

Alarm Configuring and Monitoring Guide, Cisco IOS XE 17 (Cisco ASR 900 Series)

First Published: 2023-04-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2023 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

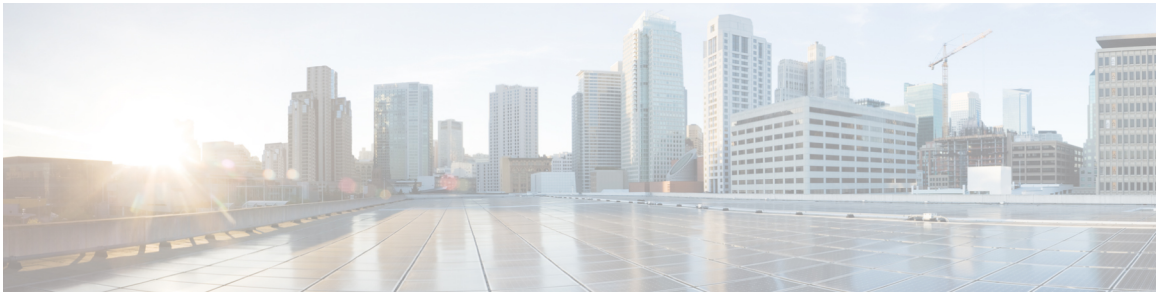
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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



CONTENTS

CHAPTER 1 **Feature History** 1

CHAPTER 2 **Alarms** 3

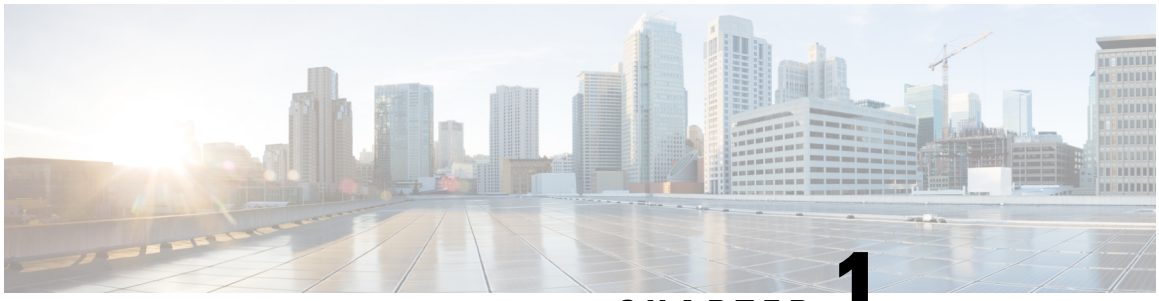
- Restrictions for Alarms 3
- SONET Alarms 4
  - Alarms at SONET Layers 4
  - SONET Alarms for APS 6
  - APS Alarms and Conditions 6
- SDH Alarm 8

CHAPTER 3 **Alarm Profiling and Auto In-Service States** 11

- Alarm Profiling 11
  - Limitations of Alarm Profiles 12
  - Alarm Profile Classification 13
    - Alarm Support for Loopback 18
  - Default Alarm Profiles 18
  - How to Configure Alarm Profile 18
    - Creating Alarm Profile 18
    - Attaching Alarm Profile to Entity 22
    - Modifying Alarm Profile 24
    - Detaching Alarm Profile 25
    - Deleting Alarm Profile 26
    - Verifying Alarm Profile for T1 or E1 Alarms 26
    - Verifying Alarm Profile for T3 or E3 Alarms 28
    - Verifying Alarm Profile for SONET or SDH 29

Alarm Profile Use Cases for T1 or E1 Alarms 33
Alarm Profile Use Cases for T3 or E3 Alarms 37
Alarm Profile Use Cases for SONET or SDH Alarms 41
Auto In-Service States for Cards 45
Restrictions for AINS 46
Service States 46
Service State Transitions 48
Equipment Service State Transitions 48
Administrative States 52
Configuration Commands 52
Enabling the AINS on Chassis 52
Disabling the AINS on Chassis 53
Pre-Provisioning the Card 53
De-Provisioning the Card 55
Administrative Commands 56
Maintenance Commands (OOS,MT) 56
In-Service Commands (IS) 56
Information Display Commands 57
Auto In-Service State for Ports 58
Restrictions for AINS for TDM Ports 58
Service States 59
Service State Transitions 60
Administrative States 62
Configuration Commands 63
Verifying Controller and Interface AINS Port Configuration 63
Configuring Secondary Admin State 65
Verifying Secondary Admin State 66
Syslog 66
Auto In-Service State for Transceiver 67
Transceiver Service State Transitions 67
Transceiver Alarms 68
How to Configure Transceiver 68
How to Configure Transceiver 68
Modifying PID for Transceiver 68

Transceiver Service State Transitions 68
Removing Transceiver Configuration 69
Verifying Transceiver Configuration 69

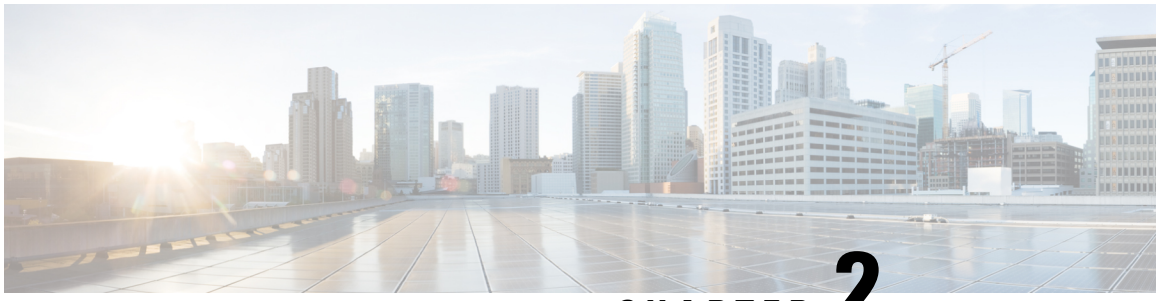


CHAPTER 1

Feature History

The following table lists the new feature supported in the Alarm Configuring and Monitoring Guide in Cisco IOS XE 17 releases.

Feature	Description
Cisco IOS XE Amsterdam 17.3.1	
Support for New Alarm Profile based on the Telcordia Profile for Chassis	The alarm profile based on Telcordia includes "Service Affecting" information for chassis entities. This information enables you to check the service affecting state for each alarm under a chassis.



CHAPTER 2

Alarms

This chapter provides information about alarms supported for SONET and SDH, and their maintenance.

Alarms are triggered when a component fails or does not perform as expected. Alarms are triggered by the chassis.

Alarms can be defined using the following two terms:

- Alarm State—It is the state the chassis enters when a certain event occurs. For example, the state of the chassis when the ambient temperature is beyond the specified limits.
- Alarm Indication—It is a visual signal to indicate the alarm state. For example, the TEMP LED glows red if the ambient temperature is beyond the specified limits, and it turns green if the ambient temperature is within specified limits.

  Typically, a failure condition detected by a chassis results in one or more error conditions sent both upstream and downstream on the network.

  - Alarm Indication Signal (AIS)—AIS alarms are reported downstream from a detecting device, and to prevent consequential downstream failures or alarms from being raised.
  - Remote Defect Indicator (RDI)—RDI alarms are always reported upstream from the detecting device.

Note Even when the controller is in the down state with alarms, the cross connection between the controllers is up.

- Restrictions for Alarms, on page 3
- SONET Alarms, on page 4
- SDH Alarm, on page 8

Restrictions for Alarms

- In T3, an AIS alarm is supported only in the framed mode and not supported in the unframed mode.
- When the T3 RAI alarm is asserted, the propagation of the RAI alarm is stopped on the T1 interface.

  This behaviour is applicable for the following interface modules:

  - A900-IMA48T-C

- A900-IMA3G-IMSG
- A900-IMA1Z8S-CXMS
- A900-IMA1Z8S-CX

SONET Alarms

Alarms at SONET Layers

SONET equipment detects events and alarms at each of the three layers — section, line and path. A SONET chassis sends alarms in both upstream and downstream directions in order to notify other devices of the problem condition.

The interface of an active alarm or defect is maintained in a down/down state. The process used to troubleshoot down/down SONET interfaces is similar to that of digital interfaces, such as T1 and T3.

The following table lists the types and sub types of SONET Alarms.

Table 1: SONET Supported Alarms

Alarm Type	Sub Alarm Type
Section Alarms	• LOS — Loss of Signal • LOF — Loss of Frame • SEF — Severely Error Frame
Line Alarms	• AIS-L — Line AIS • REI-L — Line Remote Error Indication • RDI-L — Line Remote Defect Indication • B2 — Line BIP Error (SF/SD) • TCA for B2

Alarm Type	Sub Alarm Type
Path Alarms	• AIS-P — STS Path AIS • LOP-P — STS Path Loss of Pointer • B3 (SF/SD) — STS Path BIP Error • UNEQ-P — STS Path unequipped • REI-P — STS Path Remote Error • RDI-P — STS Path Remote Defect Indication • PLM-P — STS path Payload Label Mismatch • LOM — Loss of MultiFrame • TCA for B3
VT Alarms	• AIS-V — VT Path AIS • LOP-V — VT Loss of Pointer • V-BIP (SF/SD) — VT Path BIP error • UNEQ-V — VT Path Unequipped • REI-V — VT Path Remote Error • RDI-V — VT Path Remote Defect Indication • PLM-V — VT path Payload Label Mismatch • TCA for VT Level BIP
T1 Alarms	• LOS — DS1/E1 Line loss of Signal • AIS — DS1/E1 Path Alarm Indication Signal • AIS-CI — DS1/E1 Path Alarm Indication Signal Customer Installation • LOF — DS1/E1 Path Loss of Frame • RDI/RAI — Remote Defect Indication or Remote Alarm Indication • RAI-CI — Remote Alarm Indication Customer Installation • TCA for Line and Path DS1

Alarm Type	Sub Alarm Type
T3 Alarms	• LOS — DS3/E3 Line Loss of Signal • OOF — DS3/E3 Path Loss of Frame • SEF — DS3/E3 Path Severely Errored Frame • AIS — DS3/E3 Path Alarm Indication Signal • SEF/AIS-FE — Far End SEF/AIS • TCA for Line and Path DS3

SONET Alarms for APS

Table 2: Feature History

Feature Name	Release Information	Description
SONET Alarms for APS	Cisco IOS XE 17.15.1	In APS scenarios, the existing SONET alarms follow the GR-253 standard for alarm soaking. This standardization helps filter out transient conditions by defining specific assertion and clearing times for alarms.

SONET APS Alarm Compliance Standard

On APS ports, SONET section and line alarms adhere to the GR-253 compliance standard for alarm soaking, ensuring high reliability and consistent performance across your network. These alarms incorporate a soaking period with an assertion time of 2.5 seconds and a clearing time of 10 seconds, effectively filtering out transient conditions. This reduces the incidence of false alarms and allows for more precise monitoring of network stab

APS Alarms and Conditions

Table 3: Feature History

Feature Name	Release Information	Description
New APS Alarms and Conditions	Cisco IOS XE 17.15.1	New APS alarms and conditions have been introduced to enhance network monitoring and management. These alarms are raised or cleared during APS manual, forced, and lockout switch actions, providing real-time alerts on network changes. This advanced alerting mechanism ensures that network operators are immediately informed of any alterations, enabling them to swiftly respond to and manage network conditions, thereby maintaining optimal performance and reliability.

APS Alarms

New alarms for APS channel mismatch and APS mode mismatch have been introduced to enhance network monitoring and troubleshooting capabilities.

The following table details the triggering actions and the corresponding responses required to address these alarms:

Alarm	Triggering Action	What You Should Do?
K1BYTE_APS_CHANNEL_MISMATCH	Triggers an alarm for an APS channel mismatch, indicating a configuration discrepancy.	The configuration on both Customer Edge (CE) and Provider Edge (PE) routers must be identical. It is important to verify that the settings and parameters are consistent across both routers. This includes APS settings, interface configurations, and protocol parameters. By aligning the configurations on PE and CE routers,
K2BYTE_APS_MODE_MISMATCH	Triggers an alarm for an APS mode mismatch, highlighting an inconsistency in mode settings.	The configuration on both Customer Edge (CE) and Provider Edge (PE) routers must be identical. It is important to verify that the settings and parameters are consistent across both routers. This includes APS settings, interface configurations, and protocol parameters. By aligning the configurations on PE and CE routers,

APS conditions

The APS conditions are raised based on the APS switch action commands such as manual, force and lockout that you have performed on the routers. APS conditions are typically used during maintenance activities or when a specific path needs to be reserved, ensuring that traffic does not inadvertently switch to the protected path, thereby maintaining network stability.

- **Manual**—Manually switches the traffic from active protect controller to the active controller.
- **Force**—Forces the traffic to switch from active working controller to switch to protect controller.
- **Lock out**—Locks the switch to protect port so that APS does not switch to protect controller for any failure on working port or IM. Prevents a working interface from switching to a protect interface.

The following table indicates the new APS conditions that have been introduced:

Conditions	What does it mean?
APS_NE_LOCKOUT_REQ	Indicates a Lockout Request at the near end of a SONET network. This condition is triggered when the local network element requests a lockout, preventing automatic switching to the protection path.
APS_FE_LOCKOUT_REQ	Indicates a Lockout Request at the far end of a SONET network.

Conditions	What does it mean?
APS_NE_FORCE_WK_REQ	Indicates a Forced Switch from the Working path at the near end of a SONET network.
APS_NE_FORCE_PR_REQ	Indicates a Forced Switch from the Protection path at the near end of a SONET network.
APS_FE_FORCE_WK_REQ	Indicates a Forced Switch from the Working path at the far end of a SONET network.
APS_FE_FORCE_PR_REQ	Indicates a Forced Switch from the Protection path at the far end of a SONET network.
APS_NE_MANUAL_WK_REQ	Indicates a Manual Switch from the Working path at the near end of a SONET network.
APS_NE_MANUAL_PR_REQ	Indicates a manual switch from the protect path at the near end of a SONET network.
APS_FE_MANUAL_WK_REQ	Indicates a far end manual switch from the working path, allowing remote user-initiated rerouting.
APS_FE_MANUAL_PR_REQ	Indicates a far end manual switch from the protect path, providing manual control over remote protection paths.
APS_FAIL_TO_SWITCH	Indicates a failure to switch to the protection path in a SONET network.

SDH Alarm

The following table lists the types and sub types of SDH Alarms.

