the index to which the MP is associated, or 0, if none.

loopback — Displays loopback information for the specified MEP.

linktrace — Displays linktrace information for the specified MEP.

remote-mepid — Includes specified remote MEP ID information for the specified MEP.

one-way-delay-test — Includes specified MEP information for one-way-delay-test.

two-way-delay-test — Includes specified MEP information for two-way-delay-test.

two-way-slm-test — Includes specified MEP information for two-way-slm-test.

eth-test-results — Include eth-test-result information for the specified MEP.

all-remote-mepids — Includes all remote mep-id information for the specified MEP.

Clear Commands

saa

Syntax **saa-test** [*test-name* [**owner** *test-owner*]]

Context clear

Description Clear the SAA results for the latest and the history for this test. If the test name is omitted, all the results for all tests are cleared.

Parameters *test-name* — Name of the SAA test. The test name must already be configured in the **config>saa>test** context.

owner *test-owner* **—** Specifies the owner of an SAA operation up to 32 characters in length.

Default If a *test-owner* value is not specified, tests created by the CLI have a default owner "TiMOS CLI".

Tools Command Reference

Command Hierarchies

Configuration Commands

Tools Dump Commands

```
tools
    — dump
        — eth-ring <ring-index> [clear] (This command is not supported on 7210 SAS-D devices)
        — lag lag-id <lag-id>
        — persistence
            — summary
        — router router-instance
            — dintf [<ip-address>]
            — filter-info [verbose]
            — l3-info
            — l3-stats [clear]
        — service
            — base-stats [clear]
            — dpipe service-id
            — dtls service-id
            — iom-stats [clear]
            — l2pt-diags
            — l2pt-diags clear
            — l2pt-diags detail
            — vpls-fdb-stats [clear]
            — vpls-mfib-stats [clear]
        — system
            — cpu-pkt-stats
        — system-resources slot-number
        — ethernet
            — qinq-etype
```

Tools Perform Commands

```
tools
    — perform
        — cron
            — action
                — stop [action-name] [owner action-owner] [all]
            — tod
                — re-evaluate
                    — customer customer-id [site customer-site-name]
                    — filter filter-type [filter-id]
                    — service id service-id [sap sap-id]
                    — tod-suite tod-suite-name
        — eth-cfm
        — lag
            — clear-force lag-id lag-id [sub-group sub-group-id]
            — force lag-id lag-id [sub-group sub-group-id] {active | standby}
        — log
            — test-event
```

Tools Configuration Commands

Generic Commands

tools

Syntax **tools**

Context root

Description This command enables the context to enable useful tools for debugging purposes.

Default none

Parameters **dump —** Enables dump tools for the various protocols.

perform — Enables tools to perform specific tasks.

Dump Commands

dump

Syntax **dump** *router-name*

Context tools

Description The context to display information for debugging purposes.

Default none

Parameters *router-name* — Specify a router name, up to 32 characters in length.

Default Base

eth-ring

Note: This command is not supported on 7210 SAS-D devices.

Syntax eth-ring *ring-index* [clear]

Context tools>dump

Description The command displays Ethernet-ring information.

Parameters *ring-index* — Specify ring index.

Values 1 —128

clear — This keyword clears statistics.

lag

Syntax **lag** lag-id *lag-id*

Context tools>dump

Description This tool displays LAG information.

Parameters *lag-id* — Specify an existing LAG id.

Values 1 — 6

```
*A:7210 SAS>tools>dump# lag lag-id 1
Port state      : Up
Selected subgrp : 1
NumActivePorts  : 2
ThresholdRising : 2
ThresholdFalling: 0
IOM bitmask     : 2
```

```
Config MTU      : 1522
Oper. MTU       : 1522
Bandwidth       : 200000

multi-chassis   : NO

-------------------------------------------------------------------------------
Indx   PortId   RX pkts   TX pkts   State Active Port  Cfg Oper Speed       BW AP CS
                                               Pri   Mtu Mtu
-------------------------------------------------------------------------------
   0    1/1/1         1         1      Up    yes 32768 1522 1522  1000   100000  0  2
   1    1/1/2         0         0      Up    yes 32768 1522 1522  1000   100000  0  2
```

persistence

Syntax persistence

Context tools>dump

Description This command enables the context to display persistence information for debugging purposes.

summary

Syntax **summary**

Context tools>dump>persistence

Description The context to display persistence summary information for debugging purposes.