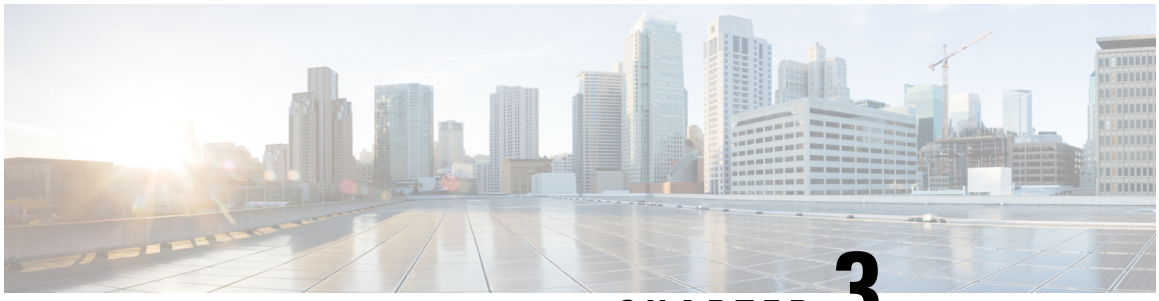
Table 4: SDH Supported Alarms

Alarm Type	Sub Alarm Type
Section Alarms	• LOS — Loss of Signal • LOF — Loss of Frame • RS-BIP — Bit Interleaved Parity

Alarm Type	Sub Alarm Type
Line Alarms	• MS-BIP — Multiplex Section-Bit Interleaved Parity • MS-REI — Multiplex Section-Remote Error Indication • MS-AIS — Multiplex Section-Alarm Indication Signal • MS-RDI — Multiplex Section-Remote Defect Indication • AU-AIS — Administrative Unit-Alarm Indication Signal • AU-LOP — Administrative Unit-Loss of Pointer
STS Path Alarms	• HP-UNEQ — High order Path-Unequipped • HP-PLM — High order Path-Payload Label Mismatch • HP-RDI — High order Path-Remote Defect Indication • HP-BIP — High order Path-Bit Interleaved Parity • HP-REI — High order Path-Remote Error Indication • TU-LOM — Tributary Unit-Loss of Multiframe • TU-AIS — Tributary Unit-Alarm Indication Signal • TU-LOP — Tributary Unit-Loss of Pointer
VT Path Alarms	• LP-UNEQ — Low order Path-Unequipped • LP-PLM — Low order Path-Payload Label Mismatch • LP-RDI — Low order Path-Remote Defect Indication • LP-RFI — Low order Path-Remote Failure Indication • LP-BIP — Low order Path-Bit Interleaved Parity • LP-REI — Low order Path-Remote Error Indication



Note TIM alarms are not supported.



CHAPTER 3

Alarm Profiling and Auto In-Service States

This chapter describes the alarm profiling feature that is used to change the alarm severity in the alarm configuration. Alarm profiling also enables you to set the administrative and service states for the Cisco ASR 900 Series Routers.

Effective Cisco IOS XE Everest 16.5.1, the Auto In-Service State (AINS) manages the interface modules in the system.

- Alarm Profiling, on page 11
- Auto In-Service States for Cards, on page 45
- Auto In-Service State for Ports, on page 58
- Auto In-Service State for Transceiver, on page 67

Alarm Profiling

The router software monitors the status of the chassis, interface module, and ports. It generates alarm messages that are based on the configured alarm conditions. To save time and effort, you can change the alarm severity in the alarm configuration using the alarm profiling feature.

The alarm profiling feature enables you to create a unique alarm profile for chassis, interface module, and port. Each alarm profile, for example, the chassis alarm profile, is defined with an alarm name. Each alarm profile is classified based on controller types. For each controller type, there is a set of alarms defined with a default severity. You can overwrite the default severity using the alarm profile and suppress the syslog facility based on their preferences. By default, the syslog facility is enabled for an alarm profile.

You can also enable Auto In Service (AINS) through the Alarm Profile. By default, AINS is disabled for an alarm profile. You must configure it using the **ains** command. For more information on the AINS feature, see the *Auto In-Service States for Cards or Ports* sections.

To configure alarm profiles, create profiles for either chassis, interface module, or port, then define severities for each alarm, and finally, attach the profile at the corresponding chassis, interface module, or port.

The highest precedence is maintained at the port level and the lowest precedence is maintained at the chassis level. For example, if the chassis profile is already attached and if you want to have a separate profile for a port, you can still create a port profile and attach it to that port. The port inherits the properties of the port profile.

After the alarm profile is attached, these behaviors are shown about the entity:

- Chassis alarm profile—When a chassis alarm profile is attached, by default, the profile is attached to all the interface modules available in the chassis. All these interfaces configured under the chassis are applied with the new alarm severity and AINS.

  Starting with the Cisco IOS XE Amsterdam 17.3.1 release, the system supports alarm profile on the chassis based on Telcordia.

- Interface Module alarm profile—When an interface module profile is attached, by default, the profile, along with AINS is attached to all ports that are enabled on the interface module.

- Port alarm profile—When a port profile is attached, the profile, along with the AINS is applied only to that port.

Note Interface module and port alarm profiles with the same name can be attached to multiple cards and ports, respectively.

The alarm profile attached to the chassis, card or interface module, and port can be detached, if the profile is no longer required. Before deleting the alarm profile, ensure that you detach the alarm profile from the chassis, interface module or port.

To log the alarms, enable the **logging alarm [critical | major | minor | informational | NR]** command at the global configuration mode.

For example, if you have enabled the logging alarm using the **logging alarm critical** command, then for the alarm profile, the alarms with only critical severity are logged when the syslog is enabled in the alarm profile.

Note

- If a port is created on the subslot after configuring the alarm profile, that port starts with default secondary admin state as "auto-in-service". The port moves to "in-service" secondary admin state after completing the default soak-timer.
- If ports are already created before the alarm profile is enabled, the ports move to "in-service" secondary admin state.

Limitations of Alarm Profiles

- The alarm profile name must not exceed 32 characters.
- For various alarms, the alarm profiles are not supported for Service Affecting (SA) or Non-Service Affecting (NSA) alarm classification for releases earlier to Cisco IOS XE Amsterdam 17.3.1.

  Starting with Cisco IOS XE Amsterdam 17.3.1, SA and NSA alarms are supported.

- For various alarms, the alarm severities such as Not Reported (NR) and Not Alarmed (NA) are not supported for releases earlier to Cisco IOS XE Amsterdam 17.3.1.

  Starting with Cisco IOS XE Amsterdam 17.3.1, NR and NA alarm severities are supported.

- The alarm profile created for chassis, interface module, or port should be attached to the respective entity. The attaching of the alarm profile of one entity to another entity is not supported. For example, the interface module alarm profile cannot be attached to the chassis alarm profile, or the opposite way.

- The attaching of alarm profile to entities such as, PSU, FAN, and RSP is not supported.
- AINS States are not supported on the PSU, FAN, and RSP in Cisco IOS XE Everest 16.6.1vS.
- Maximum of 100 alarm profiles can be created for the system or node (chassis).
- When a port having line alarm, such as SLOS, SLOF, LAIS, and LRDI is shut down, then after performing the no shutdown operation, the **show facility-alarm status** does not display the asserted line alarm. Only the LINK DOWN alarm is displayed.
- Clearing an alarm requires more than 10 seconds.
- Alarm profiling is not supported on the card protection ports (card protection, APS, and UPSR).
- The alarm severity for loopback cannot be modified using the alarm profile.
- In an SDH mode, when a service is configured without an overhead byte, and if a Path Payload Mismatch (PPLM) alarm is received on the controller, and when you delete the circuit and the service, the PPLM alarm still persists. To prevent such scenario, ensure that you configure the overhead byte on the service.
- With Telcordia profile-enabled and service configured, following are the points to note:
  - The highest alarm is displayed under the **show facility-alarm** CLI whereas the lower alarms are displayed for the **show facility-condition** CLI.
  - Alarm with severity NA is displayed under the **show facility-alarm** CLI if it is the highest alarm, otherwise the alarm is displayed under the **show facility-condition** CLI.
  - Alarm with severity NR is displayed only under the **show facility-condition** CLI.

Alarm Profile Classification

Alarm Profile Types

Alarm Profile types are based on the entities i.e. chassis, interface module and port. The chassis alarm profile is applicable to all the entities if no other specific alarm profile is attached. The interface module alarm profile is applicable to a specific interface module and the port alarm profile is applicable to individual port.

The chassis, card or interface module, and port alarm profiles are classified based on the controller type.

Controller types supported for each alarm profile:

- 48 X T1/E1 CEM Interface Module
- 48 X T3/E3 CEM Interface Module
- 1 x OC-192 Interface module or 8-port Low Rate Interface Module
- 8-port 10 Gigabit Ethernet Interface Module (8X10GE)
- 2-port 40 Gigabit Ethernet QSFP Interface Module (2X40GE)
- 1-port 100 Gigabit Ethernet Interface Module (1X100GE)
- SFP Combo IM-8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet Interface Module (1X10GE)
- 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module

Alarm Severity

Alarms are filtered based on the severity level. Depending on the requirement, you can override the default severity to a new severity.

The following severity of alarms are supported for each alarm profile associated with the controller type:

- Critical
- Major
- Minor
- Informational

Starting with Cisco IOS XE Amsterdam 17.3.1, the alarm severity of Not Reported (NR) is added. The informational severity is termed as Not Alarmed (NA).

- NA—Supported only when the alarm profile is enabled based on Telcordia
- NR—Supported only when the alarm profile is enabled based on Telcordia



Note To view the NA and NR alarm severities, you must use the alarm profile based on Telcordia. Otherwise, the system uses profiles that you create to only enable the alarm severity and not to view them.

Table 5: Feature History

Feature Name	Release Information	Description
Support for New Alarm Profile based on the Telcordia Profile for Chassis	Cisco IOS XE Amsterdam 17.3.1	The alarm profile based on Telcordia includes "Service Affecting" information for chassis entities. This information enables you to check the service affecting state for each alarm under a chassis.

Service Affecting or Non-Service Affecting Alarms

Alarm received on the controller can be broadly categorized as Service Affecting (SA) or Non-Service Affecting (NSA).

On the router platforms, the similar categorization can be performed:

- Service Affecting—Affects traffic and interrupts a service to generates alarms. For example, CEM and channel-group (iMSG) traffic services are affected to generate SA alarms. These alarms generated are Critical, Major, or Minor severity alarms. These alarms are generated based on the severity of the following scenarios:
  - The failure affects a service being provided, when the failure occurred.
  - The failure has capability to affect the ability of the network to provide service.
- Non-service Affecting—Does not interrupt a service or traffic. Default severity for the non-service affecting alarms is Minor.

Alarm Profiling Hierarchy

Based on the alarm profile applied to the chassis, interface module, or port, the corresponding alarms and their severity levels are applied in the following order of priority:

Table 6: Alarm Profile with Alarm Priority

Alarm Profile	Alarm Priority
Port profile	1
Interface module profile	2
Chassis profile	3

Alarm Profile based on Telcorida

When the alarm profile based on Telcordia is configured and attached to the chassis, the following fields are added to alarms and syslogs:

- Service Affecting—You can view the *Service Affecting* column under the profile configuration using the **show facility-alarm status** and **show facility-condition status** commands.
- Service Affecting (SA) or Non-Service Affecting (NSA) fields are appended to the alarm syslog.

The following figure lists the alarms generated for Alarm profile based on Telcordia.

Figure 1: Alarm profile based on Telcordia

		Alarm	Without CEM Service		With CEM Service	
			Severity	SA/NSA	Severity	SA/NSA
OCn	Line	SLOS	MN	NSA	CR	SA
		SLOF	MN	NSA	CR	SA
		LAIS	NR	NSA	NR	NSA
		LRDI	NR	NSA	NR	NSA
		TIM-S	MN	NSA	MN	NSA
		SD	NA	NSA	NA	NSA
		SF	NA	NSA	NA	NSA
	Path	PAIS	x	x	NR	NSA
		PLOP	x	x	CR	SA
		PUNEQ	x	x	CR	SA
		PPLM	x	x	CR	SA
		PDIP	x	x	NA	NSA
		PRDI	x	x	NR	NSA
		PRDI-C	x	x	NR	NSA
		PRDI-S	x	x	NR	NSA
		PRDI-P	x	x	NR	NSA
	VT	VT-PUNEQ	x	x	MJ	SA
		VT-PLM	x	x	NR	SA
		VT-AIS	x	x	NR	NSA
		VT-LOP	x	x	MJ	SA
		VT-RDI	x	x	NR	NSA
	DS3	LOF	x	x	MJ	SA
		AIS	x	x	NR	NSA
		RDI	x	x	NA	NSA
	DS1	LOF	x	x	MJ	SA
		AIS	x	x	NR	NSA
		RDI	x	x	NA	NSA
DS3 IM	DS3	LOS	MN	NSA	CR	SA
		LOF	MN	NSA	CR	SA
		AIS	NR	NSA	NR	NSA
		RDI	NA	NSA	NA	NSA
	DS1	LOF	x	x	MJ	SA
		AIS	x	x	NR	NSA
		RDI	x	x	NA	NSA
DS1 IM		LOS	MN	NSA	MJ	SA
		LOF	MN	NSA	MJ	SA
		AIS	NR	NSA	NR	NSA
		RDI	NA	NSA	NA	NSA

APS Alarm Severity

Starting with Cisco IOS XE 17.15.1, when a traffic is rerouted to an alternate link within the APS group, the severity of the alarms adjusts based on the service impact.

- **Service Not Affected**—When traffic is switched to an alternate link within the APS group without impacting the service, critical alarms are set with a severity of Minor or NSA (No Service Affecting). This adjustment helps network operators recognize non-disruptive switches, allowing them to prioritize more significant issues.

  Service Affected—When both the working and protection links in the APS are down, alarms are marked with a severity level of Critical or Major, indicating that the service is affected. This severity classification also applies to Card Protection Group (CPG)

Note To display the service affecting or nonservice affecting flag in the alarm, ensure that you enable the Telcordia profile. For more information on the Alarm profile, see Alarm Profiling, on page 11.

Figure 2: Alarm profile based on Telcordia for Active and Standby Link

		Alarm	Active				Standby			
			WIthout CEM Service		With CEM Service		Without CEM Service		With CEM Service	
			Severity	SA/NSA	Severity	SA/NSA	Severity	SA/NSA	Severity	SA/NSA
OCn	Line	SLOS	MN	NSA	CR	SA	MN	NSA	MN	NSA
		SLOF	MN	NSA	CR	SA	MN	NSA	MN	NSA
		LAIS	NR	NSA	NR	NSA	NR	NSA	NR	NSA
		LRDI	NR	NSA	NR	NSA	NR	NSA	NR	NSA
		TIM-S	MN	NSA	MN	NSA	MN	NSA	MN	NSA
		SD	NA	NSA	NA	NSA	NA	NSA	NA	NSA
		SF	NA	NSA	NA	NSA	NA	NSA	NA	NSA
	Path	PAIS	x	x	NR	NSA	x	x	NR	NSA
		PLOP	x	x	CR	SA	x	x	MN	NSA
		PUNEQ	x	x	CR	SA	x	x	MN	NSA
		PPLM	x	x	CR	SA	x	x	MN	NSA
		PDIP	x	x	NA	NSA	x	x	NA	NSA
		PRDI	x	x	NR	NSA	x	x	NR	NSA
		PRDI-C	x	x	NR	NSA	x	x	NR	NSA
		PRDI-S	x	x	NR	NSA	x	x	NR	NSA
		PRDI-P	x	x	NR	NSA	x	x	NR	NSA
	VT	VT-PUNEQ	x	x	MJ	SA	x	x	MN	NSA
		VT-PLM	x	x	MJ	SA	x	x	MN	NSA
		VT-AIS	x	x	NR	NSA	x	x	NR	NSA
		VT-LOP	x	x	MJ	SA	x	x	MN	NSA
		VT-RDI	x	x	NR	NSA	x	x	NR	NSA
	DS3	LOF	x	x	MJ	SA	x	x	MN	NSA
		AIS	x	x	NR	NSA	x	x	NR	NSA
		RDI	x	x	NA	NSA	x	x	NA	NSA
	DS1	LOF	x	x	MJ	SA	x	x	MN	NNSA
		AIS	x	x	NR	NSA	x	x	NR	NSA
		RDI	x	x	NA	NSA	x	x	NA	NSA
DS3 IM	DS3	LOS	MN	NSA	CR	SA	MN	NSA	MN	NSA
		LOF	MN	NSA	CR	SA	MN	NSA	MN	NSA
		AIS	NR	NSA	NR	NSA	NR	NSA	NR	NSA
		RDI	NA	NSA	NA	NSA	NA	NSA	NA	NSA
	DS1	LOF	x	x	MJ	SA	x	x	MN	NSA
		AIS	x	x	NR	NSA	x	x	NR	NSA
		RDI	x	x	NA	NSA	x	x	NA	NSA
DS1 IM		LOS	MN	NSA	MJ	SA	MN	NSA	MN	NSA
		LOF	MN	NSA	MJ	SA	MN	NSA	MN	NSA
		AIS	NR	NSA	NR	NSA	NR	NSA	NR	NSA
		RDI	NA	NSA	NA	NSA	NA	NSA	NA	NSA

Starting with Cisco IOS XE 17.15.1, the Signal Failure (SF) and Signal Degrade (SD) Bit Error Rate (BER) alarms are raised when there is a signal failure or signal degradation occurs in the traffic.

- The alarm severity for SF-BER, SD-BER alarm is critical for non-telcordia profile.

  The alarm severity for SF-BER, SD-BER alarm is NA for Telcordia profile.

The SD-BER and SF-BER alarms are supported on the following interface modules:

- 48-Port T1 or E1 CEM interface module
- 48-Port T31 or E3 CEM interface module

Voltage

For normal operation, only one power feed (A900-PWR900-D2) is sufficient but an alarm is generated if only one power feed is present. You can suppress this alarm using the Voltage alarm profile configuration.

- `Voltage Out of Ranage`

Note Voltage is applicable only to the chassis.

Alarm Support for Loopback

Starting with Cisco IOS XE Amsterdam 17.3.1 release, alarm support is provided for loopback.

When the port, path, VT, or T1 is in the loopback mode, minor or NSA alarm is raised based on the loopback status.

Starting with Cisco IOS XE Cupertino 17.9.1 release, loopback syslogs are allowed in maintenance mode on 1-port OC481/ STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-Port T1/E1 + 4-Port T3/E3 CEM and ASR 900 48 port DS3/E3 interface modules.

Telcordia Profile for Loopback Alarms

When the Telcordia is enabled on the chassis entity, you can view the loopback alarms based on the functioning of a service on that entity.

- You can view the loopback alarms using the **show facility condition status** command, only when a service is configured on the controller.
- Loopback alarm with network payload is not displayed using the **show facility condition status** command, as this loopback does not require a service to be configured on the path.

Default Alarm Profiles

The default alarm profiles are used when user-created alarm profiles are not configured. The default alarm profile contains the whole set of required alarms with severities as defined in the GR-253 standard with syslog enabled.

When the alarm profile of types such as chassis, card, or port is created, the alarm profile inherits configurations such as severity and syslog of the default profile. You can suppress the alarm with default severity and the alarm that is suppressed is not displayed under the **show alarm-profile** command.

You can also change the severity and syslog for a specific alarm, for example, SLOS alarm, and the severity and syslog remain intact for the remaining alarms set for the default profile.

How to Configure Alarm Profile

This section provides information about configuring alarm profile for chassis, interface, or port.

Creating Alarm Profile

While creating an alarm profile, note the following:

- The alarm profile name should be a string of alpha numeric characters.
- The alarm profile is associated with an alarm with controller types such as T1 or E1, T3 or E3, and SDH or SONET.
- You can suppress syslog and provide a new severity for the alarm.

Starting with Cisco IOS XE Amsterdam 17.3.1, the alarm severity NR is included. You can set the alarm severity NR while creating alarm profile for chassis, interface, and port.



Note To ensure the logging of alarms, use the **logging alarm [critical | major | minor | informational]** for releases earlier to Cisco IOS XE Amsterdam 17.3.1. From Cisco IOS XE Amsterdam 17.3.1 onwards, use the **logging alarm [critical | major | minor | informational | NR]** command.



Note You cannot provide the same profile name for chassis, interface, or port.

Creating Alarm Profile for Chassis

To create the alarm profile for chassis, use the following commands:

```
router(config)#alarm-profile profile-name chassis
router(config-alarm-profile)#alarm {ds1 | ds3 | gig | sonet/sdh}
router(config-alarm-properties)#alarm-name suppress
router(config-alarm-properties)#alarm-name severity severity-level
router(config-alarm-properties)#ains
```

The command **ains** enables Auto In-Service (AINS) on the chassis.



Note When the alarm profile is attached to the chassis, all cards and ports on the chassis inherit the severity from the chassis profile.



Note Ensure that you should not use Telcordia as the alarm profile name.

Creating Alarm Profile for Interface Module

To create the alarm profile for interface module, use the following commands:

```
 router(config)#alarm-profile profile-name card
router(config-alarm-profile)#alarm {ds1 | ds3 | gig | sonet/sdh}
router(config-alarm-properties)#alarm-name suppress
router(config-alarm-properties)#alarm-name severity severity-level
router(config-alarm-properties)#ains
```

The command **ains** enables AINS on the card.

Note When the alarm profile is attached to a card, all ports on the card inherit the severity from the interface module profile.

Note If a chassis profile is already attached and if you want to have a separate profile for an interface module, you can still create the interface module profile and attach it to that interface module. The interface module and all its ports inherit the properties of the interface module profile.

Creating Alarm Profile for Port

To create the alarm profile for port, use the following commands:

```
 router(config)#alarm-profile profile-name port
router(config-alarm-profile)#alarm {ds1 | ds3 | gig | sonet/sdh}
router(config-alarm-properties)#alarm-name suppress
router(config-alarm-properties)#alarm-name severity severity-level
router(config-alarm-properties)#ains
```

The command **ains** enables AINS on the port.

Note When the alarm profile attached to a port, only the port inherits the severity from the port profile.

Note If the chassis profile is already attached and if you want to have a separate profile for a port, you can still create a port profile and attach it to that port. The port inherits the properties of the port profile.

The following example describes on how to create the alarm profile *CHASSIS* with severity *critical* for DS1 alarm:

```
router(config)#alarm-profile CHASSIS chassis
router(config-alarm-profile)#alarm ds1
router(config-alarm-properties)#DS1_LOS suppress
router(config-alarm-properties)#DS1_LOS severity critical
router(config-alarm-properties)# ains
```

The following example describes on how to create the alarm profile *CARD* with severity *major* for DS1 alarm:

```
router(config)#alarm-profile CARD card
router(config-alarm-profile)#alarm ds1
router(config-alarm-properties)#DS1_LOS suppress
router(config-alarm-properties)#DS1_LOS severity major
router(config-alarm-properties)# ains
```

The following example describes on how to create the alarm profile *PORT* with severity *major* for DS1 alarm:

```
 router(config)#alarm-profile PORT port
router(config-alarm-profile)#alarm ds1
router(config-alarm-properties)#DS1_LOS suppress
router(config-alarm-properties)#DS1_LOS severity major
router(config-alarm-properties)# ains
```

The following example describes on how to create the alarm profile *CHASSIS* with severity *major* for DS3 alarm:

```
router(config)#alarm-profile CHASSIS chassis
router(config-alarm-profile)#alarm ds3
router(config-alarm-properties)#DS3_LOS suppress
router(config-alarm-properties)#DS3_LOS severity major
```

The following example describes on how to create the alarm profile *CARD* with severity *major* for DS3 alarm:

To create the alarm profile *CARD*, use the following commands:

```
router(config)#alarm-profile CARD card
router(config-alarm-profile)#alarm ds3
router(config-alarm-properties)#DS3_LOS suppress
router(config-alarm-properties)#DS3_LOS severity major
```

The following example describes on how to create the alarm profile *PORT* with severity *major* for DS3 alarm:

```
router(config)#alarm-profile PORT port
router(config-alarm-profile)#alarm ds3
router(config-alarm-properties)#DS3_LOS suppress
router(config-alarm-properties)#DS3_LOS severity major
```

The following example describes on how to create the alarm profile *CHASSIS* with severity *critical* for SONET or SDH alarm:

```
router(config)#alarm-profile CHASSIS chassis
router(config-alarm-profile)#alarm sonet
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity critical
```

The following example describes on how to create the alarm profile *CHASSIS* with severity *minor* for SONET or SDH alarm:

```
router(config)#alarm-profile CHASSIS chassis
router(config-alarm-profile)#alarm sonet
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity minor
```

The following example describes on how to create the alarm profile *CARD* with severity *critical* for SONET or SDH alarm:

```
router(config)#alarm-profile CARD card
router(config-alarm-profile)#alarm sonet
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity critical
```

The following example describes on how to create the alarm profile *PORT* with severity *critical* for SONET or SDH alarm:

```
router(config)#alarm-profile PORT port
router(config-alarm-profile)#alarm sonet
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity critical
```

Attaching Alarm Profile to Entity

Once the alarm profile is created, attach the alarm profile to the appropriate entity. You can apply the alarm severity and other alarm functionalities only after attaching the alarm profile to the entity.

Attaching Alarm Profile to Chassis

To attach the alarm profile to chassis, use the following commands:

```
router>enable
router#configure terminal
router(config)#alarm-profile profile-name attach chassis
router(config)#end
```

Note When an alarm profile is attached to chassis, the profile is applicable to all the cards available on the chassis, but not to cards that are inserted after the profile is attached. To attach alarm profile to cards,reattach the alarm profile to the chassis.

Attaching Telcordia Alarm Profile to Chassis

Starting with the Cisco IOS XE Amsterdam 17.3.1, you can attach a Telcordia profile to the chassis. The alarm severities Not Alarmed (NA) and Not Reported (NR) are included by default in the Telcordia profile. The alarm profile attached to chassis inherits the alarm severities of the Telcordia profile.

To attach the alarm profile based on Telcordia to chassis, use the following commands:

```
router>enable
router#configure terminal
router(config)#alarm-profile telcordia attach chassis
router(config)#end
```

Note Ensure that you use the complete **alarm-profile telcordia attach chassis** command while attaching the alarm profile based on Telcordia.

Attaching Alarm Profile to Interface Module

To attach an alarm profile to the interface module, use the following commands:

```
router>enable
router#configure terminal
router(config)#alarm-profile profile-name attach card slot/bay
router(config)#end
```

Note The alarm profile cannot be attached to a slot when there is no card available in the slot.

Attaching Alarm Profile to Port

Depending on the controller type, the alarm profile is attached to the port. The supported controller types are SONET, SDH, T1, T3, E1, and E3. Select the controller and the port, and then attach the profile to the port.

To attach the alarm profile to port, use the following commands:

```
router>enable
router#configure terminal
router(config)#controller {sonet | sdh | t1 | e1 | t3 | e3} slot/bay/port
router(config-controller)#attach profile profile-name
router(config-controller)#end
```

To attach the port profile to Ethernet interface, use the following commands:

```
router>enable
router#configure terminal
router(config)#interface gigabitethernet 0/7/0
router(config-controller)#  attach profile port
router(config-controller)#end
```

Note The following restrictions apply to the 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module:

- Only the following three AINS modes are supported:
  - 8x1G + 1x10G (default mode) Fully Subscribed
  - 16x1G+1x10G – Over Subscribed
  - 18x1G – Over Subscribed
- If you change any of the above modes, the chassis and card profiles stay unaffected; however, port profile is disabled and requires to be reattached.

The following example describes on how to attach the alarm profile ***CHASSIS***:

```
router>enable
router#configure terminal
router(config)#alarm-profile CHASSIS attach chassis
router(config)#end
```

The following example describes on how to attach the alarm profile ***CARD***:

```
router>enable
router#configure terminal
router(config)#alarm-profile CARD attach card slot/bay
router(config)#end
```

The following example describes on how to attach the alarm profile ***PORT*** on the SONET controller:

```
router>enable
router#configure terminal
router(config)#controller sonet  0/5/0
router(config-controller)#rate OC48
router(config-controller)#no ais-shut
router(config-controller)#attach profile PORT
router(config-controller)#end
```

Modifying Alarm Profile

You can modify the existing alarm profile associated with chassis, port, or interface. You can modify the alarm severity and suppress (or disable) the syslog facility. The alarm severity that you can modify are critical, major, minor, and informational.

Modifying Alarm Profile for Chassis

To modify the existing alarm configured for chassis, use the following commands:

```
router(config)#alarm-profile profile-name chassis
router(config-alarm-profile)#alarm sonet/sdh
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity major
```

Note You cannot modify the alarm profile based on Telcordia.

Modifying Alarm Profile for Interface Module

To modify the existing alarm configured for card, use the following commands:

```
router(config)#alarm-profile profile-name card
router(config-alarm-profile)#alarm sonet/sdh
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity major
```

Modifying Alarm Profile for Port

To modify the existing alarm configured for port, use the following commands:

```
router(config)#alarm-profile profile-name port
router(config-alarm-profile)#alarm sonet/sdh
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity major
```

The following example describes how to modify the existing alarm severity for the alarm profile ***CHASSIS***:

```
router(config)#alarm-profile CHASSIS chassis
router(config-alarm-profile)#alarm sonet/sdh
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity major
```

The following example describes how to modify the existing alarm severity for the alarm profile ***CARD***:

```
router(config)#alarm-profile CARD card
router(config-alarm-profile)#alarm sonet/sdh
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity major
```

The following example describes how to modify the existing alarm severity for the alarm profile ***PORT***:

```
router(config)#alarm-profile PORT port
router(config-alarm-profile)#alarm sonet/sdh
router(config-alarm-properties)#SLOF suppress
router(config-alarm-properties)#SLOF severity major
```

Detaching Alarm Profile

You can detach the existing alarm profile from chassis, interface, or port and attach a new profile. If a new alarm profile is not attached, then the default profile is attached.

Detaching Alarm Profile from Chassis

When the alarm profile associated with chassis is detached, the profile is removed from all the interfaces available in the chassis. The alarms configured for the profile have no effect on these interfaces even when alarm conditions occur.

To detach the alarm profile associated with chassis, use the following commands:

```
Router#configure terminal
Router(config)#no alarm-profile profile-name attach chassis
Router(config)#end
```

To detach the alarm profile based on Telcordia, use the following commands:

```
Router#configure terminal
Router(config)#no alarm-profile telcordia attach chassis
Router(config)#end
```

Detaching Alarm Profile from Interface Module

For the alarm profile associated with an interface module, when detached, the profile is removed from all the ports and the interfaces. While detaching alarm profile, specify the slot and subslot.

To detach the alarm profile associated with the card, use the following commands:

```
Router#configure terminal
Router(config)#no alarm-profile profile-name attach CARD 0/9
Router(config)#end
```

Detaching Alarm Profile from Port

To detach an alarm profile associated with the port, you must access the specific controller and interface. The alarm profile is detached from specific interface for the controller.

To detach the alarm profile associated with a port, use the following commands:

```
Router#configure terminal
```

```
Router(config)#controller {DS1 | DS3 | gig | sonet/sdh} slot/bay/port
Router(config-controller)#no attach profile profile-name
Router(config-controller)#end
```

The following example describes how to detach the alarm profile ***CHASSIS*** associated with chassis:

```
Router#configure terminal
Router(config)#no alarm-profile CHA attach chassis
Router(config)#end
```

The following example describes how to detach the alarm profile ***CARD*** associated with chassis:

```
Router#configure terminal
Router(config)#no alarm-profile CARD attach card 0/9
Router(config)#end
```

The following example describes how to detach the alarm profile ***PORT*** associated with chassis:

```
Router#configure terminal
Router#controller sonet 0/9/16
Router(config-controller)#no attach profile PORT
Router(config-controller)#end
```

Deleting Alarm Profile

Note Before deleting the alarm profile, detach the profile from chassis, interface, or port. Alarm profiles cannot be deleted when profiles are attached to an entity.

Deleting Alarm Profile for Chassis

To delete the alarm profile associated with the chassis, use the following command:

```
Router(config)no alarm-profile CHASSIS chassis
```

Note You cannot delete the alarm profile based on Telcordia.

Deleting Alarm Profile for Interface Module

To delete the alarm profile associated with a card, use the following command:

```
Router(config)no alarm-profile CARD card
```

Deleting Alarm Profile for Port

To delete the alarm profile associated with a port, use the following command:

```
Router(config)no alarm-profile PORT port
```

Verifying Alarm Profile for T1 or E1 Alarms

Use the following commands to verity the alarm profile configuration:

- **show alarm-profile name**—Displays the alarm profile configured for chassis.