Sample Output

```
A:ALA-B# tools dump persistence summary
===============================================================================
Persistence Summary on Slot A
===============================================================================
Client             Location            Entries in use    Status
-------------------------------------------------------------------------------
xxxxxx            cf1:\l2_dhcp.pst    200               ACTIVE
-------------------------------------------------------------------------------
Persistence Summary on Slot B
===============================================================================
Client             Location            Entries in use    Status
-------------------------------------------------------------------------------
xxxxxx              cf1:\l2_dhcp.pst    200               ACTIVE
-------------------------------------------------------------------------------
A:ALA-B#
```

system

Syntax **cpu-pkt-stats**

Context tools>dump>system

Description This command dumps tools for system information.

cpu-pkt-stats

Syntax **cpu-pkt-stats**

Context tools>dump>system

Description This command dumps statistics for CPU traffic.

system-resources

Syntax **system-resources** *slot-number*

Context tools>dump

Description This command displays system resource information.

Default none

Parameters *slot-number* — Specify a specific slot to view system resources information.

ethernet

Syntax **ethernet**

Context tools>dump

Description This command enables the context to configure the QinQ Etype.

qinq-etype

Syntax **qinq-etype**

Context tools>dump>ethernet

Description This command lists all the qinq-etypes configured by the user. A maximum of four values are listed with one of the values being a default value.

Note: The default value is not user-configurable, and is set to 0x8100 by the software.

Service Commands

service

Syntax **service**

Context tools>dump

Description Use this command to configure tools to display service dump information.

base-stats

Syntax **base-stats** [**clear**]

Context tools>dump>service

Description Use this command to display internal service statistics.

Default none

Parameters **clear —** Clears stats after reading.

dpipe

Syntax **dpipe** *service-id*

Context tools>dump>service

Description This command displays debug information for specified service.

Parameters *service-id* — Displays specified service ID details.

dtls

Syntax **dtls** *service-id*

Context tools>dump>service

Description Use this command to display TLS service statistics.

Default none

Parameters *service-id* — Displays specified service ID details.

iom-stats

Syntax **iom-stats** [**clear**]

Context tools>dump>service

Description Use this command to display IOM message statistics.

Default none

Parameters **clear —** Clears stats after reading.

l2pt-diags

Syntax **l2pt-diags**
l2pt-diags clear
l2pt-diags detail

Context tools>dump>service

Description Use this command to display L2pt diagnostics.

Default none

Parameters **clear —** Clears the diags after reading.

detail — Displays detailed information.

Sample Output

```
A:ALA-48>tools>dump>service# l2pt-diags
[ l2pt/bpdu error diagnostics ]
 Error Name       | Occurence   | Event log
 -----------------+-------------+----------------------------
[ l2pt/bpdu forwarding diagnostics ]

 Rx Frames   | Tx Frames   | Frame Type
 ------------+-------------+---------------------------------
A:ALA-48>tools>dump>service#

A:ALA-48>tools>dump>service# l2pt-diags detail
[ l2pt/bpdu error diagnostics ]
 Error Name       | Occurence   | Event log
 -----------------+-------------+----------------------------
[ l2pt/bpdu forwarding diagnostics ]

 Rx Frames   | Tx Frames   | Frame Type
 ------------+-------------+---------------------------------
[ l2pt/bpdu config diagnostics ]
 WARNING - service 700 has l2pt termination enabled on all access points :
           consider translating further down the chain or turning it off.
 WARNING - service 800 has l2pt termination enabled on all access points :
           consider translating further down the chain or turning it off.
 WARNING - service 9000 has l2pt termination enabled on all access points :
           consider translating further down the chain or turning it off.
 WARNING - service 32806 has l2pt termination enabled on all access points :
```

```
           consider translating further down the chain or turning it off.
 WARNING - service 90001 has l2pt termination enabled on all access points :
           consider translating further down the chain or turning it off.
A:ALA-48>tools>dump>service#
```

vpls-fdb-stats

Syntax **vpls-fdb** [**clear**]

Context tools>dump>service

Description Use this command to display VPLS FDB statistics.

Default none

Parameters **clear —** Clears stats after reading.

vpls-mfib-stats

Syntax **vpls-mfib-stats** [**clear**]

Context tools>dump>service

Description Use this command to display VPLS MFIB statistics.

Default none

Parameters **clear —** Clears stats after reading.

Router Commands

router

Syntax **router** *router-instance*

Context tools>dump

Description This command enables tools for the router instance.

Default none

Parameters **router** *router-instance* **—** Specifies the router name or service ID.

Values *router-name*: Base
service-id: 1 — 2147483647

Default Base

dintf

Syntax **dintf** [*ip-address*]

Context tools>dump

Description This command dumps hardware-specific information related to the active IP interfaces configured. By default, hardware information for all active IP interfaces is dumped.

Default Dumps hardware-specific information for all the active IP interfaces present within the system.

Parameters *ip-address* — Only displays the hardware information associated with the specified IP address.

Sample Output

```
A:STU# /tools dump router dintf 5.1.1.2
[************ SLOT 1 ***************]
[IP interfaces]
    Table Usage:           5/263
    [L3 SAP interface 1/1/7:360137680]
        Interface index                         54  (Svc)
        cpmtag                                  2
        primary IPv4                            5.1.1.2/24
        VRF                                     0
        primary MAC                             00:14:25:36:f7:f0
        no VRRP MAC addresses
        Local Subnet 0                          5.1.1.2/24  index=62
        admin ip_mtu                            1500
        Intf Port                               1/1/7
        No agg port
        uRPF mode                               None
        Ingress uRPF stats                      Drop=0/0
```

```
        [Host IP Map 1 entries]
            [IP Entry v4 5.1.1.1  interface=54 L3 Egress HDL=100003 Ref Cnt=0]
                [Nexthop 5.1.1.1  idx=7]
                    ref count                   1
                    # mpls nhlfes               0
                    # nexthop groups            1
                    # SDP bindings              0
                    p2mp_arp_index              0
        Subscriber ifIndex                      0
        Subscriber red ifIndex                  0
        [Subscriber Red Group 54]
            Subscriber red ifIndex              0
            Subscriber use SRRP src mac         no
            Use inter-dest Id                   no
            SRRP                                Disabled
            ref count                           1
            [Inter-dest group 0]
                Locally reachable               no
                Subscriber red ifIndex          In-use=no
                Subscriber hosts unreachable    no
                cpmtag                          15
            cpmtag                              15
        L3 SAP                                  idx=1 1/1/7:0.*
      SVLAN                                     54
      svlan_interface_index                     54
      Encap Type                                q-in-q
      HW IF Index                               1024
      L2 USER ENTRY cindex                      1
      VFP EID                                   181
      L3  BCAST EID                             182
      ARP REPLY EID                             183
      ARP REQST EID                             184
      VFP0 EID                                  185
      L3  BCAST0 EID                            186
      ARP REPLY0 EID                            187
      ARP REQST0 EID                            188
      L3  BCAST IFP                             189
      ARP IFP                                   190
      IP EXT MtcH IFP                           288
      HW Port Number                            17
A:STU#
A:ALA-A#
```

filter-info

Syntax **filter-info [verbose]**

Context tools>dump>router

Description This command dumps the hardware-specific filter information.

Parameters **verbose —** Displays the hardware information of the filter.

l3-info

Syntax **lag**

Context tools>dump>router

Description This command dumps the hardware-specific L3 information.

l3-stats

Syntax **l3-stats [clear]**

Context tools>dump>router

Description This command dumps the hardware-specific L3 statistics.