- **show facility-alarm status**—Displays the alarms status attached to a specific profile.
- **show controller**—Displays the alarm profiles configured for a specific port.
- **show logging**—Displays the alarms reporting in syslog.

To display the alarm profile configured for chassis, use the **show alarm-profile name** command:

```
Router# show alarm-profile name CHASSIS
Alarm profile CHASSIS:
  DS1:
  Alarm Name                            Severity   Syslog
  Receiver has loss of signal           CRITICAL   Enabled
  Receiver has loss of frame            INFO       Enabled
  Receiver has remote alarm             INFO       Enabled
```

To display the alarm status attached to a specfic profile, use the **show facility-alarm status** command:

```
Router# show facility-alarm status | inc 0/3/0
t1 0/3/0  Feb 01 2018 19:23:10  CRITICAL  Section Receiver has loss of signal  [1]
```

Verifying Alarm Profile for Severity Change for T1 or E1 Alarms

The following example verifies when the severity of the T1 or E1 alarms are modified for a Chassis profile. The alarm severity changes are verified using the **show alarm-profile name** command:

Create a CHASSIS alarm profile for the DS1 alarms:

```
Router(config)#alarm-profile CHASSIS chassis
Router(config-alarm-properties)#alarm ds1
Router(config-alarm-properties)#DS1_LOF severity critical
Router(config-alarm-properties)#DS1_LOF suppress
Router(config-alarm-properties)#alarm ds1
Router(config-alarm-properties)#DS1_RAI severity info
Router(config-alarm-properties)#DS1_RAI suppress
```

Verify the CHASSIS alarm profile using the **show alarm-profile name** command:

```
Router#show alarm-profile name CHASSIS
Alarm profile CHASSIS:
  Alarm Name                                        Severity       Syslog
  Receiver has loss of signal                       CRITICAL       Enabled
  Receiver has remote alarm                         MINOR          Enabled
```

Attach the CHASSIS alarm profile to chassis:

```
router>enable
router#configure terminal
router(config)#alarm-profile CHASSIS attach chassis
router(config)#end
```

Modify the severity of the CHASSIS alarm profile for the DS1 alarms:

```
Router(config)#alarm-profile CHASSIS chassis
Router(config-alarm-properties)#alarm ds1
Router(config-alarm-properties)#DS1_LOF severity major
Router(config-alarm-properties)#DS1_LOF suppress
Router(config-alarm-properties)#alarm ds1
```

```
Router(config-alarm-properties)#DS1_RAI severity info
Router(config-alarm-properties)#DS1_RAI suppress
```

Verify the CHASSIS alarm profile with modified severity:

```
Router#show alarm-profile name CHASSIS
Alarm profile CHASSIS:
DS1:
  Alarm Name                                          Severity       Syslog
  Receiver has loss of signal                         MAJOR          Enabled
  Receiver has remote alarm                           INFO           Enabled
```

Verifying Alarm Profile for T3 or E3 Alarms

Use the following commands to verity the alarm profile configuration:

- **show alarm-profile name**—Displays the alarm profile configured for chassis.
- **show facility-alarm status**—Displays the alarms status attached to a specific profile.
- **show controller**—Displays the alarm profiles configured for a specific port.
- **show logging**—Displays the alarms reporting in syslog.

To display the alarm profile configured for chassis, use the **show alarm-profile name** command:

```
Router# show alarm-profile name CHASSIS
Alarm profile CHASSIS:
  DS3:
  Alarm Name                          Severity   Syslog
  Receiver has loss of signal         MAJOR      Enabled
  DS1 Alarm Indication Signal         MINOR      Enabled
  DS1 Loss Of Frame                   INFO       Enabled
  DS1 Remote Alarm Indication         INFO       Enabled
```

To display the alarm status attached to a specfic profile, use the **show facility-alarm status** command:

```
Router# show facility-alarm status | inc 0/4/40
T3 0/4/40  Feb 01 2018 19:23:10  MAJOR  Section Receiver has loss of signal [1]
```

Verifying Alarm Profile for Severity Change for T3 or E3 Alarms

The following example verifies when the severity of the T3 or E3 alarms are modified for a Chassis profile. The alarm severity changes are verified using the **show alarm-profile name** command:

Create a CHASSIS alarm profile for the DS1 alarms:

```
Router(config)#alarm-profile CHASSIS chassis
router(config-alarm-profile)#alarm ds3
router(config-alarm-properties)#DS3_LOS suppress
router(config-alarm-properties)#DS3_LOS severity major
router(config-alarm-properties)#MCPRP_DS3_DS1_LOS suppress
router(config-alarm-properties)#MCPRP_DS3_DS1_LOS severity minor
```

Verify the CHASSIS alarm profile using the **show alarm-profile name** command:

```
Router#show alarm-profile name CHASSIS
Alarm profile CHASSIS:
  Alarm Name                                          Severity       Syslog
  Receiver has loss of signal                         MAJOR          Enabled
```

```
  DS1 Loss Of Signal                                    MINOR          Enabled
```

Attach the CHASSIS alarm profile to chassis:

```
router>enable
router#configure terminal
router(config)#alarm-profile CHASSIS attach chassis
router(config)#end
```

Modify the severity of the CHASSIS alarm profile for the DS1 alarms:

```
router(config)#alarm-profile CHASSIS chassis
router(config-alarm-profile)#alarm ds3
router(config-alarm-properties)#DS3_LOS suppress
router(config-alarm-properties)#DS3_LOS severity minor
router(config-alarm-properties)#MCPRP_DS3_DS1_LOS suppress
router(config-alarm-properties)#MCPRP_DS3_DS1_LOS severity minor
```

Verify the CHASSIS alarm profile with modified severity:

```
Router#show alarm-profile name CHASSIS
Alarm profile CHASSIS:
DS1:
  Alarm Name                                            Severity       Syslog
  Receiver has loss of signal                           MINOR          Enabled
  DS1 Loss Of Signal                                    MINOR          Enabled
```

Verifying Alarm Profile for SONET or SDH

Use the following commands to verify the alarm profile configuration:

- **show alarm-profile name**—Displays the alarm profile configured for chassis.
- **show facility-alarm status**—Displays the status of the alarms attached to a specific profile.
- **show facility-ains transceiver**—Displays the transceiver status.
- **show controller/interface**—Displays the operational alarm profile attached to the controller or interface.
- **show logging**—Displays the alarms reported in the syslog.
- **show facility-condition status**—Displays the secondary alarms on the controller, alarms when the port is in AUTO-IN-SERVICE state and the loopback alarm

To display the alarm profile configured for the chassis, use the **show alarm-profile name** command:

```
Router# show alarm-profile name CHASSIS
Alarm profile CHASSIS:
 SONET/SDH:
  Alarm Name                            Severity   Syslog
  Section Loss of Frame Failure         CRITICAL   Enabled
  Line Alarm Indication Signal          INFO       Enabled
  Line Remote Failure Indication        INFO       Enabled
  Path Alarm Indication Signal          INFO       Enabled
  Path Remote Failure Indication        INFO       Enabled
  Path Loss of Pointer                  INFO       Enabled
 DS1:
  Alarm Name                            Severity   Syslog
  Receiver has loss of signal           CRITICAL   Enabled
```

```
  Receiver has loss of frame           INFO       Enabled
  Receiver has remote alarm            INFO       Enabled
 DS3:
  Alarm Name                           Severity   Syslog
  Receiver has loss of signal          MAJOR      Enabled
  DS1 Alarm Indication Signal          MINOR      Enabled
  DS1 Loss Of Frame                    INFO       Enabled
  DS1 Remote Alarm Indication          INFO       Enabled
```

To display the alarm status attached to a specfic profile, use the **show facility-alarm status** command:

```
Router# show facility-alarm status | include 0/4/1
SONET 0/4/1  Feb 01 2018 19:23:10  INFO  Section Loss of Frame Failure [1]
```

To display the alarm status and the service affecting state for each source with Telcordia enabled, use the **show facility-alarm status** command:

```
Router#show facility-alarm status
Source                    Time                    Severity      Service Affecting  Syslog
String                 Description [Index]
------                    ------                  --------      -----------------
-------------                 -------------------
Power Supply Bay 0        Feb 10 2020 18:57:25   CRITICAL      SA
PSU_MISSING                   Power Supply/FAN Module Missing [0]
Fan Tray/Ext. ALARM:      Feb 10 2020 19:06:23   MAJOR         NSA                 Fan
Failure                   Fan Tray/Fan 7 Failure [14]
GigabitEthernet0          Feb 10 2020 18:57:25   NA            NSA
ETHERNET_PORT_ADMIN_DOWN      Physical Port Administrative State Down [2]
GigabitEthernet0/1/1      Feb 10 2020 18:57:58   CRITICAL      SA
ETHERNET_PORT_LINK_DOWN       Physical Port Link Down [1]
xcvr container 0/1/2      Feb 10 2020 18:57:52   CRITICAL      SA
XCVR_MISSING_LINK_DOWN        Transceiver Missing - Link Down [1]
xcvr container 0/1/3      Feb 10 2020 18:57:52   CRITICAL      SA
XCVR_MISSING_LINK_DOWN        Transceiver Missing - Link Down [1]
xcvr container 0/1/4      Feb 10 2020 18:57:52   CRITICAL      SA
XCVR_MISSING_LINK_DOWN        Transceiver Missing - Link Down [1]
xcvr container 0/1/5      Feb 10 2020 18:57:52   CRITICAL      SA
XCVR_MISSING_LINK_DOWN        Transceiver Missing - Link Down [1]
xcvr container 0/1/6      Feb 10 2020 18:57:52   CRITICAL      SA
XCVR_MISSING_LINK_DOWN        Transceiver Missing - Link Down [1]
xcvr container 0/1/7      Feb 10 2020 18:57:52   CRITICAL      SA
XCVR_MISSING_LINK_DOWN        Transceiver Missing - Link Down [1]
SONET 0/2/16                Feb 10 2020 19:11:16   MINOR         NSA                 SLOS
                         Section Loss of Signal Failure [0]
SONET 0/2/16                Feb 10 2020 19:11:16   NR            NSA
SONET_LINK_DOWN               Physical Port Link Down [59]
IM subslot 0/3              Feb 10 2020 18:57:38   MAJOR         NSA
                         Disabled [2]
IM subslot 0/4              Feb 10 2020 18:57:38   MAJOR         NSA
                         Disabled [2]
IM subslot 0/5              Feb 10 2020 18:57:38   MAJOR         NSA
                         Disabled [2]
System Totals  Critical: 8  Major: 4  Minor: 1 NA: 1
```

Note The SA column is displayed only when the profile based on Telcordia is attached.

```
Router#show facility-alarm status | inc 0/4/1
SONET 0/4/1  Feb 01 2018 19:23:10  INFO  Section Loss of Frame Failure [1]
```

To display the operational or attached alarm profile, use the **show interfaces** command:

```
Router#show interfaces gigabitEthernet 0/7/0
GigabitEthernet0/7/0 is down, line protocol is down
Alarm-profile: chassis_ains
  Hardware is A900-IMA8CS1Z-M, address is 5006.ab62.3a36 (bia 5006.ab62.3a36)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is force-up, media type is SX
  output flow-control is unsupported, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input

Router#show interfaces GigabitEthernet 0/1/0

GigabitEthernet0/1/0 is up, line protocol is up
Sec-admin-state: in-service, Soak-time: NA,
soak-Time-left: NA, AINS-state: IS-NR
  Hardware is A900-IMA8S1Z, address is f078.1685.3f12 (bia f078.1685.3f12)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is SX
  output flow-control is unsupported, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:00:37
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

To display the alarm status configured for chassis, use the **show facility-alarm status** command:

```
Router#show facility-alarm status
System Totals  Critical: 25  Major: 5  Minor: 0
Source           Severity      Syslog String                 Description [Index]

subslot 0/12             CRITICAL                                    Active Card Removed
OIR Alarm [0]
```

```
Power Supply Bay 3       CRITICAL      PSU_MISSING                    Power Supply/FAN
Module Missing [0]
module R1                MAJOR                                        Unknown state [0]
SONET 0/4/1              CRITICAL      SLOS                           Section Loss of Signal
 Failure [0]
SONET 0/4/1              CRITICAL      SONET_LINK_DOWN                Physical Port Link
Down [59]
xcvr container 0/4/5     INFO          XCVR_MISSING                   Transceiver Missing
[0]
xcvr container 0/4/6     INFO          XCVR_MISSING                   Transceiver Missing
[0]
xcvr container 0/4/7     INFO          XCVR_MISSING                   Transceiver Missing
[0]
xcvr container 0/7/1     CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/3     CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/4     CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/5     CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/6     CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/7     CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/8     CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/9     CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/11    CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/13    CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/14    CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/7/15    CRITICAL      XCVR_MISSING_LINK_DOWN         Transceiver Missing
- Link Down [1]
xcvr container 0/8/18    INFO          XCVR_MISSING                   Transceiver Missing
[0]
xcvr container 0/8/19    INFO          XCVR_MISSING                   Transceiver Missing
[0]
xcvr container 0/14/2    INFO          XCVR_MISSING                   Transceiver Missing
[0]
xcvr container 0/14/4    INFO          XCVR_MISSING                   Transceiver Missing
[0]
```

Verifying Alarm Profile for Severity Change for SONET or SDH Alarms

Use the **show alarm-profile** command to verify when the severity of the SONET or SDH alarms are modified for a chassis profile:

Create a port alarm profile for the SONET or SDH alarms:

```
Router(config)#alarm-profile PORT port
Router(config-alarm-properties)#alarm sonet/sdh
Router(config-alarm-properties)#lais severity critical
Router(config-alarm-properties)#puneq severity major
Router(config-alarm-properties)#pais severity major
Router(config-alarm-properties)#end
```

Verify the alarm profile using the **show alarm-profile** command:

```
Router#show alarm-profile PORT
Alarm profile PORT:
SONET/SDH:
  Alarm Name                                          Severity   Syslog
  Line Alarm Indication Signal                         CRITICAL   Enabled
  Path Alarm Indication Signal                         MINOR      Enabled
  Path Payload Unequipped                              MAJOR      Disabled
  Lower Order Path Alarm Indication Signal             MINOR      Disabled
```

Attach port alarm profile to port:

```
 Router>enable
Router#configure terminal
Router(config)#controller sonet 0/3/3
Router(config-controller)#attach profile PORT
Router(config-controller)#end
```

Modify the severity of the port alarm profile for the SONET or SDH alarms:

```
Router(config)#alarm-profile PORT port
Router(config-alarm-properties)#alarm sonet/sdh
Router(config-alarm-properties)#PAIS suppress
Router(config-alarm-properties)#LAIS severity info
Router(config-alarm-properties)# end
```

Verify the port alarm profile with modified severity:

```
Router#show alarm-profile PORT
Alarm profile PORT:
SONET/SDH:
  Alarm Name                                          Severity     Syslog
  Line Alarm Indication Signal                        INFO         Enabled
  Path Alarm Indication Signal                        MINOR        Enabled
  Path Payload Unequipped                             MAJOR        Disabled
  Lower Order Path Alarm Indication Signal            MINOR        Enabled
```

Alarm Profile Use Cases for T1 or E1 Alarms

Use Case 1

The following example explains default alarm profile having DS1_AIS alarm with severity as MINOR and syslog is enabled, and when the alarm is configured as suppressed with default severity, the alarm is not displayed under the **show alarm-profile name** command.

Use the following steps to suppress the default alarm profile:

1. Create a chassis profile, for example, *chassis* and verity that the DS1_AIS alarm is listed under the **show alarm-profile name chassis** command.
2. Set the alarm DS1_AIS as suppressed.

The alarm DS1_AIS is not displayed under the **show alarm-profile name *chassis*** command.

Create chassis profile

```
Router#configure terminal
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#end
Router#show alarm-profile name chassis
Alarm profile chassis:
  DS1:
  Alarm Name
          Severity   Syslog
  Transmitter is sending AIS
          MINOR       Enabled
  Receiver has loss of signal
          CRITICAL    Enabled
  Receiver has loss of frame
          INFO        Enabled
  Receiver has remote alarm INFO
          INFO        Enabled
```

Set the alarm DS1_AIS as suppressed

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#alarm ds1
Router(config-alarm-properties)#DS1_AIS suppress
Router(config-alarm-properties)#end
```

Note that the DS1_AIS alarm is not displayed under the `show alarm-profile name chassis` command.

```
Router#show alarm-profile name chassis
Alarm profile chassis:
  DS1:
  Alarm Name
          Severity   Syslog
  Receiver has loss of signal
          CRITICAL    Enabled
  Receiver has loss of frame
          INFO        Enabled
  Receiver has remote alarm
          INFO        Enabled
```

Use Case 2

The following example displays default profile having DS1_AIS alarm with severity as MINOR and syslog enabled, and when the alarm is configured as suppressed with severity set to INFO, the alarm is displayed under the **show alarm-profile name** command.