Parameters **clear —** Clears the hardware information of the filter.

lag

Syntax **lag**

Context tools>perform

Description This command configures tools to control LAG.

clear-force

Syntax **clear-force lag-id** *lag-id* [**sub-group** *sub-group-id*]

Context tools>perform>lag

Description This command clears a forced status.

Parameters **lag-id *lag-id* —** Specify an existing LAG id.

eth-cfm

Syntax eth-cfm

Context tools>perform

Description This command configures performance tools for eth-cfm.

force

Syntax **force lag-id** *lag-id* [**sub-group** *sub-group-id*] {**active** | **standby**}

Context tools>perform>lag

Description This command forces an active or standy status.

Parameters **active —** If **active** is selected, then all drives on the active CPM are forced.

standby — If **standby** is selected, then all drives on the standby CPM are forced.

lag-id *lag-id* **—** Specify an existing LAG id.

Values 1 — 6

log

Syntax **log**

Context tools>perform

Description Tools for event logging.

test-event

Syntax **test-event**

Context tools>perform>log

Description This command causes a test event to be generated. The test event is LOGGER event #2011 and maps to the tmnxEventSNMP trap in the TIMETRA-LOG-MIB.

Performance Tools

perform

Syntax perform

Context tools

Description This command enables the context to enable tools to perform specific tasks.

Default none

cron

Syntax **cron**

Context tools>perform

Description This command enables the context to perform CRON (scheduling) control operations.

Default none

action

Syntax **action**

Context tools>perform>cron

Description This command enables the context to stop the execution of a script started by CRON action. See the **stop** command.

stop

Syntax **stop** [*action-name*] [**owner** *action-owner*] [**all**]

Context tools>perform>cron>action

Description This command stops execution of a script started by CRON action.

Parameters *action-name* — Specifies the action name.

Values Maximum 32 characters.

owner *action-owner* **—** Specifies the owner name.

Default TiMOS CLI

all **—** Specifies to stop all CRON scripts.

tod

Syntax **tod**

Context tools>perform>cron

Description This command enables the context for tools for controlling time-of-day actions.

Default none

re-evaluate

Syntax **re-evaluate**

Context tools>perform>cron>tod

Description This command enables the context to re-evaluate the time-of-day state.

Default none

customer

Syntax **customer** *customer-id* [**site** *customer-site-name*]

Context tools>perform>cron>tod>re-eval

Description This command re-evaluates the time-of-day state of a multi-service site.

Parameters *customer-id* — Specify an existing customer ID.

Values 1 — 2147483647

site *customer-site-name* **—** Specify an existing customer site name.

filter

Syntax **filter** *filter-type* [*filter-id*]

Context tools>perform>cron>tod>re-eval

Description This command re-evaluates the time-of-day state of a filter entry.

Parameters *filter-type* — Specify the filter type.

Values ip-filter, mac-filter

filter-id — Specify an existing filter ID.

Values 1 — 65535

service

Syntax **service id** *service-id* [**sap** *sap-id*]

Context tools>perform>cron>tod>re-eval

Description This command re-evaluates the time-of-day state of a SAP.

Parameters **id** *service-id* — Specify the an existing service ID.

Values 1 — 2147483647

sap *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 137 for CLI command syntax.

tod-suite

Syntax **tod-suite** *tod-suite-name*

Context tools>perform>cron>tod>re-eval

Description This command re-evaluates the time-of-day state for the objects referring to a tod-suite.

Parameters *tod-suite-name* — Specify an existing TOD nfame.

Common CLI Command Descriptions

In This Chapter

This chapter provides CLI syntax and command descriptions for SAP and port commands.