Use the following steps to change the DS1_AIS alarm severity:

1. Create a chassis profile, for example, *chassis*.
2. Set the alarm DS1_AIS as suppressed and alarm DS1_AIS severity to INFO.

The alarm DS1_AIS is displayed under the **show alarm-profile name chassis** command.

Create chassis profile

```
Router#configure terminal
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#end
```

Set the alarm DS1_AIS as suppressed and severity to INFO

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#alarm ds1
Router(config-alarm-properties)#DS1_AIS suppress
Router(config-alarm-properties)#DS1_AIS severity INFO
Router(config-alarm-properties)#end
```

Note that the DS1_AIS alarm is displayed under the `show alarm-profile name chassis` command.

```
Router#show alarm-profile name chassis
Alarm profile chassis:
  DS1:
 Alarm Name
         Severity   Syslog
 Transmitter is sending AIS
         MINOR       Enabled
 Receiver has loss of signal
         CRITICAL    Enabled
 Receiver has loss of frame
         INFO        Enabled
 Receiver has remote alarm
         INFO        Enabled
```

Use Case 3

The following example displays default profile having DS1_LOF and DS1_RAI alarms with severities as CRITICAL and MINOR respectively. Using the chassis profile, you can set the DS1_LOF alarm severity to INFO and verify using the **show alarm-profile name** command. The show output displays the DS1_LOF as INFO and DS1_RAI as MINOR.

Use the following steps to change the DS1_LOF alarm severity:

1. Create a chassis profile, for example, *chassis*.
2. Set the alarm DS1_LOF severity to INFO.

The alarm DS1_LOF is displayed under the **show alarm-profile name chassis** command.

Create a chassis profile

```
Router#configure terminal
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#end
```

Set the alarm DS1_LOF severity to INFO

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#alarm t1
Router(config-alarm-properties)#DS1_LOF severity INFO
Router(config-alarm-properties)#end
```

Note that the DS1_LOF alarm is displayed under the `show alarm-profile name chassis` command.

```
Router#show alarm-profile name chassis
Alarm profile chassis:
 T1:
```

```
 Alarm Name
         Severity   Syslog
 Transmitter is sending AIS
         MINOR       Enabled
 Receiver has loss of signal
         CRITICAL    Enabled
 Receiver has loss of frame
         INFO        Enabled
 Receiver has remote alarm
         MINOR        Enabled
```

Use Case 4

The following example displays default profile having DS1_LOF and DS1_RAI alarms with severities as CRITICAL and MINOR respectively. Using the card profile, you can set the DS1_LOF alarm severity to MAJOR and verify using the **show alarm-profile name** command. The show output displays the DS1_LOF as MAJOR and DS1_RAI as MINOR.

Use the following steps to change the DS1_LOF alam severity:

1. Create a card profile, for example, *card*.
2. Set the alarm DS1_LOF severity to MAJOR.

The alarm DS1_LOF with severity MAJOR is displayed under the **show alarm-profile name** command.

Create a card profile and set the alarm DS1_LOF severity to MAJOR

```
Router#configure terminal
Router(config)#alarm-profile card card
Router(config-alarm-profile)#alarm ds1
Router(config-alarm-properties)#DS1_LOF severity MAJOR
Router(config-alarm-properties)#end
```

Note that the DS1_LOF with severity MAJOR and DS1_RAI with severity MINOR are displayed under the `show alarm-profile name` command.

```
Router#show alarm-profile name card
Alarm profile card:
 DS1:
Alarm Name
         Severity   Syslog
 Transmitter is sending AIS
         MINOR       Enabled
 Receiver has loss of signal
         CRITICAL    Enabled
 Receiver has loss of frame
         MAJOR        Enabled
 Receiver has remote alarm
         MINOR        Enabled
```

Use Case 5

The following example displays default profile having DS1_LOF and DS1_RAI alarms with severities as CRITICAL and MINOR respectively. Using the port profile, you can set the DS1_LOF alarm

severity to MAJOR and DS1_RAI alarm severity to INFO. Verify using the **show alarm-profile name** command. The show output displays the DS1_LOF as MAJOR and DS1_RAI as INFO.

Use the following steps to change the DS1_LOF and DS1_RAI alarm severities:

1. Create a port profile, for example, *port*.
2. Set the alarm severities DS1_LOF to MAJOR and DS1_RAI to INFO.

The alarm DS1_LOF with severity MAJOR and DS1_RAI with severity INFO are displayed under the **show alarm-profile name** command.

Create a port profile and set the alarm severities of DS1_LOF to MAJOR and DS1_RAI to INFO

```
Router#configure terminal
Router(config)#alarm-profile port port
Router(config-alarm-profile)#alarm ds1
Router(config-alarm-properties)#DS1_LOF severity MAJOR
Router(config-alarm-properties)#DS1_RAI severity MINOR
Router(config-alarm-properties)#end
```

Note that the DS1_LOF with severity MAJOR and DS1_RAI with severity INFO are displayed under the `show alarm-profile name` command.

```
Router#show alarm-profile name port
Alarm profile port:
 DS1:
Alarm Name
         Severity   Syslog
 Transmitter is sending AIS
         MINOR       Enabled
 Receiver has loss of signal
         CRITICAL    Enabled
 Receiver has loss of frame
         MAJOR        Enabled
 Receiver has remote alarm
         INFO        Enabled
```

Alarm Profile Use Cases for T3 or E3 Alarms

Use Case 1

The following example explains default alarm profile having DS3_DS1_AIS alarm with severity as MINOR and syslog is enabled, and when the alarm is configured as suppressed with default severity, the alarm is not displayed under the **show alarm-profile name** command.

Use the following steps to suppress the default alarm profile:

1. Create a chassis profile, for example, *chassis* and verity that the DS3_DS1_AIS alarm is listed under the **show alarm-profile name chassis** command.
2. Set the alarm DS3_DS1_AIS as suppressed.

The alarm DS3_DS1_AIS is not displayed under the **show alarm-profile name chassis** command.

Create chassis profile

```
Router#configure terminal
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#end
Router#show alarm-profile name chassis
Alarm profile chassis:
  DS1:
  Alarm Name
          Severity   Syslog
  DS1 Alarm Indication Signal
          MINOR       Enabled
  Transmitter is sending AIS
          MINOR       Enabled
  Receiver has loss of signal
          CRITICAL    Enabled
  Receiver has loss of frame
          INFO        Enabled
  Receiver has remote alarm
          INFO        Enabled
```

Set the alarm DS3_DS1_AIS as suppressed

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#alarm ds3
Router(config-alarm-properties)#DS3_DS1_AIS suppress
Router(config-alarm-properties)#end
```

Note that the DS3_DS1_AIS alarm is not displayed under the `show alarm-profile name chassis` command.

```
Router#show alarm-profile name chassis
Alarm profile chassis:
  DS1:
  Alarm Name
          Severity   Syslog
  Receiver has loss of signal
          CRITICAL    Enabled
  Receiver has loss of frame
          INFO        Enabled
  Receiver has remote alarm
          INFO        Enabled
```

Use Case 2

The following example displays default profile having DS3_DS1_AIS alarm with severity as MINOR and syslog enabled, and when the alarm is configured as suppressed with severity set to INFO, the alarm is displayed under the **show alarm-profile name** command.

Use the following steps to change the DS3_DS1_AIS alarm severity:

1. Create a chassis profile, for example, *chassis*.
2. Set the alarm DS3_DS1_AIS as suppressed and alarm DS3_DS1_AIS severity to INFO.

The alarm DS3_DS1_AIS is displayed under the **show alarm-profile name chassis** command.

Create chassis profile

```
Router#configure terminal
```

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#end
```

Set the alarm DS3_DS1_AIS as suppressed and severity to INFO

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#alarm ds3
Router(config-alarm-properties)#DS3_DS1_AIS suppress
Router(config-alarm-properties)#DS3_DS1_AIS severity INFO
Router(config-alarm-properties)#end
```

Note that the DS3_DS1_AIS alarm is displayed under the `show alarm-profile name chassis` command.

```
Router#show alarm-profile name chassis
Alarm profile chassis:
DS1:
  Alarm Name
          Severity   Syslog
  DS1 Alarm Indication Signal
          INFO       Enabled
  Transmitter is sending AIS
          MINOR      Enabled
  Receiver has loss of signal
          CRITICAL   Enabled
  Receiver has loss of frame
          INFO       Enabled
  Receiver has remote alarm
          INFO       Enabled
```

Use Case 3

The following example displays default profile having DS3_AIS and DS3_LOS alarms with severities as MINOR and MAJOR respectively. Using the chassis profile, you can set the DS3_LOS alarm severity to INFO and verify using the **show alarm-profile name** command. The show output displays theDS3_LOS as INFO and DS3_AIS as MINOR.

Use the following steps to change the DS3_LOS alarm severity:

1. Create a chassis profile, for example, *chassis*.
2. Set the alarm DS3_LOS severity to INFO.

The alarm DS3_LOS is displayed under the **show alarm-profile name chassis** command.

Create a chassis profile

```
Router#configure terminal
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#end
```

Set the alarm DS3_LOS severity to INFO

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#alarm ds3
Router(config-alarm-properties)#DS3_LOS severity INFO
Router(config-alarm-properties)#end
```

Note that the DS3_LOS alarm is displayed under the `show alarm-profile name chassis` command.

```
Router#show alarm-profile name chassis
Alarm profile chassis:
 T1:
  Alarm Name
           Severity   Syslog
 Transmitter is sending AIS
          MINOR       Enabled
 Receiver has loss of signal
          INFO        Enabled
 Receiver has loss of frame
          INFO        Enabled
 Receiver has remote alarm
          MINOR        Enabled
```

Use Case 4

The following example displays default profile having DS3_AIS and DS3_LOS alarms with severities as MINOR and MAJOR respectively. Using the card profile, you can set the DS3_LOS alarm severity to MINOR and verify using the **show alarm-profile name** command. The show output displays the DS3_AIS and DS3_LOS severities as MINOR.

Use the following steps to change the DS3_LOS alarm severity:

1. Create a card profile, for example, *card*.
2. Set the alarm DS3_LOS severity to MINOR.

The alarm DS3_LOS with severity MINOR is displayed under the **show alarm-profile name** command.

Create a card profile and set the alarm DS3_LOS severity to MINOR

```
Router#configure terminal
Router(config)#alarm-profile card card
Router(config-alarm-profile)#alarm ds3
Router(config-alarm-properties)#DS3_LOS severity MINOR
Router(config-alarm-properties)#end
```

Note that the DS3_LOS and DS3_AIS with severities MINOR are displayed under the `show alarm-profile name card` command.

```
Router#show alarm-profile name card
Alarm profile card:
 DS1:
Alarm Name
          Severity   ``Syslog
 Transmitter is sending AIS
          MINOR       `Enabled
 Receiver has loss of signal
          MINOR    ````Enabled
 Receiver has loss of frame
          MAJOR       Enabled
 Receiver has remote alarm
          MINOR        Enabled
```

Use Case 5

The following example displays default profile having DS3_AIS and DS3_LOS alarms with severities as MINOR and MAJOR respectively. Using the port profile, you can set the DS3_LOS alarm severity to MINOR and DS3_AIS alarm severity to INFO. Verify using the **show alarm-profile name** command. The show output displays the DS3_AIS as INFO and DS3_LOS as MINOR.

Use the following steps to change the DS3_AIS and DS3_LOS alarm severities:

1. Create a port profile, for example, *port*.
2. Set the DS3_LOS alarm severity to MINOR and DS3_AIS alarm severity to INFO.

The alarm DS3_AIS as INFO and DS3_LOS as MINOR are displayed under the **show alarm-profile name** command.

Create a port profile and set the alarm severities

```
Router#configure terminal
Router(config)#alarm-profile port port
Router(config-alarm-profile)#alarm ds3
Router(config-alarm-properties)#DS3_AIS severity INFO
Router(config-alarm-properties)#DS3_LOS severity MINOR
Router(config-alarm-properties)#end
```

Note that the DS3_AIS as INFO and DS3_LOS as MINOR are displayed under the `show alarm-profile name` command.

```
Router#show alarm-profile name port
Alarm profile port:
 DS1:
Alarm Name
         Severity   Syslog
 Transmitter is sending AIS
         INFO       Enabled
 Receiver has loss of signal
         MINOR    Enabled
 Receiver has loss of frame
         MAJOR        Enabled
 Receiver has remote alarm
         INFO        Enabled
```

Alarm Profile Use Cases for SONET or SDH Alarms

Use Case 1

In the following use case the default alarm profile has a Line Alarm Indication Signal (LAIS) alarm with severity as MINOR and syslog is enabled. When the LAIS alarm is re-configured as suppressed with default severity, the alarm is not displayed under the **show alarm-profile name** command.

1. Create a chassis profile, for example, *chassis* and verify that the LAIS alarm is listed under the **show alarm-profile name chassis** command.
2. Set the alarm LAIS as suppressed.

The alarm LAIS is not displayed under the **show alarm-profile name chassis** command.

Create chassis profile

```
Router#configure terminal
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#end
Router#show alarm-profile name chassis
Alarm profile chassis:
  SONET/SDH:
  Alarm Name
          Severity   Syslog
  Section Loss of Signal Failure
          CRITICAL   Enabled
  Section Loss of Frame Failure
          CRITICAL   Enabled
  Section Out of Frame Alignment
          CRITICAL   Enabled
  Section J0 mismatch
          CRITICAL   Enabled
  Section Bit Interleaved Parity
          CRITICAL   Enabled
  Line Alarm Indication Signal
          MINOR      Enabled
  Line Remote Failure Indication
```

Set the alarm LAIS as suppressed

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#alarm sonet/sdh
Router(config-alarm-properties)#LAIS suppress
Router(config-alarm-properties)#end
```

Use the **show alarm-profile name *chassis*** command to display the configured alarm profile.

```
Router#show alarm-profile name chassis
Alarm profile chassis:
 DS1:
  Alarm Name
          Severity   Syslog
  Section Loss of Signal Failure
          CRITICAL   Enabled
  Section Loss of Frame Failure
          CRITICAL   Enabled
  Section Out of Frame Alignment
          CRITICAL   Enabled
  Section J0 mismatch
          CRITICAL   Enabled
  Section Bit Interleaved Parity
          CRITICAL   Enabled
  Line Remote Failure Indication
          MINOR      Enabled
```

Note The LAIS alarm is not displayed under the **show alarm-profile name chassis** command.

Use Case 2

In this use case, the default profile has the LAIS alarm with severity as MINOR and syslog enabled. When the alarm is re-configured as suppressed with severity set to INFO, the alarm is displayed under the **show alarm-profile name** command.:

Use the following steps to change the LAIS alarm severity:

1. Create a chassis profile, for example, *chassis*.
2. Set the alarm LAIS as suppressed and alarm LAIS severity to INFO.

The alarm LAIS is displayed under the **show alarm-profile name chassis** command.

Create chassis profile

```
Router#configure terminal
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#end
```

Set the alarm LAIS as suppressed and severity to INFO

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#alarm sonet/sdh
Router(config-alarm-properties)#LAIS suppress
Router(config-alarm-properties)#LAIS severity INFO
Router(config-alarm-properties)#end
```

```
Router#show alarm-profile name chassis
Alarm profile chassis:
  SONET/SDH:
Alarm Name                                    Severity     Syslog
Section Loss of Signal Failure                CRITICAL     Enabled
Section Loss of Frame Failure                 CRITICAL     Enabled
Section Out of Frame Alignment                CRITICAL     Enabled
Section J0 mismatch                           CRITICAL     Enabled
Section Bit Interleaved Parity                CRITICAL     Enabled
Line Alarm Indication Signal                INFO         Disabled
Line Remote Failure Indication                MINOR        Enabled
```

Note that the LAIS alarm is displayed under the **show alarm-profile name *chassis*** command.

Use Case 3

In this use case, the default profile has Section Loss of Signal (SLOS) and Path Alarm Indication Signal (PAIS) alarms with severity as CRITICAL. Using the chassis profile, severity of the PAIS alarm is set to INFO, which is then verified using the **show alarm-profile name** command. The show output displays the SLOS as CRITICAL and PAIS as INFO.

Use the following steps to change the PAIS alarm severity:

1. Create a chassis profile, for example, *chassis*.
2. Set the alarm PAIS severity to INFO.

Create a chassis profile

```
Router#configure terminal
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#end
```

Set the alarm PAIS severity to INFO

```
Router(config)#alarm-profile chassis chassis
Router(config-alarm-profile)#alarm sonet/sdh
Router(config-alarm-properties)#PAIS severity INFO
Router(config-alarm-properties)#end
```

```
Router#show alarm-profile name chassis
Alarm profile chassis:
  SONET/SDH:
Alarm Name                                    Severity     Syslog
Section Loss of Signal Failure               CRITICAL     Enabled
Section Loss of Frame Failure                   CRITICAL     Enabled
Section Out of Frame Alignment                  CRITICAL     Enabled
Section J0 mismatch                             CRITICAL     Enabled
Section Bit Interleaved Parity                  CRITICAL     Enabled
Line Alarm Indication Signal                    INFO         Disabled
Line Remote Failure Indication                  MINOR        Enabled
Path Alarm Indication Signal                 INFO         Enabled
```

Note that the PAIS alarm is displayed under the **show alarm-profile name *chassis*** command.

Use Case 4

In this use case, the default profile has SLOS and PAIS alarms with severity as CRITICAL. Using the card profile, set the PAIS alarm severity to MAJOR and verify the severity using the **show alarm-profile name** command. The show output displays the SLOS as MAJOR and PAIS as CRITICAL.

Use the following steps to change the PAIS alarm severity:

1. Create a card profile, for example, *card*.
2. Set the alarm SLOS severity to MAJOR.

Create a card profile and set the alarm SLOS severity to MAJOR

```
Router#configure terminal
Router(config)#alarm-profile card card
Router(config-alarm-profile)#alarm sonet/sdh
Router(config-alarm-properties)#SLOS severity MAJOR
Router(config-alarm-properties)#end
```

```
Router#show alarm-profile name card
Alarm profile card:
 SONET/SDH:
  Alarm Name                                       Severity   Syslog
  Section Loss of Signal Failure                  MAJOR      Enabled
  Section Loss of Frame Failure                      CRITICAL   Enabled
  Section Out of Frame Alignment                     CRITICAL   Enabled
  Section J0 mismatch                                CRITICAL   Enabled
  Section Bit Interleaved Parity                     CRITICAL   Enabled
  Line Alarm Indication Signal                       INFO       Disabled
  Path Alarm Indication Signal                    CRITICAL   Enabled
```

Note The new severity levels for SLOS are displayed under the **show alarm-profile name *card*** command.

Use Case 5

In this use case, the default profile has the DS1_LOS and DS1_PAIS alarms with severity as CRITICAL. Using the port profile, set the DS1_LOS alarm severity to MAJOR and DS1_AIS alarm severity to MINOR. Verify the new severity levels of the alarms by using the **show alarm-profile name** command.

Use the following steps to change the DS1_LOS and DS1_AIS alarm severities:

1. Create a port profile, for example, *port*.
2. Set the alarm severities DS1_LOS to MAJOR and DS1_AIS to MINOR.

Create a port profile and set the alarm severities of DS1_LOS to MAJOR and DS1_AIS to MINOR

```
Router#configure terminal
Router(config)#alarm-profile port port
Router(config-alarm-profile)#alarm sonet/sdh
Router(config-alarm-properties)#DS1_LOS severity MAJOR
Router(config-alarm-properties)#DS1_AIS severity MINOR
Router(config-alarm-properties)#end
```

```
Router#show alarm-profile name port
Alarm profile port:
SONET/DSH:
 Alarm Name Severity Syslog
DS1 Loss Of Signa MAJOR Enabled
Section Loss of Frame Failure CRITICAL Enabled
Line Alarm Indication Signal CRITICAL Disabled
Line Remote Failure Indication MINOR Enabled
DS1 Alarm Indication Signal MINOR Enabled
Path Remote Failure Indication
```

Note The new severity levels for DS1_LOS and DS1_AIS are displayed under the **show alarm-profile name *port*** command.

Auto In-Service States for Cards

The ASR 900 router supports a subset of the generic state requirements for Network Elements (NE) as defined in Telecordia GR-1093. GR-1093 defines the Service States of the NEs, such as Interface Modules, ports, and circuits.

The ASR 900 router supports Cisco's standard representation for interface modules, along with representing them in the states defined in the Telecordia GR-1093.

AINS is enabled by default for the Telcordia alarm profile. When Telcordia is enabled, AINS is enabled by default for the chassis, card and port alarm profiles. However, if any alarm profile is configured before enabling Telcordia, then AINS is not enabled on that particular entity, you have to enable AINS manually.

Restrictions for AINS

Service States

Service states of IMs include a Primary State (PST), a Primary State Qualifier (PSTQ), and one or more Secondary States (SST). The following table lists all the PSTs and PSTQs.

Table 7: Service State Primary States and Primary State Qualifiers

Primary State, Primary State Qualifier	Definition
IS-NR (In-Service and Normal)	The entity is fully operational and will perform as provisioned.
OOS-AU (Out-of-Service and Autonomous)	The entity is not operational because of an autonomous event.
OOS-AUMA (Out-of-Service and Autonomous Management)	The entity is not operational because of an autonomous event and has also been administratively removed from service.
OOS-MA (Out-of-Service and Management)	The entity has been administratively removed from service.

Note Autonomous event: Is trigerred by a faulty card, card physically not present, mismatched equipment, or a software download

Management: Are Administrative commands. For more information, see the *Administrative Commands* section.

Autonomous-Management event: Is a combination of autonomous and management event.

The following table defines the ANSI and ETSI SSTs.

Table 8: Secondary States

Secondary State	Definition	Supported in Cisco IOS XE Everest 16.5.1

AINS (Automatic In-Service)	The transition of the entity to the IS-NR service state is delayed. Transition to the IS-NR state depends on correction of conditions. Alarm reporting is suppressed, but traffic is carried. Raised fault conditions, whether or not their alarms are reported, can be retrieved through the Network Management Service, for example, the EPNM.	No
DSBLD (Disabled)	The entity was manually removed from service and does not provide its provisioned functions. All services are disrupted; unable to carry traffic.	No
FLT (Failed)	The entity has a raised alarm or condition; traffic is not carried, all services are disrupted. • In case of a permanent failure due to hardware/software, then the entity remains in this state. • In case of transient events, such as software crash of the module, the entity may intermittently attain this state.	Yes
MEA (Mismatched Equipment)	If the installed module/equipment is not the same as the module/equipment pre-provisioned on the bay, then the entity is said to be in mismatched state. It is traffic impacting.	Yes
MT (Maintenance)	The entity has been administratively removed from service for a maintenance activity but still performs its provisioned functions. Alarm reporting is suppressed, and traffic continues to be forwarded, as long as autonomous conditions such as FLT and MEA are not encountered.	Yes
SWDL (Software Download)	The equipment is involved in a software and database download. This SST applies only to equipment.	Yes

UEQ (Unequipped)	The equipment is not physically present (that is, an empty slot). This SST applies only to equipment.	Yes

Service State Transitions

This section describes the transition from one service state to the next state for cards. A service state transition is based on the action performed on the entity and port.

Equipment Service State Transitions

Table 9: Equipment Service State Transitions

Current Service State	Action	Next Service State
Empty	Assign the entity type to bay	• If entity is supported in the bay or has hardware resources to bring up the entity: OOS-AU,UEQ • If entity is not supported in the bay or does not have hardware resources to bring up the entity: Command has no effect or gets rejected.
	Insert card after assignment	• If the entity is not faulty, IS-NR • If entity is faulty hardware: OOS-AU,FLT • If entity inserted is different from the assigned card: OOS-AU,MEA
	Insert card without assignment	• If the entity is not faulty, IS-NR • If entity is faulty hardware: OOS-AU,FLT

IS-NR	Delete card assignment	• If bay is assigned an entity type: The entity type is removed, but card remains in IS-NR. • If mode gets changed, entity is reset and: OOS-AU,SWDL, if hardware resources available, or OOS-AU,FLT if hardware resources are unavailable.
	Administratively change the card state to OOS,MT	OOS-MA,MT
	Pull the card	• If bay is assigned an entity type: OOS-AU,UEQ • If bay is not assigned an entity type: Empty
	Reset the card	OOS-AU,SWDL
	Card is faulty	OOS-AU,FLT
OOS-AU,SWDL	Bootup activity completed	IS-NR
	Pull the card	• If bay is assigned an entity type: OOS-AU,UEQ • If bay is not assigned an entity type: Empty
	Delete card assignment	• If bay is assigned an entity type: The entity type is removed, but card remains in IS-NR. • If bay is not assigned an entity type: Command has no effect/gets rejected.
	Administratively change the card state to OOS,MT	OOS-AUMA,SWDL and MT

OOS-AU,UEQ	Delete card assignment	Empty
	Administratively change the card state to OOS,MT	OOS-AUMA,UEQ and MT
	Insert the card	• If the entity is not faulty, IS-NR • If the entity is faulty hardware: OOS-AU,FLT • If the entity inserted is different from the assigned card: OOS-AU,MEA
OOS-AU,MEA	Delete the card assignment.	• If the entity is supported on bay: OOS-AU,SWDL and eventually, IS-NR. • If entity is not supported on bay: OOS-AU,FLT
	Administratively change the card state to OOS,MT	OOS-AUMA,MEA and MT
	Pull the card.	OOS-AU,UEQ
OOS-AUMA,FLT	Administratively change the card state to OOS,MT	OOS-AUMA,FLT and MT
	Delete the card.	OOS-AU, FLT
OOS-MA,MT	Pull the card. Administratively remove the maintenance	IS-NR
	Pull the card	OOS-AUMA,UEQ and MT
	Reset the card	OOS-AU,SWDL and MT
	Card goes faulty	OOS-AU,FLT and MT

OOS-AUMA,MT & SWDL	Bootup activity complete	OOS-MA,MT
	Pull the card	OOS-AU,UEQ and MT
	Delete card assignment	• If bay is assigned an entity type: The entity type is removed, and card goes to OOS-AU,SWDL. • If mode gets changed, entity is reset and: OOS-AU,SWDL, if hardware resources available, or OOS-AU,FLT if hardware resources are unavailable.
	Administratively remove the maintenance	OOS-AU,SWDL
OOS-AU,MT & UEQ	Delete card assignment	Empty
	Administratively remove the maintenance	OOS-AUMA, UEQ
	Pull the card	OOS-AU,UEQ
OOS-AU, MEA & MT	Delete the card assignment	Empty
	Administratively remove the maintenance	OOS-AUMA,MEA
	Pull the card	• If bay is assigned an entity type: OOS-AU,SWDL and eventually, IS-NR. • If bay is not assigned an entity type: OOS-AU,FLT

OOS-AU,FLT & MT	Delete the card assignment.	OOS-AU,FLT
	Administratively remove the maintenance	OOS-AU,FLT
	Reset the card.	OOS-AU,FLT and MT
	Card faulty condition is cleared	IS-NR

Administrative States

Administrative states are used to manage service states. Administrative states consist of a PST and an SST. The following table lists the supported administrative states.

Table 10: Administrative States

Equipment Administrative State (PST,SST)	Definitions	Support for Equipment State Model
IS	Puts the entity administratively in service.	Yes (Default administrative state of equipment)
IS,AINS	Puts the entity administratively in automatic in-service.	No
OOS,DSBLD	Removes the entity from service and disables it.	No
OOS,MT	Entity removed administratively from service for maintenance purpose.	Yes
OOS,OOG	(VCAT circuits only) Removes a VCAT member cross-connect from the service and the group of members.	No

Configuration Commands

The following sections describe the commands to pre-provision and de-provision the card.

Enabling the AINS on Chassis

```
Router(config)#alarm-profile chassis_ains chassis
Router(config-alarm-profile)#ains
Router(config-alarm-profile)#exit
Router(config)#alarm-profile chassis_ains attach chassis
```

Disabling the AINS on Chassis

```
Router(config)#alarm-profile chassis_ains chassis
Router(config-alarm-profile)#no ains
```

Pre-Provisioning the Card

The **platform hw-module configuration** command is used to pre-provision a card type to a particular bay. This command ensures that the IM is supported in that particular bay and has the necessary hardware resources to bring up the module. Otherwise, the command is rejected. Pre-provisiong is also termed as card assignment in this document.