Topics in this chapter include:

Common Service Commands

sap

Syntax [**no**] **sap** *sap-id*

Description This command specifies the physical port identifier portion of the SAP definition.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

The *sap-id* can be configured in one of the following formats:

Type	Syntax	Example
port-id	*slot*/*mda*/*port*[.*channel*]	1/1/5
null	[*port-id* | *lag-id*]	*port-id*: 1/1/3 *lag-id*: lag-3
dot1q	[*port-id* | *lag-id*]:qtag1	*port-id*:qtag1: 1/1/3:100 *lag-id*:qtag1:lag-3:102
qinq	[port-id | lag-id]:qtag1.qtag2	port-id:qtag1.qtag2: 1/1/3:100.10 lag-id:qtag1.qtag2: lag-10

port

Syntax **port** *port-id*

Description This command specifies a port identifier.

Parameters *port-id* — The *port-id* can be configured in one of the following formats.

port-id slot/mda/port

Standards and Protocol Support (7210 SAS D)

Standards Compliance

IEEE 802.1ab-REV/D3 Station
And Media Access Control
Connectivity Discovery
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the
First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3z 1000BaseSX/LX
IANA-IFType-MIB
IEEE8023-LAG-MIB

Protocol Support

DIFFERENTIATED SERVICES

RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev3260)
RFC 2598 An Expedited Forwarding PHB
RFC 3140 Per-Hop Behavior Identification Codes
RFC 4115 A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic

TCP/IP

RFC 768 UDP
RFC 1350 The TFTP Protocol (Rev.
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1519 CIDR
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Intervaland Transfer Size option

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol
draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt SSH Connection Protocol
draft-ietf-secsh- newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

NETWORK MANAGEMENT

ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SMMIB
RFC 2575 SNMP-VIEW-BASEDACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 - Simple Network Management Protocol (SNMP) Applications
RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 - SNMP MIB
draft-ietf-disman-alarm-mib-04.txt

PROPRIETARY MIBs

TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-DOT3-OAM-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IEEE8021-CFM-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-NTP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-SAS-IEEE8021-CFM-MIB.mib
TIMETRA-SAS-GLOBAL-MIB.mib
TIMETRA-SAS-PORT-MIB.mib

TIMETRA-SAS-QOS-MIB.mib
TIMETRA-SAS-SYSTEM-MIB.mib
TIMETRA-SCHEDULER-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRTR-MIB.mib

Standards and Protocol Support (7210 SAS E)

Standards Compliance

IEEE 802.1ab-REV/D3 Station And Media Access Control Connectivity Discovery
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3z 1000BaseSX/LX
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
IANA-IFType-MIB
IEEE8023-LAG-MIB
ITU-T G.8032 Ethernet Ring Protection Switching (version 1)

Protocol Support

DIFFERENTIATED SERVICES

RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev3260)
RFC 2598 An Expedited Forwarding PHB
RFC 3140 Per-Hop Behavior Identification Codes

MULTICAST

RFC 1112 Host Extensions for IP Multicasting (Snooping)
RFC 2236 Internet Group Management Protocol, (Snooping)
RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)

TCP/IP

RFC 768 UDP
RFC 1350 The TFTP Protocol (Rev.
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1519 CIDR
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Intervaland Transfer Size option

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol
draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt SSH Connection Protocol
draft-ietf-secsh- newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

NETWORK MANAGEMENT

ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SMMIB
RFC 2575 SNMP-VIEW-BASEDACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 - Simple Network Management Protocol (SNMP) Applications
RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 - SNMP MIB
draft-ietf-disman-alarm-mib-04.txt

PROPRIETARY MIBs

ALCATEL-IGMP-SNOOPING-MIB.mib
TIMETRA-CAPABILITY-7210-SAS-E-V1v0.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-DOT3-OAM-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IEEE8021-CFM-MIB.mib
TIMETRA-LAG-MIB.mib

TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-NTP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-SAS-ALARM-INPUT-MIB.mib
TIMETRA-SAS-IEEE8021-CFM-MIB.mib
TIMETRA-SAS-GLOBAL-MIB.mib
TIMETRA-SAS-PORT-MIB.mib
TIMETRA-SAS-QOS-MIB.mib
TIMETRA-SAS-SYSTEM-MIB.mib
TIMETRA-SCHEDULER-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRTR-MIB.mib

Index