The IMs supported on the ASR 900 routers are:

Interface Module	Description
A900-IMA1Z8S-CX	1 port 10G/OC192/OTN2 + 8 port 1G/OC48/OTN1 IM
A900-IMA2F	2x40G IM
A900-IMA2Z	2x10G IM
A900-IMA48D-C	48 port T1E1 IM
A900-IMA48T-C	48 port T3E3 IM
A900-IMA8CS1Z-M	16x1G+1x10G SFP IM
A900-IMA8CT1Z-M	8x1G+1x10G Copper IM
A900-IMA8Z	8x10G IM
A900-IMA3G-IMSG	1-port OC481/ STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-Port T1/E1 + 4-Port T3/E3 CEM Interface Module
A900-IMA1C	1-port 100 Gigabit Ethernet Interface Module

To pre-provision the card:

```
Router> enable
Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf))# hw-module slot/bay IM_name
```

Verifying the Pre-Provisioning of the Card

To view the configuration of the IMs in the system, use the following command

```
Router# show pl hw-configuration

Slot      Cfg IM Type         Actual IM Type      Op State              Admin State
--------- ------------------- ------------------- -------------------   ------------------

 0/0      -                   -                   Empty                 N/A
 0/1      -                   -                   Empty                 N/A
 0/2      -                   A900-IMA2F          OOS-AU,FLT            IS
 0/3      A900-IMA48T-C       -                   OOS-AU,UEQ            IS
 0/4      -                   -                   Empty                 N/A
```

```
 0/5      -                    -                    Empty                N/A
 0/6      -                    -                    Empty                N/A
 0/7      -                    -                    Empty                N/A
 0/8      -                    -                    Empty                N/A
 0/9      -                    -                    Empty                N/A
 0/10     -                    -                    Empty                N/A
 0/11     -                    NCS4200-1T8S-10CS    IS-NR                IS
 0/12     -                    A900-IMA2Z           IS-NR                IS
 0/13     -                    -                    Empty                N/A
 0/14     -                    -                    Empty                N/A
 0/15     -                    NCS4200-48T1E1-CE    IS-NR                IS
```

After an IM is inserted in to the bay, if the IM type being configured through the command is different from the IM type present in the bay, then the command is rejected. For example:

```
Router(conf-plat-hw-conf)# hw-module 0/2 ?
  A900-IMA1Z8S-CX  1 port 10G/OC192/OTN2 + 8 port 1G/OC48/OTN1 IM
  A900-IMA48D-C    48 port T1E1 IM
  A900-IMA48T-C    48 port T3E3 IM
  A900-IMA8CS1Z-M  16x1G+1x10G SFP IM
Router(conf-plat-hw-conf)# hw-module 0/2 A900-IMA48D-C
CLI Rejected: Bay 2 has SPA (A900-IMA2F) already inserted; cannot assign SPA (A900-IMA48D-C)
Router(conf-plat-hw-conf)#
```

However, if the type of the IM inserted is same as the IM type being assigned, the command is accepted.

```
Router(conf-plat-hw-conf)# hw-module 0/12 ?
  A900-IMA1Z8S-CX  1 port 10G/OC192/OTN2 + 8 port 1G/OC48/OTN1 IM
  A900-IMA2F       2x40G IM
  A900-IMA2Z       2x10G IM
  A900-IMA48D-C    48 port T1E1 IM
  A900-IMA48T-C    48 port T3E3 IM
  A900-IMA8CS1Z-M  16x1G+1x10G SFP IM
  A900-IMA8CT1Z-M  8x1G+1x10G CU IM
  A900-IMA8Z       8x10G IM

Router(conf-plat-hw-conf)# hw-module 0/12 A900-IMA2Z
Router(conf-plat-hw-conf)#


Router# show platform hw-configuration

Slot      Cfg IM Type          Actual IM Type       Op State              Admin State
--------- -------------------- -------------------- --------------------  ------------------

 0/0      -                    -                    Empty                N/A
 0/1      -                    -                    Empty                N/A
 0/2      -                    A900-IMA2F           OOS-AU,FLT           IS
 0/3      A900-IMA48T-C        -                    OOS-AU,UEQ           IS
 0/4      -                    -                    Empty                N/A
 0/5      -                    -                    Empty                N/A
 0/6      -                    -                    Empty                N/A
 0/7      -                    -                    Empty                N/A
 0/8      -                    -                    Empty                N/A
 0/9      -                    -                    Empty                N/A
 0/10     -                    -                    Empty                N/A
 0/11     -                    NCS4200-1T8S-10CS    IS-NR                IS
 0/12     A900-IMA2Z           A900-IMA2Z           IS-NR                IS
 0/13     -                    -                    Empty                N/A
 0/14     -                    -                    Empty                N/A
 0/15     -                    NCS4200-48T1E1-CE    IS-NR                IS
```

You can use the **hw-module** *slot/bay IM_name* command along with the **mode** attribute. For example,

```
Router(conf-plat-hw-conf))# hw-module 0/12 NCS4200-1T8S-10CS mode 5G
```

While using the **mode** attribute, the following conditions apply:

- If an IM is already present in the bay, the IM is restarted to accommodate for the mode change.
- If there is no IM in the bay, hardware resources are checked, support for that mode on that particular bay is checked, and if there are no problems, the configuration is accepted.

De-Provisioning the Card

A slot may be de-provisioned while it is empty or populated with an IM using the no form of the **hw-module** command under the **platform hw-module configuration** command submode:

```
ROUTER# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ROUTER(config)# platform hw conf
ROUTER# show platform hw-conf

Slot      Cfg IM Type          Actual IM Type      Op State              Admin State
--------- -------------------- ------------------- --------------------  ------------------

 0/0      -                    -                   Empty                 N/A
 0/1      -                    -                   Empty                 N/A
 0/2      -                    A900-IMA2F          OOS-AU,FLT            IS
 0/3      A900-IMA48T-C        -                   OOS-AU,UEQ            IS
 0/4      -                    -                   Empty                 N/A
 0/5      -                    -                   Empty                 N/A
 0/6      -                    -                   Empty                 N/A
 0/7      -                    -                   Empty                 N/A
 0/8      -                    -                   Empty                 N/A
 0/9      -                    -                   Empty                 N/A
 0/10     -                    -                   Empty                 N/A
 0/11     -                    NCS4200-1T8S-10CS   IS-NR                 IS
 0/12     A900-IMA2Z           A900-IMA2Z          IS-NR                 IS
 0/13     -                    -                   Empty                 N/A
 0/14     -                    -                   Empty                 N/A
 0/15     -                    NCS4200-48T1E1-CE   IS-NR                 IS


ROUTER(conf-plat-hw-conf)# no hw-module 0/12 A900-IMA2Z
ROUTER# show platform hw-conf
Slot      Cfg IM Type          Actual IM Type      Op State              Admin State
--------- -------------------- ------------------- --------------------  ------------------

 0/0      -                    -                   Empty                 N/A
 0/1      -                    -                   Empty                 N/A
 0/2      -                    A900-IMA2F          OOS-AU,FLT            IS
 0/3      A900-IMA48T-C        -                   OOS-AU,UEQ            IS
 0/4      -                    -                   Empty                 N/A
 0/5      -                    -                   Empty                 N/A
 0/6      -                    -                   Empty                 N/A
 0/7      -                    -                   Empty                 N/A
 0/8      -                    -                   Empty                 N/A
 0/9      -                    -                   Empty                 N/A
 0/10     -                    -                   Empty                 N/A
 0/11     -                    NCS4200-1T8S-10CS   IS-NR                 IS
 0/12     -                    A900-IMA2Z          IS-NR                 IS
 0/13     -                    -                   Empty                 N/A
 0/14     -                    -                   Empty                 N/A
 0/15     -                    NCS4200-48T1E1-CE   IS-NR                 IS
```

Administrative Commands

The following sections describe the administrative commands used for the AINS feature.

Maintenance Commands (OOS,MT)

The maintenance commands are used to administratively put the IM in a bay in maintenance mode. These commands are accepted only if that bay has an IM type pre-provisioned, as described in the *Pre-Provisioning the Card* section.

```
Router# configure terminal
Router(config)# hw-module slot/subslot maintenance
Router(hw-config)# end
```

In-Service Commands (IS)

The in-service command is the **no** form of the maintenance command. The in-service command administratively puts the IM in a bay in in-service mode.

```
Router# configure terminal
Router(hw-config)# no hw-module slot/subslot maintenance
Router(config)# end
```



Note If the card assignment is removed on a bay with maintenance mode enabled, then the maintenance attribute is also cleared from that bay.

The following example explains how to put the IM in a bay in in-service mode:

```
ROUTER# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ROUTER(config)# platform hw-module configuration
ROUTER(conf-plat-hw-conf)# hw-module 0/12 A900-IMA2Z
ROUTER(conf-plat-hw-conf)# hw-module subslot 0/12 maintenance
ROUTER# show platform hw-conf

Slot      Cfg IM Type         Actual IM Type      Op State              Admin State
--------- ------------------- ------------------- --------------------  ------------------

 0/0      -                   -                   Empty                 N/A
 0/1      -                   -                   Empty                 N/A
 0/2      -                   A900-IMA2F          OOS-AU,FLT            IS
 0/3      A900-IMA48T-C       -                   OOS-AU,UEQ            IS
 0/4      -                   -                   Empty                 N/A
 0/5      -                   -                   Empty                 N/A
 0/6      -                   -                   Empty                 N/A
 0/7      -                   -                   Empty                 N/A
 0/8      -                   -                   Empty                 N/A
 0/9      -                   -                   Empty                 N/A
 0/10     -                   -                   Empty                 N/A
 0/11     -                   NCS4200-1T8S-10CS   IS-NR                 IS
 0/12     A900-IMA2Z          A900-IMA2Z          OOS-MA,MT             OOS,MT
 0/13     -                   -                   Empty                 N/A
 0/14     -                   -                   Empty                 N/A
 0/15     -                   NCS4200-48T1E1-CE   IS-NR                 IS

ROUTER(config)# platform hw configuration
ROUTER(conf-plat-hw-conf)# no hw-module 0/12 A900-IMA2Z
```

```
Maintenance mode flag set for this bay will be cleared if you proceed. Continue? [yes/no]:
 yes
ROUTER# show platform hw-conf

Slot      Cfg IM Type          Actual IM Type      Op State              Admin State
--------- -------------------- ------------------- --------------------  -------------------

 0/0      -                    -                   Empty                 N/A
 0/1      -                    -                   Empty                 N/A
 0/2      -                    A900-IMA2F          OOS-AU,FLT            IS
 0/3      A900-IMA48T-C        -                   OOS-AU,UEQ            IS
 0/4      -                    -                   Empty                 N/A
 0/5      -                    -                   Empty                 N/A
 0/6      -                    -                   Empty                 N/A
 0/7      -                    -                   Empty                 N/A
 0/8      -                    -                   Empty                 N/A
 0/9      -                    -                   Empty                 N/A
 0/10     -                    -                   Empty                 N/A
 0/11     -                    NCS4200-1T8S-10CS   IS-NR                 IS
 0/12     -                    A900-IMA2Z          IS-NR                 IS
 0/13     -                    -                   Empty                 N/A
 0/14     -                    -                   Empty                 N/A
 0/15     -                    NCS4200-48T1E1-CE   IS-NR                 IS
```

Information Display Commands

The following show command is used to display the configured IM type information, physical IM type, as well as the Service State (Op State) and Admin State (Admin State) for the various modules:

```
Router# show platform hw-configuration

Slot   Cfg IM Type          Actual IM Type      Op State            Ad State IM Op Mode
BW
------ -------------------- ------------------- ------------------ -------- ------------
--
 0/0   -                    -                   Empty               N/A      -

 0/1   -                    A900-IMA8T          IS-NR               IS       -

 0/2   -                    -                   Empty               N/A      -

 0/3   -                    NCS4200-1T8S-10CS   IS-NR               IS       10G_CEM

 0/4   -                    -                   Empty               N/A      -

 0/5   -                    -                   Empty               N/A      -

 0/6   -                    -                   Empty               N/A      -

 0/7   -                    -                   Empty               N/A      -

 0/8   NCS4200-48T1E1-CE   NCS4200-48T1E1-CE   IS-NR               IS       -

 0/9   -                    A900-IMA4OS         OOS-AU,FLT          IS       -

 0/10  -                    NCS4200-48T3E3-CE   IS-NR               IS       -

 0/11  -                    -                   Empty               N/A      -

 0/12  -                    A900-IMA2Z          IS-NR               IS       -
```

```
0/13  -                   -                   Empty               N/A       -
0/14  -                   -                   Empty               N/A       -
0/15  -                   -                   Empty               N/A       -
```

Auto In-Service State for Ports

Effective Cisco IOS XE Everest 16.6.1, the Cisco ASR 900 Series routers with RSP3 module support management of equipment and port state model in two modes—the transport mode and router mode.

By default, the network equipment (NE) supports:

Note Network Equipment includes only Interface Modules (IM) and state models that are not applicable for RSP and fan modules.

- Both modes of management from the north-bound interface
- All existing router mode features and a subset of transport mode features according to the ITU-T X.731.GR1093

Note To get support for all transport mode features, you must manually configure all transport mode features.

- Complete set of port transport mode features such as, AINS soak timer on every bay
- Configuration of the new alarm profile command for required slots
- The default time limit is 15 minutes.
- The maximum time limit for the soak timer is 48 hours.The minimum time limit is 15 minutes.

Note You can configure the minimum time limit in multiples of 15, that is, 15, 30, 45 minutes and so on.

Restrictions for AINS for TDM Ports

- There is a 10% deviation on soak running time. For example, if the default timer is for 15 minutes, the soak timer runs for 16.5 minutes.
- You cannot shut down the port if the port is in Maintenance and auto-in-service state.
- A port can be put in loopback state only when the secondary admin state is "maintenance".

Service States

Service states of IMs include a Primary State (PST), a Primary State Qualifier (PSTQ), and one or more Secondary States (SST). The following table lists all the PSTs and PSTQs.

Table 11: Service State Primary States and Primary State Qualifiers

Primary State, Primary State Qualifier	Definition
IS-NR (In-Service and Normal)	The entity is fully operational and performs as provisioned.
OOS-AU (Out-of-Service and Autonomous)	The port is not operational because of an autonomous event.
OOS-AUMA (Out-of-Service and Autonomous Management)	The port is not operational because of an autonomous event and has also been administratively removed from service.
OOS-MA (Out-of-Service and Management)	The port has been manually removed from service.

Note Autonomous events: Is triggered by a faulty port, port not connected, port physically not present, mismatched equipment, or a software download

Management: Are Administrative commands. For more information, see the *Administrative Commands* section.

Autonomous-Management events: Is a combination of autonomous and management events.

The following table defines the ANSI and ETSI SSTs.

Table 12: Secondary States

Secondary State	Definition
AINS (Automatic In-Service)	The transition of the entity to the IS-NR service state is delayed. Transition to the IS-NR state depends on correction of conditions, or on a soak timer. Alarm reporting is suppressed, but traffic is carried. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.
DSBLD (Disabled)	The port was manually removed from service and does not provide its provisioned functions. All services are disrupted; the port is unable to carry traffic.
FLT (Fault)	The port has a raised alarm or condition.
LPBK (Loopback)	The port is in loopback mode.
MEA (Mismatched Equipment)	Not applicable.

MT (Maintenance)	The port has been manually removed from service for a maintenance activity but still performs its provisioned functions. Alarm reporting is suppressed, but traffic is carried. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.
SWDL (Software Download)	Not applicable.
UAS (Unassigned)	Not applicable.
UEQ (Unequipped)	Not applicable.

Service State Transitions

This section describes the transition from one service state to the next state for cards. A service state transition is based on the action performed on the entity and port.

Port Service State Transitions

Table 13: Port Service State Transitions

Current Service State	Action	Next Service State
IS-NR	Put the port or cross-connect in the OOS,MT administrative state.	OOS-MA,MT
	Put the port or cross-connect in the OOS, DSBLD administrative state.	OOS-MA,DSBLD
	Put the port or cross-connect in the IS, AINS administrative state	OOS-AU,AINS
	Alarm/condition is raised.	OOS-AU,FLT
OOS-AU,AINS	Put the port or cross-connect in the IS administrative state.	IS-NR
	Put the port or cross-connect in the OOS,MT administrative	OOS-MA,MT
	Alarm/condition is raised.	OOS-AU,AINS & FLT

OOS-AU,AINS & FLT	Alarm/condition is cleared.	OOS-AU,AINS
	Put the port or cross-connect in the IS administrative state.	OOS-AU, FLT Admin command request is to move the port state from AINS to IS. FLT is secondary state and admin commands doesn't have restriction. Admin commands are accepted and moved to appropriate state based on new state rules. On admin command to IS, systems stop soaking timer, check for defects. If port has some defects, port is put in OOS-AU, FLT. If port does not have any defects, it transitions to IS-NR (as per IS-NR state rules), On admin command to IS, systems stop soaking timer, check for defects. If port has defects, port is put in OOS-AU, FLT. If port does not have any defects, it transitions to IS-NR (as per IS-NR state rules)
	Put the port or cross-connect in the OOS,MT administrative state	OOS-AUMA,FLT & MT
OOS-AU,FLT	Alarm/condition is cleared.	IS-NR
	Put the port or cross-connect in the AINS administrative state.	OOS-AU,AINS & FLT
	Put the port or cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD
	Put the port or cross-connect in the OOS,MT administrative state	OOS-AUMA,FLT & MT

OOS-AUMA,FLT & LPBK & MT	Release the loopback	OOS-AUMA,FLT & MT
	Alarm/condition is cleared.	OOS-MA,LPBK & MT Acoording to the standard, LPBKis allowed only when port is in MT. LPBK is an admin command, while port is in MT state. FLT is another secondary state, independent of MT state. If port has defects, it displays FLT.
OOS-AUMA,FLT & MT	Alarm/condition is cleared.	OOS-MA,MT
	Put the port or cross-connect in the IS administrative state.	OOS-AU, FLT
	Put the port or cross-connect in the AINS administrative state.	OOS-AU,AINS & FLT
	Put the port or cross-connect in a loopback	OOS-AUMA,FLT & LPBK & MT
OOS-MA,DSBLD	Put the port or cross-connect in the IS administrative state.	IS-NR
	Put the port or cross-connect in the IS,AINS administrative state	OOS-AU,AINS
OOS-MA,LPBK & MT	Release the loopback	OOS-MA,MT
	Alarm/condition is raised.	OOS-AUMA,FLT & LPBK & MT
OOS-MA,MT	Put the port or cross-connect in the IS administrative state.	IS-NR
	Put the port or cross-connect in the IS,AINS administrative state	OOS-AU,AINS
	Put the port or cross-connect in loopback.	OOS-MA,LPBK & MT
	Alarm/condition is raised.	OOS-AUMA,FLT & MT

Administrative States

Administrative states are used to manage service states. Administrative states consist of a PST and an SST. The following table lists the supported administrative states.

Table 14: Administrative States

Equipment Administrative State (PST,SST)	Definitions	Support for Equipment State Model	Support for Port State Model
IS	Puts the entity in service.	Yes (Default administrative state of equipment)	Yes
IS,AINS	Puts the entity in automatic in-service.	Support only with Pre-provision.	Yes
OOS,DSBLD	Removes the entity from service and disables it.	Not Applicable	Yes
OOS,MT	Removes the entity removed from service for maintenance purpose.	Yes	Yes
OOS,OOG	(VCAT circuits only) Removes a VCAT member cross-connect from the service and from the group of members.	Not Applicable	Not Applicable

Configuration Commands

The following sections describe the commands to pre-provision and de-provision the ports.

Note a. The AINS state on a port is controlled by AINS flag in the attached profile to a port

Verifying Controller and Interface AINS Port Configuration

```
Router#show controllers t1 0/4/0
T1 0/4/0 is down
Alarm-profile: A900-IMA3G-IMSG
Sec-admin-state: auto-in-service, Soak-time: 15(min),
soak-Time-left: 15(min) (pending), AINS-state: OOS-AU,AINS & FLT
  Applique type is A900-IMA3G-IMSG
  Receiver has loss of signal.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  BER thresholds:  SF = 10e-3  SD = 10e-6
  Data in current interval (200 seconds elapsed):
   Near End
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 200 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 203 Unavail Secs
     2 Path Failures, 0 SEF/AIS Secs
```

```
   Far End
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 2 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     2 Errored Secs, 0 Bursty Err Secs, 2 Severely Err Secs, 0 Unavail Secs
     0 Path Failures
```

```
Router# show interfaces GigabitEthernet 0/1/0

GigabitEthernet0/1/0 is up, line protocol is up
Sec-admin-state: in-service, Soak-time: NA,
soak-Time-left: NA, AINS-state: IS-NR
  Hardware is A900-IMA8S1Z, address is f078.1685.3f12 (bia f078.1685.3f12)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is SX
  output flow-control is unsupported, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:00:37
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

```
Router# show facility-ains status
Slot   Cfg IM Type         Actual IM Type      Op State           Ad State IM Op Mode
------ ------------------- ------------------- ------------------ -------- ------------
 0/0   -                   -                   Empty              N/A      -
 0/1   -                   -                   Empty              N/A      -
 0/2   -                   NCS4200-48T1E1-CE   N/A                N/A      -
 0/3   -                   A900-IMA8S1Z        IS-NR              IS       -
 0/4   -                   NCS4200-3GMS        IS-NR              IS       -
 0/5   -                   -                   Empty              N/A      -

IFNAME                        Op State                Ad State            Alarm
------                        --------                --------            -----
T1 0/4/0                      OOS-AU,AINS             auto-in-service     -
T1 0/4/1                      OOS-AU,AINS             auto-in-service     -
GigabitEthernet0/3/0          IS-NR                   in-service          -
GigabitEthernet0/3/1          IS-NR                   in-service          -
GigabitEthernet0/3/2          IS-NR                   in-service          -
GigabitEthernet0/3/3          IS-NR                   in-service          -
GigabitEthernet0/3/4          IS-NR                   in-service          -
GigabitEthernet0/3/5          IS-NR                   in-service          -
GigabitEthernet0/3/6          IS-NR                   in-service          -
GigabitEthernet0/3/7          IS-NR                   in-service          -
TenGigabitEthernet0/3/8       OOS-AU,FLT              in-service          -
```

```
Router# show facility-ains status
Slot   Cfg IM Type         Actual IM Type      Op State           Ad State IM Op Mode
------ ------------------- ------------------- ------------------ -------- ------------
```

```
 0/0   -                   -                   Empty             N/A      -
 0/1   -                   -                   Empty             N/A      -
 0/2   -                   NCS4200-48T1E1-CE   N/A               N/A      -
 0/3   -                   A900-IMA8S1Z        IS-NR             IS       -
 0/4   -                   NCS4200-3GMS        IS-NR             IS       -
 0/5   -                   -                   Empty             N/A      -

Router#show pl hw-configuration
Slot   Cfg IM Type         Actual IM Type      Op State          Ad State IM Op Mode
------ ------------------- ------------------- ----------------- -------- ------------
 0/0   -                   -                   Empty             N/A      -
 0/1   -                   -                   Empty             N/A      -
 0/2   -                   NCS4200-48T1E1-CE   N/A               N/A      -
 0/3   -                   A900-IMA8S1Z        IS-NR             IS       -
 0/4   -                   NCS4200-3GMS        IS-NR             IS       -
 0/5   -                   -                   Empty             N/A      -
```

Configuring Secondary Admin State

The secondary admin states are:

- auto-in-service
- in-service
- maintenance

Configuring the Auto-in-service Secondary Admin State

```
Router> enable
Router# configure terminal
Router(config)# controller sonet 0/2/0
Router(config-controller)# secondary-admin-state ?
auto-in-service Configure the port as auto-in-service
in-service      Configure the port as in-service
maintenance     Configure the port as maintenance

Router(config-controller)# secondary-admin-state auto-in-service hours 1 minutes 45
```

Configuring the In-service Secondary Admin State

```
Router> enable
Router# configure terminal
Router(config)# controller sonet 0/2/0
Router(config-controller)# secondary-admin-state ?
auto-in-service Configure the port as auto-in-service
in-service      Configure the port as in-service
maintenance     Configure the port as maintenance

Router(config-controller)# secondary-admin-state in-service
```

Configuring the Maintenance Secondary Admin State

```
Router> enable
Router# configure terminal
Router(config)# controller sonet 0/2/0
Router(config-controller)# secondary-admin-state ?
auto-in-service Configure the port as auto-in-service
in-service      Configure the port as in-service
maintenance     Configure the port as maintenance

Router(config-controller)# secondary-admin-state maintenance
```

Verifying Secondary Admin State

Verifying Auto-in-service

```
Router# show controller SONET 0/2/0

SONET 0/2/0 is up.
Sec-admin-state: auto-in-service, Soak-time: 15(min),
soak-Time-left: 16(min) (running), AINS-state: OOS-AU,AINS
Hardware is NCS4200-1T8S-10CS

Port configured rate: OC3
Applique type is Channelized Sonet
Clock Source is Internal
Medium info:
Type: Sonet, Line Coding: NRZ,
Alarm Throttling: OFF
```

Verifying In-service

```
Router# show controller SONET 0/2/0

SONET 0/2/0 is up.
Sec-admin-state: in-service, Soak-time: NA,
soak-Time-left: NA, AINS-state: IS-NR
Hardware is NCS4200-1T8S-10CS

Port configured rate: OC3
Applique type is Channelized Sonet
Clock Source is Internal
Medium info:
Type: Sonet, Line Coding: NRZ,
Alarm Throttling: OFF
```

Verifying Maintenance

```
Router# show controller SONET 0/2/0

SONET 0/2/0 is up.
Sec-admin-state: maintenance, Soak-time: NA,
soak-Time-left: NA, AINS-state: OOS-MA,MT
  Hardware is NCS4200-1T8S-10CS

 Port configure rate: OC3
 Applique type is Channelized Sonet
 Clock Source is Internal
Medium Info:
 Type: Sonet, Line Coding: NRZ,
Alarm Throttling: OFF
```

Syslog

After the AINS port soak completion, use the following command to view the syslog:

```
Router# show logging | Include AINS

 May 18 19:57:12.455 IST: %AINS_SUBSYS-6-AINS_TIMEOUT: Soak timer run on SONET 0/2/3 has
complete
```

Auto In-Service State for Transceiver

The transceiver module is a logical entity that represents a Transceiver equipment. The module can be created using a CLI command or created automatically when the Transceiver (pluggable) is inserted into a port. The Transceiver hardware details are auto-discovered after inserting the pluggable transceiver module successfully into the port, and these details could not be modified. The port rate is accessed from the controller for TDM ports and interface type for ethernet ports. You can perform the rate configuration manually and if the configured rate mismatches with the transceiver, then the pluggable module moves to the Out of Service state.

The transceiver connected to port supports the AINS functionality. For example, if an alarm is raised during the AINS state, then the alarm is not reported, and the syslog is not generated. You need to enable AINS under the alarms profile and the profile should be attached to the corresponding port.

You can remove the transceiver configuration manually from the port; however, the port rate configuration is not removed. The port rate configuration needs to be removed separately.

Transceiver Service State Transitions

Table 15: Transceiver Service State Transitions

Current Service State	Action	Next Service State
IS-NR	Reset the pluggable equipment.	IS-NR
IS-NR	When the PID is modified through configuration and the configuration is not matching with the pluggable equipment. Insert the matching or supported pluggable equipment or configure the correct PID of the pluggable equipment.	OOS-AU, MEA
OOS-AU, MEA	Insert a matching pluggable equipment or configure the correct PID of the pluggable equipment.	IS-NR
OOS-AU, UEQ	Insert the supported pluggable equipment.	IS-NR
OOS-AUMA, UAS	Provision the supported pluggable equipment.	IS-NR
OOS-AU, UAS, UEQ	Insert the supported pluggable equipment or configure the transceiver and then insert the configured PID transceiver.	IS-NR

Transceiver Alarms

The following table describes alarms generated for transceiver and how to clear the alarms.

Table 16: Transceiver Alarms

Alarm	When does the Alarm Trigger?	How to Clear the Alarm?
Transceiver missing	When the transceiver is configured with the pluggable equipment not present, for example, SFP or SFPP is not available.	Insert the configured transceiver or delete the configuration.
Transceiver Improper Removal	The transceiver is removed while the router is operational.	Reinsert the transceiver.
Transceiver Mismatch	When the configured PID is not matching with the transceiver equipment present.	Reconfigure the PID value using the **hw-module <slot>/<bay> transceiver <port> pid <PID>** command.

How to Configure Transceiver

How to Configure Transceiver

Modifying PID for Transceiver

If you know the PID value of the transceiver, you can modify the PID value.

To modify PID for transceiver, enter the following commands:

```
router(config)#platform hw-module configuration
router(conf-plat-hw-conf)#hw-module <slot>/<bay> transceiver <port> pid <PID>
```

The following example shows how to modify PID for transceiver:

```
AP2(config)#platform hw-module configuration
AP2(conf-plat-hw-conf)#hw-module 0/11 transceiver 18 pid ONS-SI-155-L1
AP2(conf-plat-hw-conf)#end
```

Transceiver Service State Transitions

Table 17: Transceiver Service State Transitions

Current Service State	Action	Next Service State
IS-NR	Reset the pluggable equipment.	IS-NR

Current Service State	Action	Next Service State
IS-NR	When the PID is modified through configuration and the configuration is not matching with the pluggable equipment. Insert the matching or supported pluggable equipment or configure the correct PID of the pluggable equipment.	OOS-AU, MEA
OOS-AU, MEA	Insert a matching pluggable equipment or configure the correct PID of the pluggable equipment.	IS-NR
OOS-AU, UEQ	Insert the supported pluggable equipment.	IS-NR
OOS-AUMA, UAS	Provision the supported pluggable equipment.	IS-NR
OOS-AU, UAS, UEQ	Insert the supported pluggable equipment or configure the transceiver and then insert the configured PID transceiver.	IS-NR

Removing Transceiver Configuration

To remove the transceiver configuration, use the **no** form of the command:

```
router(config)#platform hw-module configuration
router(conf-plat-hw-conf)#no hw-module <slot>/<bay> transceiver <port> pid <PID>
```

The following example shows how to remove configuration from transceiver:

```
AP2(config)#platform hw-module configuration
AP2(conf-plat-hw-conf)#no hw-module 0/11 transceiver 18 pid TESTPID
AP2(conf-plat-hw-conf)#end
```

Verifying Transceiver Configuration

Use the following commands to verify the transceiver configuration:

- **show facility-ains transceiver**—Displays the transceiver status.

To display the transceiver status, use the **show facility-ains transceiver** command:

```
router#show facility-ains transceiver
 Transceiver   Prov Type  Prov PID          Inserted PID      XCVR State  Op State
   Ad State
 -----------  ---------   --------          ------------      ----------  --------
   --------
 0/11/16      Configured  SFP-OC3-MM        SFP-OC3-MM         Enabled     IS-NR
```

```
   in-service
0/11/17      None                                              Not Present OOS-AU,UAS,UEQ
   auto-in-service
0/11/18      Configured  ONS-SI-155-L1      ONS-SI-155-L1      Enabled     IS-NR
   in-service
0/11/19      Configured  ONS-SI-622-SR-MM   ONS-SI-622-SR-M    Enabled     IS-NR
   in-service
0/14/16      Configured  SFP-OC48-SR        SFP-OC48-SR        Enabled     IS-NR
   in-service
0/14/17      None                                              Removed     OOS-AU,UAS,UEQ
   auto-in-service
0/14/18      None                                              Removed     OOS-AU,UAS,UEQ
   auto-in-service
0/14/19      None                                              Removed     OOS-AU,UAS,UEQ
   auto-in-service
0/4/0        None                                              Not Present OOS-AU,UAS,UEQ
   auto-in-service
0/4/2        None                                              Not Present OOS-AU,UAS,UEQ
   auto-in-service
0/4/4        None                                              Not Present OOS-AU,UAS,UEQ
   auto-in-service
0/4/6        None                                              Not Present OOS-AU,UAS,UEQ
   auto-in-service
0/4/8        Configured  TESTPIDRECONFIGURE                    Not Present OOS-AU,UEQ,AINS
  auto-in-service
0/4/10       None                                              Not Present OOS-AU,UAS,UEQ
   auto-in-service
0/4/12       None                                              Not Present OOS-AU,UAS,UEQ
   auto-in-service
0/4/14       None                                              Not Present OOS-AU,UAS,UEQ
   auto-in-service
0/4/16       None                                              Not Present OOS-AU,UAS,UEQ
   auto-in-service
0/8/0        Configured  QSFP-40G-SR4                          Not Present OOS-AUMA,UEQ
   in-service
0/8/1        Configured  QSFP-40G-LR4          QSFP-40G-LR4    Enabled     IS-NR
   in-service
```